ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 51 / 30 · COMMODITY MALWARE

Loader and Stealer Feeds
Seven Relay Candidates, 908 Held Rows

How 3,500 examined endpoints across 3,311 hosts split into seven cloud and VPS relay candidates, 700 victim-labelled Ramnit rows, and 208 telecom and CDN collisions

Two-week observation window ending 21 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

11,819
Global feed sightings across Emotet, RedLine Stealer, Raccoon Stealer, LokiBot, and Ramnit

7 / 6 IPs
Dedicated cloud and VPS relay candidates (5 Emotet, 2 RedLine) across 6 withheld IPv4s; C2 uncorroborated

700 / 599
Examined victim-labelled Ramnit endpoints withheld across 599 hosts

208 / 42
Broadband telecom ISP, Emotet-labelled carrier, and Cloudflare or Akamai rows across 42 networks

What Is in This Report. 11 chapters and two appendices.

How 3,500 examined endpoints across 3,311 hosts split into seven cloud and VPS relay candidates, 700 victim-labelled Ramnit rows, and 208 telecom and CDN collisions

01	Executive Summary	04
02	Five Malware Labels, One Analytical Model	07
03	Cloud and VPS Relay Candidates: Emotet and RedLine Stealer	11
04	Proxy-Fronted Panels and Victim Feeds: Raccoon, LokiBot, and Ramnit	14
05	Why Blind IP Blocking Breaks Broadband ISPs, CDNs, and Victim Networks	17
06	Feed Labels Against Cloud and VPS Relay Candidates	21
07	What Defenders Should Do	24
08	Detection Rules	26
09	Indicators	29
10	Scope and Limits	32
11	Sources	34
A	Indicators of compromise (8)	36
B	Detection rules (4 files)	37

IN SHORT

In a two-week observation window ending 21 November 2026, Odin by Brandefense examined 3,500 endpoints across 3,311 hosts from 11,819 sightings labelled as Emotet, RedLine Stealer, Raccoon Stealer, LokiBot, and Ramnit. Only seven cloud and VPS endpoints across six IPv4 addresses survived initial collision checks, and none carried independent C2 beacon corroboration. Meanwhile, all 700 examined Ramnit rows carried an upstream victim label and 208 rows sat on broadband ISPs or shared CDNs. Keep unverified feed IPs off static block lists and hunt HTTP, SOAP, and process signals.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 21 November 2026, Odin by Brandefense examined 3,500 endpoints across 3,311 hosts from 11,819 sightings labelled as Emotet, RedLine Stealer, Raccoon Stealer, LokiBot, and Ramnit. Only seven cloud and VPS endpoints across six IPv4 addresses survived initial collision checks, and none carried independent C2 beacon corroboration. Meanwhile, all 700 examined Ramnit rows carried an upstream victim label and 208 rows sat on broadband ISPs or shared CDNs. Keep unverified feed IPs off static block lists and hunt HTTP, SOAP, and process signals.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Security teams frequently import bulk malware feeds into perimeter firewalls without cyber threat intelligence platform review, expecting every listed IPv4 address to belong to an attacker server. Across these feeds, upstream exports mix cloud and VPS listings with broadband, shared proxy, and victim-labelled addresses.

Blocking raw Emotet or Ramnit IP lists cuts off broadband subscribers, breaks websites behind Cloudflare, and leaves proxy-fronted panels that defenders can review with external attack surface management online. Because none of the 3,311 hosts in our study spans two families, we present the five families as an analytical model.

1. **Only seven cloud and VPS relay candidates remain among 3,500 examined rows.**
   Across 11,819 global sightings and 34 upstream "confirmed" records, collision filtering left five Emotet endpoints on four cloud and VPS addresses plus two RedLine Stealer endpoints. Because independent C2 beacon corroboration is not documented for those six addresses, all 3,500 examined endpoints across 3,311 hosts stay withheld.

2. **All 700 examined Ramnit rows carry an upstream victim label and were withheld.**
   Ramnit accounts for 6,804 global sightings (57.6% of the five-family total) and carries an explicit victim classification in upstream feeds. That pool includes four entries marked verified on FTP port 21 and port 8443. Blocking raw Ramnit exports blackholes 599 victim-labelled enterprise and broadband hosts in China, South Korea, Thailand, and Indonesia rather than verified attacker command servers.

3. **Telecom carriers and shared CDNs account for 208 collateral collision rows.**
   Seventy-three LokiBot candidates sit behind shared Cloudflare proxies; 66 Emotet rows sit on broadband carriers or Akamai edge nodes; 65 RedLine and four Raccoon rows belong to subscriber ISPs. Network signatures for SOAP contracts, PHP gates, and multipart POSTs can flag matching traffic without static IP blocks; each match needs triage.

Three Decisions for Leaders

1. **Require an independent protocol or endpoint signal before blocking feed IPv4 addresses.** Even the seven dedicated cloud and VPS relay candidates across Amazon Web Services, DigitalOcean, and Hetzner lacked documented C2 beacon proof. Keep all 3,500 uncorroborated, ISP, CDN, and victim-labelled endpoints out of static firewall deny lists.
2. **Quarantine victim-tagged botnet feeds and shared CDN ranges before firewall import.** Route Ramnit victim records, broadband telecom networks, and Cloudflare or Akamai proxy addresses to threat-hunting workflows instead of outbound deny lists.
3. **Shift loader and stealer defense to wire-level HTTP, SOAP, and endpoint process rules.** Alert on RedLine WCF SOAP headers, LokiBot PHP submission paths, Raccoon `/config` posts, and `regsvr32.exe` or `rundll32.exe` outbound network sessions.

