BRANDEFENSE COUNTRY REPORT · ITALY 2026

# Brandefense Italia: panorama delle minacce informatiche 2026

Continuità dei servizi, mercati delle identità e riscontri sulle rivendicazioni

Odin by Brandefense
Periodo di ricerca: 22 novembre 2026
Versione 1.0 · Edizione pubblica di ricerca · TLP:CLEAR · Revisione: 23 novembre 2026

**132 su 250**
voci candidate del portafoglio associate a offerte di credenziali al momento della verifica

**802 371**
pubblicazioni con etichetta Italia conteggiate per data di pubblicazione, non attacchi

**286**
registrazioni di rivendicazioni ransomware associate all'Italia nel periodo del rapporto

**20**
azioni con responsabili e prove di completamento

INDICE

# Indice

**Translated with AI**

Questa edizione è stata tradotta con l'IA dal testo originale inglese. In caso di differenze, prevale l'edizione inglese.


| | | |
|---|---|---|
| 01 | Sintesi | 05 |
| | Mappa del rapporto | 09 |
| 02 | Contesto digitale e operativo dell'Italia | 10 |
| 03 | Esposizione nazionale: voci candidate del portafoglio | 14 |
| 04 | Cosa osserviamo sul dark web | 20 |
| 05 | Esempi di bersagli e casi per settore | 36 |
| 06 | Hacktivismo, DDoS e attività recente | 50 |
| 07 | Attori delle minacce ed evidenze dei collegamenti | 58 |
| 08 | L'economia delle frodi | 70 |
| 09 | Approfondimento su banche e finanza | 75 |
| 10 | Normativa e risposta nazionale | 79 |
| 11 | Prospettive | 84 |
| 12 | Piano d'azione | 88 |
| A | Appendice A. Fonti, ambito e confidenza | 96 |
| B | Appendice B. Registro delle evidenze | 99 |
| C | Appendice C. Fonti | 102 |
| D | Appendice D. Glossario | 106 |
| | Informazioni sul rapporto | 108 |

| | |
|---|---|
| Consiglio e dirigenti | 01 05 11 12 |
| CISO e responsabili della sicurezza | 03 04 05 10 12 |
| SOC e analisti | 04 06 07 B |
| Antifrode e tutela dei clienti | 08 09 12 |
| Legale e comunicazione | 05 06 10 12 |

# Informazioni sull'edizione

Tradotto con l'IA. In caso di differenze, prevale l'edizione inglese.

Preparato da Odin by Brandefense con l'assistenza dell'IA. Le osservazioni arrivano alla rilevazione del 22 novembre, anziché alla fine della giornata.

Le evidenze sull'Italia richiedono risposte distinte alle interruzioni dei servizi, alle offerte di dati identificativi e alle rivendicazioni prive di riscontri indipendenti.

**802 371**

pubblicazioni con etichetta Italia conteggiate, non attacchi

**132 su 250**

voci candidate del portafoglio associate a offerte di credenziali al momento della verifica

**57/100**

valore nazionale Atlas per il portafoglio selezionato

**286**

registrazioni di rivendicazioni ransomware associate all'Italia, non intrusioni confermate

# Indice e percorsi di lettura

| Capitolo | Domanda | Lettore principale |
|---|---|---|
| 1 Sintesi | Cosa devono decidere prima i responsabili? | Consiglio e CISO |
| 2 Contesto | Quali caratteristiche dei servizi italiani incidono sul rischio? | CISO e continuità |
| 3 Esposizione nazionale | Cosa dimostra l'insieme selezionato? | Identità e infrastrutture |
| 4 Dark web | Cosa è stato effettivamente pubblicizzato sull'Italia? | Analisi delle minacce |
| 5 Casi per settore | Cosa è successo e cosa deve cambiare? | Responsabili dei servizi |
| 6 Hacktivismo e DDoS | Cosa hanno dichiarato gli autori e confermato le autorità? | SOC e comunicazione |
| 7 Attori delle minacce | Quali collegamenti hanno riscontri? | Analisi delle minacce |
| 8 Economia delle frodi | Come diventano bersagli i processi di identità e pagamento? | Antifrode e finanza |
| 9 Banche | Quali rischi per clienti e dipendenti richiedono responsabili distinti? | Banche e tesoreria |
| 10 Normativa | Quali obblighi si applicano a ciascun soggetto? | Legale e risposta |
| 11 Prospettive | Quali segnali devono cambiare il piano? | Direzione della sicurezza |
| 12 Piano d'azione | Chi fa cosa e come si dimostra il completamento? | Tutte le funzioni |

Leggete i capitoli 1, 5 e 12 per le decisioni della direzione. I capitoli 3, 4, 6 e 7 presentano le evidenze operative. I capitoli 8-10 trattano frodi, banche e obblighi di segnalazione. L'appendice A spiega popolazioni e limiti; l'appendice B collega i riferimenti stabili delle evidenze al testo.

**Osservazione** indica una pubblicazione conservata, un controllo pubblico misurato o una dichiarazione pubblicata da una fonte. **Rivendicazione** indica un'affermazione di un attore o venditore. **Valutazione** indica la nostra interpretazione, con un'alternativa e le evidenze necessarie a modificarla. Queste etichette si applicano alle singole affermazioni, anche all'interno dello stesso incidente.

CAPITOLO 01

# Sintesi

01

QUESTO CAPITOLO RISPONDE

Cosa dimostrano le evidenze sull'Italia e quali decisioni devono prendere prima i responsabili?

**4**

decisioni che collegano continuità, identità, pagamenti e segnalazione degli incidenti


Quattro decisioni per i responsabili 07

L'anno in cifre 07

CAPITOLO 01

# Sintesi

IN SINTESI

Le evidenze sull'Italia comprendono disservizi confermati, accessi a dati identificativi e rivendicazioni criminali con riscontri diversi. Un'università ha documentato il ripristino dopo un ransomware. Una recente comunicazione commerciale ha confermato accessi ai recapiti, senza dimostrare il furto di dati di pagamento. Il resoconto ufficiale del periodo olimpico distingue i tentativi DDoS dagli effetti sui servizi. Tenete separate queste popolazioni. Verificate i segnali sulle identità, provate il ripristino dipendente dai fornitori, confermate i cambiamenti nei pagamenti e simulate la decisione di notifica.

**1. Volume delle pubblicazioni e incidenti rispondono a domande diverse.** La fonte conta 802 371 pubblicazioni con etichetta Italia. Gennaio e febbraio contengono il 91,9% del totale. Un corpus conservato separatamente contiene 16 613 pubblicazioni distinte, comprese 839 pubblicazioni di forum con etichetta Italia. Il corpus conservato è parziale e non casuale. Queste popolazioni non dimostrano il volume nazionale degli attacchi né la prevalenza delle famiglie criminali. [S1]

**2. Le pubblicazioni estorsive sono diffuse, ma le singole affermazioni restano non verificate.** Ransompedia registra 286 voci associate all'Italia, con 59 valori distinti nei nomi dei gruppi. Qilin, The Gentlemen e Lockbit5 rappresentano 95 voci, pari al 33,2%. Una voce è una rivendicazione. Registrazioni diverse possono nominare la stessa organizzazione, mentre i casi non pubblicati restano assenti. [S2]

**3. Le interruzioni confermate rendono il ripristino una decisione sul servizio.** L'avviso ransomware della Sapienza documenta sistemi interessati e ripristino, mantenendo i limiti sulle esposizioni informative ancora irrisolte. Altri casi sostenuti dalle fonti descrivono interruzioni presso fornitori e strutture sanitarie. Un server ripristinato non dimostra che un processo aziendale o clinico sia pronto. Provate il servizio effettivo. [S5][S25][S27]

**4. L'accesso recente ai recapiti richiede indicazioni precise ai clienti.** Unicoop Firenze ha confermato accessi ad alcuni recapiti, dichiarando che i servizi continuavano. Le sue informazioni sulla sicurezza escludono il coinvolgimento di dati delle carte e password. La risposta deve affrontare impersonificazioni credibili, senza trasformare l'accesso ai recapiti in un'affermazione di accesso ai conti bancari. [S7][S8]

**5. Le offerte attuali di credenziali richiedono verifiche nel portafoglio selezionato.** Alla verifica, le offerte di credenziali erano associate a 132 voci candidate nel portafoglio di 250 voci. Il valore nazionale Atlas è 57 su 100. Almeno 759 724 associazioni di dispositivi e 113 259 485 credenziali storiche si sovrappongono. Non dimostrano utenti unici o intrusioni confermate. Le misure dei controlli passivi restano non disponibili. [S3]

## Quattro decisioni per i responsabili

1. **Provare il servizio insieme ai suoi fornitori.** Richiedete una prova di ripristino per un servizio importante e per le sue dipendenze di identità, hosting e comunicazione. Il completamento deve dimostrare l'utilizzabilità aziendale. I casi universitari, cloud e sanitari spiegano perché il ripristino del servizio richiede evidenze proprie (§5).
2. **Includere sessioni e recupero nella risposta sulle identità.** Inviate al team identità le evidenze su credenziali e sessioni specifiche dell'organizzazione. Verificate appartenenza, validità attuale, protezione e precedenti interventi prima di agire con effetti sui servizi. Revocate le sessioni coinvolte quando i riscontri lo giustificano. Verificate che il recupero non possa ricreare l'accesso (§§3-4 e 12).
3. **Verificare l'autorità di pagamento fuori dal canale della richiesta.** Un mittente plausibile, un documento noto, una conversazione reale o una voce convincente non dimostrano l'autorizzazione. Confermate nuovi beneficiari e istruzioni modificate tramite recapiti conosciuti indipendentemente. Provate il processo con una richiesta urgente e riservata attribuita a un dirigente (§§8-9).
4. **Preparare i registri per notifiche e comunicazioni.** Il legale deve disporre di una matrice degli obblighi specifica per soggetto, compreso il momento che avvia ogni termine. La comunicazione deve separare rivendicazione, effetto verificato e azione. Simulate entrambi con un disservizio del fornitore accompagnato da una vendita dichiarata di dati (§§6, 10 e 12).

## L'anno in cifre

### 802 371

Pubblicazioni con etichetta Italia conteggiate per data di pubblicazione fino alla rilevazione

COSA NON INDICA

Non attacchi, vittime o scambi conclusi

### 16 613

Pubblicazioni distinte conservate nel corpus combinato parziale

COSA NON INDICA

Non una quota rappresentativa della criminalità informatica nazionale

### 839

Pubblicazioni di forum conservate con etichetta Italia

COSA NON INDICA

Non l'intera popolazione conteggiata con l'etichetta nazionale

### 286

Registrazioni di rivendicazioni ransomware associate all'Italia

COSA NON INDICA

Non intrusioni verificate indipendentemente

### 270

Valori distinti nei nomi delle vittime di quelle registrazioni

COSA NON INDICA

Non organizzazioni o incidenti unici convalidati

### 250

Voci candidate nel portafoglio selezionato

COSA NON INDICA

Non organizzazioni indipendenti convalidate

### 42

Carte di pagamento distinte associate all'Italia, visibili in chiaro nelle pubblicazioni conservate

COSA NON INDICA

Visione limitata alle pubblicazioni, non prevalenza dei furti o perdite per frode (§8.6)

### 18

Schede caso: affermazioni clandestine, casi da fonti pubbliche, campagne e un'esclusione

COSA NON INDICA

Non un totale nazionale degli incidenti

Le prime tre righe usano [S1], quelle sulle rivendicazioni [S2], quella sui candidati [S3]. L'osservazione limitata sulle carte usa [S4].

**Cosa non possono spiegare queste cifre.** Pubblicazioni, rivendicazioni, campagne, stime delle persone interessate e notifiche misurano elementi diversi. Non possono formare un totale nazionale degli attacchi. Un maggior numero di segnalazioni può riflettere più visibilità, oltre a cambiamenti nell'attività. I casi sostengono decisioni senza trattare queste popolazioni come intercambiabili.

PUNTI CHIAVE

01

Le interruzioni confermate e i dati pubblicizzati richiedono evidenze e responsabili diversi.

02

La risposta sulle identità deve comprendere sessioni, recupero e autorità di pagamento.

03

Valutate la preparazione attraverso esiti dei servizi provati e decisioni di notifica documentate.

# Mappa del rapporto

Dodici capitoli, cinque percorsi di lettura. Partite dalla domanda del vostro ruolo, poi usate i riferimenti ai casi e alle evidenze per verificare l'affermazione che sostiene ogni decisione.

| | | |
|---|---|---|
| **Consiglio e dirigenti** | Quali decisioni su servizi, identità e pagamenti devono essere finanziate? | 01 05 11 12 |
| **CISO e responsabili della sicurezza** | Quali evidenze cambiano le nostre priorità? | 03 04 05 10 12 |
| **SOC e analisti** | È una rivendicazione, una ripubblicazione o un danno operativo confermato? | 04 06 07 B |
| **Antifrode e tutela dei clienti** | Cosa può fare un attaccante con recapiti e dati identificativi? | 08 09 12 |
| **Legale e comunicazione** | Quali fatti possiamo dichiarare e quali termini si applicano? | 05 06 10 12 |

01 Sintesi
Risultati più solidi e quattro decisioni

02 Contesto digitale e operativo dell'Italia
Servizi digitali, fornitori e visibilità delle segnalazioni

03 Esposizione nazionale: voci candidate del portafoglio
Segnali di esposizione del portafoglio selezionato

04 Cosa osserviamo sul dark web
Ambito e significato delle osservazioni nei mercati clandestini

05 Esempi di bersagli e casi per settore
Casi sostenuti dalle fonti e risposta per settore

06 Hacktivismo, DDoS e attività recente
Rivendicazioni di disservizi, resoconti ufficiali e attività recente

07 Attori delle minacce ed evidenze dei collegamenti
Evidenze sugli attori e limiti dei collegamenti

08 L'economia delle frodi
Raccolta di identità, abuso di account e frodi nei pagamenti

09 Approfondimento su banche e finanza
Decisioni bancarie per le popolazioni di clienti e dipendenti

10 Normativa e risposta nazionale
NIS2, obblighi pubblici, GDPR e DORA

11 Prospettive
Scenari condizionali e cambiamenti della valutazione

12 Piano d'azione
Azioni assegnate e prove di completamento

CAPITOLO 02

# Contesto digitale e operativo dell'Italia

02

QUESTO CAPITOLO RISPONDE

Quali caratteristiche dei servizi italiani spiegano le priorità di questo rapporto?

**3**

decisioni collegate: identità, continuità e dipendenza dai fornitori


2.1 Seguire il servizio dietro il titolo 11

2.2 I fornitori condivisi possono generare interruzioni comuni 11

2.3 Gli eventi importanti attirano rivendicazioni visibili 12

2.4 Le segnalazioni cambiano ciò che le autorità vedono 12

2.5 Mantenere visibili gli incidenti precedenti senza ridatarli 12

CAPITOLO 02

# Contesto digitale e operativo dell'Italia

IN SINTESI

I cittadini dipendono dai servizi pubblici digitali, le organizzazioni da fornitori condivisi. Gli eventi importanti creano bersagli visibili per gli attacchi alla disponibilità. L'ampliamento degli obblighi di segnalazione in Italia cambia anche ciò che le autorità osservano. Queste caratteristiche spiegano perché rivendicazioni sui siti, interruzioni dei fornitori e offerte di dati identificativi richiedono decisioni diverse. Mappate i servizi e i processi di approvazione indispensabili alla vostra organizzazione.

## 2.1 Seguire il servizio dietro il titolo

I casi riguardano istruzione, fornitori di infrastrutture, sanità, cultura, commercio e amministrazione. Non dimostrano tassi di incidente uguali tra i settori. Mostrano percorsi diversi da un evento tecnico alle conseguenze sul servizio. Sistemi universitari indisponibili, archivi cifrati di un fornitore e accessi ai recapiti generano attività operative diverse. [S5][S24][S27][S7]

Il responsabile del servizio deve prima accertare quale funzione si sia fermata o quali informazioni siano state consultate. Deve poi stabilire chi possa verificarlo. Un controllo del sito non dimostra lo stato di una piattaforma interna di prenotazione. L'attività commerciale in corso non dimostra l'assenza di accessi a informazioni personali. Entrambe le osservazioni possono essere corrette se riguardano risorse diverse.

L'unità utile per la difesa è un servizio aziendale con dipendenze identificate. Individuate il suo fornitore di identità, l'hosting, gli accessi di assistenza, il canale di comunicazione e la fonte di ripristino. Assegnate un responsabile capace di giudicare l'utilizzabilità aziendale. È una raccomandazione di pianificazione derivata dai casi, non una misurazione nazionale della concentrazione dei fornitori.

## 2.2 I fornitori condivisi possono generare interruzioni comuni

Il rapporto ACN di agosto descrive la cifratura di un'area condivisa presso un fornitore ICT, con effetti sui clienti che la utilizzavano. Il rapporto associa il caso a Titan. Non pubblica un totale dei clienti né dimostra il coinvolgimento di ogni servizio. L'osservazione sostiene indagini sulle singole dipendenze, non una conclusione su tutti i fornitori cloud. [S13]

Rendere nuovamente disponibili archivi o server non ripristina necessariamente applicazioni, autenticazione, transazioni o registrazioni riconciliate. Gli acquisti e i team di continuità devono concordare come provare queste condizioni. Gli aggiornamenti del fornitore devono permettere a ogni cliente di stabilire se il proprio servizio sia interessato.

Verificate se accessi alla produzione, amministrazione delle copie e approvazione del ripristino dipendano dalle stesse identità o dallo stesso ambiente di controllo. Il rapporto non afferma che queste configurazioni abbiano causato un caso specifico. Sono domande per una revisione autorizzata del progetto e una prova di ripristino.

## 2.3 Gli eventi importanti attirano rivendicazioni visibili

Il periodo olimpico ha generato rivendicazioni DDoS contro servizi digitali collegati all'evento e alla diplomazia. ACN distingue gli effetti sui siti dal regolare svolgimento dell'evento. Nel suo resoconto ufficiale afferma che nessun incidente informatico ha inciso sul regolare svolgimento delle gare o sui servizi essenziali associati. Ciò non rende fittizio ogni tentativo di interruzione. Identifica gli effetti osservati e quelli non osservati. [S10]

Biglietteria, alloggi, informazioni sui trasporti, comunicazione pubblica e assistenza richiedono verifiche separate. L'organizzatore deve sapere quale fornitore confermi ogni funzione e quale canale resti utilizzabile quando il sito principale non è disponibile. Un elenco di siti rivendicato non sostituisce queste verifiche dei servizi.

I temi politici appartengono agli autori o alle fonti che li richiamano. Gli autori del rapporto non prendono posizione su decisioni governative, migrazione, Russia/Ucraina, Israele/Gaza o altre controversie politiche. Le dichiarazioni sulle motivazioni rilevano solo quando aiutano a valutare una rivendicazione, i tempi o la comunicazione. Non dimostrano la responsabilità tecnica.

## 2.4 Le segnalazioni cambiano ciò che le autorità vedono

Il resoconto ACN di febbraio spiega che gli obblighi operativi di notifica NIS2 hanno ampliato la visibilità da gennaio 2026. Precisa che questa maggiore visibilità non corrispondeva a un aumento equivalente degli impatti osservati. La dichiarazione riguarda la popolazione delle segnalazioni e il periodo di ACN. Non dimostra un aumento o una riduzione delle minacce nazionali sottostanti. [S10] Per gennaio-giugno 2026, ACN riporta 2171 eventi informatici, in aumento del 47% rispetto allo stesso periodo del 2025, e 1072 incidenti con impatto confermato. ACN precisa che la maggiore visibilità delle notifiche NIS2 spiega gran parte dell'aumento; questi totali ufficiali restano distinti dai conteggi Brandefense di pubblicazioni e rivendicazioni. [S75]

L'Operational Summary di ottobre riporta 691 eventi e 394 incidenti con impatto confermato. Il resoconto ANSA del 20 novembre conferma queste cifre principali. Il documento rivede anche osservazioni precedenti. Un grafico mensile deve indicare l'edizione della fonte utilizzata, perché successive indagini possono modificare una classificazione precedente. I valori iniziali e quelli rivisti non devono diventare implicitamente un'unica serie. [S49] [S65]

Per un consiglio di amministrazione, più notifiche possono significare che il processo individua eventi prima invisibili. Per capire il danno, chiedete durata, servizi coinvolti, categorie informative, ripristino e ricorrenza. Contate questi esiti separatamente dagli avvisi e dalle segnalazioni.

## 2.5 Mantenere visibili gli incidenti precedenti senza ridatarli

Alcune pubblicazioni del 2026 riguardano attività precedenti. Gli avvisi di giugno ai clienti ferroviari riguardano attività di fine 2025. Diverse decisioni del Garante riguardano incidenti del 2024 o 2025. Sono rilevanti per notifiche, frodi e lezioni sui controlli, ma non sono nuove intrusioni del 2026. [S45][S40][S41][S42]

Il rapporto distingue le date di evento, rivendicazione, comunicazione, aggiornamento e decisione. Una successiva dichiarazione di ripristino aggiorna lo stesso caso. Una ripubblicazione criminale non dimostra una nuova estrazione. Una decisione del regolatore è un'osservazione sull'applicazione delle norme, non la prova che l'attacco sia avvenuto nella data della decisione.

PUNTI CHIAVE

01

Servizi aziendali e dipendenze sono l'unità utile per decidere sulla continuità.

02

Le rivendicazioni sui siti di un evento non dimostrano l'interruzione dell'evento.

03

Le date di pubblicazione e segnalazione devono restare separate da quelle degli eventi.

CAPITOLO 03

# Esposizione nazionale: voci candidate del portafoglio

QUESTO CAPITOLO RISPONDE

Quali segnali di esposizione del portafoglio selezionato richiedono le prime verifiche?

## 132 su 250

voci candidate del portafoglio associate a offerte di credenziali al momento della verifica


3.1 Scheda dell'insieme 15

3.2 Conteggi dei segnali per settore 16

3.3 Dispositivi, documenti e domini imitativi richiedono responsabili diversi 17

3.4 Copertura dei controlli passivi 18

3.5 Trasformare i segnali in verifiche 18

CAPITOLO 03

# Esposizione nazionale: voci candidate del portafoglio

IN SINTESI

Alla verifica, le offerte di credenziali erano associate a 132 voci candidate nel portafoglio di 250 voci. Il valore nazionale Atlas è 57 su 100. Il portafoglio registra almeno 759724 associazioni di dispositivi e 113259485 associazioni di credenziali storiche. Queste osservazioni sovrapposte non dimostrano persone uniche o intrusioni confermate. Convalidate le offerte attuali, indagate sui dispositivi associati ai dipendenti e assegnate le altre evidenze degli account al responsabile del servizio.

## 3.1 Scheda dell'insieme

| Voce | Definizione |
|---|---|
| Popolazione | 250 voci candidate del portafoglio in dodici settori |
| Selezione | Selezione ragionata per rilevanza pubblica, economica o settoriale; non una graduatoria dei ricavi |
| Unità | Un dominio principale candidato per voce del portafoglio; appartenenza e indipendenza organizzativa richiedono verifica |
| Rilevazione dell'esposizione | 21-22 novembre 2026; i dati storici non sono limitati all'anno del rapporto |
| Prima osservazione | 228 dei 250 domini candidati hanno restituito dati DNS pubblici il 22 novembre 2026 |
| Interpretazione | Organizzazioni collegate e servizi condivisi possono avere impronte digitali sovrapposte |
| Valore nazionale Atlas | 57 su 100 per questo portafoglio selezionato |
| Controlli passivi | Non sono pubblicate analisi utilizzabili di DMARC, SPF, DKIM, DNSSEC, TLS o intestazioni web |
| Generalizzazione | L'elenco non stima la prevalenza nazionale o settoriale |

Brandefense Atlas fornisce la valutazione dell'esposizione; il rapporto pubblica soltanto il valore nazionale. I conteggi datati seguenti descrivono i domini selezionati, anziché perimetri aziendali convalidati. Un valore maggiore indica maggiore esposizione osservata sulla scala 0-100. Non quantifica la probabilità di un attacco. Le associazioni ai domini non stabiliscono nazionalità o posizione degli utenti. [S3]

## 3.2 Conteggi dei segnali per settore

La tabella separa associazioni dei dispositivi, credenziali storiche e voci candidate associate a offerte attuali di credenziali. Le popolazioni si sovrappongono. Le cifre dei dispositivi sono totali minimi osservati; un dispositivo o una credenziale può ricorrere su domini collegati. Non sono pubblicate valutazioni settoriali. [S3]

| Settore | Voci candidate | Dispositivi | Credenziali | Voci associate a offerte |
|---|---|---|---|---|
| Amministrazione pubblica | 40 | 136 907 | 578 774 | 17 |
| Banche e finanza | 25 | 83 725 | 1 662 877 | 14 |
| Istruzione | 30 | 90 020 | 3 505 654 | 21 |
| Sanità | 20 | 5 147 | 152 478 | 4 |
| Assicurazioni | 10 | 13 037 | 109 972 | 5 |
| Energia e servizi essenziali | 20 | 53 735 | 308 222 | 9 |
| Trasporti e logistica | 20 | 56 248 | 157 468 | 13 |
| Manifattura e industria | 25 | 24 414 | 431 897 | 9 |
| Commercio e consumi | 20 | 64 048 | 120 737 | 14 |
| Telecomunicazioni e servizi digitali | 10 | 139 177 | 105 986 323 | 7 |
| Media e sport | 15 | 87 068 | 220 547 | 10 |
| Turismo e ospitalità | 15 | 6 198 | 24 536 | 9 |
| **Totale** | **250** | **759 724** | **113 259 485** | **132** |

### Le offerte attuali di credenziali sono associate a 132 voci candidate del portafoglio; i conteggi settoriali descrivono segnali distinti

Le colonne usano scale distinte. Le offerte attuali di credenziali sono in corallo: voci con offerte / voci candidate selezionate; le altre celle riportano conteggi.

| | Associazioni dispositivi (almeno) | Credenziali storiche | Offerte attuali di credenziali |
|---|---|---|---|
| Amministrazione pubblica | 136 907 | 578 774 | 17/40 |
| Banche e finanza | 83 725 | 1 662 877 | 14/25 |
| Istruzione | 90 020 | 3 505 654 | 21/30 |
| Sanità | 5 147 | 152 478 | 4/20 |
| Assicurazioni | 13 037 | 109 972 | 5/10 |
| Energia e servizi essenziali | 53 735 | 308 222 | 9/20 |
| Trasporti e logistica | 56 248 | 157 468 | 13/20 |
| Manifattura e industria | 24 414 | 431 897 | 9/25 |
| Commercio e consumi | 64 048 | 120 737 | 14/20 |
| Telecomunicazioni e servizi digitali | 139 177 | 105 986 323 | 7/10 |
| Media e sport | 87 068 | 220 547 | 10/15 |
| Turismo e ospitalità | 6 198 | 24 536 | 9/15 |

Fonte: associazioni di esposizione per 250 voci candidate del portafoglio selezionato, 21-22 novembre 2026. I dispositivi sono totali minimi; le credenziali storiche si sovrappongono e non dimostrano account distinti o intrusioni confermate. I controlli passivi non sono disponibili [S3].