The Study in Numbers

Number	What it is
11,819	Global feed sightings across Emotet, RedLine Stealer, Raccoon Stealer, LokiBot, and Ramnit
3,500 / 3,311	Examined endpoints (700 per family) across 3,311 distinct hosts and 2,368 `/24` subnets
7 / 6 IPs	Dedicated cloud and VPS relay candidates (5 Emotet, 2 RedLine) across 6 withheld IPv4s; C2 uncorroborated
700 / 599	Examined victim-labelled Ramnit endpoints withheld across 599 hosts
208 / 42	Broadband telecom ISP, Emotet-labelled carrier, and Cloudflare or Akamai rows across 42 networks
2,585	Other unconfirmed port, TLS fingerprint, and historical panel candidates held for hunting
8	Published TLS JARM indicators in Appendix A (plus 5 text-only wire signatures in Chapter 9)

How to use this report.

Security leaders can start with Chapters 1, 6, and 7. Network and firewall teams should read Chapters 3, 4, 5, and 7. SOC analysts and detection engineers should go directly to Chapters 8 and 9. Threat intelligence analysts will find the hosting breakdown and scope limits in Chapters 2, 5, 6, and 10; the Odin Research blog collects related cases.

02

CHAPTER 02

Five Malware Labels, One Analytical Model

IN SHORT

Zero hosts among the 3,311 distinct hosts in our sample carry labels from more than one family. We present Emotet, RedLine Stealer, Raccoon Stealer, LokiBot, and Ramnit together as an analytical model of feed-list collisions, not as one threat actor. Keep uncorroborated feed lists off firewalls and hunt protocol signals.

INSIDE THIS CHAPTER

From 11,819 global sightings to 3,500 examined endpoints 07

Geographic and hosting split 08

02 Five Malware Labels, One Analytical Model

Modular Windows loaders (Emotet), Malware-as-a-Service information stealers (RedLine Stealer and Raccoon Stealer), PHP credential panels (LokiBot), and legacy banking worms (Ramnit) serve distinct criminal roles. Even so, threat feeds often ship all five inside one indicator stream without separating attacker servers from victim or proxy addresses. None of the five families in this report overlaps with Monographs 24 or 35.

Comparing host records across all 3,500 examined endpoints shows zero shared hosts across families. Our 3,311 distinct hosts equal 678 Emotet, 683 RedLine, 700 Raccoon, 651 LokiBot, and 599 Ramnit hosts, with zero shared custom certificates across the seven cloud and VPS relay candidates. At the `/24` prefix level (2,368 distinct `/24` blocks), 21 commercial hosting blocks hold candidates from two families.

Those 21 blocks include 10 Raccoon and RedLine, 8 LokiBot and RedLine, 2 LokiBot and Raccoon, and 1 Emotet and Raccoon prefixes. The shared prefixes may reflect co-tenant VPS hosting at M247 Europe SRL, Hetzner Online GmbH, OVH SAS, and Delis LLC; they do not establish operator identity. Figure 1 maps the four functional groups in our analytical model and their defensive split.