Il totale storico delle credenziali comprende 29 686 862 registrazioni da archivi di violazioni, 8 899 179 registrazioni da log di infostealer e 74 673 444 registrazioni da combolist. Sono associazioni di registrazioni, non account unici, password appena sottratte o intrusioni del 2026. Appartenenza, attualità e precedenti interventi richiedono verifica. [S3]

I log di infostealer contengono dati di accesso catturati da malware che sottrae informazioni su dispositivi infetti. Le combolist raccolgono coppie di indirizzi email o nomi utente e password. Questi termini descrivono tipi di registrazioni, non quando le credenziali siano state sottratte o se funzionino ancora. [S69][S70]

## 3.3 Dispositivi, documenti e domini imitativi richiedono responsabili diversi

Di almeno 759 724 associazioni di dispositivi, 75 253 sono associate ai dipendenti. Le restanti 684 471 non rientrano in tale classificazione; possono riguardare clienti, studenti o altri utenti. Appartenenza e stato attuale non sono accertati. L'associazione a un dominio non identifica un'intrusione nell'infrastruttura dell'organizzazione. [S3]

La rilevazione registra anche 2 976 associazioni di documenti esposti e 40 409 osservazioni di domini imitativi. Sono segnali distinti, non dispositivi aggiuntivi o siti di phishing verificati. Un'associazione documentale non stabilisce chi abbia pubblicato il documento, se sia ancora sensibile o se vi sia stata una divulgazione non autorizzata. [S3]

Un'offerta attuale descrive credenziali proposte in vendita e richiede una verifica del singolo account. Non dimostra vendita conclusa, accesso valido o intrusione interna confermata. Assegnate le evidenze dei dipendenti ai team identità ed endpoint, quelle degli altri account al servizio pertinente e quelle documentali al responsabile delle informazioni.

## 3.4 Copertura dei controlli passivi

La prima osservazione DNS copre 228 dei 250 domini candidati. Non è una valutazione dell'igiene. In questa edizione non sono disponibili misure utilizzabili dei controlli passivi. Non sono quindi pubblicate percentuali su DMARC, SPF, DKIM, DNSSEC, TLS o intestazioni web. Misure mancanti non dimostrano controlli mancanti. [S3]

## 3.5 Trasformare i segnali in verifiche

| Segnale | Prima verifica | Prova di completamento |
|---|---|---|
| Offerta attuale di credenziali | Accertare appartenenza e rilevanza attuale dell'account | Esito datato della verifica identità |
| Associazione di dispositivo ai dipendenti | Accertare appartenenza dell'endpoint, sessioni e risposta precedente | Risultati su endpoint e identità |
| Altra associazione di dispositivo | Identificare relazione con il servizio ed evidenze di frode | Esito del servizio o antifrode |
| Associazione di documento esposto | Accertare provenienza, sensibilità e autorizzazione alla divulgazione | Decisione del responsabile delle informazioni |
| Osservazione di dominio imitativo | Accertare appartenenza, contenuto ed evidenze di impersonificazione | Esito dell'indagine sul dominio |

Una valutazione nazionale non rende intercambiabili queste attività. La sovrapposizione tra capogruppo, controllate e fornitori limita l'indipendenza dei totali. Conservate date di osservazione ed evidenze degli account prima di scegliere interventi invasivi. Confermate dominio candidato e servizio prima di attribuire un'osservazione a una persona giuridica.

PUNTI CHIAVE

01

Convalidate le offerte di credenziali associate a 132 su 250 voci candidate del portafoglio.

02

Associazioni di dispositivi e credenziali storiche sono registrazioni sovrapposte, non intrusioni confermate.

03

Assegnate le evidenze su identità, servizi, informazioni e domini ai responsabili capaci di accertarne la rilevanza attuale.

CAPITOLO 04

# Cosa osserviamo sul dark web

04

QUESTO CAPITOLO RISPONDE

Cosa dimostrano le pubblicazioni conservate sulla pubblicità clandestina collegata all'Italia?

**802 371**

pubblicazioni con etichetta Italia conteggiate per data di pubblicazione, non attacchi


4.1 Scheda dell'insieme 21
4.2 La concentrazione mensile richiede spiegazioni prima di essere interpretata 22
4.3 Cosa offrono effettivamente gli esempi 23
4.4 Sei schede caso da fonti proprie 24
4.5 Affermazioni recenti e storiche richiedono date proprie 31
4.6 Altre rivendicazioni su accessi e infrastrutture 32
4.7 Trasformare un annuncio in un compito di verifica delimitato 34

CAPITOLO 04

# Cosa osserviamo sul dark web

IN SINTESI

Il volume con etichetta Italia si concentra all'inizio dell'anno, ma i conteggi non spiegano da soli l'attività sottostante. Gli esempi di forum conservati mostrano richieste di dati, offerte di documenti identificativi, pubblicità di accessi alla posta e file etichettati per settore. Diversi hanno contenuti bloccati o date storiche esplicite. Dimostrano annunci e affermazioni, non accessi validi o nuove intrusioni. Verificate provenienza, età e rilevanza prima di decidere che un'organizzazione richieda una risposta all'incidente.

## 4.1 Scheda dell'insieme

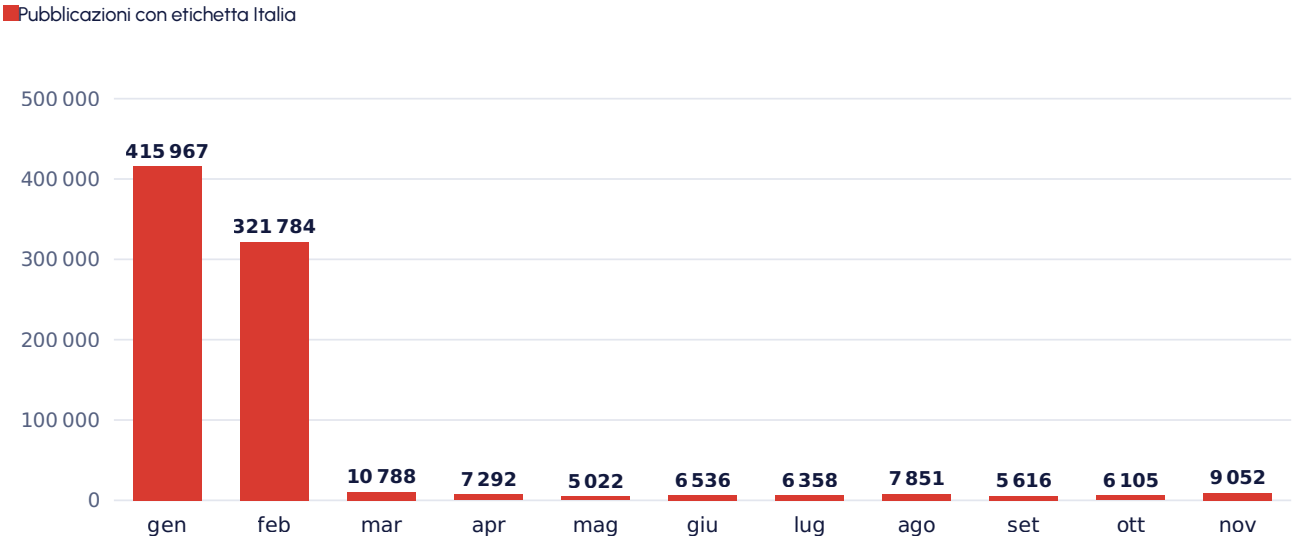
| Voce | Definizione |
|---|---|
| Fonte | Osservazioni di mercati clandestini e messaggistica conservate da Odin by Brandefense |
| Periodo | Data di pubblicazione dal 1 gennaio alla rilevazione del 22 novembre |
| Conteggio nazionale | 802 371 pubblicazioni con etichetta Italia; l'etichetta non dimostra che l'Italia sia il bersaglio |
| Materiale conservato | 16 613 pubblicazioni distinte in un corpus combinato parziale, comprese 839 pubblicazioni di forum con etichetta Italia (di cui 195 datate 9-22 novembre 2026) |
| Schede delle evidenze | Diciassette estratti oscurati con riferimenti B stabili |
| Unità | Pubblicazioni e annunci, non intrusioni verificate, vendite o persone uniche |
| Limite principale | Il testo conservato non dimostra il contenuto di file bloccati o pubblicizzati |

La fonte è [S1]. La popolazione conteggiata e quella dei testi conservati sono diverse. Il rapporto non tratta la seconda come un campione rappresentativo di ogni pubblicazione etichettata. Non presume neppure che i temi dei forum spieghino il traffico di messaggistica. Un estratto selezionato illustra un'affermazione, non la sua frequenza nazionale.

## 4.2 La concentrazione mensile richiede spiegazioni prima di essere interpretata

| Mese | Pubblicazioni etichettate | Lettura |
|---|---|---|
| Gennaio | 415 967 | Conteggio delle pubblicazioni |
| Febbraio | 321 784 | Conteggio delle pubblicazioni |
| Marzo | 10 788 | Conteggio delle pubblicazioni |
| Aprile | 7 292 | Conteggio delle pubblicazioni |
| Maggio | 5 022 | Conteggio delle pubblicazioni |
| Giugno | 6 536 | Conteggio delle pubblicazioni |
| Luglio | 6 358 | Conteggio delle pubblicazioni |
| Agosto | 7 851 | Conteggio delle pubblicazioni |
| Settembre | 5 616 | Conteggio delle pubblicazioni |
| Ottobre | 6 105 | Conteggio delle pubblicazioni |
| Novembre | 9 052 | Periodo parziale fino alla rilevazione |
| **Totale** | **802 371** | **Pubblicazioni, non attacchi** |

### Gennaio e febbraio contengono la maggior parte delle pubblicazioni etichettate; la serie non misura gli attacchi




Fonte: conteggi Brandefense delle pubblicazioni con etichetta Italia, 1 gennaio–22 novembre 2026; novembre arriva alla rilevazione. Le pubblicazioni etichettate e il corpus parziale conservato sono popolazioni distinte, non attacchi [S1].

Gennaio e febbraio contengono 737 751 pubblicazioni, pari al 91,9% del totale. Il calcolo non identifica una quota di bot, un'ondata di attacchi riusciti o una tendenza della minaccia sottostante. Pubblicità ripetuta, differenze di copertura e attività effettiva delle campagne sono spiegazioni possibili che richiedono altre evidenze. Non sceglietene una dal solo volume. [S1]

Nemmeno i mesi successivi dimostrano una riduzione dei danni nazionali. Gli incidenti possono avvenire senza pubblicazioni clandestine, mentre gli annunci possono continuare dopo l'evento sottostante. Novembre è parziale. Il grafico serve a comprendere il volume osservato dalla fonte, non a confrontare esiti nazionali tra periodi diversi.

## 4.3 Cosa offrono effettivamente gli esempi

| Tema osservato | Schede | Affermazione dimostrata | Irrisolto |
|---|---|---|---|
| Richieste di dati etichettati Italia | B01 · B03 | Gli autori cercavano dati e includevano l'Italia | Acquisto, origine e validità |
| Pubblicità di account finanziari | B02 | Un annuncio elencava banche di più Paesi | Esistenza, appartenenza e uso degli account |
| Pubblicità di documenti identificativi | B04 | L'Italia compariva in un'offerta per più Paesi | Autenticità ed esito delle verifiche |
| Log etichettati con una banca | B05 | Un bot pubblicizzava un file con un'etichetta bancaria | Contenuto e intrusione nei sistemi del servizio |
| Accesso alla posta | B06 | Un annuncio di accesso aveva contenuti bloccati | Validità attuale e titolari degli account |
| Affermazione su nomi di clienti | B07 | Chi caricava il materiale ne riconosceva la scarsa qualità | Persone distinte, fonte e attualità |
| File con etichetta sanitaria | B08 | Una raccolta di formati misti era associata a un operatore | Autenticità, contenuto clinico e data dell'evento |
| Database commerciale | B09 | Un venditore pubblicizzava dati e campioni | Origine, età e composizione geografica |
| Recente affermazione sui media | B10 | Una pubblicazione di novembre pubblicizzava materiale bloccato | Contenuto, autenticità e nuova intrusione |
| Dati storici di un sito | B11 | La pubblicazione datava il database al 2016 | Autenticità e rilevanza attuale |
| Offerta di accesso remoto | B12 | Un annuncio separato dichiarava accesso a servizi aziendali collegati all'Italia | Validità attuale e controllo dell'accesso |

L'etichetta settoriale fornisce una domanda da verificare. Non basta per identificare un processo aziendale coinvolto o dichiarare un'estrazione di dati. Il contenuto bloccato è un limite sostanziale: il titolo non permette di valutare il file pubblicizzato. Anche l'offerta di un campione resta un'affermazione finché evidenze autorizzate non ne dimostrano il contenuto.

## 4.4 Sei schede caso da fonti proprie

A

CASO A

### Una richiesta cita l'Italia senza dimostrare una vittima

Scheda di evidenza B01 | 10 feb 2026 | Forum | Trasversale

Annuncio non verificato

| | |
|---|---|
| OSSERVAZIONE | Una pubblicazione di forum di febbraio chiedeva dati francesi e italiani per domini di posta selezionati e prove prima dell'acquisto. Una richiesta separata di gennaio includeva l'Italia tra più mercati. [S1] |
| ACCERTATO | Le pubblicazioni conservate dimostrano la domanda e le etichette geografiche o dei servizi richieste. Non dimostrano acquisti né l'origine di un file. |
| ALTERNATIVE | Un acquirente potrebbe cercare vecchi elenchi, credenziali degli utenti, registrazioni aggregate o materiale etichettato male. La richiesta non implica un'intrusione presso il fornitore. |
| RISPOSTA | Confrontate la categoria richiesta con i processi di identità e dei clienti dell'organizzazione. Segnalate le evidenze attuali specifiche dell'organizzazione, non la presenza del Paese nell'elenco di un acquirente. |

**Conclusione**

Confrontate la categoria richiesta con i processi di identità e dei clienti dell'organizzazione. Segnalate le evidenze attuali specifiche dell'organizzazione, non la presenza del Paese nell'elenco di un acquirente.

Scheda di evidenza B01 — 10 feb 2026

**kurkenluvsdh** | Forum | Forum | English

ORIGINALE

Buying France + Italy Data [...] i ONLY need these domains [...] need tests before buy.

TRADUZIONE

Acquisto di dati Francia + Italia [...] mi servono SOLO questi domini [...] servono prove prima dell'acquisto.

**Accertato**
Un acquirente ha chiesto dati per domini di posta italiani e francesi selezionati e ha chiesto di provarli.

**Non accertato**
Acquisti, validità, fonte o intrusioni presso un fornitore di posta.

Scheda di evidenza B03 — 27 gen 2026

**exelo** | Forum | Forum | English

ORIGINALE

[database solicitation removed] [...] IT ITALY [...]

TRADUZIONE

[richiesta di database rimossa] [...] IT ITALIA [...]

**Accertato**
Un'identità di forum cercava database e includeva esplicitamente l'Italia tra più mercati.

**Non accertato**
Origine, attualità, validità o usi successivi dei dati.

Chiedere di provare i dati non dimostra che la prova sia avvenuta o abbia avuto successo. La distinzione conta quando un avviso trasforma il desiderio di un acquirente in una capacità presumibilmente disponibile. Mantenete il prodotto richiesto e l'esito in campi distinti.

CASO B

B

## La pubblicità di documenti identificativi include l'Italia

Scheda di evidenza B04 | 19 ago 2026 | Forum | Servizi di identità

Annuncio non verificato

| | |
|---|---|
| **OSSERVAZIONE** | Un annuncio di agosto includeva l'Italia tra i Paesi di un'offerta di documenti identificativi. [S1] |
| **ACCERTATO** | La pubblicazione dimostra un prodotto dichiarato e l'uso previsto nelle verifiche. Non dimostra documenti autentici, vendite concluse o apertura riuscita di account. |
| **ALTERNATIVE** | Il materiale potrebbe essere falso, obsoleto, copiato da un altro venditore oppure autentico. L'estratto non risolve queste alternative. |
| **RISPOSTA** | Provate apertura e recupero degli account con documenti sintetici plausibili. Documentate quali ulteriori evidenze siano necessarie prima che un documento da solo autorizzi un account o un cambiamento dei recapiti. |

**Conclusione**

Provate apertura e recupero degli account con documenti sintetici plausibili. Documentate quali ulteriori evidenze siano necessarie prima che un documento da solo autorizzi un account o un cambiamento dei recapiti.

Scheda di evidenza B04 — 19 ago 2026

**Jaded** | Forum | Forum | English

ORIGINALE

DIGITAL KYC Documents for your VERIFICATION NEEDS [...] Countries Listed Down Below: [...] Italy [...]

TRADUZIONE

Documenti KYC DIGITALI per le vostre ESIGENZE DI VERIFICA [...] Paesi elencati sotto: [...] Italia [...]

**Accertato**
Un annuncio di documenti identificativi includeva l'Italia in un'offerta per più Paesi.

**Non accertato**
Che i documenti fossero autentici, utilizzabili nelle verifiche o effettivamente venduti.

La domanda difensiva rilevante non è se l'annuncio sembri professionale. È quale decisione interna accetterebbe il materiale dichiarato. La domanda rimane utile anche quando l'autenticità non è risolta.

CASO C

C

## Un titolo sull'accesso alla posta nasconde il contenuto sostanziale

Annuncio non verificato

Scheda di evidenza B06 | 20 ago 2026 | Forum | Servizi di posta

| | |
|---|---|
| **OSSERVAZIONE** | Una pubblicazione di forum di agosto pubblicizzava accessi alla posta italiana, con il contenuto sostanziale bloccato. [S1] |
| **ACCERTATO** | L'annuncio esiste. Il rapporto non dimostra quantità, titolari degli account, accessi attuali o intrusioni presso il fornitore. |
| **ALTERNATIVE** | Un titolo può descrivere credenziali storiche, dati degli utenti, pubblicità copiata o accessi attivi. Il contenuto bloccato lascia irrisolta l'affermazione. |
| **RISPOSTA** | Se il monitoraggio autorizzato fornisce evidenze specifiche dell'organizzazione, verificate account, stato delle sessioni e precedenti interventi. Non deducete che vi sia stato accesso a un fornitore italiano di posta. |

**Conclusione**

Se il monitoraggio autorizzato fornisce evidenze specifiche dell'organizzazione, verificate account, stato delle sessioni e precedenti interventi. Non deducete che vi sia stato accesso a un fornitore italiano di posta.

Scheda di evidenza B06 — 20 ago 2026

**MegaCloud** | Forum | Forum | English

ORIGINALE

[quantity removed] Italy HQ MAIL Access [...] Content locked

TRADUZIONE

[quantità rimossa] Italia Accesso MAIL HQ [...] Contenuto bloccato

**Accertato**
Una pubblicazione di forum pubblicizzava accessi alla posta italiana; i contenuti sostanziali erano bloccati.

**Non accertato**
Quantità dichiarata, validità degli accessi, titolari degli account o compromissione dei sistemi del servizio.

Scheda di evidenza B12 — 2 apr 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

country: Italy [...] access: RDWEB [...] price: [negotiation text removed]

TRADUZIONE

Paese: Italia [...] accesso: RDWEB [...] prezzo: [testo della trattativa rimosso]

**Accertato**
Un venditore di forum pubblicizzava accessi web remoti associati a un'organizzazione italiana del settore eventi.

**Non accertato**
Che l'accesso funzionasse, l'identità dell'organizzazione, la via d'ingresso, il furto di dati o una vendita conclusa.

Credenziali e sessioni possono sostenere decisioni di risposta diverse. L'annuncio da solo non dimostra nessuna delle due. I team identità devono ricevere l'evidenza specifica e il suo limite, non un'etichetta generale di compromissione del Paese.

CASO D

D

## L'etichetta bancaria di un bot non identifica l'estrazione

Scheda di evidenza B05 | 4 giu 2026 | Forum | Banche

Annuncio non verificato

| | |
|---|---|
| **OSSERVAZIONE** | A giugno un sistema di caricamento automatico pubblicizzava un file etichettato come log bancari. [S1] |
| **ACCERTATO** | Sono conservati l'etichetta e la pubblicazione. L'estratto non dimostra contenuto dei file, account validi dei clienti o accessi ai sistemi della banca. |
| **ALTERNATIVE** | L'etichetta potrebbe riferirsi a log degli utenti, elenchi assemblati, materiale precedente o descrizioni promozionali inesatte. La fonte non permette di scegliere. |
| **RISPOSTA** | Inviate le eventuali evidenze convalidate sui singoli account al responsabile appropriato di identità o antifrode. Tenete l'esposizione dei dispositivi dei clienti separata dalle accuse sulle infrastrutture bancarie. |

**Conclusione**

Inviate le eventuali evidenze convalidate sui singoli account al responsabile appropriato di identità o antifrode. Tenete l'esposizione dei dispositivi dei clienti separata dalle accuse sulle infrastrutture bancarie.

Scheda di evidenza B05 — 4 giu 2026

**Forum bot** | Forum | Forum | English

ORIGINALE

[bank label removed] Logs Txt Database [...] Content Type: Database Dump

TRADUZIONE

[etichetta bancaria rimossa] Database di log Txt [...] Tipo di contenuto: esportazione di database

**Accertato**
Un sistema di caricamento automatico del forum pubblicizzava un file con un'etichetta di log bancari.

**Non accertato**
Una violazione della banca, credenziali valide dei clienti, provenienza o contenuti del file.

Scheda di evidenza B02 — 18 apr 2026

**Jiskaa** | Forum | Forum | English

ORIGINALE

ITALY · [bank names removed] [...]

TRADUZIONE

ITALIA · [nomi delle banche rimossi] [...]

**Accertato**
Un annuncio elencava banche italiane insieme a banche, portafogli e conti aziendali di altri Paesi.

**Non accertato**
Che gli account esistessero, appartenessero all'inserzionista o fossero usati per frodi.

L'annuncio di account vicino elenca servizi finanziari di vari Paesi. La presenza di banche italiane non dimostra che l'inserzionista possedesse account o li usasse per frodi. Restano affermazioni diverse anche quando compaiono nello stesso mercato.

CASO E

E

## Dati commerciali pubblicizzati con campioni

Scheda di evidenza B09 | 6 ago 2026 | Forum | Commercio

Annuncio non verificato

| | |
|---|---|
| OSSERVAZIONE | Un venditore di agosto pubblicizzava un database commerciale etichettato Italia e offriva campioni. [S1] |
| ACCERTATO | La pubblicazione conservata dimostra l'annuncio. Non dimostra conteggio, composizione geografica, età, autenticità o vendita conclusa. |
| ALTERNATIVE | L'etichetta potrebbe descrivere clienti, contatti commerciali, vecchie registrazioni o materiale assemblato fuori dal commerciante. Un campione dichiarato non identifica indipendentemente il sistema di origine. |
| RISPOSTA | Valutate la provenienza tramite canali autorizzati prima di associare un incidente. Preparate indicazioni sui contatti con i clienti se informazioni attuali credibili potrebbero sostenere impersonificazioni. |

### Conclusione

Valutate la provenienza tramite canali autorizzati prima di associare un incidente. Preparate indicazioni sui contatti con i clienti se informazioni attuali credibili potrebbero sostenere impersonificazioni.

Scheda di evidenza B09 — 6 ago 2026

**wizard** | Forum | Forum | English

ORIGINALE

italian Database [retailer removed] [...] Total lines [volume removed] [...]

TRADUZIONE

Database italiano [commerciante rimosso] [...] Totale righe [volume rimosso] [...]

**Accertato**
Un venditore pubblicizzava un database commerciale etichettato Italia e offriva campioni.

**Non accertato**
Conteggio dichiarato, composizione geografica, età dei dati, autenticità o vendita conclusa.

Scheda di evidenza B07 — 28 set 2026

**updap** | Forum | Forum | English

ORIGINALE

[provider and volume removed] (ONLY NAMES) [...] The data is bad but I'm still leaking [...]

TRADUZIONE

[fornitore e volume rimossi] (SOLO NOMI) [...] I dati sono scadenti ma li sto comunque pubblicando [...]

**Accertato**
Un autore pubblicizzava nomi di clienti associati a un fornitore di software aziendale, riconoscendo la scarsa qualità dei dati.

**Non accertato**
Numero di persone distinte, stato di cliente, fonte, attualità o intrusione riuscita.

Una distinta affermazione su nomi di clienti di software riconosce esplicitamente la scarsa qualità dei dati. Mostra perché le registrazioni pubblicizzate non devono diventare automaticamente persone interessate. Nomi ripetuti, campi incompleti e stato di cliente incerto richiedono un denominatore definito prima della pubblicazione.

CASO F

F

## File con etichetta sanitaria restano una raccolta non verificata

Annuncio non verificato

Scheda di evidenza B08 | 18 ott 2026 | Forum | Sanità

| | |
|---|---|
| **OSSERVAZIONE** | Una pubblicazione di forum di ottobre associava una raccolta di file di formati misti a un operatore sanitario. [S1] |
| **ACCERTATO** | La pubblicazione descrive formati di file e un'associazione con l'operatore. Non dimostra contenuti clinici, autenticità, furto o un nuovo incidente. |
| **ALTERNATIVE** | La raccolta potrebbe riguardare materiale amministrativo, un evento precedente, fonti miste o un'etichetta inesatta. Non si presume una corrispondenza con il caso sanitario confermato. |
| **RISPOSTA** | Tenete separate continuità clinica ed esposizione delle informazioni. Il responsabile del servizio deve verificare sistema e categoria dei dati dichiarati prima di comunicazioni pubbliche o decisioni sulla notifica ai pazienti. |

### Conclusione

Tenete separate continuità clinica ed esposizione delle informazioni. Il responsabile del servizio deve verificare sistema e categoria dei dati dichiarati prima di comunicazioni pubbliche o decisioni sulla notifica ai pazienti.

Scheda di evidenza B08 18 ott 2026

**updap** Forum Forum English

ORIGINALE

[healthcare provider removed] [...] Format: Folders, XLS, PNG, ODS, ODT and others [...]

TRADUZIONE

[operatore sanitario rimosso] [...] Formato: cartelle, XLS, PNG, ODS, ODT e altri [...]

**Accertato**
Una pubblicazione di forum associava una raccolta di file di formati misti a un operatore sanitario.

**Non accertato**
Che i file fossero cartelle cliniche, fossero rubati, fossero autentici o riguardassero un nuovo incidente.

## updap

Identità di forum Non valutato

### IN ITALIA, 2026

**Settembre**
Pubblica un'affermazione su soli nomi collegati a software aziendale, B07

**Ottobre**
Pubblica un'offerta sanitaria di file misti, B08

### BERSAGLI DICHIARATI

Rivendicazioni descritte tramite ruoli generici

### NELLE FONTI PUBBLICHE

[S1] Pubblicazioni conservate B07 e B08

### LA NOSTRA VALUTAZIONE

L'alias comune di chi carica il materiale collega le pubblicazioni. Non dimostra identità dei file, furto comune, paternità o vendite concluse.

CONFIDENZA
Alta per l'associazione tra pubblicazioni; identità e affermazioni sottostanti non verificate

## 4.5 Affermazioni recenti e storiche richiedono date proprie

L'annuncio dell'11 novembre su un database dei media rientra nel periodo recente, ma il suo contenuto era bloccato. Sostiene l'osservazione di una pubblicazione recente, non di una nuova intrusione. Una pubblicazione di febbraio su dati di un sito riporta esplicitamente il 2016. Non può dimostrare un nuovo incidente del 2026. [S1]

**Scheda di evidenza B10** — 11 nov 2026

**Linda2000** | Forum | Forum | English

ORIGINALE

[media organisation removed] Database Italy [...] Hidden Content [...]

TRADUZIONE

[organizzazione dei media rimossa] Database Italia [...] Contenuto nascosto [...]

**Accertato**
Una pubblicazione di novembre pubblicizzava un database associato a un'organizzazione dei media; il download era bloccato.

**Non accertato**
Contenuto dei file, attualità, autenticità, validità degli accessi o una nuova intrusione.

**Scheda di evidenza B11** — 2 feb 2026

**Tanaka** | Forum | Forum | English

ORIGINALE

Italy [website removed] WordPress Database [...] format: sql date: 2016 [...]

TRADUZIONE

Italia [sito rimosso] Database WordPress [...] formato: sql data: 2016 [...]

**Accertato**
Una pubblicazione di forum di febbraio etichettava il database di un sito italiano con la data 2016.

**Non accertato**
Un nuovo incidente del 2026, accessi attuali, autenticità dei dati o significato della data storica indicata.

**Scheda di evidenza B12** — 2 apr 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

country: Italy [...] access: RDWEB [...] price: [negotiation text removed]

TRADUZIONE

Paese: Italia [...] accesso: RDWEB [...] prezzo: [testo della trattativa rimosso]

**Accertato**
Un venditore di forum pubblicizzava accessi web remoti associati a un'organizzazione italiana del settore eventi.

**Non accertato**
Che l'accesso funzionasse, l'identità dell'organizzazione, la via d'ingresso, il furto di dati o una vendita conclusa.

Un'offerta separata di aprile pubblicizza accessi RDWEB collegati all'Italia. [S1] RDWEB significa Remote Desktop Web Access, un portale web per l'accesso a desktop remoti. [S72] L'etichetta del servizio non dimostra che il venditore controllasse una sessione funzionante. Nessun collegamento concreto unisce questa offerta agli annunci di log bancari o posta. Tenete separata ogni affermazione, anche quando lo stesso team dovrebbe verificarle. [S1]

## 4.6 Altre rivendicazioni su accessi e infrastrutture

Gli ulteriori esempi seguenti restano non verificati. Non si presume alcun collegamento con un incidente del fornitore segnalato ufficialmente. Nessun accesso dichiarato è stato provato. Ampliano le domande di verifica oltre i sei casi di studio. [S1]

| Pubblicazione | Ruolo generale | Affermazione pubblicizzata | Domanda di verifica |
|---|---|---|---|
| Gennaio | Commerciante al dettaglio | Rivendicazione su un database di identità dei clienti | Si possono accertare provenienza e popolazione coinvolta? |
| Gennaio | Servizi immobiliari | Offerta di un elenco di contatti professionali | Quali provenienza e uso autorizzato hanno riscontri? |
| Gennaio | Registrazioni degli utenti di un servizio | Affermazioni su password temporanee e dati di localizzazione | Esistono account o sistemi attuali effettivamente corrispondenti? |
| 30 gennaio | Azienda automobilistica | Pannello amministrativo e informazioni aziendali | Sistema e accesso dichiarati appartengono all'organizzazione? |
| 2 febbraio | Istituto finanziario | Informazioni dichiarate come provenienti dai sistemi del personale | Esistono evidenze sul personale sostenute da riscontri, oltre all'etichetta? |
| Febbraio | Servizi ai consumatori | Affermazioni su recapiti, adesioni e registrazione di dispositivi | Si possono accertare provenienza e rilevanza attuale? |
| Febbraio | Servizi automobilistici | Annuncio di dati sui clienti o sui servizi | Quali evidenze collegano il materiale alla fonte dichiarata? |
| Gennaio-febbraio | Servizi pubblici | Annunci di accesso a caselle e pannelli amministrativi | Quali account e privilegi effettivi si possono verificare? |
| 6 aprile | Operatore industriale | Accessi VPN e utenti collegati all'Italia in un catalogo per più Paesi | Esistono account dichiarati attuali e rilevanti? |
| Aprile-maggio | Gestori di siti | Offerte di accesso tramite webshell | Evidenze autorizzate identificano una risorsa coinvolta? |
| 26 aprile | Progetto di un servizio essenziale | Fotografie di progetto, livelli geografici e documenti aziendali | Quali dati sono autentici, senza dedurre accessi ai controlli fisici? |

| Pubblicazione | Ruolo generale | Affermazione pubblicizzata | Domanda di verifica |
|---|---|---|---|
| 14 maggio | Piattaforma software legata alle telecomunicazioni | Affermazioni su abbonati, attivazione e controllo | Quale funzione dichiarata può accertare il responsabile del servizio? |
| 18 maggio | Fornitore ICT | Accesso amministrativo e presunta estensione ai clienti | L'accesso ai clienti ha riscontri indipendenti? |

I documenti di progetto di un servizio essenziale non dimostrano il controllo dei processi fisici. Un presunto accesso amministrativo al fornitore non dimostra accessi a tutti i clienti. Queste distinzioni devono comparire nel primo passaggio di consegne, prima che un'etichetta grave diventi una conclusione pubblica.

**Scheda di evidenza B13** — 18 mag 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

I'm selling full access Domain Admin for an Italian company named [supplier removed]. [...]

TRADUZIONE

Vendo accesso completo Domain Admin a un'azienda italiana chiamata [fornitore rimosso]. [...]

**Accertato**
Un'offerta di accesso a un fornitore IT dichiarava anche accessi ulteriori ai clienti.

**Non accertato**
Accessi funzionanti, esposizione dei clienti, furto di dati, vendita o collegamenti a un distinto incidente del fornitore riferito pubblicamente.

**Scheda di evidenza B14** — 14 mag 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

Data Exposed: [...] Subscriber PII [...] Mobile subscriber provisioning records [...]

TRADUZIONE

Dati esposti: [...] Dati personali degli abbonati [...] Registrazioni di attivazione degli abbonati mobili [...]

**Accertato**
Una pubblicazione dichiarava esposizione di dati sugli abbonati e sulle attivazioni, nonché capacità di controllo su una piattaforma software legata alle telecomunicazioni.

**Non accertato**
Autenticità, controllo funzionante, operatori interessati, impatto sui servizi o accessi attuali.

**Scheda di evidenza B15** — 26 apr 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

Data Content: [...] field photos [...] GIS files [...] [project details removed]

TRADUZIONE

Contenuti: [...] fotografie sul campo [...] file GIS [...] [dettagli del progetto rimossi]

**Accertato**
Un venditore pubblicizzava materiale di rilievo, cartografia e consegna degli appaltatori per un progetto idrico.

**Non accertato**
Autenticità, riservatezza, origine dei file o accessi ai sistemi di controllo operativo.

**Scheda di evidenza B16** — 30 gen 2026

**Forum seller** | Forum | Forum | English

ORIGINALE

Admin dashboard includes [...] asking $5k [...]

TRADUZIONE

Il pannello amministrativo include [...] richiesta di $5k [...]

**Accertato**
Un venditore offriva accessi amministrativi nel settore automobilistico e indicava un prezzo richiesto.

**Non accertato**
Accessi funzionanti, ricavi, impatto sui clienti, compromissione dei pagamenti o vendita conclusa.

## 4.7 Trasformare un annuncio in un compito di verifica delimitato

Un passaggio informativo utile indica prodotto dichiarato, organizzazione o ruolo rilevante, data, tipo di fonte ed evidenze mancanti. Identifica il team capace di verificare la rilevanza di account, servizi o dati. L'azione deve essere proporzionata a quella specifica affermazione.

Un segnale su uno specifico account può richiedere un intervento tempestivo sulle identità. Un'offerta generica per più Paesi può richiedere monitoraggio anziché contenimento esteso. Un campione credibile di dati dei clienti può giustificare indicazioni antifrode preventive mentre la fonte resta incerta. Nessuna di queste decisioni richiede di presentare l'affermazione del venditore come incidente nazionale accertato.

PUNTI CHIAVE

**01**

Etichette nazionali e annunci dimostrano osservazioni, non attacchi o vendite concluse.

**02**

Materiale bloccato, scadente o storico richiede limiti espliciti.

**03**

Inviate l'affermazione specifica al team capace di verificarne la rilevanza.

CAPITOLO 05

# Esempi di bersagli e casi per settore

QUESTO CAPITOLO RISPONDE

Quali eventi hanno riscontri, quali restano rivendicazioni e cosa deve fare prima ogni responsabile?

**12**

riferimenti a fonti pubbliche che separano casi, campagne ed esclusioni


5.1 Decisioni settoriali 37

5.2 Schede caso sostenute dalle fonti 40

5.3 Campagne e un'esclusione documentata 47

5.4 Chiudere il percorso con il responsabile 48

CAPITOLO 05

# Esempi di bersagli e casi per settore

IN SINTESI

I casi confermati mostrano interruzioni, accessi non autorizzati e conseguenze sui fornitori. Altre notizie restano rivendicazioni, interpretazioni contestate o incidenti precedenti comunicati più tardi. I casi mantengono queste distinzioni, anche quando un'organizzazione conferma l'evento ma non il furto dei dati o l'identità dell'attore. Assegnate un responsabile dalla tabella della prima risposta, poi verificate il limite del caso prima di agire.

## 5.1 Decisioni settoriali

La tabella collega ogni problema a una verifica. È una guida basata sui casi, non un confronto dei tassi di incidente settoriali.

### Istruzione

EVIDENZA

Ransomware universitario confermato e avviso di ripristino

SIGNIFICATO

Ripristino e valutazione del rischio sui dati richiedono registri distinti

PRIMA RISPOSTA

Provare i processi degli studenti e amministrativi dopo il ripristino

### Cloud e ICT

EVIDENZA

Interruzione del fornitore e cifratura di un'area condivisa

SIGNIFICATO

I processi dei clienti possono dipendere dalla risorsa coinvolta

PRIMA RISPOSTA

Provare un percorso di ripristino separato per quella dipendenza

## Sanità

EVIDENZA

Resoconti su incidente, ripristino e comunicazioni ai pazienti

SIGNIFICATO

Cure ripristinate ed esposizione dei dati amministrativi richiedono decisioni distinte

PRIMA RISPOSTA

Verificare le cure e riconciliare ambito dei dati e comunicazioni

## Commercio

EVIDENZA

Accessi confermati ai recapiti dei soci

SIGNIFICATO

Attività commerciale ed esposizione dei dati possono coesistere

PRIMA RISPOSTA

Verificare i contatti inattesi con i clienti tramite canali noti

## Cultura

EVIDENZA

Incidente amministrativo con contestazione di rivendicazioni più ampie

SIGNIFICATO

Un disservizio IT non dimostra perdita di sicurezza fisica

PRIMA RISPOSTA

Confermare ogni effetto dichiarato con il gestore

## Progetti di trasporto

EVIDENZA

Risposta aziendale citata; lavori dichiarati in corso

SIGNIFICATO

IT degli uffici e lavori fisici sono affermazioni diverse

PRIMA RISPOSTA

Verificare separatamente dipendenze aziendali e ingegneristiche

## Servizi essenziali

EVIDENZA

Ripristino dopo interruzioni delle funzioni aziendali

SIGNIFICATO

Gli effetti amministrativi non dimostrano interruzioni dell'erogazione

PRIMA RISPOSTA

Ottenere accettazioni separate dai responsabili aziendali e dei processi

## Servizi finanziari

EVIDENZA

Campagne ufficiali di phishing e frodi segnalate

SIGNIFICATO

La frode può sfruttare processi di approvazione legittimi

PRIMA RISPOSTA

Confermare istruzioni modificate fuori dal canale richiedente

### Servizi pubblici

EVIDENZA

Avvisi ufficiali su phishing di caselle e identità

SIGNIFICATO

Mittenti e marchi fidati possono essere abusati

PRIMA RISPOSTA

Esaminare sessioni e modifiche al recupero degli account

### Scuole

EVIDENZA

Messaggi minacciosi senza intrusioni accertate

SIGNIFICATO

La sicurezza delle comunicazioni richiede comunque azioni

PRIMA RISPOSTA

Conservare i messaggi e attivare il referente della polizia

## 5.2 Schede caso sostenute dalle fonti

I riferimenti P identificano materiale dei casi da fonti pubbliche. Sono parafrasi degli analisti, non citazioni clandestine. Un caso può contenere affermazioni con riscontri diversi. Le date degli aggiornamenti non creano ulteriori incidenti.

CASO G

### Ripristino universitario confermato dopo il ransomware (P01)

Istruzione

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | Sapienza Università di Roma conferma che il ransomware è iniziato il 1 febbraio 2026. Il suo avviso di aprile descrive effetti su riservatezza e disponibilità. [S5] |
| CRONOLOGIA | Le prime notizie descrivevano lo spegnimento precauzionale della rete e il ripristino con ACN. La chiusura è avvenuta il 2 aprile ed è stata comunicata internamente il 9 aprile. [S6][S5] |

| | |
|---|---|
| ACCERTATO | Sono stati coinvolti circa 400 server fisici e virtuali. Portali universitari e servizi agli studenti sono stati interrotti. I dati interessati sono stati cifrati. [S5] |
| LIMITI | L'università non ha trovato evidenze di furto, diffusione pubblica o uso fraudolento dei dati specificati. Il suo avviso non identifica un attore. [S5] |
| RISPOSTA | Separate ripristino e valutazione dei dati personali. Provate processi degli studenti, finanziari e amministrativi, verificate le registrazioni e conservate un elenco datato delle domande irrisolte sull'esposizione. |

**Conclusione**

Separate ripristino e valutazione dei dati personali. Provate processi degli studenti, finanziari e amministrativi, verificate le registrazioni e conservate un elenco datato delle domande irrisolte sull'esposizione.

Il caso sostiene il lavoro di ripristino senza una ricostruzione speculativa sull'attore. Incidenti concomitanti altrove non dimostrano una via di accesso o un operatore comuni. La chiusura richiede un servizio provato e una valutazione aggiornata del rischio sui dati, non soltanto un ticket infrastrutturale.

CASO H

H

## Un incidente del fornitore raggiunge un processo pubblico di pagamento (P02)

Cloud e servizi pubblici

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | Un fornitore cloud ha riconosciuto un incidente del 23 marzo. La stampa ha collegato l'interruzione a un servizio comunale di pagamento delle sanzioni. [S24][S25] |
| CRONOLOGIA | Le notizie di aprile descrivevano difficoltà nei pagamenti e indagini coordinate dalla procura, affidate alla Polizia Postale. I termini di pagamento sono stati prorogati. [S25] |
| RIVENDICAZIONE | Il collegamento con Qilin compare nella stampa come rivendicazione criminale. Riconoscere un'interruzione non dimostra indipendentemente l'identità dell'attaccante. [S24] |
| LIMITI | Le prime dichiarazioni non dimostravano estrazioni. Gli ambienti del fornitore e del cliente richiedono esami separati. |
| RISPOSTA | Identificate la dipendenza interrotta e le transazioni da riconciliare. Provate una via alternativa e verificate gli accessi dei clienti dopo il ripristino. |

**Conclusione**

Identificate la dipendenza interrotta e le transazioni da riconciliare. Provate una via alternativa e verificate gli accessi dei clienti dopo il ripristino.

I clienti hanno bisogno di informazioni sufficienti a decidere se sospendere un processo, offrire una via manuale o cambiare una scadenza. Il contratto deve identificare chi fornisca questi fatti e come gli aggiornamenti raggiungano i clienti durante un disservizio.

CASO I

## I ■ Un museo contesta interpretazioni più ampie (P03)

Cultura

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | La stampa di febbraio citava il resoconto di un museo su un incidente IT amministrativo. Le visite e diverse funzioni per i visitatori risultavano operative. [S23] |
| NOTIZIE SUCCESSIVE | Ad aprile la stampa descriveva un'indagine per tentata estorsione e affermazioni su informazioni di sicurezza. Il museo contestava l'esistenza di riscontri per quelle affermazioni. [S23] |
| LIMITE ACCERTATO | Il museo dichiarava che gli spostamenti delle collezioni citati erano programmati per lavori edilizi. Non devono diventare una conseguenza informatica dimostrata. [S23] |
| ALTERNATIVE | Un incidente amministrativo reale, un'affermazione sul possesso di dati e una descrizione inesatta delle conseguenze fisiche possono coesistere. |
| RISPOSTA | Confermate con il gestore gli effetti su risorse e servizi. Evitate di amplificare dettagli di sicurezza fisica. Distinguete l'IT indisponibile dall'esposizione informativa accertata. |

**Conclusione**

Confermate con il gestore gli effetti su risorse e servizi. Evitate di amplificare dettagli di sicurezza fisica. Distinguete l'IT indisponibile dall'esposizione informativa accertata.

Un'indagine dimostra che le accuse sono esaminate, non tutte le affermazioni di un resoconto. Questa distinzione impedisce inoltre ai comunicatori di ripetere come propria conclusione la pressione desiderata dall'attore.

CASO J

## J ■ Un servizio essenziale ripristina le funzioni aziendali (P04)

Servizi essenziali

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | La dichiarazione pubblica di Alto Calore data l'attacco al 9 agosto. L'aggiornamento del 16 settembre annuncia il ritorno alle attività aziendali, con lavoro ancora da svolgere. [S26] |
| LIMITE ACCERTATO | |

L'avviso riguarda le funzioni aziendali. Non dimostra interruzioni fisiche dell'acqua né l'identità di un attore.

| | |
|---|---|
| ALTERNATIVE | Sistemi amministrativi e processi operativi possono avere stati di ripristino diversi. Altre notizie usano una data diversa di agosto. Il caso mantiene quella della dichiarazione ufficiale. |
| RISPOSTA | Ottenete accettazioni separate dai responsabili aziendali e dei processi. Verificate fatturazione, registrazioni dei clienti e ordini di lavoro insieme alle comunicazioni operative. |

**Conclusione**

Ottenete accettazioni separate dai responsabili aziendali e dei processi. Verificate fatturazione, registrazioni dei clienti e ordini di lavoro insieme alle comunicazioni operative.

La continuità delle operazioni fisiche non elimina l'interruzione aziendale. Il ripristino degli accessi amministrativi non dimostra che ogni registrazione sia completa. Un registro del ripristino deve nominare funzione, verifica e responsabile che accetta l'esito. [S26]

K

CASO K

## La sanità ripristina i servizi e separa le domande sull'esposizione (P05)

Sanità

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | La Direzione di un gruppo sanitario regionale conferma un incidente del 31 agosto. Il primo resoconto descrive IT, telefoni ed email indisponibili. [S27] |
| RESOCONTO OPERATIVO | Rai ha riferito appuntamenti interrotti e lavoro manuale. Alcune attività continuavano: il caso non dimostra che tutte le cure si siano fermate. [S28] |
| AGGIORNAMENTO | Una dichiarazione successiva della Direzione riferisce il ripristino di contatti, attività ambulatoriale e sale operatorie. Identifica INC Ransom e dichiara che non sono stati pagati né negoziati riscatti. [S29] |
| AGGIORNAMENTO SULL'ESPOSIZIONE | Il servizio Rai del 17 novembre descrive lettere ai pazienti datate 16 ottobre che confermano la pubblicazione online di alcune informazioni amministrative. Elenca nomi, date di nascita, prestazioni ricevute, medici e importi pagati. [S71] |
| LIMITI | Rai cita il responsabile della protezione dei dati del fornitore: descrive una parte circoscritta dell'archivio e comunicazioni postali individuali. Il fornitore distingue documenti amministrativi e referti clinici. La distinta rivendicazione sui file pubblicizzati in B08 resta non verificata. [S71][S1] |

| | |
|---|---|
| RISPOSTA | Verificate cure sicure e riconciliate documenti cartacei ed elettronici. Provate comunicazioni indipendenti dall'ambiente coinvolto. Il responsabile privacy deve riconciliare l'esposizione dei dati riferita, la popolazione interessata e lo stato delle comunicazioni. |

**Conclusione**

Verificate cure sicure e riconciliate documenti cartacei ed elettronici. Provate comunicazioni indipendenti dall'ambiente coinvolto. Il responsabile privacy deve riconciliare l'esposizione dei dati riferita, la popolazione interessata e lo stato delle comunicazioni.

La continuità clinica richiede criteri di accettazione che i soli piani aziendali possono trascurare. Confermate riconciliazione delle registrazioni, contatti del personale e accesso alle informazioni critiche dei pazienti. Sono verifiche raccomandate, non accuse che il gruppo non le abbia svolte.

Una notizia separata del 16 novembre cita un dirigente sanitario regionale. Conferma attività anomala nel sistema di prenotazione segnalata il 5 novembre e relative contromisure. Estensione dell'accesso ai dati e rapporto con altri problemi di prenotazione restavano sotto indagine. È un'altra comunicazione, non la prova che tutti i problemi derivassero dalla stessa intrusione o dal Case K. [S64]

L

CASO L

## Accesso ai recapiti senza furto accertato di dati di pagamento (P06)

Commercio

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | Unicoop Firenze ha confermato accessi a un sistema di gestione dei soci e ad alcuni recapiti. Ha dichiarato l'isolamento dei server coinvolti e la notifica alle autorità. [S7] |
| STATO DEI SERVIZI | La dichiarazione indica che i servizi aziendali continuavano. Le informazioni sulla sicurezza escludono il coinvolgimento di password, PIN, codici di accesso e dati delle carte di pagamento. [S7][S8] |
| DENOMINATORE | Il totale dei soci non è un conteggio confermato delle persone interessate. Un titolo sul numero dei soci non fornisce il denominatore mancante dell'incidente. [S9] |
| LIMITI | L'avviso non dimostra collegamenti con distinti incidenti di refrigerazione o una campagna internazionale. |
| RISPOSTA | Avvertite delle richieste inattese che usano recapiti familiari. Confermate istruzioni su account o pagamenti tramite canali noti e aggiornate i consigli al cambiare dell'ambito. |

**Conclusione**

Avvertite delle richieste inattese che usano recapiti familiari. Confermate istruzioni su account o pagamenti tramite canali noti e aggiornate i consigli al cambiare dell'ambito.

L'avviso del 17 novembre rientra nell'attività recente. La data di pubblicazione non dimostra il primo accesso. L'assistenza ai clienti deve mantenere questa distinzione quando risponde su quali contatti richiedano indicazioni.

CASO M

M

## Le notizie sui documenti mescolano denominatori diversi (P07)

Servizi aziendali

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| **CONFERMA** | I giornalisti hanno ottenuto conferma aziendale di un incidente che coinvolgeva un numero contenuto di persone. La stampa associava il materiale a un fornitore di servizi digitali. [S31][S32] |
| **MATERIALE OSSERVATO** | Una testata descriveva contratti e registrazioni anagrafiche in un archivio. Sono osservazioni giornalistiche, non totali delle persone interessate confermati dall'azienda. [S32] |
| **LIMITI** | Contratti e registrazioni possono sovrapporsi. Non possono essere sommati né trasformati in totali di conti bancari attuali. La modalità di estrazione riferita resta irrisolta. |
| **ALTERNATIVE** | I documenti possono provenire da un servizio, partner, esportazione o processo precedente. Un archivio pubblicato non identifica indipendentemente l'estrazione. |
| **RISPOSTA** | Verificate categorie documentali e rapporti tra servizi prima delle decisioni di notifica. Avvertite delle richieste che usano veri dettagli contrattuali per ottenere password o approvazioni. |

### Conclusione

Verificate categorie documentali e rapporti tra servizi prima delle decisioni di notifica. Avvertite delle richieste che usano veri dettagli contrattuali per ottenere password o approvazioni.