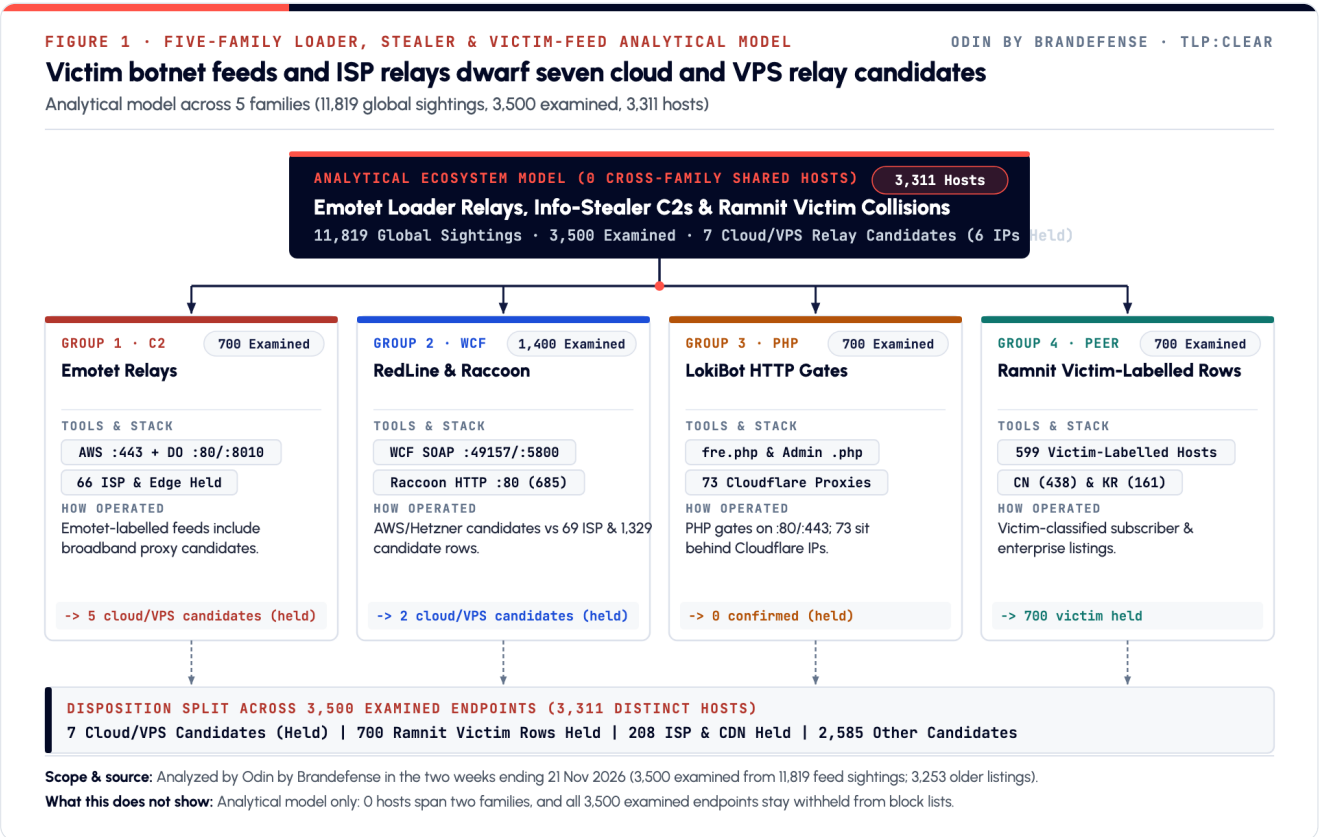


Figure 1: Victim botnet feeds and ISP relays dwarf seven cloud and VPS relay candidates

From 11,819 global sightings to 3,500 examined endpoints

Global sightings total 11,819 entries across the five families. Ramnit leads with 6,804 sightings across 47 countries (57.6%), followed by RedLine Stealer with 2,247 across 48 countries (19.0%) and Emotet with 1,053 across 59 countries (8.9%).

LokiBot accounts for 885 sightings across 8 countries (7.5%), and Raccoon Stealer accounts for 830 across 34 countries (7.0%). Upstream feeds assign Emotet, RedLine, and Raccoon to command-and-control, LokiBot to panel management, and Ramnit explicitly to a victim category.

Within our 3,500-endpoint sample (700 per family), 247 rows carry last-seen dates inside the two-week window ending 21 November 2026 (59 Emotet, 9 RedLine, and 179 Ramnit rows). The other 3,253 rows carry earlier upstream feed listing dates from 2020 through October 2026 rather than continuous observation by Odin by Brandefense.

Only seven cloud and VPS endpoints (0.20% of examined rows; 0.059% of global sightings) across six IPv4 addresses survived initial collision filtering, and none had independent C2 corroboration. All six addresses and the remaining 3,493 endpoints (99.80%) across 3,305 hosts stay withheld.

Family	Category	Sightings	Feed "verified"	Examined / hosts	Cloud/VPS relay candidates	ISP & CDN held	Victim held	Other candidates
Emotet	C2	1,053	26	700 / 678	5 (4 IPs held)	66	0	629
RedLine Stealer	C2	2,247	4	700 / 683	2 (2 IPs held)	65	0	633
Raccoon Stealer	C2	830	0	700 / 700	0	4	0	696
LokiBot	Management	885	0	700 / 651	0	73 (Cloudflare)	0	627
Ramnit	Victim	6,804	4	700 / 599	0	0	700 (100%)	0

Geographic and hosting split

Across the 3,500 examined endpoints, 2,881 map to 65 countries, while 619 historical panel records carry an unattributed country code. Those 619 rows include 587 LokiBot, 14 Raccoon, 11 RedLine, 4 Ramnit, and 3 Emotet entries, with 583 lacking current ASN routing.

China leads attributed volume with 498 endpoints (438 victim-labelled Ramnit rows and 60 Emotet rows), followed by the United States (451), the Netherlands (407), Germany (304), and Russia (191). South Korea (176, including 161 victim-labelled Ramnit rows), the United Kingdom (97), Singapore (79), Finland (71), France (70), and Uruguay (57) complete the top locations.