La familiarità dei documenti può rendere convincente un contatto fraudolento senza attribuire autorità legittima a chi chiama. La risposta deve identificare ciò che il chiamante potrebbe sapere, poi proteggere la decisione che quelle informazioni potrebbero influenzare.

CASO N

## N ■ Una società di progetto separa la risposta IT dai lavori (P08)

Trasporti e costruzioni

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| CONFERMA | La stampa cita una società di progetto dei trasporti che descrive isolamento, assistenza specialistica e notifica alle autorità. Dichiarava che attività operative e lavori non erano stati coinvolti. [S30] |
| CRONOLOGIA | L'evento riferito era di ottobre, con comunicazione più ampia a novembre. La comunicazione successiva non crea una nuova intrusione. [S30] |
| RIVENDICAZIONE | Collegamento a un gruppo criminale e volume dei dati erano riportati con riserve. La fonte non li presentava come risultati accertati. |
| LIMITI | Un'indagine non è un'attribuzione finale. Comunicazioni d'ufficio, sistemi ingegneristici e lavori fisici richiedono evidenze distinte. |
| RISPOSTA | Verificate accessi ai documenti di progetto, identità degli appaltatori e registrazioni ingegneristiche approvate. Ottenete conferma dai responsabili dei processi indipendentemente dal ripristino dei sistemi d'ufficio. |

### Conclusione

Verificate accessi ai documenti di progetto, identità degli appaltatori e registrazioni ingegneristiche approvate. Ottenete conferma dai responsabili dei processi indipendentemente dal ripristino dei sistemi d'ufficio.

CASO O

## O ■ L'archiviazione condivisa produce conseguenze per i clienti (P09)

Servizi ICT

Incidente confermato dalla fonte; si applicano limiti

| | |
|---|---|
| RESOCONTO UFFICIALE | ACN descrive la cifratura di un'area condivisa presso un fornitore ICT, con effetti sui clienti che la utilizzavano. [S13] |
| ASSOCIAZIONE | Il rapporto associa Titan all'incidente. L'attribuzione della fonte non si estende a ogni cliente o all'intero ambiente. |
| LIMITI | Il passaggio non fornisce un totale dei clienti né una data precisa dell'evento. Non si presume che coincida con un altro caso nominato. |
| RISPOSTA | Mappate la risorsa dietro ogni servizio importante. Provate separazione degli accessi, accessi al ripristino e accettazione da parte di ogni cliente con un'esercitazione autorizzata. |

**Conclusione**

Mappate la risorsa dietro ogni servizio importante. Provate separazione degli accessi, accessi al ripristino e accettazione da parte di ogni cliente con un'esercitazione autorizzata.

## 5.3 Campagne e un'esclusione documentata

Una copertura utile comprende campagne ed esclusioni. Questi riferimenti aiutano a decidere senza creare altre vittime confermate.

P

CASO P

### Caselle pubbliche trasportano un'esca per le credenziali (P10)

Amministrazione pubblica

Campagna riferita

| | |
|---|---|
| OSSERVAZIONE UFFICIALE | CERT-AGID descrive caselle pubbliche abusate per distribuire messaggi a tema documentale ai precedenti corrispondenti, usando un servizio legittimo di collaborazione. [S17] |
| ACCERTATO | La fonte sostiene l'abuso delle caselle e la ricerca di credenziali. Non dimostra intrusioni nella piattaforma di collaborazione o in ogni organizzazione destinataria. |
| ALTERNATIVE | Una corrispondenza familiare può riflettere una storia reale mentre il messaggio attuale è fraudolento. Familiarità del mittente e fiducia nella destinazione sono decisioni distinte. |
| RISPOSTA | Esaminate accessi, sessioni, inoltro e modifiche al recupero. Avvertite separatamente i corrispondenti e accertate se i destinatari abbiano inserito credenziali. |

**Conclusione**

Esaminate accessi, sessioni, inoltro e modifiche al recupero. Avvertite separatamente i corrispondenti e accertate se i destinatari abbiano inserito credenziali.

Q

CASO Q

### Pacchetti identificativi creano possibili frodi successive (P11)

Identità e frodi

Campagna riferita

| | |
|---|---|
| OSSERVAZIONE UFFICIALE | CERT-AGID descrive smishing a tema sussidi che cerca informazioni su identità, reddito e lavoro. Distingue la raccolta dai possibili usi successivi. [S18] |

| | |
|---|---|
| INTERPRETAZIONE | Le informazioni potrebbero sostenere altre impersonificazioni o domande di credito. La fonte non dimostra un prestito o una perdita bancaria. |
| LIMITI | Furto di documenti e apertura di un conto finanziario sono popolazioni diverse. Il rapporto non deduce incassi criminali conclusi. |
| RISPOSTA | Provate apertura e recupero usando informazioni sintetiche considerate note all'attaccante. Inviate le esposizioni autentiche di documenti ai processi antifrode e di identità. |

**Conclusione**

Provate apertura e recupero usando informazioni sintetiche considerate note all'attaccante. Inviate le esposizioni autentiche di documenti ai processi antifrode e di identità.

R

CASO R

### Un disservizio tecnico viene escluso (P12)

Servizi pubblici

Disservizio tecnico escluso

| | |
|---|---|
| RESOCONTO UFFICIALE | Una risposta ministeriale parlamentare attribuisce l'interruzione della rete giudiziaria del 6 maggio a un guasto tecnico del fornitore, non a un attacco o a un'intrusione. [S46] |
| LIMITE | Indisponibilità e intrusione informatica non sono sinonimi. La risposta non risolve incidenti distinti presso fornitori. |
| RISPOSTA | Conservate un campo sulla causa e le evidenze che la sostengono. Documentate perché sia stata chiusa una prima ipotesi di attacco. |

**Conclusione**

Conservate un campo sulla causa e le evidenze che la sostengono. Documentate perché sia stata chiusa una prima ipotesi di attacco.

## 5.4 Chiudere il percorso con il responsabile

Per ogni caso, il responsabile dell'incidente deve indicare funzione interessata, evidenze attuali e verifica successiva. Usate uno stato datato anziché un'etichetta permanente copiata da un primo titolo. Documentate se la rivendicazione criminale sia stata effettivamente associata all'evento.

La stessa disciplina serve quando le evidenze indeboliscono una notizia. Manutenzione, comunicazioni precedenti o attribuzioni sbagliate devono restare nel registro di revisione con il motivo dell'esclusione. Togliere un evento dal totale delle minacce non significa che non sia stato necessario rispondere.

PUNTI CHIAVE

01

Confermate separatamente effetti sui servizi, ambito dei dati e identità dell'attore.

02

Gli aggiornamenti modificano un caso esistente, anziché creare un incidente.

03

Un'esclusione documentata rafforza la copertura quando il motivo è esplicito.

CAPITOLO 06

# Hacktivismo, DDoS e attività recente

QUESTO CAPITOLO RISPONDE

Cosa hanno dichiarato gli autori, cosa hanno accertato le autorità e cosa è cambiato vicino alla chiusura?

## 9-22 Nov

periodo recente fino alla rilevazione


6.1 Cronologia di tipi distinti di evidenze 51
6.2 Rivendicazioni olimpiche ed effetti ufficiali 52
6.3 Le ondate successive richiedono nuove evidenze 53
6.4 Attività recente: 9-22 novembre 55
6.5 I controlli fisici richiedono un responsabile del processo 56
6.6 Preparare una comunicazione pubblica che resista ai nuovi fatti 57

CAPITOLO 06

# Hacktivismo, DDoS e attività recente

IN SINTESI

Nel periodo olimpico le rivendicazioni erano visibili. ACN riferiva effetti limitati sui siti e nessun impatto sul regolare svolgimento delle gare o sui servizi essenziali dell'evento. I resoconti successivi distinguono tentativi di interruzione e intrusioni. Le comunicazioni recenti aggiungono dubbi su recapiti e documenti. I messaggi minacciosi restano separati dagli accessi ai sistemi. Confermate la funzione coinvolta, mantenete le rivendicazioni esterne come tali e preparate un canale alternativo sullo stato dei servizi.

## 6.1 Cronologia di tipi distinti di evidenze

Le date seguenti identificano pubblicazioni o eventi esplicitamente datati. Le descrizioni mantengono la distinzione. Rivendicazioni degli attori, ripubblicazioni di terzi e resoconti ufficiali hanno etichette separate.

| | |
|---|---|
| 4 feb 2026 | **Ministro degli Esteri, secondo AP**<br>Dichiara sventati gli attacchi contro siti diplomatici e olimpici; l'origine è una sua caratterizzazione |
| 17 feb 2026 | **Bollettino CSIRT Italia, ripubblicato a livello regionale**<br>Descrive nuove frodi tramite email aziendali contro organizzazioni italiane |
| 6 giu 2026 | **Canale in lingua spagnola**<br>Attribuisce rivendicazioni su bersagli italiani a NoName057(16); nessuna pubblicazione primaria dell'attore o interruzione verificata accertata |
| 31 ago 2026 | **Direzione sanitaria, riprodotta dalla stampa**<br>Conferma un incidente; avvisi successivi distinguono ripristino e domande sui dati |
| 8 ott 2026 | **Ministero degli Esteri**<br>Dichiara mitigato l'attacco al sito senza disservizi; l'avviso non nomina attori |
| 12 ott 2026 | **BDAnonymousTeam**<br>Rivendica attività contro un sito informativo pubblico; effetto non verificato |
| 22 ott 2026 | **BDAnonymousTeam**<br>Rivendica attività contro un sito aeroportuale; effetto non verificato |
| 29 ott 2026 | **Pubblicazioni tradotte di NoName057(16)**<br>Ripetono un'affermazione su un sito legato alla difesa; nessun effetto confermato sui servizi |
| 7 nov 2026 | **Notizie di stampa**<br>Riferiscono la risposta di una società di progetto dei trasporti; i lavori risultano in corso |
| 11 nov 2026 | **Notizie di stampa**<br>Descrivono messaggi minacciosi alle scuole; la consegna non dimostra accessi ai sistemi |
| 16 nov 2026 | **Decisione del Consiglio UE** |

Aggiunge NoName057(16) a un allegato di misure restrittive; la designazione non accerta ogni incidente italiano

| | |
|---|---|
| 16 nov 2026 | **Dirigente sanitario citato da Rai**<br>Conferma precedenti anomalie nelle prenotazioni e contromisure; l'ambito degli accessi resta sotto indagine |
| 17 nov 2026 | **Unicoop Firenze**<br>Conferma alcuni accessi ai recapiti dei soci; i servizi aziendali continuano |
| 17 nov 2026 | **Rai, che cita un responsabile sanitario della protezione dei dati**<br>Riferisce dati amministrativi online e lettere ai pazienti datate 16 ottobre; aggiornamento sull'incidente di agosto |
| 19 nov 2026 | **Conferma aziendale citata dalla stampa**<br>Descrive un incidente circoscritto associato a materiale documentale |
| 19 nov 2026 | **Ministro dell'Interno, informativa parlamentare**<br>Riferisce un attacco informatico alla refrigerazione in Italia il 2 novembre; responsabilità e coordinamento irrisolti [S74] |
| 20 nov 2026 | **Operational Summary ACN di ottobre**<br>Pubblica osservazioni operative e revisioni dei mesi precedenti |

Un annuncio di forum conservato dell'11 novembre associa materiale bloccato a un'organizzazione dei media (B10). È un'evidenza di pubblicazione recente, non un'intrusione recente verificata. Una richiesta separata di un acquirente per log bancari aziendali italiani dimostra domanda, non possesso o un incidente bancario. [S1]

## 6.2 Rivendicazioni olimpiche ed effetti ufficiali

AP ha riferito la dichiarazione del ministro degli Esteri secondo cui gli attacchi contro siti diplomatici e olimpici erano stati sventati. Il ministro ne caratterizzava l'origine come russa senza fornire in quel resoconto un'attribuzione tecnica dettagliata. Il rapporto mantiene la sua attribuzione, senza assegnare indipendentemente un operatore statale. [S11]

ACN distingue gli effetti sui siti dal regolare svolgimento dell'evento. Nella sintesi della campagna DDoS di febbraio 2026, ACN ha riportato indisponibilità temporanea dei siti per il 6% degli eventi registrati. Non è un tasso di successo di ogni rivendicazione né una misura di tutti i DDoS nazionali. [S10]

| Punto | Versione dell'autore | Resoconto ufficiale | Valutazione |
|---|---|---|---|
| Bersagli | Pubblicazioni e notizie nominavano siti diplomatici e dell'evento | Il ministro descriveva tentativi; ACN tratta i DDoS collegati all'evento | Verificare privatamente ogni servizio |
| Effetto sui siti | Gli autori presentavano i disservizi come un risultato | ACN registra indisponibilità temporanea per una minoranza di eventi DDoS | Popolazioni diverse non possono diventare un rapporto numerico |
| Effetto sull'evento | Le rivendicazioni sui siti attiravano attenzione sull'evento | ACN dichiara gare regolari e servizi essenziali non interessati | Gli effetti sui siti non dimostrano interruzioni dell'evento |
| Attribuzione | I resoconti citati non identificano un alias specifico dell'autore delle rivendicazioni | Il ministro caratterizzava l'origine senza una base tecnica pubblica dettagliata | Mantenere l'attribuzione della fonte e l'identità irrisolta dell'operatore |
| Dati | Le rivendicazioni di disservizi non dimostravano accessi | Il resoconto citato non accerta furti derivanti da queste rivendicazioni | Valutare accuse separate sui dati con evidenze proprie |

Verificate privatamente il servizio preciso, ottenete la telemetria del fornitore e confermate il percorso dell'utente. Indicate il tentativo, l'esperienza degli utenti e l'azione successiva. Una risposta proporzionata non richiede di accettare cifre infondate degli attori o pubblicare un elenco esteso dei servizi coinvolti.

## 6.3 Le ondate successive richiedono nuove evidenze

ACN riferisce nuovi DDoS hacktivisti a fine maggio, con indisponibilità o rallentamenti generalmente temporanei. Il resoconto di agosto non riporta campagne particolarmente significative nella visione nazionale di quel mese. Nessuna delle due osservazioni dimostra l'assenza di attività minori. [S14][S13]

L'avviso del Ministero degli Esteri dell'8 ottobre dichiara un attacco mitigato senza disservizi e verifiche sui siti diplomatici e consolari. Non nomina NoName057(16), la Russia o un'intrusione riuscita. Notizie successive non possono fornire retroattivamente un'attribuzione assente da quell'avviso. [S12]

Una ripubblicazione conservata in lingua spagnola del 6 giugno attribuisce a NoName057(16) rivendicazioni su bersagli italiani. Dimostra la ripubblicazione, non una pubblicazione originale conservata dell'attore né un'interruzione, durata o effetto verificati. Non contraddice la dichiarazione più circoscritta di ACN su campagne particolarmente significative in un periodo diverso. [S1]

Scheda di evidenza B17 — 6 giu 2026

**Channel relay** | Canale di ripubblicazione in spagnolo | Telegram | Spanish

ORIGINALE

Comenzamos el día con ciberataques a Italia [...]

TRADUZIONE

Iniziamo la giornata con attacchi informatici all'Italia [...]

**Accertato**

Una ripubblicazione in spagnolo attribuiva a NoName057(16) rivendicazioni contro portali pubblici italiani e altre organizzazioni.

**Non accertato**

Una pubblicazione originale dell'attore, interruzioni verificate, durata, causa, impatto o identità dell'operatore.

Le pubblicazioni conservate di ottobre comprendono anche rivendicazioni su un sito informativo pubblico e un sito aeroportuale sotto il nome BDAnonymousTeam. Successive pubblicazioni tradotte di NoName057(16) ripetono un'affermazione su un sito legato alla difesa. Sono affermazioni distinte, senza effetti operativi confermati o collegamenti tecnici comuni accertati qui. Non ampliano la dichiarazione ministeriale ufficiale dell'8 ottobre. [S1]

Un nome può ricorrere, cambiare amministratori o essere adottato da un altro autore. La ricomparsa da sola non dimostra continuità dell'operatore o dell'infrastruttura. I team di analisi devono mantenere le evidenze dietro ogni associazione, senza presumere che ogni pubblicazione successiva appartenga alla stessa operazione.

## NoName057(16)

Autore di rivendicazioni DDoS | Filorusso, secondo la descrizione del Consiglio UE [S63]

### IN ITALIA, 2026

**6 giugno**

Un canale in spagnolo ripubblica rivendicazioni su bersagli italiani, B17

**16 novembre**

Il Consiglio UE aggiunge il gruppo all'elenco delle misure restrittive informatiche

### BERSAGLI DICHIARATI

Siti italiani indicati nelle rivendicazioni e ripubblicazioni conservate

### NELLE LORO PAROLE

"[Traduzione della ripubblicazione] Iniziamo la giornata con attacchi informatici all'Italia [...]" B17

### NELLE FONTI PUBBLICHE

[S1] B17 conserva una ripubblicazione delle rivendicazioni, non un'interruzione verificata indipendentemente

[S63] La decisione (PESC) 2026/2546 del Consiglio aggiunge il soggetto; la caratterizzazione resta attribuita alla fonte

LA NOSTRA VALUTAZIONE

La ripubblicazione conservata dimostra una rivendicazione, non un'interruzione verificata o l'identità dell'operatore. La designazione del Consiglio non accerta la responsabilità per singoli incidenti italiani.

CONFIDENZA

Alta per la ripubblicazione conservata e la designazione pubblicata dal Consiglio; responsabilità ed effetti restano non verificati per le rivendicazioni italiane ripubblicate

## 6.4 Attività recente: 9-22 novembre

La vista recente dei forum usa lo stesso filtro con etichetta Italia e conserva 195 pubblicazioni distinte datate 9-22 novembre 2026, sottoinsieme delle 839 pubblicazioni di forum conservate in §4.1. Sono pubblicazioni delle fonti, non incidenti verificati o necessariamente attività nuove. La vista non dimostra copertura nazionale completa del mercato clandestino. Convalidate account, dati o servizio pubblicizzati prima dell'escalation. [S1]

Le osservazioni dei forum comprendono offerte di amministrazione di tenant, elenchi di contatti aziendali e strumenti di phishing a tema bancario. [S1] Un tenant è l'ambiente gestito di un'organizzazione all'interno di un servizio cloud. L'amministrazione del tenant consiste nella gestione di quell'ambiente. [S73] Gli annunci non dimostrano un'intrusione attuale presso un'organizzazione selezionata. L'offerta presenta una raccolta di contatti; provenienza e vendita conclusa restano non verificate. [S1]

Il periodo termina alla rilevazione del 22 novembre. Una pubblicazione al suo interno può riguardare un evento precedente. La tabella identifica quindi cosa aggiunga la fonte recente.

| Osservazione | Nuove informazioni | Irrisolto | Responsabile |
|---|---|---|---|
| Avviso della cooperativa | Accesso confermato ai recapiti e continuità dei servizi | Primo accesso e denominatore finale delle persone interessate | Privacy e assistenza clienti |
| Comunicazione sulle prenotazioni sanitarie | Il dirigente conferma precedenti anomalie e contromisure | Ambito dei dati e relazione con altri problemi di prenotazione | Responsabili sanitari e privacy |
| Aggiornamento sanitario (P05) | Rai riferisce lettere ai pazienti e dati amministrativi circoscritti online | Inventario completo dell'esposizione e popolazione interessata | Responsabile privacy |
| Decisione del Consiglio UE | NoName057(16) aggiunto a un allegato di misure restrittive | Responsabilità per un evento italiano specifico | Legale e analisi |
| Notizie sui documenti | Conferma aziendale accanto alle osservazioni giornalistiche sull'archivio | Via di accesso, sovrapposizioni e popolazione finale | Privacy e responsabile del servizio |
| Informativa sulla refrigerazione | Il ministro riferisce un attacco del 2 novembre alla refrigerazione della distribuzione alimentare [S74] | Responsabilità, coordinamento e cause nei singoli siti | Responsabile del processo e risposta |

| Osservazione | Nuove informazioni | Irrisolto | Responsabile |
|---|---|---|---|
| Notizie sulle minacce alle scuole | Messaggi minacciosi e indagini | Attore comune ed eventuali accessi ai sistemi | Sicurezza e referente della polizia |
| Rapporto di ottobre | Quadro operativo nazionale aggiornato | Non misura l'attività conclusa di novembre | Analisi delle minacce |
| Pubblicazioni clandestine | Segnale recente separato conservato | Autenticità e collegamento ai casi ufficiali | Analisi e risposta |

L'aggiornamento sanitario del 17 novembre riguarda l'incidente di agosto del Case K. Rai riferisce lettere datate 16 ottobre e la distinzione del fornitore tra documenti amministrativi e referti clinici. Aggiorna P05; non aggiunge un caso. [S71]

La comunicazione sanitaria del 16 novembre riguarda attività segnalata prima nello stesso mese. La decisione del Consiglio è uno sviluppo giuridico, non un incidente. Entrambe rientrano nell'osservazione recente mantenendo il proprio tipo di evidenza. [S63][S64]

L'avviso della cooperativa del 17 novembre rientra qui. Le precedenti comunicazioni sul progetto dei trasporti sono contesto antecedente. L'informativa sulla refrigerazione del 19 novembre aggiorna le evidenze ufficiali su un evento precedente. La pubblicazione recente non cambia la data dell'evento. [S7][S30][S74]

I messaggi minacciosi richiedono conservazione, segnalazione e comunicazioni sicure. Riceverli non dimostra accessi ai sistemi scolastici. I conteggi di ondate diverse non devono essere sommati senza evidenze di destinatari distinti. Il rapporto non li conta come intrusioni scolastiche confermate. [S36]

## 6.5 I controlli fisici richiedono un responsabile del processo

Una pubblicazione conservata di maggio dichiarava accesso a un'interfaccia italiana di controllo delle piene. Non erano accertati accessi funzionanti o effetti fisici. La rivendicazione è separata dall'offerta di aprile sui dati di un progetto di servizi essenziali. [S1]

Le notizie di inizio novembre trattavano refrigerazione della filiera alimentare e rivendicazioni criminali. Le premesse delle interrogazioni parlamentari registrano preoccupazioni ed eventi riferiti, non risultati tecnici del governo. Non possono accertare indipendentemente attaccante, meccanismo o estensione. [S34]

Il 19 novembre il ministro dell'Interno ha riferito al Parlamento che un attacco informatico del 2 novembre aveva colpito sistemi di refrigerazione della distribuzione alimentare in Italia. Separatamente, ha definito prematuro attribuire la responsabilità a soggetti ostili coordinati. Il suo resoconto nazionale non accerta la causa di ogni singolo malfunzionamento segnalato. [S74]

Il resoconto di un supermercato separato mostra il limite. Il responsabile riferiva variazioni di temperatura e intervento manuale, ma non poteva confermare né escludere un attacco informatico. Quel sito è escluso dal conteggio degli attacchi confermati. Una lettura fisica modificata richiede comunque indagini. [S35]

Separate sicurezza fisica e attribuzione. Usate la procedura sicura manuale o di isolamento approvata dal responsabile del processo. Conservate registrazioni degli accessi e delle sessioni dei manutentori. Verificate indipendentemente stato degli apparecchi e sicurezza dei prodotti. Ripristinare un'impostazione non dimostra che la merce esposta sia rimasta sicura.

Il rapporto non deduce un operatore comune dietro DDoS, minacce, raccolta ostile di dati personali e casi di refrigerazione. Tempi o messaggi politici simili non bastano. Una campagna comune richiede un collegamento concreto verificato rispetto ai singoli eventi.

## 6.6 Preparare una comunicazione pubblica che resista ai nuovi fatti

Una prima dichiarazione utile identifica lo stato verificato del servizio, le incertezze rimanenti e l'azione per gli utenti. Indica il canale del prossimo aggiornamento. Se circola una rivendicazione, descrivetela come affermazione esterna senza ripeterne dimensioni prive di riscontri.

Comunicazione e SOC devono concordare chi verifichi la disponibilità. Il legale deve valutare le notifiche dai fatti accertati. I fornitori devono conoscere la telemetria necessaria ai clienti. Provate questi passaggi quando sito principale e normale canale di messaggistica sono indisponibili.

PUNTI CHIAVE

**01**

Le rivendicazioni sulla disponibilità richiedono evidenze specifiche del servizio e un denominatore definito.

**02**

Una comunicazione recente non dimostra un'intrusione recente.

**03**

Sicurezza fisica, risposta e attribuzione richiedono decisioni distinte.

CAPITOLO 07

# Attori delle minacce ed evidenze dei collegamenti

QUESTO CAPITOLO RISPONDE

Quali attori compaiono nelle evidenze e cosa dimostrano le associazioni?