Commercial cloud or VPS provider	Rows	Primary families seen	Study note
Amazon.com, Inc.	190	Emotet (124), RedLine (45), Raccoon (21)	2 upstream-confirmed relay candidates (US, UK) + 188 other candidates
DigitalOcean, LLC	117	Emotet (102), Raccoon (9), RedLine (6)	4 upstream-confirmed Emotet endpoints (3 droplets) + 113 other candidates
Hetzner Online GmbH	97	Raccoon (47), Emotet (39), RedLine (11)	1 upstream-confirmed RedLine endpoint (FI) + 96 other candidates
RootLayer Web Services Ltd.	80	RedLine Stealer (80)	Includes 2 withheld port 3389 RDP collisions
OVH SAS	70	Emotet (35), RedLine (20), Raccoon (14), LokiBot (1)	Shared VPS candidates (0 upstream-confirmed)
Partner LLC	70	Raccoon Stealer (70)	Historical HTTP port 80 candidates
STARK INDUSTRIES SOLUTIONS LTD	54	Raccoon (51), RedLine (3)	Offshore VPS candidates
M247 Europe SRL	53	Raccoon Stealer (53)	European HTTP port 80 candidates
AEZA GROUP Ltd	44	Raccoon Stealer (44)	Commercial HTTP port 80 candidates
SERV.HOST GROUP LTD	41	RedLine Stealer (41)	High-port WCF VPS candidates

CHAPTER 03

Cloud and VPS Relay Candidates: Emotet and RedLine Stealer

IN SHORT

Emotet and RedLine Stealer account for all seven dedicated cloud and VPS relay candidates (six IPv4 addresses) in this study. Twenty-three other upstream "confirmed" rows in those two families failed review due to telecom listings, lure certificates, or port 3389 RDP collisions. Because independent C2 beacon corroboration is not documented for the six cloud and VPS addresses, withhold them from static block lists and deploy wire rules for Emotet POSTs and RedLine SOAP contracts.

INSIDE THIS CHAPTER

Emotet: five cloud and VPS relay candidates vs broadband proxy listings 11

RedLine Stealer: two dedicated relay candidates vs port 3389 RDP and telecom collisions 12

03 Cloud and VPS Relay Candidates: Emotet and RedLine Stealer

Emotet (MITRE ATT&CK S0367) places infected Windows computers (T1583.005) in front of backend cloud servers as Epoch reverse proxies on ports 443, 8443, 8080, 2083, 80, and 8010. On infected hosts, Emotet commonly launches DLLs via `regsvr32.exe` (T1218.010) and `rundll32.exe` (T1218.011).

RedLine Stealer (S1240), built in C# `.NET`, exposes Windows Communication Foundation (WCF) `BasicHttpBinding` SOAP services (`hxxp://tempuri[.]org/IRemoteEndpoint/`) over high TCP ports such as 1912, 55615, 25920, 27667, 49157, and 5800. Figure 2 maps all five families to their wire behaviors and detections.

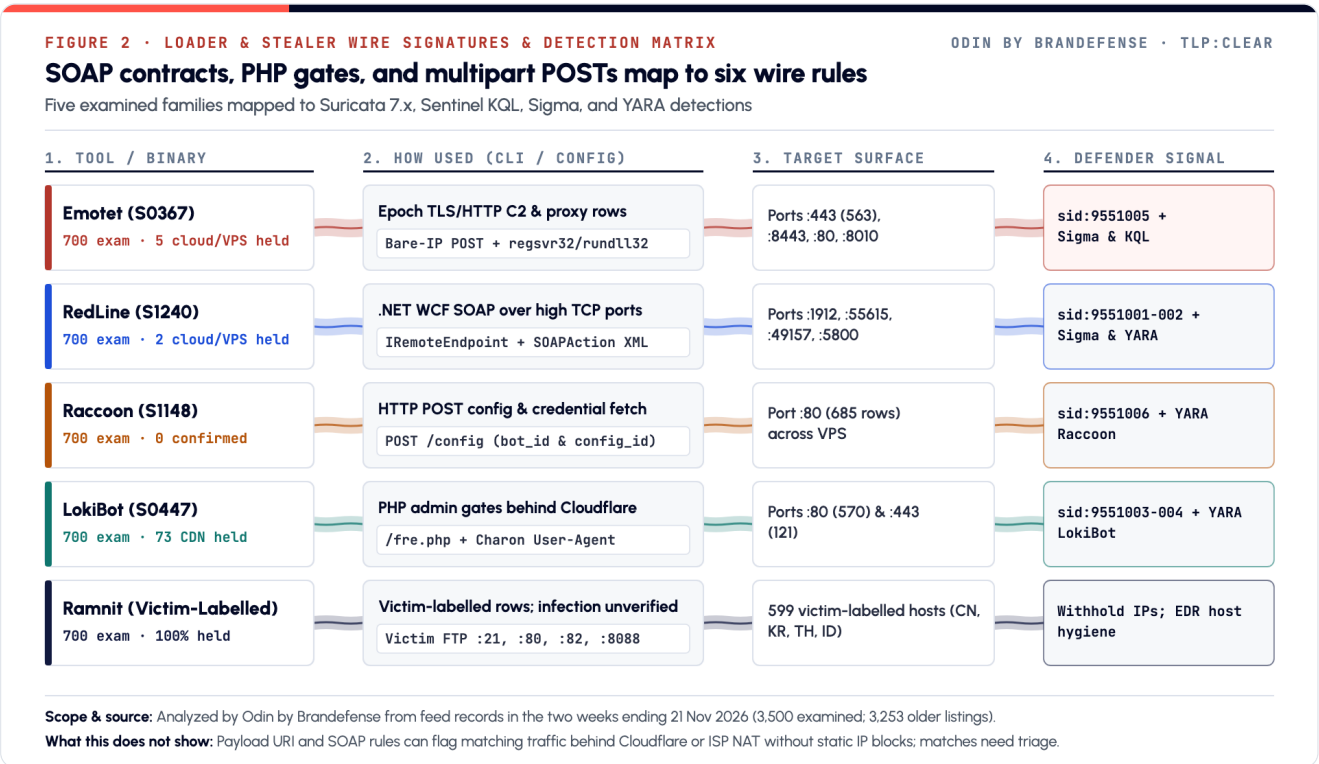


Figure 2: SOAP contracts, PHP gates, and multipart POSTs map to six wire rules

Emotet: five cloud and VPS relay candidates vs broadband proxy listings

Emotet accounts for 1,053 sightings across 59 countries, with 700 endpoints examined across 678 hosts (21 multi-port hosts across 43 rows) and 622 `/24` subnets. Port 443 leads with 563 endpoints (80.4%), followed by 8443 (48), 2083 (29), 8080 (27), 80 (19), 8010 (2), and 444 (2). Leading countries include the United States (171), Germany (117), China (60), Russia (45), France (41), Singapore (37), the United Kingdom (22), and the Netherlands (20).

Twenty-six examined Emotet rows carried an upstream "confirmed" label. Independent C2 corroboration for the five cloud and VPS endpoints is not documented.

- **US AWS port 443 relay candidate (address withheld)** on Amazon.com, Inc. in the United States, presenting a custom domain TLS certificate (withheld) and JARM prefix `29d29d07d29d`.
- **German DigitalOcean ports 80 and 8010 relay candidate (address withheld)** on DigitalOcean, LLC in Germany, a dual-port droplet listening on HTTP ports 80 and 8010.

- **Two US DigitalOcean port 80 relay candidates (addresses withheld)** on DigitalOcean, LLC in the United States, paired droplets sharing one custom certificate profile on port 80.

Twenty-one other upstream-confirmed Emotet rows failed collision review. Two port 443 hosts sat on a regional broadband carrier in southern China, where infection and proxy behavior were not verified for each host. Six dual-port 443 and 8443 rows across three Huawei Cloud hosts presented spoofed financial-brand certificates without corroborated Emotet C2 traffic.

Six Alibaba Cloud port 443 rows came from a single uncorroborated batch. Seven HTTP port 80 and 8010 rows at JSC Selectel and Data Storage Center JSC also lacked handshake proof. Overall, 66 Emotet-labelled rows (9.4%) sit on telecom carriers (45 rows across 16 countries) or Akamai Connected Cloud edge nodes (21 rows). Those telecom rows include four port 8443 nodes in South Korea sharing JARM prefix `2ad2ad0002ad`.

RedLine Stealer: two dedicated relay candidates vs port 3389 RDP and telecom collisions

RedLine Stealer accounts for 2,247 sightings across 48 countries, with 700 endpoints examined across 683 hosts and 427 `/24` subnets. High WCF ports dominate: TCP 1912 (124, 17.7%), 80 (112, 16.0%), 55615 (107, 15.3%), 25920 (57, 8.1%), 443 (35, 5.0%), 27667 (21), 55123 (8), and 16383 (8). Sixty-five RedLine rows expose default Windows machine certificates.

Four RedLine endpoints carried an upstream "confirmed" label. Independent C2 corroboration for the two dedicated cloud and VPS endpoints is not documented:

- **One UK AWS port 49157 endpoint and one Finnish Hetzner port 5800 endpoint (addresses withheld)** on Amazon.com, Inc. and Hetzner Online GmbH lacked independent WCF SOAP beacon corroboration.
- **Two Dutch port 3389 endpoints (addresses withheld)** on RootLayer Web Services Ltd. (alongside one suspected port 3389 host) were withheld because Windows Remote Desktop TLS handshakes triggered false C2 labels without WCF SOAP evidence.

Sixty-five RedLine rows (9.3%) belong to subscriber telecom networks, led by 57 port 25920 leases on a national telecom carrier in Uruguay plus eight broadband leases across seven other countries.

CHAPTER 04

Proxy-Fronted Panels and Victim Feeds: Raccoon, LokiBot, and Ramnit

IN SHORT

Raccoon Stealer (700 examined), LokiBot (700 examined), and Ramnit (700 examined from 6,804 sightings) produced zero corroborated block-list addresses. Seventy-three LokiBot rows point to shared Cloudflare proxy IPs, Raccoon rows carry stale 2025 listing dates, and all 700 Ramnit rows carry an upstream victim label. Catch LokiBot and Raccoon via HTTP URI signatures and keep Ramnit victim lists off firewalls.

INSIDE THIS CHAPTER

Raccoon Stealer and LokiBot: stale port 80 VPS pools and 73 Cloudflare proxies 14

Ramnit: why all 700 victim-labelled rows (from 6,804 sightings) are withheld 14

04 Proxy-Fronted Panels and Victim Feeds: Raccoon, LokiBot, and Ramnit

Raccoon Stealer and LokiBot: stale port 80 VPS pools and 73 Cloudflare proxies

Raccoon Stealer (MITRE ATT&CK S1148) has 830 sightings across 34 countries. We examined 700 endpoints on 700 hosts and 419 `/24` subnets. Its HTTP `POST` check-in uses `/config` with `bot_id` and `config_id`.