**286**

registrazioni di rivendicazioni ransomware associate all'Italia nel periodo del rapporto


7.1 Un collegamento probatorio non è un'operazione comune 59
7.2 Le pubblicazioni ransomware restano rivendicazioni 63
7.3 I Paesi comparabili danno contesto, non una classifica del rischio 64
7.4 I tempi di pubblicazione differiscono da quelli dell'intrusione 65
7.5 L'attribuzione dei casi ufficiali resta della fonte 66
7.6 Contesto di spionaggio pubblicato nel 2026 67
7.7 Sfruttamento web e phishing richiedono verifiche diverse 68

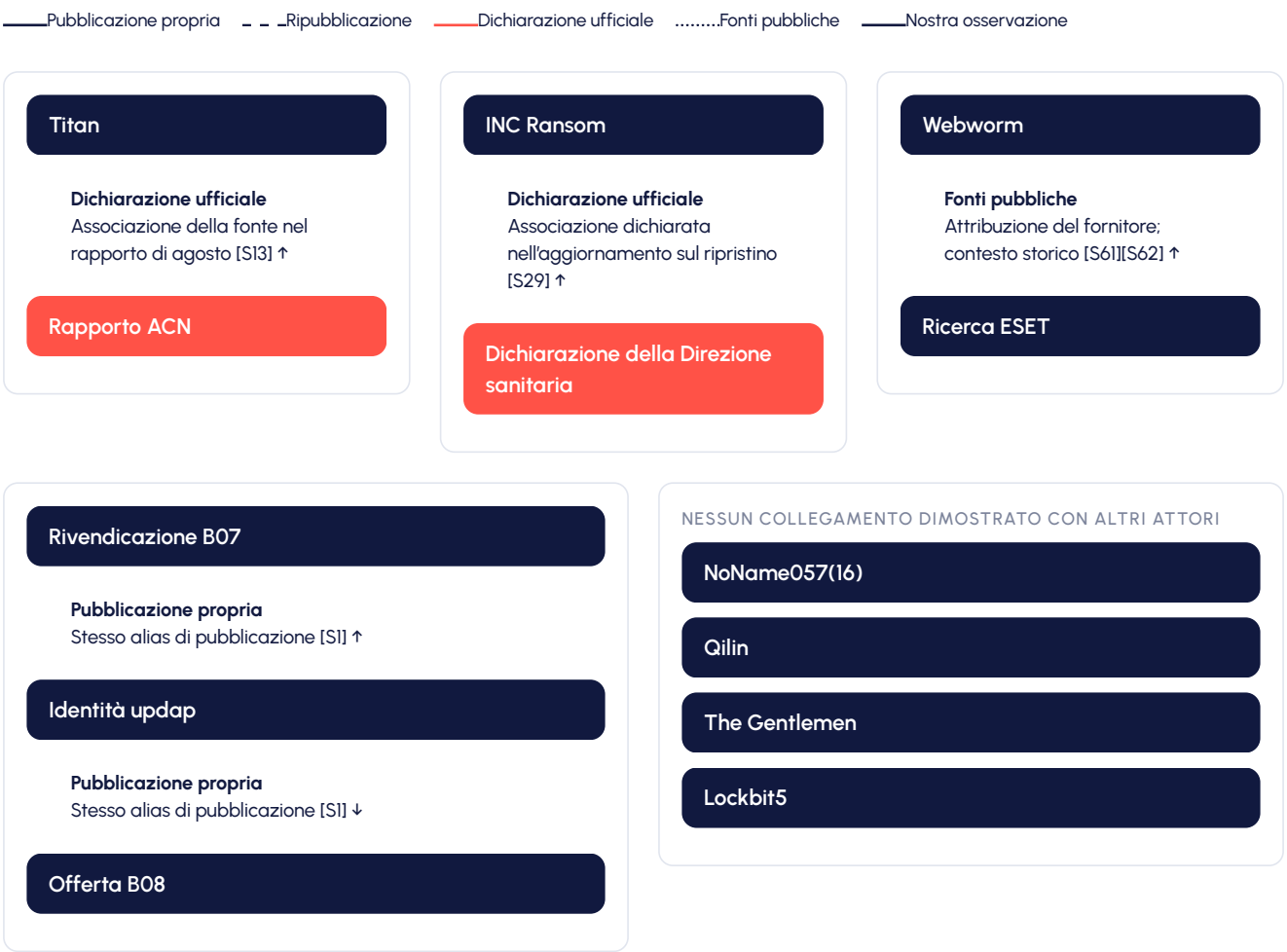
CAPITOLO 07

# Attori delle minacce ed evidenze dei collegamenti

IN SINTESI

Ransompedia registra numerosi marchi estorsivi che nominano organizzazioni associate all'Italia. Sono registrazioni di pubblicazioni, non intrusioni verificate indipendentemente. L'attribuzione hacktivista resta collegata a ogni autore o autorità citata. Gli avvisi di phishing descrivono spesso comportamenti senza identificare un operatore. Usate i nomi degli attori per trovare evidenze rilevanti, poi verificate l'affermazione specifica dell'organizzazione prima di scegliere la risposta.

## 7.1 Un collegamento probatorio non è un'operazione comune




La vista delle relazioni collega una fonte a una rivendicazione osservata, una voce o un caso riferito. Ogni collegamento indica il tipo di evidenza. L'associazione allo stesso Paese, settore o tema politico non dimostra proprietà comune, un operatore condiviso o cooperazione tra gruppi.

La mappa delle relazioni sopra mostra soltanto le attribuzioni delle fonti e l'alias di pubblicazione condiviso che collega B07 e B08. Quando il rapporto discute i servizi di frode come una sequenza possibile, tale sequenza è un modello analitico separato che identifica decisioni sui controlli passibili di abuso. Non afferma che lo stesso venditore abbia fornito documenti, aperto un account e mosso denaro in uno specifico caso osservato. I collegamenti concreti richiederebbero evidenze proprie.

## Qilin

Etichetta di rivendicazioni estorsive | Non valutato

### IN ITALIA, 2026

2026

35 registrazioni italiane nel materiale ransomware conservato

### BERSAGLI DICHIARATI

Organizzazioni nominate dalla fonte delle rivendicazioni

### NELLE FONTI PUBBLICHE

[S2] 35 delle 286 registrazioni italiane

### LA NOSTRA VALUTAZIONE

I conteggi descrivono rivendicazioni estorsive pubbliche. Non dimostrano cifratura, perdite o identità dell'operatore.

CONFIDENZA

Alta per i conteggi delle registrazioni conservate

## The Gentlemen

Etichetta di rivendicazioni estorsive | Non valutato

### IN ITALIA, 2026

2026

32 registrazioni italiane; l'etichetta della fonte è Thegentlemen

### BERSAGLI DICHIARATI

Organizzazioni nominate dalla fonte delle rivendicazioni

### NELLE FONTI PUBBLICHE

[S2] 32 delle 286 registrazioni italiane

### LA NOSTRA VALUTAZIONE

Tenete la verifica di ogni rivendicazione separata dalla reputazione associata al nome del gruppo.

CONFIDENZA
Alta per i conteggi delle registrazioni conservate

## Lockbit5

Etichetta di rivendicazioni estorsive | Non valutato

### IN ITALIA, 2026

2026

28 registrazioni italiane con questa etichetta della fonte

### BERSAGLI DICHIARATI

Organizzazioni nominate dalla fonte delle rivendicazioni

### NELLE FONTI PUBBLICHE

[S2] 28 delle 286 registrazioni italiane

### LA NOSTRA VALUTAZIONE

L'etichetta della fonte resta un'etichetta. Non dimostra indipendentemente continuità con un'altra operazione.

CONFIDENZA
Alta per i conteggi delle registrazioni conservate

## Titan

Associazione ransomware ed etichetta di rivendicazioni | Non valutato

### IN ITALIA, 2026

**Agosto**

ACN associa a Titan un incidente nell'archiviazione condivisa di un fornitore ICT anonimo

**2026**

11 registrazioni italiane nel materiale ransomware

### BERSAGLI DICHIARATI

Un fornitore non nominato e gli archivi dei clienti, secondo ACN

### NELLE FONTI PUBBLICHE

[S13] ACN descrive cifratura con effetti sui clienti che usavano un'area condivisa

[S2] 11 registrazioni italiane

### LA NOSTRA VALUTAZIONE

L'associazione della fonte non dimostra che ogni voce riguardi questo incidente o che lo stesso operatore controlli un altro alias.

CONFIDENZA

Alta per la descrizione ufficiale; collegamenti più ampi non accertati

## INC Ransom

Incidente attribuito dalla fonte ed etichetta di rivendicazioni | Non valutato

### IN ITALIA, 2026

**Settembre**

La Direzione di un operatore sanitario identifica INC Ransom in un aggiornamento sul ripristino

**2026**

7 registrazioni italiane nel materiale ransomware

### BERSAGLI DICHIARATI

Un gruppo sanitario descritto genericamente nel resoconto della Direzione

### NELLE FONTI PUBBLICHE

[S29] Dichiarazione della Direzione ripubblicata dalla stampa locale

[S2] 7 registrazioni italiane

LA NOSTRA VALUTAZIONE

Attribuite l'associazione dell'incidente alla Direzione. Non usate una successiva offerta di forum per dimostrare un nuovo furto o un secondo incidente.

CONFIDENZA

Alta per la dichiarazione conservata; contenuti degli archivi e collegamenti più ampi non verificati

## 7.2 Le pubblicazioni ransomware restano rivendicazioni

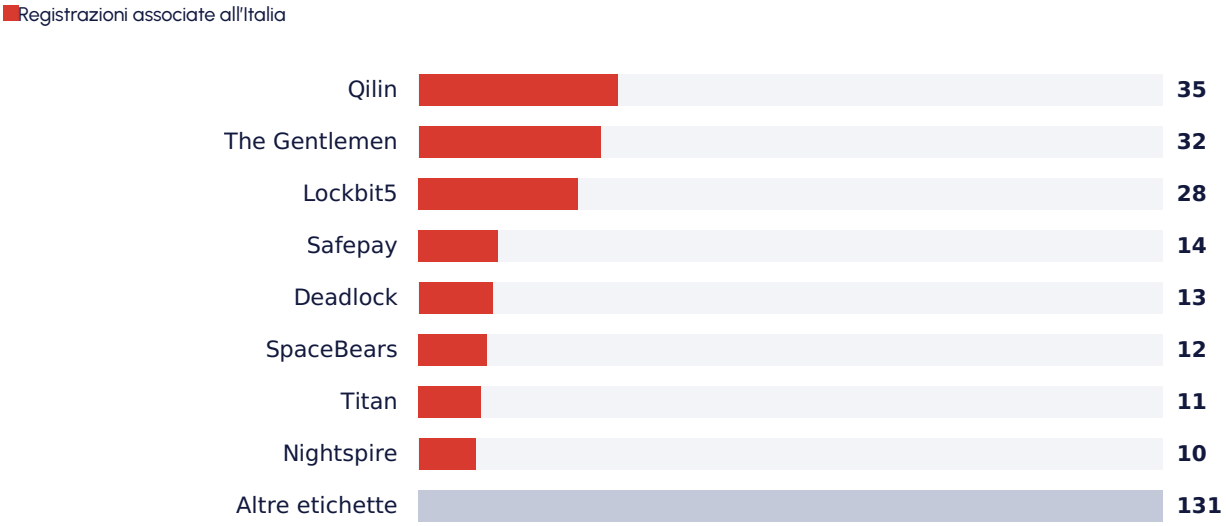
Ransompedia contiene 286 registrazioni associate all'Italia datate nel periodo del rapporto. Contengono 270 valori distinti nei nomi delle vittime e 59 nei nomi dei gruppi. Sono popolazioni di registrazioni della fonte. Nessuno dei conteggi dei nomi distinti è un totale verificato di organizzazioni, operatori o incidenti. Una pubblicazione può ripetere un'affermazione precedente. [S2]

Nel CSV per settore, `distinct_feed_names` conta i valori distinti dei nomi delle vittime all'interno di ciascun settore. I nomi possono ricorrere in più settori, quindi i conteggi settoriali non sono additivi e non vanno sommati. Per l'insieme completo delle registrazioni si usa il conteggio globale di 270. [S2]

Le prime tre etichette dei gruppi rappresentano 95 delle 286 registrazioni, pari al 33,2%. Le altre sono 191, pari al 66,8%. La distribuzione descrive le pubblicazioni monitorate, non la ripartizione del danno ransomware italiano. Non dimostra quale gruppo abbia causato più fermo operativo o perdite finanziarie.

| Etichetta del gruppo | Registrazioni | Lettura |
|---|---|---|
| Qilin | 35 | Pubblicazioni associate all'attore |
| The Gentlemen | 32 | Pubblicazioni associate all'attore |
| Lockbit5 | 28 | Pubblicazioni associate all'attore |
| Safepay | 14 | Pubblicazioni associate all'attore |
| Deadlock | 13 | Pubblicazioni associate all'attore |
| Space Bears | 12 | Pubblicazioni associate all'attore |
| Titan | 11 | Pubblicazioni associate all'attore |
| Nightspire | 10 | Pubblicazioni associate all'attore |
| Altre etichette | 131 | Registrazioni monitorate rimanenti |
| **Totale** | **286** | **Non intrusioni nazionali confermate** |

### Tre etichette di gruppi rappresentano un terzo delle registrazioni associate all'Italia




Fonte: registrazioni Brandefense Ransompedia associate all'Italia, 1 gennaio–22 novembre 2026; novembre parziale. Le date delle pubblicazioni non dimostrano quelle delle intrusioni [S2].

Nel flusso della fonte, The Gentlemen compare come Thegentlemen e Space Bears compare con lo spazio, mentre alcune fonti esterne scrivono SpaceBears. La risposta alla singola registrazione parte da un ruolo e da un'ipotesi sul servizio interessato, non da una dichiarazione automatica di violazione. Verificate la corrispondenza del soggetto con l'organizzazione, le eventuali conferme pubbliche e la possibile origine in un evento precedente. Riconciliate privatamente gli alias prima di trattare nomi ripetuti come organizzazioni distinte.

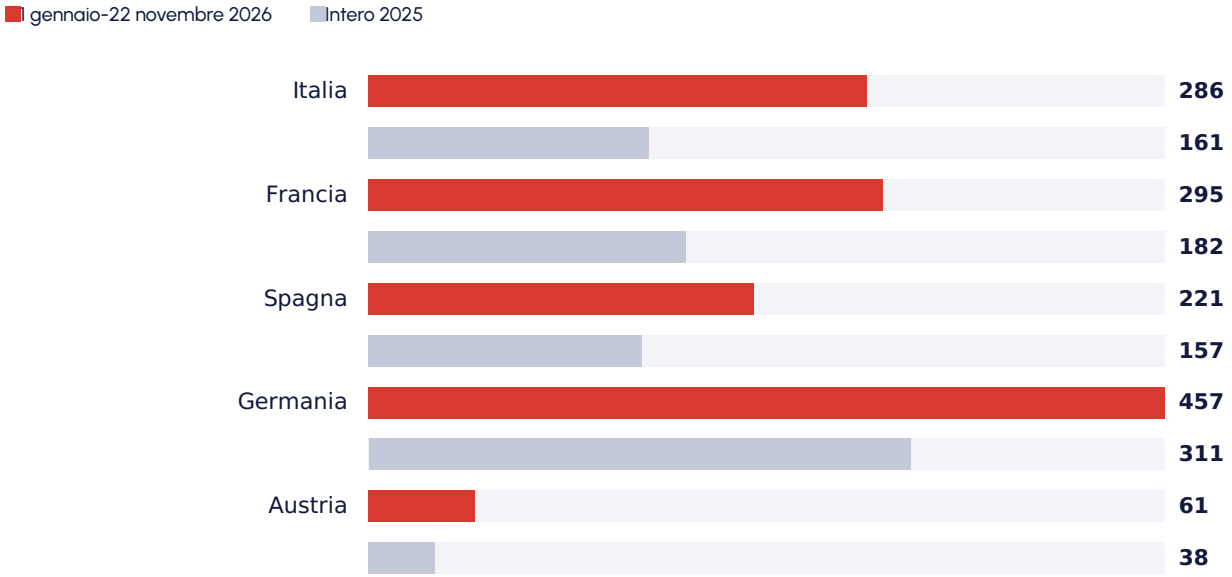
## 7.3 I Paesi comparabili danno contesto, non una classifica del rischio

Francia e Austria offrono contesto sui servizi confinanti e transfrontalieri. La Germania permette il confronto con una grande economia industriale. La Spagna offre un confronto europeo mediterraneo. Sono Paesi scelti per rilevanza, non campioni nazionali equivalenti. Etichette nazionali e copertura delle pubblicazioni richiedono la stessa cautela dell'insieme italiano.

I paesi di confronto sono stati scelti come esempi esclusivamente per fornire un contesto; la loro selezione non implica una classifica né una valutazione politica.

| Paese | Periodo 2026 | Intero 2025 | Interpretazione |
|---|---|---|---|
| Italia | 286 | 161 | Registrazioni associate al Paese |
| Francia | 295 | 182 | Stessa fonte, popolazione nazionale diversa |
| Spagna | 221 | 157 | Stessa fonte, popolazione nazionale diversa |
| Germania | 457 | 311 | Stessa fonte, popolazione nazionale diversa |
| Austria | 61 | 38 | Stessa fonte, popolazione nazionale diversa |

### I conteggi regionali descrivono pubblicazioni monitorate, non la prevalenza nazionale degli incidenti



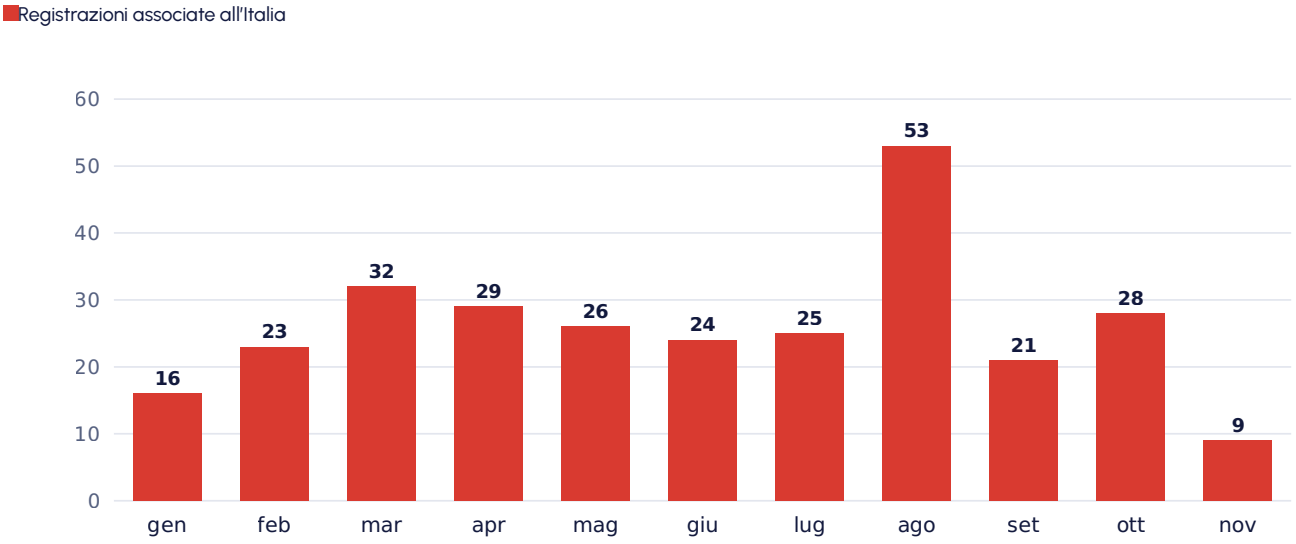

Periodi disuguali e popolazioni nazionali differenti; non è una classifica nazionale del rischio. Fonte: registrazioni Brandefense Ransompedia associate all'Italia, 1 gennaio-22 novembre 2026; novembre parziale. Le date delle pubblicazioni non dimostrano quelle delle intrusioni [S2].

Il periodo 2026 è incompleto; il 2025 è un anno intero. La tabella quindi non calcola tassi di crescita. Popolazioni nazionali, modalità di segnalazione e scelte di pubblicazione degli attori differenti impediscono anche una classifica della sicurezza nazionale. La domanda utile è quali marchi estorsivi ed esempi settoriali meritino monitoraggio per una specifica organizzazione. [S2]

## 7.4 I tempi di pubblicazione differiscono da quelli dell'intrusione

La serie italiana registra 16 voci a gennaio, 23 a febbraio, 32 a marzo e 29 ad aprile. Ne registra 26 a maggio, 24 a giugno, 25 a luglio e 53 ad agosto. Settembre ne ha 21, ottobre 28 e il periodo parziale di novembre 9. Il totale è 286. [S2]

### Agosto ha più pubblicazioni di rivendicazioni; le date di pubblicazione non dimostrano quelle delle intrusioni




Fonte: registrazioni Brandefense Ransompedia associate all'Italia, 1 gennaio–22 novembre 2026; novembre parziale. Le date delle pubblicazioni non dimostrano quelle delle intrusioni [S2].

Le 53 registrazioni di agosto sono il maggior conteggio mensile di pubblicazioni nel periodo della fonte. L'osservazione non dimostra un picco di intrusioni riuscite ad agosto né una causa. Pubblicazioni ritardate, accuse ripetute e variazioni della visibilità sono alternative. Usate le date per ordinare la revisione delle pubblicazioni, non per prevedere probabilità stagionali di attacco.

## 7.5 L'attribuzione dei casi ufficiali resta della fonte

Una Direzione sanitaria identifica INC Ransom nel proprio aggiornamento. ACN associa Titan al caso di un fornitore ICT anonimo. La stampa riferisce la rivendicazione di Qilin per il caso cloud. Queste affermazioni hanno riscontri diversi e devono restare distinte dai totali più ampi dei gruppi in Ransompedia. [S29][S13][S24]

Il rapporto non collega indipendentemente ogni registrazione sotto un'etichetta di gruppo allo stesso operatore tecnico. Non deduce neppure che un incidente confermato convalidi le altre rivendicazioni del gruppo. Per la risposta contano comportamenti e risorse coinvolte, più dell'importazione di un profilo completo senza evidenze corrispondenti.

Il materiale limitato utilizzato qui non accerta indipendentemente una nuova intrusione italiana del 2026 collegata a uno Stato. È una dichiarazione sulla copertura, non la conclusione che l'Italia non abbia affrontato spionaggio. Ricerche storiche dei fornitori offrono il contesto separato seguente.

## 7.6 Contesto di spionaggio pubblicato nel 2026

### Webworm

Contesto di spionaggio pubblicato nel 2026 | Allineato alla Cina, secondo ESET

IN ITALIA, 2026

Maggio

ESET pubblica una ricerca su una campagna del 2025 che comprendeva bersagli governativi italiani

BERSAGLI DICHIARATI

Enti pubblici nel resoconto storico della campagna di ESET

NELLE FONTI PUBBLICHE

[S61] ESET descrive bersagli e attribuzione

[S62] Analisi tecnica e tabella delle tecniche del fornitore

LA NOSTRA VALUTAZIONE

Il recupero da parte di ESET dell'immagine di una macchina virtuale governativa italiana indica un accesso del 2025 alla gestione della virtualizzazione o agli archivi delle immagini, senza chiarire l'ingresso iniziale né dimostrare una nuova intrusione italiana nel 2026.

CONFIDENZA

Come indicato da ESET; non viene dedotto un nuovo conteggio nazionale degli incidenti

La pubblicazione ESET di maggio 2026 descrive una campagna del 2025 che comprendeva bersagli governativi italiani. ESET l'attribuisce a Webworm, gruppo che descrive come allineato alla Cina. La pubblicazione nel 2026 non dimostra una nuova intrusione italiana nel periodo del rapporto. [S61]

Nel resoconto tecnico di ESET, i file recuperati da uno spazio di archiviazione cloud usato dagli attaccanti comprendevano immagini di macchine virtuali di un ente governativo italiano, con stato attivo e configurazione. Tale evidenza indica un accesso alla gestione della virtualizzazione o a un archivio delle immagini, lasciando irrisolti ingresso iniziale ed estensione nella rete. Gli esempi seguenti della tabella del fornitore riguardano l'intera campagna storica, non tecniche osservate indipendentemente in Italia nel 2026. [S62]

TECNICHE CITATE NELLA RICERCA DELLA FONTE, PER TATTICA

| Ricognizione | Esecuzione | Persistenza | Comando e controllo | Esfiltrazione |
|---|---|---|---|---|
| T1595.002 Scansione delle vulnerabilità | T1059.003 Shell di comandi Windows | T1547.001 Chiavi di avvio del registro o cartella di avvio | T1102.002 Comunicazione bidirezionale tramite servizi web | T1567.002 Esfiltrazione verso archiviazione cloud |

Voci selezionate dalla tabella delle tecniche dell'intera campagna di ESET [S62]. È contesto storico pubblicato nel 2026, non un inventario di tecniche osservate presso organizzazioni italiane nel periodo del rapporto. [S62]

Per chi difende, l'esposizione delle immagini richiede di isolare l'amministrazione degli hypervisor, limitare l'accesso agli archivi di copie e immagini, e ruotare credenziali o segreti presenti negli stati catturati. La nostra verifica del 2026 ha coperto pubblicazioni ACN e CERT-AGID, bollettini CSIRT regionali, pubblicazioni clandestine conservate e fonti pubbliche in quattro lingue, senza trovare un'intrusione statale italiana del 2026 confermata indipendentemente. Questo limite riflette la visibilità delle fonti pubbliche e non l'assenza di spionaggio; non assegnate tecniche storiche o attribuzioni del fornitore a un nuovo incidente senza evidenze corrispondenti. [S61][S62]

## 7.7 Sfruttamento web e phishing richiedono verifiche diverse

Il bollettino ClickFix di gennaio descrive siti WordPress italiani abusati per presentare schermate di verifica ingannevoli che incoraggiano azioni manuali. Identifica vulnerabilità note e protezioni inadeguate degli accessi amministrativi come fattori rilevanti nelle campagne osservate. Sono indicazioni a livello di campagna, non risultati su ogni organizzazione candidata. [S19]

Il team web deve censire componenti effettivi e versioni supportate prima di applicare un avviso. Il SOC deve indagare separatamente sull'interazione dell'utente con i contenuti ingannevoli e sulle eventuali successive evidenze di identità o dispositivi. Rimuovere contenuti web malevoli e intervenire sul dispositivo di un utente sono attività distinte.

Un bollettino CSIRT di settembre riferisce lo sfruttamento di Joomla Content Editor per installare webshell e alterare siti di organizzazioni in Italia. La fonte non accerta incidenti presso le organizzazioni dell'insieme selezionato. [S58]

I limiti esatti delle versioni indicati dal produttore sono mantenuti sotto come riferimento tecnico. Usate una versione attualmente supportata che contenga la correzione. Verificate poi l'installazione e indagate sugli accessi precedenti pertinenti. [S59][S60]

```
Prodotto: Joomla Content Editor
Identificatore: CVE-2026-48907
Interessate: versioni precedenti a 2.9.99.5
Prima versione corretta: 2.9.99.5
Ulteriore rafforzamento discusso dal produttore: 2.9.99.6
```

L'avviso sulla correzione per sistemi precedenti distingue l'intervento specifico dal più ampio rafforzamento della versione successiva. NVD registra l'identificatore. La prima versione corretta è un limite storico, non un'affermazione sull'ultima versione supportata alla chiusura. [S59][S60]

L'inventario dei componenti deve identificare installazione effettiva e responsabile. La correzione richiede verifiche autorizzate e revisione delle attività precedenti pertinenti. Un aggiornamento riuscito non dimostra indipendentemente l'assenza di accessi precedenti.