In our sample, 685 of 700 Raccoon rows (97.9%) listen on TCP port 80. Leading locations include the Netherlands (211), Germany (119), the United States (77), Russia (76), Finland (54), and the United Kingdom (43). Zero Raccoon rows carried upstream verification, and all 700 carry feed listing dates on or before 15 December 2025 (696 candidates plus 4 telecom ISP rows). Blocking recycled VPS addresses nearly a year later risks breaking reassigned tenant workloads.

Raccoon Stealer VPS provider	Examined rows
Partner LLC	70
M247 Europe SRL	53
STARK INDUSTRIES SOLUTIONS LTD	51
Hetzner Online GmbH	47
AEZA GROUP Ltd	44
Galaxy LLC	40

LokiBot (MITRE ATT&CK S0447; 885 sightings across 8 countries) accounts for 700 examined endpoints across 651 hosts and 489 `/24` subnets, including 46 multi-port hosts across 95 rows. Its servers run PHP administration panels (`PvqDq929BSx_A_D_M_I_N_a.php`) and binary credential gates (`fre.php`) with `Charon; Inferno` User-Agent strings on port 80 (570, 81.4%) and port 443 (121, 17.3%).

Zero LokiBot rows carried upstream verification, and all 700 carry listing dates on or before 7 May 2026. Critically, **73 LokiBot endpoints (10.4%) resolve to Cloudflare, Inc. shared anycast IPv4 addresses**. Blocking those 73 Cloudflare proxy IPs breaks enterprise access to thousands of unrelated websites while leaving the origin PHP panel online.

Ramnit: why all 700 victim-labelled rows (from 6,804 sightings) are withheld

Ramnit accounts for **6,804 global sightings across 47 countries (57.6% of all 11,819 sightings)** and carries an explicit `victim` classification in upstream feeds. Following the 2015 Europol takedown across roughly 3.2 million infected PCs, upstream feeds continue to log Ramnit victim or sinkhole-peer sightings, though infection or sinkhole status was not independently verified on every host.

Our 700 examined Ramnit endpoints span 599 distinct hosts and 432 `/24` subnets, including 55 multi-port hosts exposing up to nine ports on a single host.

Exposed ports on those 700 victim-labelled Ramnit rows reflect ordinary customer services. Leading ports include HTTP port 80 (257), 82 (43), 8088 (39), 8081 (28), 88 (26), 443 (26), 81 (26), 9201 (21), and FTP port 21. Four Ramnit rows carried a "confirmed" tag in the upstream feed. Those four rows comprised three FTP port 21 servers in China and one port 8443 telecom host in Thailand with an OAuth single-sign-on lure certificate.

Overall, 655 of 700 Ramnit rows (93.6%) sit in China (438), South Korea (161, with 158 on one national carrier), Thailand (34), and Indonesia (22). Under our victim-protection rules, **all 700 Ramnit rows (100%) are withheld**.

05

CHAPTER 05

Why Blind IP Blocking Breaks Broadband ISPs, CDNs, and Victim Networks

IN SHORT

Combining 700 victim-labelled Ramnit endpoints with 208 telecom and CDN collision endpoints means 908 of our 3,500 examined rows (25.9%) sit on victim-labelled customer hosts, residential ISPs, or shared Cloudflare and Akamai proxies. Windows TLS fingerprints also collide directly between RedLine candidates and victim-labelled Ramnit rows. Replace blind IP feed blocks with URI, SOAP, and process detections.

INSIDE THIS CHAPTER

Three ways raw loader and botnet feeds cause self-inflicted outages 17

TLS JARM overlap and certificate collisions across 1,163 endpoints 18

05 Why Blind IP Blocking Breaks Broadband ISPs, CDNs, and Victim Networks

Figure 3 shows how victim-labelled rows, broadband listings, and Cloudflare-fronted PHP gates enter raw threat feeds. It contrasts them with seven cloud and VPS candidates across six withheld IPv4 addresses.

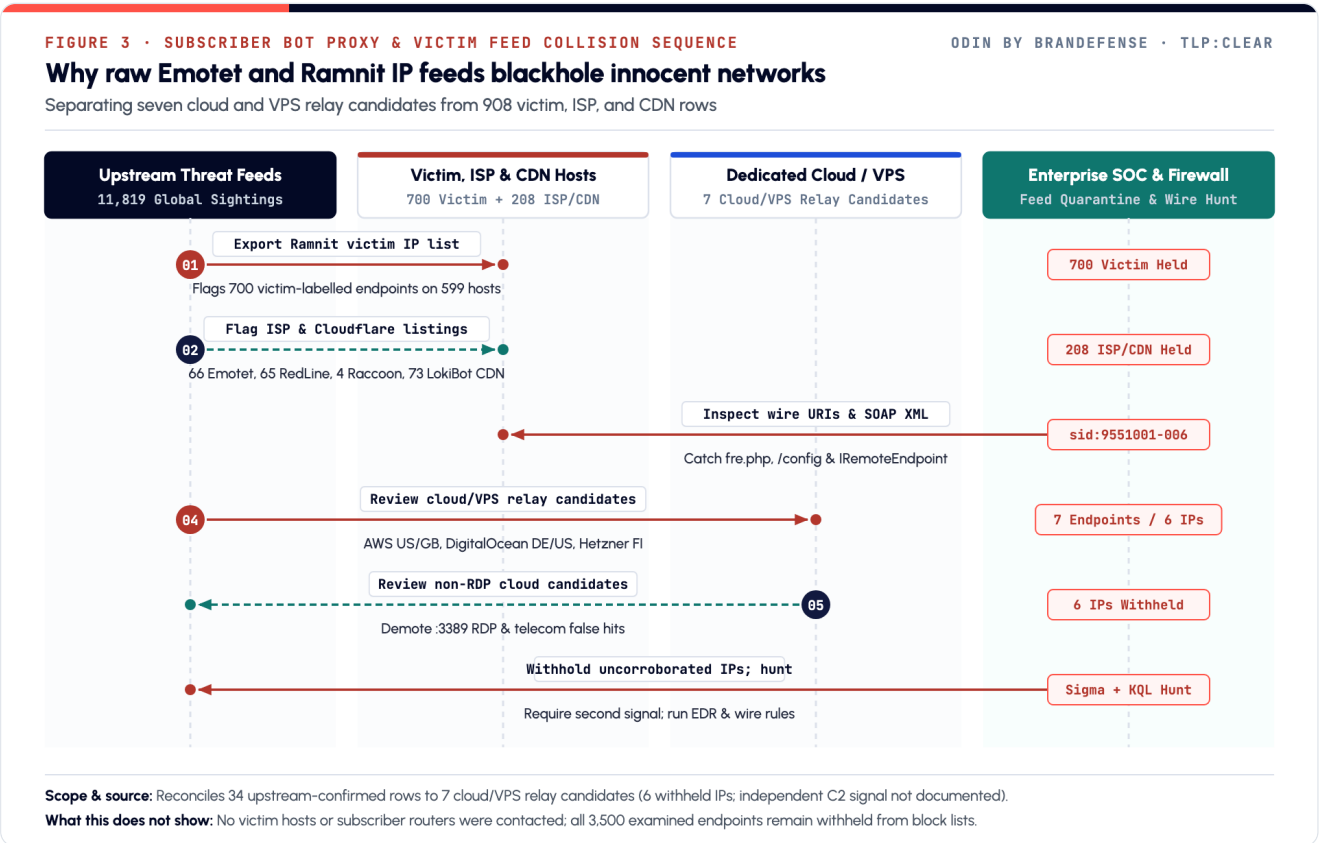


Figure 3: Why raw Emotet and Ramnit IP feeds blackhole innocent networks

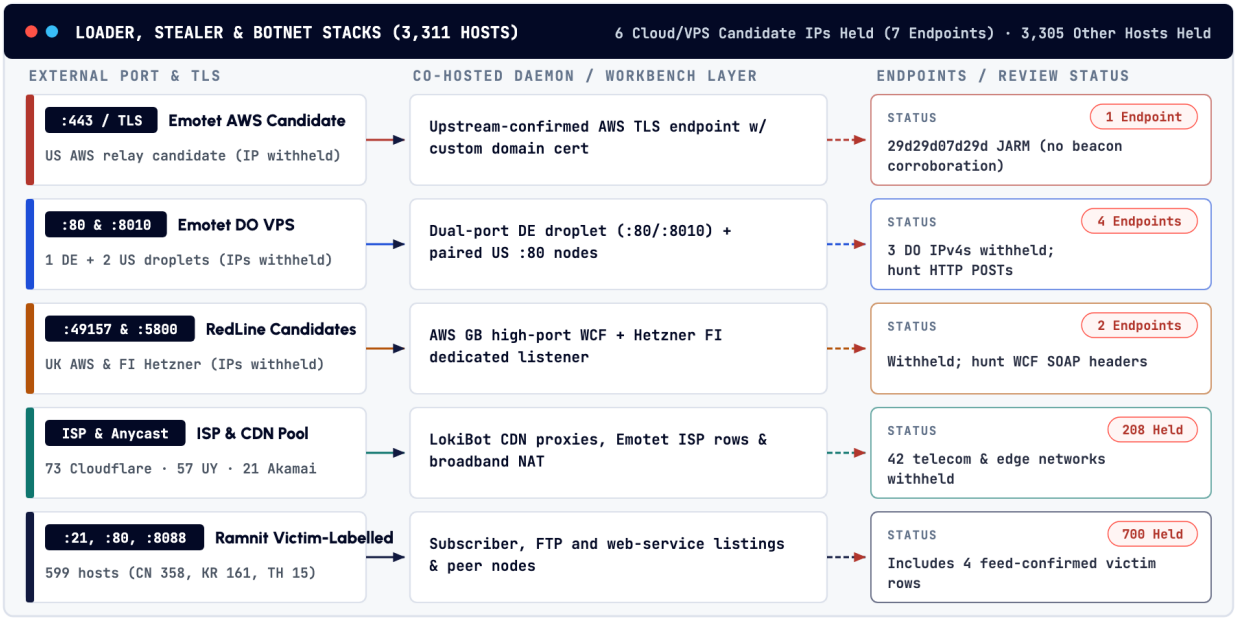
Three ways raw loader and botnet feeds cause self-inflicted outages