PUNTI CHIAVE

01

Registrazioni ed etichette dei gruppi misurano pubblicazioni, non intrusioni o operatori verificati.

02

Mantenete ogni attribuzione collegata alla fonte che sostiene quel caso.

03

Associate un avviso tecnico alle risorse effettive prima di trasformarlo in un intervento.

CAPITOLO 08

# L'economia delle frodi

08

QUESTO CAPITOLO RISPONDE

Come diventano strumenti di frode le informazioni identificative e le comunicazioni fidate?

**4**

decisioni: prova dell'identità, fiducia nella sessione, autorità di pagamento e avviso ai clienti


8.1 Le informazioni identificative non attribuiscono autorità 71

8.2 I temi dei servizi pubblici raggiungono i dati di pagamento 71

8.3 L'accesso alla casella rende più plausibile una falsa richiesta di pagamento 72

8.4 Un conteggio settimanale di campagne conta campagne 72

8.5 I resoconti della polizia aggiungono esiti, mantenendo periodi propri 73

8.6 Materiale sulle carte nelle pubblicazioni: una visione limitata 73

8.7 Prezzi e servizi descrivono offerte, non transazioni 73

CAPITOLO 08

# L'economia delle frodi

IN SINTESI

Le campagne ufficiali mostrano richieste di documenti identificativi, credenziali e informazioni di pagamento, spesso con temi familiari di servizi pubblici o aziende. I documenti cercati possono sostenere altre impersonificazioni. Gli avvisi non dimostrano ogni frode successiva. Le offerte clandestine aggiungono una visione separata di domanda e pubblicità. Verificate cosa potrebbe sapere un attaccante, proteggete la decisione che potrebbe influenzare e confermate le istruzioni di pagamento tramite canali conosciuti indipendentemente.

## 8.1 Le informazioni identificative non attribuiscono autorità

Nome, indirizzo, immagine di un documento o dettaglio contrattuale possono rendere credibile una conversazione. Non dimostrano che il chiamante possieda un account o possa approvare un pagamento. Le raccomandazioni antifrode del rapporto si concentrano su questo confine decisionale. Assistenza, recupero degli account e finanza devono provare cosa accada quando l'attaccante conosce già le normali informazioni anagrafiche.

L'avviso CERT-AGID di gennaio a tema sussidi descrive la raccolta di documenti identificativi, reddituali e lavorativi. Presenta il successivo abuso legato al credito come possibile finalità. La distinzione conta: una richiesta documentale è un tentativo di raccolta osservato. Un prestito effettivamente aperto richiederebbe ulteriori evidenze. [S18]

Per chi difende, il passo successivo è identificare il processo che accetta le informazioni come prova. Un test sintetico può verificare se l'assistenza riveli altre informazioni, cambi un recapito o ripristini l'accesso dopo aver ricevuto documenti plausibili. Documentate la decisione del processo e le evidenze richieste, senza usare i dati di vittime reali.

## 8.2 I temi dei servizi pubblici raggiungono i dati di pagamento

L'avviso di gennaio sul rinnovo della tessera sanitaria descrive campagne che chiedono dati personali. Alcune varianti chiedono dati delle carte con il pretesto di una spesa di consegna. L'avviso riguarda l'impersonificazione, non prova un'intrusione nel servizio della tessera sanitaria. Il numero delle campagne non misura persone interessate o pagamenti riusciti. [S16]

Un avviso separato di gennaio a tema fiscale descrive un falso accesso SPID. Un avviso regionale di aprile descrive un'altra esca sul rinnovo dell'identità digitale. Gli avvertimenti sostengono indicazioni ai clienti sui temi familiari dei servizi. Non dimostrano che ogni destinatario abbia inserito credenziali né accessi alle infrastrutture di un fornitore d'identità. [S15][S22]

Un avviso deve spiegare quale decisione evitare e quale percorso usare invece. Indirizzate le persone a un canale del servizio conosciuto indipendentemente. Evitate di inoltrare immagini contenenti una destinazione malevola funzionante. L'obiettivo è ridurre l'autorità di una richiesta plausibile, non chiedere a ogni utente di riconoscere ogni dettaglio visivo.

## 8.3 L'accesso alla casella rende più plausibile una falsa richiesta di pagamento

Il bollettino di febbraio sulle frodi tramite email aziendali descrive phishing di credenziali e codici monouso, seguito dall'abuso di corrispondenza commerciale e domini imitativi. La fonte è un'osservazione di campagna, non una stima delle perdite italiane per frode. Sostiene verifiche ulteriori rispetto al nome visualizzato in un messaggio di pagamento. [S20]

Una conversazione autentica su una fattura può contenere una modifica fraudolenta del pagamento. Il controllo rilevante è la conferma tramite un recapito stabilito prima della richiesta sospetta. La finanza deve conservare beneficiario confermato, approvatore e prova della richiamata. Una richiesta urgente o riservata deve seguire lo stesso processo, anche quando sembra provenire da un dirigente.

La risposta sulle identità deve riguardare anche l'ambiente del mittente. Esaminate cronologia delle sessioni, impostazioni di recupero, accessi delegati e inoltri quando una casella è coinvolta. Il solo cambio della password può lasciare irrisolti altri accessi o rapporti di fiducia. Verificate queste condizioni con un processo autorizzato, senza presumere che il bollettino dimostri l'attività attuale di un account specifico.

## 8.4 Un conteggio settimanale di campagne conta campagne

Il riepilogo CERT-AGID del 14-20 marzo registra 103 campagne malevole: 66 dirette a bersagli italiani e 37 generiche che interessavano l'Italia. I falsi avvisi di sanzioni rappresentavano 24 campagne di phishing dirette all'Italia. Altri temi erano banche, pagamenti e ordini. Le cifre descrivono la popolazione settimanale di quella fonte. [S21]

Non forniscono un totale annuale nazionale degli incidenti. Più messaggi possono appartenere a una campagna. Un'organizzazione può ricevere molti messaggi senza un'intrusione accertata. La domanda operativa è se l'organizzazione abbia osservato il tema, se qualcuno abbia interagito e quale azione sulle identità o sui pagamenti sia seguita.

Il SOC può collegare la domanda ai registri di assistenza e antifrode. Conservate il messaggio sospetto, stabilite quale account o processo abbia toccato e assegnate la chiusura. La misurazione deve distinguere consegna bloccata, interazione dell'utente, credenziali inserite e abuso confermato. Sono categorie interne suggerite, non conteggi dedotti dall'avviso nazionale.

## 8.5 I resoconti della polizia aggiungono esiti, mantenendo periodi propri

Un comunicato dei Carabinieri di giugno copre frodi tentate e concluse tramite falsificazione dell'identità del chiamante da novembre 2025 a maggio 2026. Riferisce denunce alla procura e fondi recuperati. La popolazione a cavallo di due anni non può diventare un conteggio degli incidenti del 2026. Attività investigative e accuse devono restare distinte dalle condanne. [S38]

Le notizie di luglio attribuiscono un'indagine sulle impersonificazioni bancarie alla Polizia Postale, con il coordinamento di una procura. La fonte descrive misure cautelari, non risultati giudiziari definitivi. Il caso sostiene un avvertimento sui contatti bancari fraudolenti. Non dimostra intrusioni nelle banche di cui si usava l'identità. [S39]

Un'azione storica aggiunge un altro limite. Un comunicato della Guardia di Finanza di maggio riguarda presunte frodi online nel 2022-2025. Rientra nel contesto della risposta, non nel totale degli incidenti attuali. La precisione temporale impedisce di leggere un'indagine riuscita del 2026 come prova di nuovi attacchi del 2026. [S57]

## 8.6 Materiale sulle carte nelle pubblicazioni: una visione limitata

AMBITO DEI DATI DELLE SCHEDE

Le eventuali cifre sulle carte del rapporto riguardano soltanto carte di pagamento apparse in chiaro nelle pubblicazioni dark web raccolte per il rapporto. Brandefense rileva carte rubate anche con altri metodi, estranei a questo rapporto. Questa visione non misura il furto nazionale di carte o le perdite per frode.

In questa visione limitata, 42 carte distinte associate all'Italia sono apparse in 38 pubblicazioni conservate. Questo non dimostra che fossero attive, che l'emittente abbia subito intrusioni o che vi siano state frodi. Dalle osservazioni non deriva una stima nazionale di furti o perdite. L'associazione al Paese non stabilisce residenza del titolare o luogo della frode. Gli emittenti devono verificare i segnali rilevanti con le proprie evidenze sulle autorizzazioni e sulla tutela dei clienti. [S4]

La distinzione operativa resta importante anche quando si osserva una registrazione simile a una carta. Uno stato pubblicizzato o stampato non dimostra una transazione conclusa. Gli emittenti devono usare le proprie evidenze sulle autorizzazioni e sulle frodi per stabilire se intervenire su una carta. La riemissione dipende dalle regole dell'emittente e dal rischio convalidato.

## 8.7 Prezzi e servizi descrivono offerte, non transazioni

Le evidenze conservate non forniscono una serie di prezzi comparabili pubblicata. Il rapporto non deduce valore di mercato o transazioni concluse da annunci isolati. Usate il prodotto osservato e il limite di verifica per decidere se approfondire. [S1]

Un'offerta di pannello automobilistico indicava un prezzo richiesto di 5 000 USD (B16). È un singolo prezzo pubblicizzato, non una transazione conclusa o una media di mercato. [S1]

Il prezzo richiesto da un venditore non dimostra una vendita conclusa, l'identità dell'acquirente o il valore di un accesso autentico. Un annuncio per più Paesi può citare l'Italia senza identificare una vittima italiana. Le informazioni utili sono prodotto dichiarato, pubblico cercato e verifica necessaria prima dell'azione di un'organizzazione.

Quando servizi di identità, account e pagamenti compaiono insieme, ogni sequenza che li colleghi resta un modello analitico, salvo evidenze concrete sui partecipanti. Testi simili o pubblicazioni vicine possono mostrare un tema di mercato comune senza dimostrare operatori comuni. Evitate di trasformare il modello in un'organizzazione criminale nominata.

PUNTI CHIAVE

**01**

Le informazioni familiari possono sostenere impersonificazioni senza conferire autorità.

**02**

Campagne, richieste documentali, frodi concluse e fondi recuperati restano popolazioni distinte.

**03**

Proteggete modifiche ai pagamenti e recupero degli account con approvazioni verificate indipendentemente.

CAPITOLO 09

# Approfondimento su banche e finanza

09

QUESTO CAPITOLO RISPONDE

Quali rischi bancari riguardano dipendenti, clienti e autorità di pagamento, e chi deve verificarli?

**3**

responsabili distinti: identità, antifrode e tesoreria


9.1 Un portafoglio misurato con popolazioni distinte 76

9.2 Un ordine pratico per la valutazione 77

9.3 Il problema dell'autorità di pagamento raggiunge i dirigenti 77

9.4 Separare i consigli ai clienti dalle affermazioni sull'infrastruttura 77

9.5 Segnali su carte, account e trasferimenti richiedono evidenze diverse 78

CAPITOLO 09

# Approfondimento su banche e finanza

IN SINTESI

Le offerte attuali di credenziali sono associate a 14 delle 25 voci candidate di banche e finanza. Le associazioni ai domini comprendono dispositivi dei dipendenti e altri dispositivi, insieme a credenziali storiche. Convalidate la rilevanza attuale degli account, proteggete il recupero dei clienti e verificate le modifiche ai pagamenti. Tenete separati accessi del personale, associazioni dei dispositivi dei clienti, osservazioni sulle carte e pagamenti autorizzati dopo un inganno. Assegnate ogni segnale al team capace di verificarne la rilevanza attuale prima dell'escalation.

## 9.1 Un portafoglio misurato con popolazioni distinte

Alla verifica, le offerte di credenziali erano associate a 14 delle 25 voci candidate di banche e finanza. Le associazioni ai domini totalizzano almeno 83725 dispositivi, compresi 1636 associati ai dipendenti, e 1662877 credenziali storiche. Le restanti 82089 associazioni di dispositivi non sono classificate come dipendenti; appartenenza e attualità restano non verificate. [S3]

Un sottoinsieme bancario distinto comprende 12 voci candidate nel portafoglio di 25 voci di banche e finanza. Le osservazioni su dispositivi, credenziali e carte non dimostrano la stessa persona o evento. Il portafoglio completo e il sottoinsieme hanno denominatori diversi. Non sono pubblicate valutazioni di banche o settori. [S3][S4]

| Sottoinsieme bancario | Conteggio osservato |
|---|---|
| Voci candidate | 12 |
| Voci con osservazioni di carte | 6 |
| Voci associate a offerte attuali di credenziali | 10 |
| Associazioni di dispositivi dei dipendenti | 1546 |
| Altre associazioni di dispositivi | 60912 |

I conteggi descrivono il sottoinsieme di 12 voci nel portafoglio candidato di 25 voci di banche e finanza. I totali dei dispositivi sono osservazioni minime e possono sovrapporsi. Le carte osservate non dimostrano validità o frodi concluse. [S3][S4]

Un emittente non deve dedurre un'intrusione sul server dalla registrazione di malware di un cliente. Viceversa, l'apparente esposizione di un cliente può rilevare per le frodi anche senza effetti sull'infrastruttura della banca. Separate ipotesi tecnica e decisione di tutela del cliente, affinché nessun team scarti le evidenze rilevanti dell'altro.

## 9.2 Un ordine pratico per la valutazione

Stabilite prima se il segnale riguardi un'identità attiva del personale, un processo del cliente o un annuncio non verificato. Gli accessi del personale e privilegiati devono entrare nel processo identità, comprese le verifiche su sessioni e recupero. Le evidenze sui clienti devono raggiungere antifrode e assistenza. Una rivendicazione di vendita di dati deve raggiungere analisi e risposta per valutarne la provenienza.

Documentate poi ciò che è stato convalidato. L'esito deve indicare se l'identità appartenga all'organizzazione, se l'evidenza sia abbastanza attuale da giustificare azioni e quali interventi esistano già. Una vecchia password in un elenco storico non dimostra accessi attuali. Anche un annuncio attuale richiede una verifica del singolo account.

Definite infine l'escalation. Account privilegiati attivi, sessioni inspiegate o modifiche non autorizzate al recupero meritano gestione dell'incidente secondo le regole locali. Un elenco massivo non verificato può richiedere monitoraggio e verifiche della provenienza dei campioni tramite canali autorizzati. Nessuna risposta deve dipendere dal solo numero di registrazioni pubblicizzato.

## 9.3 Il problema dell'autorità di pagamento raggiunge i dirigenti

La stampa di settembre descrive una presunta frode di febbraio presso un istituto di gestione patrimoniale, con messaggio di un dirigente e voce di un presunto professionista. Le notizie indicano importi non recuperati diversi dopo un recupero sostanziale. Il rapporto non considera il trasferimento iniziale come perdita finale né verifica indipendentemente la componente IA riferita. [S56]

I limiti sui nomi e sui fatti non eliminano la lezione decisionale. Una richiesta di un dirigente richiede le stesse verifiche di beneficiario e autorità degli altri pagamenti. Riservatezza e urgenza devono attivare il percorso documentato, non consentire di saltare la conferma. La tesoreria deve sapere chi possa fermare o richiamare un pagamento e quanto rapidamente raggiungere quel canale.

Un'esercitazione utile combina una conversazione dall'aspetto autentico, documenti plausibili e un dirigente indisponibile. La prova di completamento è se il personale abbia usato recapiti noti indipendentemente e documentato le approvazioni richieste. La prova deve verificare anche che il secondo approvatore controlli le evidenze indipendentemente, anziché avallare soltanto la prima decisione.

## 9.4 Separare i consigli ai clienti dalle affermazioni sull'infrastruttura

Le comunicazioni recenti su recapiti e documenti possono sostenere avvisi mirati ai clienti senza dimostrare il furto di password bancarie. Spiegate che i criminali potrebbero citare informazioni autentiche e chiedere una nuova azione. Indicate ai clienti l'app conosciuta, la filiale o il canale pubblicato del servizio per verificare. Non lasciate intendere che conoscere un numero di contratto conceda accesso all'account.

Quando un'azienda esclude il coinvolgimento di informazioni di pagamento, mantenete la dichiarazione come resoconto aziendale. Se le evidenze cambiano, aggiornate i consigli e documentate la base. Una dichiarazione provvisoria deve essere precisa abbastanza da resistere al cambiamento: categorie note dei dati, valutazione attuale e canale del prossimo aggiornamento.

Gli operatori di assistenza devono poter rispondere ai clienti preoccupati da una rivendicazione pubblica. La risposta deve distinguere un incidente specifico dell'organizzazione da un annuncio generico sul Paese. L'assistenza deve evitare di confermare ulteriori dettagli identificativi a un chiamante inatteso che conosca già alcune informazioni corrette.

## 9.5 Segnali su carte, account e trasferimenti richiedono evidenze diverse

Le evidenze di autorizzazione delle carte appartengono all'emittente e al processo di pagamento del commerciante. Il recupero degli account riguarda identità e antifrode. Un trasferimento aziendale approvato dopo un inganno riguarda tesoreria e relativo processo antifrode. Collegare le registrazioni può rivelare una sequenza, ma non le rende unità intercambiabili.

Una revisione interna deve mantenere segnale osservato, servizio interessato, azione proposta e prova di chiusura. Un totale unico denominato esposizione può nascondere la differenza tra una credenziale obsoleta, una sessione attuale e un pagamento concluso. Usate code separate con un responsabile comune dell'escalation quando le evidenze le collegano.

Per i soggetti finanziari, DORA aggiunge un quadro di segnalazione e resilienza, discusso nel capitolo 10. Applicabilità e criterio di incidente grave vanno verificati per soggetto e servizio. L'incidente di un fornitore non è automaticamente un incidente grave per ogni cliente finanziario. [S54]

PUNTI CHIAVE

**01**

Le offerte di credenziali associate a 14 delle 25 voci candidate finanziarie richiedono verifiche degli account.

**02**

Identità del personale, frodi ai clienti e autorità di tesoreria richiedono responsabili distinti delle verifiche.

**03**

Un'esercitazione realistica sui pagamenti prova conferme indipendenti, canali di blocco e recupero.

CAPITOLO 10

# Normativa e risposta nazionale

10

QUESTO CAPITOLO RISPONDE

Quali norme riguardano il soggetto, quali fatti avviano i termini e chi documenta la decisione di notifica?

**4**

quadri con ambiti e condizioni differenti


10.1 Partire dall'applicabilità 80
10.2 NIS2: contano conoscenza e anno di inserimento applicabile 80
10.3 Gli obblighi pubblici richiedono una verifica separata dell'ambito 81
10.4 Il GDPR distingue notifica e comunicazione agli interessati 81
10.5 DORA è un quadro per il settore finanziario 82
10.6 Le lezioni dell'applicazione delle norme restano legate agli eventi precedenti 82
10.7 Una designazione è diversa dall'attribuzione di un incidente 82
10.8 La matrice delle notifiche deve funzionare durante un disservizio 83

CAPITOLO 10

# Normativa e risposta nazionale

IN SINTESI

L'Italia ha recepito NIS2 nel 2024. Gli obblighi di notifica e controllo dipendono dall'inclusione del soggetto, dall'anno di inserimento e dalle disposizioni applicabili. Il GDPR riguarda il rischio sui dati personali. DORA disciplina i soggetti finanziari interessati e gli incidenti ICT gravi. Anche gli altri obblighi pubblici richiedono una verifica dell'ambito. Costruite una matrice specifica per soggetto, documentate la conoscenza dei fatti e assegnate un sostituto per le notifiche prima dell'incidente.

## 10.1 Partire dall'applicabilità

La tabella guida alla lettura dei testi verificati e non è consulenza legale. I legali dell'organizzazione devono confermare applicabilità attuale, esclusioni e disposizioni attuative. Una pubblicazione con etichetta nazionale da sola non dimostra un incidente significativo per legge.

| Quadro | Destinatari | Punto verificato | Prima azione |
|---|---|---|---|
| Decreto legislativo 138/2024 | Soggetti essenziali e importanti nell'ambito previsto | Il recepimento italiano di NIS2 è entrato in vigore il 16 ottobre 2024 | Confermare inclusione, soggetto e servizi rilevanti |
| Attuazione NIS | Soggetti inseriti nell'elenco e relativo anno di ingresso | La guida ACN indica scadenze diverse nel 2026 e 2027 secondo l'anno di inserimento | Conservare la comunicazione di inserimento e la determinazione applicabile |
| Legge 90/2024 | Specifiche amministrazioni e operatori, con esclusioni | L'articolo 1 contiene obblighi di segnalazione degli incidenti | Verificare ambito e sovrapposizioni con altri regimi |
| GDPR | Titolari e responsabili che trattano dati personali | Le valutazioni del rischio e del rischio elevato servono a decisioni di notifica diverse | Coinvolgere i legali privacy e documentare la valutazione |
| DORA | Soggetti finanziari e rapporti nel suo ambito | Si applica dal 17 gennaio 2025; gli incidenti ICT gravi richiedono segnalazione | Confermare ambito del soggetto e autorità competente |

I testi sono [S50]-[S54]. Non sostengono un termine universale per tutte le organizzazioni italiane. Un gruppo multinazionale deve mappare soggetti giuridici e servizi, senza presumere che la sede determini ogni obbligo.

## 10.2 NIS2: contano conoscenza e anno di inserimento applicabile

L'articolo 25 definisce le fasi per gli incidenti significativi: pre-notifica entro 24 ore dalla conoscenza, notifica entro 72 ore e relazione finale entro un mese dalla notifica. Tratta inoltre relazioni intermedie, incidenti in corso e una regola particolare per i servizi fiduciari. Le notifiche devono avvenire senza ingiustificato ritardo. [S50]

I soggetti interessati notificano al CSIRT Italia. Per gli incidenti significativi che incidono sui servizi fiduciari, l'articolo 25 prevede per i prestatori un termine di notifica di 24 ore anziché le ordinarie 72 ore. [S50]

La guida ACN del 2026 distingue i soggetti inseriti nel 2025 da quelli inseriti nel 2026. Indica rispettivamente gennaio 2026 e gennaio 2027 per gli obblighi di notifica, con date diverse per le misure di base. Determinazioni applicabili e comunicazione di inserimento restano necessarie per interpretare la decorrenza precisa. Non sostituitele con una data nazionale generalizzata. [S51]

La preparazione operativa richiede un processo documentato sulla conoscenza dei fatti. Identificate chi riceva segnalazioni dei fornitori, evidenze dei clienti e risultati del SOC. Conservate quando l'organizzazione abbia appreso fatti rilevanti per la significatività. La ricostruzione forense successiva aggiorna il registro. Non deve cancellare la decisione precedente né ritardare la segnalazione richiesta finché scompaia ogni incertezza.

## 10.3 Gli obblighi pubblici richiedono una verifica separata dell'ambito

L'articolo 1 della legge 90/2024 specifica amministrazioni e operatori soggetti agli obblighi di segnalazione, con esclusioni e sovrapposizioni da esaminare. Il testo contiene fasi di notifica misurate dalla conoscenza. Nella norma sanzionatoria distingue inoltre l'inosservanza ripetuta entro cinque anni. Non è una sanzione automatica al primo ritardo. [S52]

Ai sensi dell'articolo 1 modificato, usate le procedure ACN per entrambe le fasi. Inviate la segnalazione iniziale senza ritardo ed entro 24 ore dalla conoscenza dell'incidente. Inviate la notifica completa entro 72 ore dallo stesso momento di conoscenza dell'incidente. L'inosservanza ripetuta entro cinque anni comporta una sanzione di 25 000–125 000 euro alle condizioni indicate. Ambito ed esclusioni continuano ad applicarsi. [S67]

Per un servizio pubblico, identificate quali obblighi riguardino l'ente responsabile, una società in house o un fornitore. Il contratto deve indicare chi fornisca i fatti sull'incidente e con quali tempi. L'avviso contrattuale non sostituisce la valutazione legale dell'organizzazione. Una segnalazione del fornitore non deve diventare implicitamente una notifica completata dal cliente.

Un'esercitazione deve provare il passaggio quando il sistema coinvolto normalmente conserva contatti ed evidenze. Il registro di completamento deve mostrare notificante, sostituto, autorità, informazioni disponibili e aggiornamento successivo. Il legale deve convalidare la matrice prima dell'esercitazione, non mentre decorrono i termini.

## 10.4 Il GDPR distingue notifica e comunicazione agli interessati

Le indicazioni del Garante spiegano la notifica del titolare senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza, salvo che il rischio per le persone sia improbabile. Il responsabile informa tempestivamente il titolare. La comunicazione agli interessati usa una valutazione del rischio elevato, con le eccezioni applicabili. Tutte le violazioni richiedono documentazione, comprese quelle non notificate. [S53]

Una decisione di giugno su una casella editoriale mostra che le valutazioni del regolatore sugli articoli 33 e 34 possono differire. Non deve diventare una regola che imponga comunicazioni identiche per ogni incidente di posta. La decisione riguarda attività storica e serve qui alla precisione giuridica, non come incidente attuale. [S43]

La risposta deve accertare categorie dei dati, accessi, disponibilità, servizi coinvolti e incertezze. I legali privacy documentano quindi la decisione sul rischio e gli aggiornamenti. Cifratura confermata, vendita non verificata e avviso sui recapiti possono creare domande diverse. Nessuno deve ricevere una conclusione automatica da un modello.