1. **Victim-tagged worm and sinkhole logs (700 Ramnit endpoints on 599 hosts).** Upstream `victim` tags on customer FTP (port 21) and web devices (ports 80, 81, 82, 88, 8081, 8088) flag suspected victim or sinkhole-peer hosts without verifying every host, not attacker C2 infrastructure.
2. **Broadband proxy candidates and DHCP rotation (114 telecom ISP rows across 40 carriers).** Subtracting 73 Cloudflare and 21 Akamai rows from the 208-row collision pool (42 networks) leaves 114 telecom ISP rows. Those rows include 57 RedLine port 25920 leases in Uruguay, 45 Emotet-labelled telecom leases across 16 countries, 8 other RedLine ISP leases, and 4 Raccoon ISP leases. Infection and proxy behavior were not verified for each host, and dynamic DHCP rotation can reassign residential addresses within days.
3. **Shared CDN reverse proxies and edge nodes (94 Cloudflare and Akamai endpoints).** Blocking 73 Cloudflare proxy addresses or 21 Akamai Connected Cloud addresses causes immediate business web outages while attackers rotate domains. Figure 4 contrasts the six dedicated cloud and VPS relay candidate hosts (seven endpoints, addresses withheld) with the 3,305 other withheld hosts.

FIGURE 4 · CLOUD & VPS RELAY CANDIDATES VS WITHHELD COLLISION SURFACES ODIN BY BRANDEFENSE · TLP:CLEAR

Six cloud and VPS relay candidate hosts contrast with 3,305 other withheld hosts

Architectural comparison across Emotet/RedLine relay candidates, ISP/Cloudflare collisions, and Ramnit victim-labelled rows



Scope & source: Analyzed by Odin by Brandefense from feed records in the two weeks ending 21 Nov 2026 across 3,311 hosts (3,253 older listings).
What this does not show: All 3,311 examined hosts remain withheld from public block lists pending independent C2 signals.

Figure 4: Six cloud and VPS relay candidate hosts contrast with 3,305 other withheld hosts

TLS JARM overlap and certificate collisions across 1,163 endpoints

TLS JARM fingerprints appear on 1,163 examined endpoints across 369 unique hashes (2,337 non-JARM rows), and X.509 certificates appear on 1,066 endpoints across 697 subjects (2,434 non-TLS rows). Emotet's top JARM (`2ad2ad0002ad` prefix, 96 rows) spans both cloud candidates and broadband telecom rows in South Korea and China.

Worse still, the next three top JARMs reflect standard Windows SChannel TLS stacks that **collide directly between RedLine candidates and victim-labelled Ramnit hosts**. Prefix `14d14d16d14d` spans 55 rows (34 RedLine, 13 Ramnit, 8 others) and `26d26d16d26d` spans 47 rows (31 Ramnit, 14 RedLine, 2 others). Prefix `2ad2ad16d2ad` spans another 43 rows (31 RedLine, 11 Ramnit, 1 Raccoon).

Certificate or JARM group	Rows	Family breakdown	Relay candidates	Defender guidance
Custom domain certificates	837	259 Emotet, 215 Ramnit, 197 RedLine, 155 Raccoon, 11 LokiBot	4	Withhold unverified IPs and domains; pair with HTTP/TLS wire rules
Default Windows host certs	86	65 RedLine, 16 Raccoon, 5 Ramnit	1	Never block port 3389 RDP certs; pair with WCF SOAP rules
Generic portal mimic certs	44	18 Emotet, 18 Raccoon, 8 RedLine	0	Hunt only; reused across VPS parking templates
Financial-brand lure certs	23	22 Emotet (Huawei Cloud), 1 Raccoon	0	Withhold IPs; 6 feed-confirmed Emotet rows lacked C2 proof
OAuth and SSO lure certs	19	18 Ramnit, 1 Emotet	0	Withhold victim hosts; monitor outbound credential phishing
IP-literal (26) & `localhost` (19)	45	Seen across all 5 families	0	Generic server defaults; never block on certificate alone
Top 3 Windows SChannel JARMs	145	79 RedLine, 55 Ramnit-labelled, 8 Raccoon, 2 Emotet, 1 LokiBot	0	Heavy victim and Windows Server overlap; pair with EDR logs
Emotet `2ad2ad0002ad` JARM	96	96 Emotet (cloud and broadband telecom rows)	0	Hunt paired with `regsvr32.exe` and `rundll32.exe` egress

CHAPTER 06

Feed Labels Against Cloud and VPS Relay Candidates

IN SHORT

Importing raw lists for these five families straight into a firewall would block 599 victim-labelled Ramnit hosts, 114 broadband ISP addresses, and 94 Cloudflare or Akamai edge addresses. Only seven dedicated cloud and VPS endpoints (0.20% of examined rows; 0.059% of global sightings) survived collision checks, and all six IPv4 addresses remain withheld pending independent C2 corroboration. Keep raw feed lists off firewalls and hunt wire and endpoint signals.

INSIDE THIS CHAPTER

Why 27 of 34 feed-confirmed rows failed collision checks 21

Four other ways to read the 3,493 non-relay endpoints 22

06 Feed Labels Against Cloud and VPS Relay Candidates

Figure 5 compares global sighting volumes and the 208-row ISP and CDN pool against the seven cloud and VPS relay candidates.