## 10.5 DORA è un quadro per il settore finanziario

DORA si applica dal 17 gennaio 2025. Riguarda gestione del rischio ICT, test, gestione degli incidenti e rapporti con terzi per i soggetti nel suo ambito. L'articolo 19 disciplina la segnalazione degli incidenti ICT gravi all'autorità competente pertinente. Anche il suo rapporto settoriale con NIS2 richiede verifica dell'applicabilità. [S54]

I soggetti coperti dalle istruzioni pubblicate della Banca d'Italia inviano segnalazioni tramite la piattaforma INFOSTAT. Gli operatori assicurativi devono usare le istruzioni DORA e le modalità di segnalazione applicabili dell'IVASS. Questi percorsi delle singole fonti non sostituiscono la verifica dell'autorità per ciascun soggetto. [S66] [S68]

Il rapporto non importa in DORA le scadenze di NIS2 o GDPR. Il soggetto finanziario deve usare matrice normativa attuale, processo di classificazione e canale dell'autorità competente. L'incidente di un fornitore ICT richiede una valutazione degli effetti reali o probabili sui servizi di quel soggetto, non una classificazione automatica da un titolo.

## 10.6 Le lezioni dell'applicazione delle norme restano legate agli eventi precedenti

Una decisione del Garante del 2026 sulle telecomunicazioni riguarda incidenti notificati a febbraio 2025 e impersonificazione dell'assistenza presso punti vendita. La lezione di sicurezza riguarda accessi e verifiche. L'attività sottostante deve restare fuori dal totale degli eventi del 2026. I campi legati ai pagamenti in quel caso differiscono dalle carte osservate in chiaro nelle pubblicazioni. [S40]

Altre decisioni riguardano un evento del 2024 presso una società di consulenza, una dichiarazione aziendale su credenziali VPN rubate in un altro incidente storico e accessi condivisi presso un fornitore sanitario. Offrono lezioni specifiche sui controlli, senza dimostrare che le stesse vie abbiano causato i casi del 2026 del rapporto. [S41][S42] [S44]

## 10.7 Una designazione è diversa dall'attribuzione di un incidente

La decisione (PESC) 2026/2546 del Consiglio, datata 16 novembre, aggiunge NoName057(16) a un allegato di misure restrittive. L'allegato descrive il gruppo come filorusso. Il rapporto mantiene questa caratterizzazione come quella del Consiglio. La designazione non accerta indipendentemente la responsabilità per ogni evento italiano discusso qui. [S63]

La decisione è registrata come evidenza di contesto nazionale, non come consiglio sull'attuazione delle sanzioni. Mantenete il suo status giuridico separato dalle affermazioni su un sito o uno specifico operatore.

## 10.8 La matrice delle notifiche deve funzionare durante un disservizio

| Decisione | Registro | Responsabile |
|---|---|---|
| Soggetto e servizio rientrano nell'ambito? | Regime applicabile e motivo dell'esclusione | Legale |
| Quando è avvenuta la conoscenza rilevante? | Data, ora e fatti a sostegno | Responsabile dell'incidente |
| Cosa si sa dell'impatto? | Servizi, durata, categorie dei dati e incertezza | Responsabili del servizio e privacy |
| Quale fase è richiesta? | Autorità, canale, scadenza e aggiornamento successivo | Notificante nominato |
| Cosa cambia la valutazione? | Nuove evidenze e revisione programmata | Responsabile dell'incidente e legale |

Conservate una copia accessibile tramite un percorso approvato indipendente dall'ambiente coinvolto. Provate il sostituto per le notifiche e il contatto con l'autorità. Dopo l'esercitazione, correggete i fatti e i passaggi mancanti, anziché registrare soltanto che l'incontro sia avvenuto.

PUNTI CHIAVE

**01**

Ambito e anno di inserimento precedono la scelta del termine di notifica.

**02**

Notifica delle violazioni di dati personali e comunicazione agli interessati sono decisioni distinte.

**03**

Conservate conoscenza, fatti e motivazione legale in un registro utilizzabile.

CAPITOLO 11

# Prospettive

11

QUESTO CAPITOLO RISPONDE

Quali sviluppi devono cambiare le priorità difensive sull'Italia dopo questa rilevazione?

**5**

valutazioni condizionali con segnali espliciti di cambiamento


11.1 Valutazioni principali 85

11.2 Cosa cambierebbe la valutazione 86

11.3 Scenari condizionali per pianificare 86

11.4 Cosa non può prevedere il rapporto 87

CAPITOLO 11

# Prospettive

IN SINTESI

Pianificate dalle vie sostenute dai riscontri: interruzioni dei fornitori, frodi su identità e pagamenti, rivendicazioni sulla disponibilità e servizi pubblici vulnerabili. I dati non misurano la probabilità di un attacco futuro o l'efficacia di uno specifico controllo. Ogni valutazione seguente identifica le evidenze che cambierebbero la decisione. Esaminate il segnale, verificatene la rilevanza per i vostri servizi e aggiornate il piano quando cambiano le evidenze.

## 11.1 Valutazioni principali

| Valutazione | Confidenza | Base e limite | Responsabile |
|---|---|---|---|
| L'indipendenza del ripristino merita priorità per i servizi importanti | Alta per l'utilità decisionale | Diversi casi confermati documentano interruzioni; nessuna stima nazionale di prevalenza | Continuità e responsabile del servizio |
| Recapiti e dati identificativi possono sostenere impersonificazioni credibili | Alta per il meccanismo | Campagne ufficiali di raccolta e comunicazioni recenti; abuso successivo non accertato in ogni caso | Antifrode e assistenza |
| Una rivendicazione visibile richiede una rapida verifica del servizio | Alta | Resoconti ufficiali e degli autori usano misure diverse; i soli tempi non chiariscono l'impatto | SOC e comunicazione |
| Nuove evidenze sulle sessioni specifiche dell'organizzazione richiedono una tempestiva revisione delle identità | Condizionale | Dipende da appartenenza, attualità e stato corrente dell'account | Identità e risposta |
| Nuove segnalazioni di intrusioni in servizi critici potrebbero cambiare le priorità settoriali | Condizionale | La copertura attuale dei casi è parziale; gli incidenti non comunicati restano invisibili | CISO e analisi |

La confidenza riguarda ogni affermazione, non un attore o settore. Un'alta confidenza nella necessità di provare il ripristino non implica una probabilità quantificata di ransomware. Una valutazione condizionale diventa operativa solo quando le evidenze specificate sono rilevanti per l'organizzazione.

## 11.2 Cosa cambierebbe la valutazione

| Interpretazione attuale | Nuova evidenza | Decisione modificata |
|---|---|---|
| I dati di un venditore restano non verificati | Una verifica autorizzata li collega a un sistema attuale oppure l'organizzazione conferma accessi | Risposta su incidente, privacy e tutela dei clienti |
| La rivendicazione su un sito ha effetti operativi incerti | Registri del fornitore e del responsabile del servizio confermano effetti persistenti sugli utenti | Capacità di mitigazione e priorità di continuità |
| L'incidente del fornitore ha una dipendenza delimitata | Emergono altri effetti sostenuti da riscontri su clienti o servizi | Mappa delle dipendenze e ambito del ripristino |
| Una credenziale potrebbe essere storica | Sono confermati sessione attuale, account attivo o modifica non autorizzata al recupero | Revoca delle sessioni ed escalation dell'incidente |
| Una notizia sui controlli fisici ha causa incerta | Letture del gestore ed evidenze degli accessi sostengono un'interferenza non autorizzata | Sicurezza fisica, isolamento e risposta specialistica |
| Un caso resta senza attribuzione | Un resoconto tecnico o ufficiale credibile pubblica collegamenti di supporto | Valutazione dell'attore e ricerche pertinenti |

Una nuova etichetta deve seguire un cambiamento nell'affermazione sostenuta dalle evidenze. Documentate cosa sia stato aggiunto e cosa resti irrisolto. Evita che un titolo clamoroso sostituisca, senza fatti di supporto, una valutazione più precisa del servizio o dell'identità.

## 11.3 Scenari condizionali per pianificare

**Interruzione del fornitore.** Se un fornitore critico segnala cifratura o perdita di un servizio condiviso, attivate la mappa delle dipendenze e il percorso alternativo provato. Cercate evidenze su impatto e ripristino specifiche del cliente. Lo scenario non presume che ogni cliente sia coinvolto o che il volume di dati rubati dichiarato sia corretto.

**Esposizione di identità.** Se dati appena osservati contengono informazioni attuali credibili su clienti o contratti, preparate indicazioni antifrode e di assistenza mentre prosegue la verifica autorizzata. Non aspettate un'attribuzione completa per proteggere un processo esposto. Conservate nelle dichiarazioni pubbliche l'incertezza su origine e popolazione interessata.

**Campagna sulla disponibilità.** Se canali degli attori pubblicano un elenco di bersagli rilevante per l'organizzazione, controllate preparazione della mitigazione e canale alternativo sullo stato. Verificate percorsi effettivi degli utenti e osservazioni del fornitore. Non dichiarate un'interruzione persistente da un singolo controllo fallito del sito o da un'immagine dell'attore.

**Impersonificazione nei pagamenti.** Se una richiesta cambia il beneficiario o richiama urgenza e segretezza, usate conferma indipendente e contatto di escalation. Mittente familiare, voce convincente o documento autentico non devono evitare il processo. Il segnale è il cambiamento di autorità richiesto, non una supposizione sull'uso dell'IA.

**Problema sui controlli fisici.** Se le letture del processo cambiano in modo inatteso o gli accessi del manutentore non trovano spiegazione, usate la procedura approvata di stato sicuro e conservate le evidenze degli accessi. Il responsabile del processo decide la sicurezza operativa. Gli analisti valutano separatamente le rivendicazioni, senza ritardare le azioni di sicurezza per cercare l'attribuzione.

## 11.4 Cosa non può prevedere il rapporto

Il rapporto non può derivare probabilità di attacco, perdite finanziarie o efficacia dei controlli dai conteggi delle pubblicazioni. Più rivendicazioni possono riflettere scelte editoriali degli attori e visibilità. Meno pubblicazioni osservate possono riflettere la copertura della fonte. Un'indagine appena pubblicata può rivelare attività precedente. Queste alternative restano rilevanti dopo la rilevazione.

L'orizzonte appropriato di pianificazione è la prossima decisione con le sue evidenze. Mantenete responsabile, segnale, azione e prova di chiusura. Rivedeteli dopo una comunicazione pertinente, una modifica del fornitore o una prova di ripristino. Un calendario fisso da solo non deve decidere se la valutazione del rischio sia cambiata.

PUNTI CHIAVE

**01**

Pianificate sulle vie sostenute da riscontri e sulle decisioni dei servizi che influenzano.

**02**

Ogni valutazione richiede un segnale capace di modificarla.

**03**

I conteggi di pubblicazioni e rivendicazioni non prevedono perdite o probabilità di attacco.

CAPITOLO 12

# Piano d'azione

12

QUESTO CAPITOLO RISPONDE

Chi deve fare cosa nei prossimi 90 giorni e come si dimostrerà il completamento?

**20**

azioni con responsabili e prove di completamento


12.1 La sequenza 89

12.2 Cosa conta come completamento 92

12.3 Prime decisioni per ruolo 92

12.4 Evitare controlli che risolvono l'affermazione sbagliata 93

12.5 Come può aiutare Brandefense 93

CAPITOLO 12

# Piano d'azione

IN SINTESI

Partite dalla ricezione delle evidenze, dalla responsabilità delle notifiche e da un servizio importante provato. Affrontate poi sessioni delle identità, recupero dei clienti, autorità di pagamento e dipendenze dai fornitori. Usate immediatamente i risultati attuali specifici dell'organizzazione: il calendario non giustifica ritardi nella risposta. Entro il giorno 90, fornite al consiglio prove di completamento e responsabili nominati per le lacune rimanenti.

## 12.1 La sequenza

La tabella propone una sequenza del programma. Una minaccia attuale rilevante deve entrare immediatamente nel processo di gestione degli incidenti dell'organizzazione. Le scadenze seguenti sono obiettivi gestionali suggeriti, non affermazioni sui termini legali.

| 1Giorni 1-30 | |
|---|---|
| Confermare la ricezione di rivendicazioni pertinenti, evidenze sulle sessioni e avvisi dei fornitori | |
| RESPONSABILE<br>CISO e analisi | PROVA DI COMPLETAMENTO<br>Fonte, coda e sostituto documentati; ricevuto un avviso di prova |
| Mappare un servizio importante attraverso identità, hosting, assistenza e ripristino | |
| RESPONSABILE<br>Responsabili del servizio e continuità | PROVA DI COMPLETAMENTO<br>Mappa approvata con dipendenze esterne e canali di contatto |
| Nominare notificante, sostituto e responsabile dell'applicabilità legale | |
| RESPONSABILE<br>CISO e legale | PROVA DI COMPLETAMENTO<br>Matrice approvata per ogni soggetto rilevante |
| Verificare le evidenze attuali sulle identità specifiche dell'organizzazione prima di azioni con effetti operativi | |
| RESPONSABILE<br>Identità e risposta | PROVA DI COMPLETAMENTO<br>Esito datato, appartenenza e interventi documentati |
| Esaminare sessioni, inoltri e modifiche al recupero inspiegati degli account coinvolti | |
| RESPONSABILE<br>Messaggistica e SOC | PROVA DI COMPLETAMENTO<br>Registro dell'indagine e decisioni motivate di contenimento |

### Confermare un canale pubblico sullo stato utilizzabile e indipendente dal sito principale

RESPONSABILE
Comunicazione

PROVA DI COMPLETAMENTO
Modello di messaggio approvato e canale alternativo provato

### Identificare software dei servizi pubblici e applicare aggiornamenti di sicurezza supportati

RESPONSABILE
Responsabili infrastrutture e web

PROVA DI COMPLETAMENTO
Inventario delle versioni e verifica autorizzata della correzione

## 2Giorni 31-60

### Eseguire un ripristino cronometrato del servizio importante, compreso il processo del cliente

RESPONSABILE
Infrastrutture e responsabile del servizio

PROVA DI COMPLETAMENTO
Accettazione aziendale e confronto dei tempi di recupero

### Verificare l'indipendenza degli accessi al ripristino dalle identità di produzione

RESPONSABILE
Identità e continuità

PROVA DI COMPLETAMENTO
Revisione degli accessi, percorso approvato ed esito del test

### Richiedere conferma indipendente di nuovi beneficiari e istruzioni di pagamento modificate

RESPONSABILE
Finanza e tesoreria

PROVA DI COMPLETAMENTO
Procedura e richiesta simulata autorizzata intercettata

### Provare il recupero dei clienti contro un attaccante con informazioni personali plausibili

RESPONSABILE
Antifrode e assistenza

PROVA DI COMPLETAMENTO
Debolezze registrate, corrette e nuovamente provate

### Dare priorità all'autenticazione resistente al phishing per accessi privilegiati e remoti

RESPONSABILE
Identità

PROVA DI COMPLETAMENTO
Copertura e piano approvato delle eccezioni per gruppo di utenti

### Censire i mittenti legittimi prima di rafforzare l'autenticazione del dominio

RESPONSABILE
Messaggistica

PROVA DI COMPLETAMENTO
Responsabili dei mittenti, evidenze di allineamento e piano graduale

### Provare la mitigazione del sito con il fornitore e verifiche reali del servizio

RESPONSABILE

Rete e referente del fornitore

PROVA DI COMPLETAMENTO

Registro della mitigazione e percorso utente verificato

### Richiedere ai fornitori chiave informazioni sull'incidente e sul ripristino specifiche per il cliente

RESPONSABILE

Acquisti e responsabile del servizio

PROVA DI COMPLETAMENTO

Contratto o accordo operativo con contatti e criteri di accettazione

### Esaminare gli accessi dei manutentori ai controlli fisici con i responsabili dei processi

RESPONSABILE

Operazioni e sicurezza fisica

PROVA DI COMPLETAMENTO

Percorsi approvati, monitoraggio e procedura di stato sicuro

## 3Giorni 61-90

### Riconciliare registrazioni offline e ripristinate nell'esercitazione del servizio

RESPONSABILE

Responsabili aziendali e dei dati

PROVA DI COMPLETAMENTO

Elenco eccezioni chiuso o assegnato con accettazione datata

### Simulare notifiche e comunicazioni con evidenze incomplete

RESPONSABILE

Responsabile dell'incidente e legale

PROVA DI COMPLETAMENTO

Registro della conoscenza, motivazione delle notifiche e aggiornamenti cronometrati

### Provare una richiesta di pagamento di un dirigente con documenti plausibili e urgenza

RESPONSABILE

Finanza e antifrode

PROVA DI COMPLETAMENTO

Approvazioni indipendenti ed evidenze del canale di blocco

### Riferire al consiglio test conclusi, eccezioni e responsabilità rimanenti

RESPONSABILE

CISO

PROVA DI COMPLETAMENTO

Documento al consiglio collegato alle evidenze e decisioni successive datate

## 12.2 Cosa conta come completamento

Una procedura scritta serve solo se la decisione può essere attuata. La ricezione delle evidenze richiede un avviso provato. Il ripristino richiede l'accettazione del responsabile del servizio. Una regola sui pagamenti richiede una richiesta simulata che segua il percorso approvato. La matrice delle notifiche richiede un'esercitazione cronometrata con fatti incompleti.

Il consiglio deve distinguere lavoro concluso ed eccezioni accettate. Un'eccezione richiede motivo, responsabile, misura compensativa e data di revisione. Un miglioramento promesso dal fornitore deve restare aperto fino all'arrivo della prova di completamento. Il resoconto del programma deve mantenere la differenza, senza considerare chiuse tutte le azioni pianificate.

| Misura | Criterio di completamento suggerito |
|---|---|
| Ricezione delle evidenze pertinenti | Un test raggiunge la coda responsabile e il sostituto |
| Evidenze attuali sulle identità | Ogni elemento conservato specifico dell'organizzazione ha un esito datato |
| Ripristino del servizio | Il processo aziendale supera il test entro l'obiettivo approvato oppure la correzione ha un responsabile |
| Modifiche ai pagamenti | La conferma indipendente è dimostrata in una prova autorizzata |
| Recupero dei clienti | I tentativi sintetici di impersonificazione producono l'esito approvato |
| Ripristino del fornitore | Sono disponibili fatti specifici del cliente e criteri di accettazione |
| Segnalazione degli incidenti | Sono dimostrati soggetto applicabile, registro della conoscenza, notificante e percorso di aggiornamento |
| Comunicazione | Rivendicazione, effetto accertato e azione dell'utente restano distinti |

Sono criteri di accettazione raccomandati. Non misurano i controlli attuali delle organizzazioni selezionate. Ogni organizzazione deve adattarli a criticità dei servizi, regole interne e obblighi legali.

## 12.3 Prime decisioni per ruolo

| Ruolo | Prima decisione | Evidenza da richiedere |
|---|---|---|
| Consiglio | Quale servizio richiede per primo un ripristino dimostrato? | Mappa delle dipendenze e prova di accettazione aziendale |

| Ruolo | Prima decisione | Evidenza da richiedere |
|---|---|---|
| CISO | Chi riceve le evidenze e può attivare l'escalation? | Ricezione funzionante e coda con responsabile |
| SOC | Quale rivendicazione o segnale possiamo verificare ora? | Registri del fornitore, delle identità e del responsabile del servizio |
| Identità | Quali account, sessioni e stati di recupero sono rilevanti? | Appartenenza, validità e registro del contenimento autorizzato |
| Antifrode | Quale decisione del cliente possono influenzare i dati esposti? | Esiti delle prove di recupero e assistenza |
| Tesoreria | Chi conferma indipendentemente l'autorità di pagamento? | Evidenze di richiamata e approvazione |
| Legale | Quali soggetti e regimi si applicano ai fatti? | Matrice di applicabilità e cronologia della conoscenza |
| Comunicazione | Quale stato del servizio si può dichiarare ora? | Stato verificato dal responsabile e canale del prossimo aggiornamento |
| Operazioni | Quale stato fisico richiede una gestione sicura? | Letture del responsabile del processo e percorsi di accesso approvati |

## 12.4 Evitare controlli che risolvono l'affermazione sbagliata

Non ordinate un cambio generalizzato delle password solo perché un venditore pubblicizza recapiti. Accertate prima se siano coinvolte credenziali o sessioni. Non accettate il sito ripristinato come prova del funzionamento di un processo critico. Provate il processo. Non trattate un'immagine dell'attore come attribuzione finale o valutazione completa dell'impatto.

Analogamente, una politica email più forte non impedisce ogni messaggio da domini imitativi o da caselle già abusate. Mantenete nel piano controlli su identità, pagamenti e processi dei clienti. Le raccomandazioni sono complementari perché le evidenze descrivono più vie di danno.

Un problema sui controlli fisici richiede un responsabile del processo, anche quando gli analisti non possono confermare l'attore. Una decisione legale di notifica richiede fatti pertinenti e ambito, anche durante l'analisi forense. Allineate i responsabili alla decisione che possono verificare, senza aspettare una ricostruzione totale che risolva tutto.

## 12.5 Come può aiutare Brandefense

Brandefense può aiutare i team a collegare informazioni esterne sulle minacce a domini, marchi e servizi gestiti. Questo rapporto usa pubblicazioni osservate, rivendicazioni ransomware pubbliche e notizie verificate per identificare domande da convalidare. Non promette che ogni affermazione criminale sia verificabile o che le credenziali storiche restino utilizzabili.

Discutete con Brandefense quali evidenze servano al team, come raggiungano i responsabili e quale processo di risposta esistente le riceva. Portate dipendenze dei servizi, confini delle identità e problemi di frode ai clienti. L'esito utile è un percorso concordato dalle evidenze alle azioni, con limiti chiari e criteri di completamento.

Richiedi una demo

PUNTI CHIAVE

01

Stabilite prima ricezione funzionante delle evidenze e responsabilità delle notifiche.

02

Dimostrate con prove ripristino, approvazione indipendente dei pagamenti e tutela dei clienti.

03

Riferite evidenze completate ed eccezioni assegnate, non soltanto procedure scritte.

APPENDICI

# Appendici

A–D

QUESTO CAPITOLO RISPONDE

Quali evidenze sostengono l'edizione e dove contano i limiti?

**4**

popolazioni separate: pubblicazioni, rivendicazioni, voci candidate del portafoglio e casi riferiti


Appendice A. Fonti, ambito e confidenza 96

Appendice B. Registro delle evidenze 99

Appendice C. Fonti 102

Appendice D. Glossario 106

# Appendice A. Fonti, ambito e confidenza

I paesi di confronto sono stati scelti come esempi esclusivamente per fornire un contesto; la loro selezione non implica una classifica né una valutazione politica.

## A.1 Periodo e rilevazione

Il periodo principale è 1 gennaio-22 novembre 2026 per data di pubblicazione. Le osservazioni si fermano alla rilevazione del 22 novembre, non alla fine della giornata. La sezione recente copre il 9-22 novembre fino a quel momento. Le date dell'incidente e della pubblicazione restano distinte.

Rapporti ufficiali, decisioni dei regolatori e dichiarazioni di ripristino possono riguardare eventi precedenti. Questi elementi sono etichettati come contesto storico o di comunicazione. Non diventano intrusioni attuali perché pubblicati nel 2026. Gli aggiornamenti modificano un caso esistente, salvo evidenze separate di un altro evento.

## A.2 Popolazioni delle fonti proprie

I conteggi con etichetta nazionale descrivono 802 371 pubblicazioni. Il materiale di forum conservato contiene 839 pubblicazioni con etichetta Italia esaminate separatamente, compreso il sottoinsieme recente di 195 pubblicazioni del 9-22 novembre 2026. Diciassette estratti selezionati illustrano domanda, pubblicità e rivendicazioni. Non stimano la frequenza di ogni tema nell'intera popolazione conteggiata con etichetta nazionale. [S1]

Ransompedia contribuisce registrazioni associate ai Paesi. Le 286 registrazioni italiane e i 270 valori distinti dei nomi delle vittime sono unità diverse. Nessuno dimostra un totale di intrusioni verificate o un censimento dell'estorsione. Etichette dei gruppi e date di pubblicazione mantengono il significato della fonte. I confronti regionali usano la stessa fonte conservando limiti di popolazione e copertura. [S2]

Il portafoglio candidato di 250 voci è selezionato per ruolo. Il valore nazionale Atlas è 57 su 100. Alla verifica, le offerte di credenziali erano associate a 132 voci candidate. Associazioni di dispositivi e credenziali si sovrappongono. La risposta dei domini non ne dimostra appartenenza o indipendenza. Le misure dei controlli passivi restano non disponibili. [S3]

## A.3 Casi da fonti pubbliche

La ricerca pubblica ha considerato avvisi informatici ufficiali, dichiarazioni pubbliche, stampa, decisioni dei regolatori e materiale sulla risposta giudiziaria. I passaggi usati come fatti sono stati letti. Dichiarazioni dirette, documenti ufficiali riprodotti altrove e dichiarazioni aziendali citate dalla stampa mantengono descrizioni differenti nel rapporto.

La ricerca ha considerato materiale italiano, inglese, russo e turco. La visione delle fonti resta incompleta, soprattutto per alcuni archivi delle autorità e la copertura delle singole organizzazioni. Il rapporto non dichiara un censimento nazionale completo. L'assenza di un caso non dimostra che non sia avvenuto un incidente.

Le interrogazioni parlamentari richiedono particolare attenzione. Le premesse possono ripetere accuse e notizie. Non sono automaticamente risultati del governo o dell'ente coinvolto. Una risposta ministeriale è un tipo di evidenza diverso. Il rapporto conserva questa distinzione nella discussione sulla refrigerazione e nell'esclusione del disservizio tecnico.

## A.4 Schede e relazioni

I riferimenti B riproducono brevi estratti oscurati delle pubblicazioni conservate. Omissioni e identificatori rimossi compaiono tra parentesi quadre. I riferimenti P identificano parafrasi di casi da fonti pubbliche, compresi campagne e un'esclusione. Un riferimento P non è una citazione autentica dell'attore.

Un alias comune sostiene un'associazione tra pubblicazioni. Titoli simili, riconoscimenti a un altro alias o campi sovrapposti non dimostrano identità dei file, paternità, operatori comuni o vendite concluse. Le mappe indicano le evidenze dei collegamenti. Sequenze più ampie di frode sono modelli analitici, salvo un collegamento concreto mostrato.

## A.5 Materiale sulle carte

Il materiale sulle carte è limitato a carte di pagamento apparse in chiaro nelle pubblicazioni raccolte per il rapporto. Brandefense rileva carte rubate anche con altri metodi esterni al rapporto. La popolazione non misura furti nazionali di carte, carte attive o perdite per frode. L'azione dell'emittente richiede una propria verifica. [S4]

## A.6 Confidenza e alternative

L'alta confidenza può descrivere una pubblicazione conservata o il testo di una dichiarazione ufficiale senza convalidare l'affermazione criminale sottostante. La confidenza media descrive un'interpretazione con un riscontro e un'alternativa esplicita. Non verificato significa non accertato indipendentemente; non significa falso o confermato.

Un incidente confermato può mantenere ignoti attore, ambito dell'estrazione o accesso iniziale. Un servizio ripristinato può mantenere domande irrisolte sui dati. Una rivendicazione può rilevare per il monitoraggio senza dimostrare intrusioni. Il rapporto tiene separate queste affermazioni in sintesi, schede, figure e raccomandazioni.

## A.7 Nomi e protezione dei dati

I nomi delle vittime sono usati solo quando il pacchetto registra conferma ufficiale e ampia copertura giornalistica. Negli altri casi, le descrizioni restano abbastanza generiche da adattarsi a più organizzazioni. I percorsi delle fonti che nominano vittime non pubblicate sono sostituiti dal sito dell'editore, omettendo l'indirizzo dell'articolo. La corrispondenza esatta resta nel registro privato delle evidenze.

Gli alias degli attori compaiono solo quando servono a spiegare le evidenze. Contatti, informazioni personali, identificatori delle vittime e materiale offensivo funzionante sono esclusi. Il rapporto non afferma che Brandefense abbia inviato notifiche, salvo che un registro datato lo dimostri.

## A.8 Confronto con edizioni successive

Le edizioni successive devono indicare popolazione, data e denominatore propri. Un dominio candidato resta una voce candidata finché non sia convalidato da evidenze specifiche dell'organizzazione. Una nuova conferma ufficiale aggiorna il caso pertinente senza modificare la data storica dell'osservazione.

Cifre di sintesi, tabelle, schede delle evidenze e grafici usano le stesse popolazioni della rilevazione nell'edizione inglese e in quella italiana.

# Appendice B. Registro delle evidenze

## B.1 Estratti delle pubblicazioni conservate

I riferimenti B sono evidenze oscurate delle pubblicazioni. Le date di pubblicazione non dimostrano quelle delle intrusioni. Le indicazioni Accertato e Non accertato nelle schede definiscono l'affermazione sostenuta.

| Scheda | Pubblicazione | Sede | Alias | Lingua | Capitolo |
|---|---|---|---|---|---|
| B01 | 2026-02-10 | Forum | kurkenluvsdh | Inglese | 4 |
| B02 | 2026-04-18 | Forum | Jiskaa | Inglese | 4 |
| B03 | 2026-01-27 | Forum | exelo | Inglese | 4 |
| B04 | 2026-08-19 | Forum | Jaded | Inglese | 4 |
| B05 | 2026-06-04 | Forum | Bot del forum | Inglese | 4 |
| B06 | 2026-08-20 | Forum | MegaCloud | Inglese | 4 |
| B07 | 2026-09-28 | Forum | updap | Inglese | 4 |
| B08 | 2026-10-18 | Forum | updap | Inglese | 4 |
| B09 | 2026-08-06 | Forum | wizard | Inglese | 4 |
| B10 | 2026-11-11 | Forum | Linda2000 | Inglese | 4 |
| B11 | 2026-02-02 | Forum | Tanaka | Inglese | 4 |
| B12 | 2026-04-02 | Forum | Venditore del forum | Inglese | 4 |
| B13 | 2026-05-18 | Forum | Venditore del forum | Inglese | 4 |
| B14 | 2026-05-14 | Forum | Venditore del forum | Inglese | 4 |
| B15 | 2026-04-26 | Forum | Venditore del forum | Inglese | 4 |
| B16 | 2026-01-30 | Forum | Venditore del forum | Inglese | 4 |
| B17 | 2026-06-06 | Canale di ripubblicazione in spagnolo | Ripubblicazione del canale | Spagnolo | 6 |

## B.2 Casi ed esclusioni da fonti pubbliche

I riferimenti P identificano analisi basate sulle fonti, non citazioni clandestine. La colonna delle date distingue evento, pubblicazione o aggiornamento quando necessario.

| Riferimento | Data | Ruolo | Tipo di evidenza | Capitolo |
|---|---|---|---|---|
| P01 | 2026-02-01; aggiornamento 2026-04-09 | Università | Incidente confermato e avviso di ripristino | 5 |
| P02 | 2026-03-23; notizie di aprile | Cloud e processo comunale | Interruzione riconosciuta dall'azienda e rivendicazione | 5 |
| P03 | Febbraio; notizie di aprile | Amministrazione museale | Incidente e successive accuse contestate | 5 |
| P04 | Agosto; avviso 2026-09-16 | Servizio idrico | Dichiarazione ufficiale di ripristino aziendale | 5 |
| P05 | 2026-08-31; avvisi di settembre; aggiornamento 2026-11-17 | Gruppo sanitario | Dichiarazioni della Direzione e aggiornamento privacy riferiti dalla stampa | 5 |
| P06 | Avviso 2026-11-17 | Cooperativa di consumo | Dichiarazione diretta sull'accesso ai recapiti | 5 |
| P07 | Notizie 2026-11-19 | Servizio documentale | Conferma aziendale citata dalla stampa | 5 |
| P08 | Evento di ottobre; comunicazione di novembre | Progetto dei trasporti | Dichiarazione aziendale citata dalla stampa | 5 |
| P09 | Rapporto operativo di agosto | Fornitore ICT | Resoconto ufficiale anonimo del caso | 5 |
| P10 | Avviso 2026-01-27 | Utenti della posta pubblica | Osservazione ufficiale di campagna | 5 |
| P11 | Avviso 2026-01-30 | Destinatari di richieste di documenti identificativi | Osservazione ufficiale di campagna | 5 |
| P12 | 2026-05-06; risposta di giugno | Servizio IT giudiziario | Disservizio tecnico escluso dal conteggio informatico | 5 |

## B.3 Conteggio degli esempi

Il rapporto contiene diciotto schede caso: sei casi clandestini e dodici riferimenti pubblici. Questi ultimi comprendono nove casi relativi a incidenti, due campagne e un'esclusione. Un caso ufficiale anonimo può comunque avere una data imprecisa. Sono conteggi di casi di studio, non un totale nazionale degli incidenti.

Il registro privato di copertura mantiene altre menzioni, contesto storico e candidati esclusi con motivazioni. Un aggiornamento riferito può condividere la chiave dell'incidente con un avviso precedente. La sola data di pubblicazione non basta a creare una nuova voce di incidente.

# Appendice C. Fonti

I numeri di fonte che non compaiono sono stati ritirati durante la revisione e non sono citati.

**S1:** Odin by Brandefense, Italy-tagged post counts and retained forum observations, publication dates 1 January–22 November 2026, collection snapshot 22 November 2026. Own data; no public source address.

**S2:** Brandefense Ransompedia, Italy and regional comparison listing records, extracted 22 November 2026. Own data; no public source address.

**S3:** Brandefense Atlas, valutazioni dell'esposizione, associazioni ai domini di Blackhole, portafoglio selezionato di voci candidate e prime osservazioni dei domini pubblici, 21–22 novembre 2026. Misure dei controlli passivi non disponibili. Dati propri; nessun indirizzo pubblico della fonte.

**S4:** Odin by Brandefense, narrow card-material review of retained posts, 22 November 2026. Own data; no public source address.

**S5:** Sapienza Università di Roma, "Chiusura dell'incidente informatico dello scorso febbraio", 9 April 2026. https://www.uniroma1.it/it/node/538826. Verified on 22 November 2026.

**S6:** ANSA, "Attacco hacker all'università La Sapienza di Roma", 2 February 2026. https://www.ansa.it/amp/canale_legalita_scuola/notizie/mur/2026/02/02/attacco-hacker-alluniversita-la-sapienza-di-roma_5bce4cb1-c3a0-45bc-a888-8b8eed713b7c.html. Verified on 22 November 2026.

**S7:** Unicoop Firenze, official incident press note, 17 November 2026. https://www.coopfirenze.it/news-e-media/comunicati-stampa/nota-stampa. Verified on 22 November 2026.

**S8:** Unicoop Firenze, security information and incident questions. https://www.coopfirenze.it/news-e-media/sicurezza. Verified on 22 November 2026.

**S9:** ANSA, report of Unicoop Firenze's incident statement and membership context, 17 November 2026. https://www.ansa.it/toscana/notizie/2026/11/17/attacco-hacker-a-banca-dati-unicoop-firenze-coop-con-12-milioni-di-soci_9dbd5b8d-512c-4d76-bf30-171f84b4a9ac.html. Verified on 22 November 2026.

**S10:** ACN, Operational Summary febbraio 2026, official-authored report first published on 26 March 2026 and reproduced in its March 2026 revised file by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/03/Operational_Summary_feb26_CLEAR_rev.pdf. Verified on 23 November 2026.

**S11:** Associated Press, "Italy averted Russian-linked cyberattacks targeting Winter Olympics websites, foreign minister says", 4 February 2026. https://apnews.com/article/italy-winter-olympics-us-cyberattacks-security-01b6af8e64606f31836c91faa6653d12. Verified on 22 November 2026.

**S12:** Foreign ministry, official notice on mitigated website attacks, 8 October 2026. https://www.esteri.it/it/sala_stampa/archivionotizie/comunicati/2026/10/la-farnesina-respinge-nuovi-tentativi-di-attacchi-informatici-al-proprio-sito-e-alle-infrastrutture-nazionali/. Verified on 22 November 2026.

**S13:** ACN, Operational Summary agosto 2026, official-authored report reproduced by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/09/Operational_Summary_ago26_CLEAR.pdf. Verified on 22 November 2026.

**S14:** ACN, Operational Summary maggio 2026, official-authored report reproduced by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/06/Operational_Summary_mag26_CLEAR.pdf. Verified on 22 November 2026.

**S15:** CERT-AGID, tax-brand impersonation seeking SPID credentials, 20 January 2026. https://cert-agid.gov.it/news/sfruttato-il-logo-di-ade-per-una-campagna-di-phishing-mirata-al-furto-di-credenziali-spid/. Verified on 22 November 2026.

**S16:** CERT-AGID, renewed health-card-expiry phishing campaigns, 22 January 2026. https://cert-agid.gov.it/news/ancora-una-campagna-di-phishing-su-scadenza-tessera-sanitaria-breve-sintesi-del-contesto/. Verified on 22 November 2026.

**S17:** CERT-AGID, public-administration mailbox abuse and credential phishing using a collaboration platform, 27 January 2026. https://cert-agid.gov.it/news/sfruttate-utenze-della-pa-compromesse-per-tentare-il-furto-di-credenziali-microsoft-365-tramite-figma/. Verified on 22 November 2026.

**S18:** CERT-AGID, benefit-themed smishing collecting income and employment information, 30 January 2026. https://cert-agid.gov.it/news/smishing-a-tema-inps-finiscono-nel-mirino-anche-i-dati-del-cud-e-le-informazioni-lavorative/. Verified on 22 November 2026.

**S19:** CSIRT Toscana, official republication of CSIRT-ITA bulletin on ClickFix and abused WordPress sites, 27 January 2026. https://csirt.regione.toscana.it/clickfix-portali-wordpress-vulnerabili-utilizzati-per-distribuire-codice-malevolo-bl01-260127-csirt-ita/. Verified on 22 November 2026.

**S20:** CSIRT Toscana, official republication of CSIRT-ITA business email compromise bulletin, 17 February 2026. https://csirt.regione.toscana.it/thread-hijacking-rilevate-attivita-malevole-che-utilizzano-tecniche-di-business-email-compromise-bl01-260217-csirt-ita/. Verified on 22 November 2026.

**S21:** CERT-AGID, weekly campaign review for 14-20 March 2026. https://cert-agid.gov.it/news/sintesi-riepilogativa-delle-campagne-malevole-nella-settimana-del-14-20-marzo/. Verified on 22 November 2026.

**S22:** CSIRT Umbria, digital-identity phishing warning, 23 April 2026. https://csirt.regione.umbria.it/novita/cybersecurity-alert-14/. Verified on 22 November 2026.

**S23:** ANSA, museum administrative incident and disputed later security allegations, 3 April 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

**S24:** Cybersecitalia, report quoting a cloud provider's incident acknowledgement, 27 March 2026. Article URL withheld to protect victim identity. https://www.cybersecitalia.it/. Verified on 22 November 2026.

**S25:** ANSA, cloud-provider interruption and municipal payment-service investigation, 1 April 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

**S26:** Alto Calore, "Siamo tornati", 16 September 2026. Wide-reporting checks include Tom's Hardware, 14 September, and Irpiniaoggi, 28 September. https://altocalore.it/siamo-tornati/. Verified on 22 November 2026.

**S27:** Nordestnews, healthcare Direction's incident statement reproduced on 3 September 2026. Article URL withheld to protect victim identity. https://www.nordestnews.it/. Verified on 22 November 2026.

**S28:** Rai, healthcare service interruption and manual-work reporting, September 2026. Article URL withheld to protect victim identity. https://www.rainews.it/. Verified on 22 November 2026.

**S29:** Trieste Cafe, healthcare Direction's recovery update reproduced on 10 September 2026. Article URL withheld to protect victim identity. https://www.triestecafe.it/. Verified on 22 November 2026.

**S30:** l'Adige, transport-project company incident statement and investigation, November 2026. Article URL withheld to protect victim identity. https://www.ladige.it/. Verified on 22 November 2026.

**S31:** Cybersecurity360, company-confirmed document-related incident and fraud-risk reporting, 19 November 2026. Article URL withheld to protect victim identity. https://www.cybersecurity360.it/. Verified on 22 November 2026.

**S32:** Fanpage, company confirmation and journalists' observations of contract and identity material, November 2026. Article URL withheld to protect victim identity. https://www.fanpage.it/. Verified on 22 November 2026.

**S34:** Camera dei deputati, parliamentary questions concerning reported refrigeration incidents. Preambles are questioners' statements. (article URL withheld). https://www.camera.it/ Verified on 22 November 2026.

**S35:** Rai, manager account of changed refrigeration temperatures without confirmation of cyber cause, 3 November 2026. Article URL withheld to protect victim identity. https://www.rainews.it/. Verified on 22 November 2026.

**S36:** L'Espresso, school-threat messages and the distinction from system intrusion, 13 November 2026. https://lespresso.it/c/innovazione/2026/11/13/attacchi-informatici-scuole-allarmi-bomba-educazione-digitale-in-italia/65911. Verified on 22 November 2026.

**S38:** Carabinieri, official digital-fraud investigation statement, 3 June 2026; underlying activity November 2025-May 2026. https://www.carabinieri.it/in-vostro-aiuto/informazioni/comunicati-stampa/truffe-digitali-operazione-nella-capitale-44-denunce-e-1-milione-di-euro-recuperato. Verified on 22 November 2026.

**S39:** ANSA, Polizia Postale banking-impersonation investigation under prosecutor coordination, 3 July 2026. https://www.ansa.it/puglia/notizie/2026/07/03/si-spacciavano-per-operatori-bancari-truffando-utenti-18-arresti_c2db0c8e-daef-4ca2-83c5-f5c8d4cb890f.html. Verified on 22 November 2026.

**S40:** Garante, 2026 decision concerning telecom incidents notified in February 2025 (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

**S41:** Garante, 2026 decision concerning an April 2024 consultancy incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

**S42:** Garante, 2026 decision concerning a historical engineering-consultancy incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

**S43:** Garante, 2026 decision on a historical editorial-mailbox incident and reporting duties (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

**S44:** Garante, 2026 decision on a historical healthcare-software incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

**S45:** La Repubblica, rail-customer notification reporting concerning late-2025 activity, 26 June 2026. Article URL withheld to protect victim identity. https://www.repubblica.it/. Verified on 22 November 2026.

**S46:** Camera dei deputati, published ministerial answer on a supplier technical fault affecting judicial services, 26 June 2026. https://documenti.camera.it/leg19/resoconti/assemblea/html/sed0682/leg.19.sed0682.allegato_b.pdf. Verified on 22 November 2026.

**S49:** ACN, Operational Summary ottobre 2026, official-authored document published 20 November and read through its reproduced source text. https://media.agenziagiornalisticaopinione.it/2026/11/Operational_Summary_ott26_CLEAR.pdf. Verified on 22 November 2026.

**S50:** Gazzetta Ufficiale, Legislative Decree 138/2024, including Article 25; Italy's NIS2 transposition. https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/sg. Verified on 22 November 2026.

**S51:** ACN, Vademecum NIS, September 2026 edition, official-authored guide reproduced by Sistema FairPlay. https://www.sistemafairplay.it/pdf/news/VademecumNIS_2026_v1.pdf. Verified on 22 November 2026.

**S52:** Gazzetta Ufficiale, Law 90/2024, Article 1. https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.codiceRedazionale=24G00108&art.dataPubblicazioneGazzetta=2024-07-02&art.flagTipoArticolo=0&art.idArticolo=1&art.idGruppo=1&art.idSottoArticolo=1&art.idSottoArticolo1=10&art.progressivo=0&art.versione=1. Verified on 22 November 2026.

**S53:** Garante, official guidance on personal-data breach notification and communication. https://www.garanteprivacy.it/data-breach. Verified on 22 November 2026.

**S54:** EUR-Lex, Regulation (EU) 2022/2554, Digital Operational Resilience Act. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng. Verified on 22 November 2026.

**S56:** ANSA, report on alleged executive-payment fraud, prosecutor investigation and differing recovery figures, 25 September 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

**S57:** Guardia di Finanza, online-fraud enforcement statement concerning alleged 2022-2025 activity, 25 May 2026. https://www.gdf.gov.it/it/gdf-comunica/notizie-ed-eventi/comunicati-stampa/anno-2026/maggio/truffe-online-e-carte-di-credito-clonate. Verified on 22 November 2026.

**S58:** CSIRT Toscana, official republication of CSIRT-ITA bulletin on Joomla Content Editor exploitation and Italian defacement, 17 September 2026. https://csirt.regione.toscana.it/joomla-jce-rilevato-sfruttamento-cve-2026-48907-al-fine-di-distribuire-webshell-utilizzate-per-defacement-bl01-260917-csirt-ita/. Verified on 22 November 2026.

**S59:** Joomla Content Editor, vendor fix and legacy security-patch notices, June 2026. https://www.joomlacontenteditor.net/news/jce-pro-2-9-99-5-released and https://www.joomlacontenteditor.net/downloads/editor/security-patch/security-patch-for-jce-2-7-x-to-2-9-x. Verified on 22 November 2026.

**S60:** NIST National Vulnerability Database, CVE-2026-48907; official record checked for this review. https://nvd.nist.gov/vuln/detail/CVE-2026-48907. Verified on 22 November 2026.

**S61:** ESET, research press notice on Webworm European government targeting; 2026 publication concerning 2025 activity. https://www.eset.com/us/about/newsroom/research/eset-research-china-aligned-webworm-european-governments-targeted/. Verified on 22 November 2026.

**S62:** ESET WeLiveSecurity, "Webworm: New burrowing techniques"; historical campaign analysis and vendor technique table. https://www.welivesecurity.com/en/eset-research/webworm-new-burrowing-techniques/. Verified on 22 November 2026.

**S63:** Council of the European Union, Council Decision (CFSP) 2026/2546, dated 16 November 2026, restrictive-measures annex. https://publications.europa.eu/resource/cellar/c1d158d5-e1a2-11f1-aefc-01aa75ed71a1.0006.01/DOC_1. Verified on 22 November 2026.

**S64:** Rai, regional health executive's account of earlier booking-system abnormal activity and countermeasures, 16 November 2026. https://www.rainews.it/ (article URL withheld). Verified on 22 November 2026.

**S65:** ANSA, report corroborating ACN's October operational figures, 20 November 2026. https://www.ansa.it/sito/notizie/cronaca/2026/11/20/agenzia-cyber-ad-ottobre-rilevati-473-account-di-istituzioni-compromessi_cf5ebefa-c41a-43c7-9d2d-b1441db9abaa.html. Verified on 22 November 2026.

**S66:** Banca d'Italia, instructions for major ICT incidents and significant cyber threats under DORA. https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html. Verified on 22 November 2026.

**S67:** Ministry of Economy and Finance, amended Law 90/2024 Article 1, in force from 10 October 2025. https://def.finanze.it/DocTribFrontend/executePrintArticolo.do?articolo=Articolo+1&codiceOrdinamento=0000000000000010000000000000

# Appendice D. Glossario

- **Recupero dell'account:** processo per riottenere accesso dopo la perdita di password, dispositivo o altro fattore di autenticazione.
- **Rivendicazione dell'attore:** affermazione di un venditore o autore non accertata indipendentemente.
- **Popolazione interessata:** persone, account o organizzazioni sostenuti dalle evidenze di un particolare evento.
- **Frode tramite email aziendali:** inganno che usa comunicazioni commerciali per ottenere pagamenti non autorizzati o altre azioni aziendali.
- **Insieme candidato:** elenco selezionato da verificare prima che le misure descrivano confini organizzativi confermati.
- **Combolist:** elenco di coppie di indirizzi email o nomi utente e password. [S70]
- **Etichetta nazionale:** associa una pubblicazione a un Paese senza dimostrare che sia un bersaglio ostile.
- **Credenziale:** informazione usata per accedere, per esempio nome utente e password.
- **DDoS:** interruzione distribuita del servizio, con traffico da più fonti per comprometterne la disponibilità.
- **DMARC, SPF e DKIM:** standard di autenticazione email che sostengono verifiche su mittenti consentiti e uso dei domini.
- **DNSSEC:** firme che sostengono la verifica delle informazioni DNS.
- **DORA:** regolamento UE sulla resilienza operativa digitale, per soggetti e rapporti compresi nel suo ambito finanziario.
- **Valutazione dell'esposizione:** giudizio sintetico che richiede una popolazione della fonte definita e non dimostra di per sé un'intrusione.
- **Esfiltrazione:** rimozione non autorizzata di informazioni; un annuncio da solo non dimostra che sia avvenuta.
- **GDPR:** regolamento generale UE sulla protezione dei dati.
- **HSTS:** istruzione del sito che indica ai browser compatibili di usare connessioni HTTPS cifrate.
- **Verifica dell'identità:** accertare che una persona sia chi dichiara di essere.
- **Voce di rivendicazione:** affermazione pubblicata di estorsione o possesso di dati, che può restare non verificata o ripetere materiale precedente.
- **MFA:** autenticazione che usa più di un fattore.
- **NIS2:** direttiva UE sulla sicurezza delle reti e delle informazioni, recepita in Italia dal decreto legislativo 138/2024.
- **Phishing:** messaggi o pagine ingannevoli che cercano informazioni, accessi o azioni dannose.
- **Autenticazione resistente al phishing:** accesso progettato per collegare l'autenticazione al servizio legittimo anziché a una pagina copiata.
- **Ransomware:** software malevolo usato per limitare l'accesso a sistemi o informazioni, comunemente in un tentativo di estorsione.
- **RDWEB:** Remote Desktop Web Access, un portale web per l'accesso a desktop remoti. [S72]

- **Obiettivo di ripristino:** traguardo approvato dall'azienda per ripristinare un servizio o limitare la perdita di dati.
- **Ripubblicazione:** ripetizione da parte di terzi di un'affermazione dell'attore o di un'altra fonte.
- **Sessione:** periodo di accesso autenticato che può restare rilevante dopo un cambio di password.
- **Rilevazione:** momento in cui si fermano le osservazioni per un'edizione.
- **SPID:** sistema pubblico italiano di identità digitale.
- **Log di infostealer:** registrazione di dati di accesso catturati da malware che sottrae informazioni su un dispositivo infetto. [S69]
- **Amministrazione del tenant:** gestione dell'ambiente di un'organizzazione all'interno di un servizio cloud. Quell'ambiente è il tenant. [S73]
- **TLP:CLEAR:** informazioni condivisibili senza restrizioni secondo il Traffic Light Protocol, fatti salvi altri obblighi applicabili.
- **TLS:** protocollo che sostiene connessioni di rete cifrate e verifiche dei certificati dei server.
- **Webshell:** codice sul server che permette azioni remote non autorizzate; il rapporto non fornisce esempi funzionanti.

# Informazioni sul rapporto

Preparato da Odin by Brandefense per la serie Brandefense Country Report · Italy 2026. La versione 1.0 è stata pubblicata per la prima volta il 22 novembre 2026 e rivista il 23 novembre 2026; registra osservazioni fino alla rilevazione del 22 novembre 2026. Il periodo principale per data di pubblicazione inizia il 1 gennaio 2026. La sezione recente copre il 9-22 novembre fino alla rilevazione.

Il rapporto mantiene separate osservazioni, rivendicazioni, attribuzioni delle fonti e interpretazioni degli analisti. Non stima tutta la criminalità informatica che interessa l'Italia. Le raccomandazioni descrivono attività che un'organizzazione può verificare; non affermano che ogni organizzazione attualmente manchi di quei controlli. Il valore nazionale Atlas descrive il portafoglio selezionato. Le misure dei controlli passivi restano non disponibili in questa edizione.

L'edizione italiana è tradotta dal master inglese con assistenza dell'IA e riporta l'avviso "Tradotto con l'IA". In caso di differenze di significato prevale l'edizione inglese.

© 2026 Brandefense. Tutti i diritti riservati.

ABOUT BRANDEFENSE

# Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
**4.7** / 5

COVERAGE
**3** pillars
CTI, DRPS, EASM

MONITORING
**24** / 7
Open, deep and dark web

REQUEST A DEMO

## Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

# Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.




### Top InfoSec Innovator

2026




### Deloitte Technology Fast 500 EMEA

2024




### Global InfoSec Awards

2025




### Cybersecurity Excellence Awards

2025

## See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

# See what attackers see. Before they act.


UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO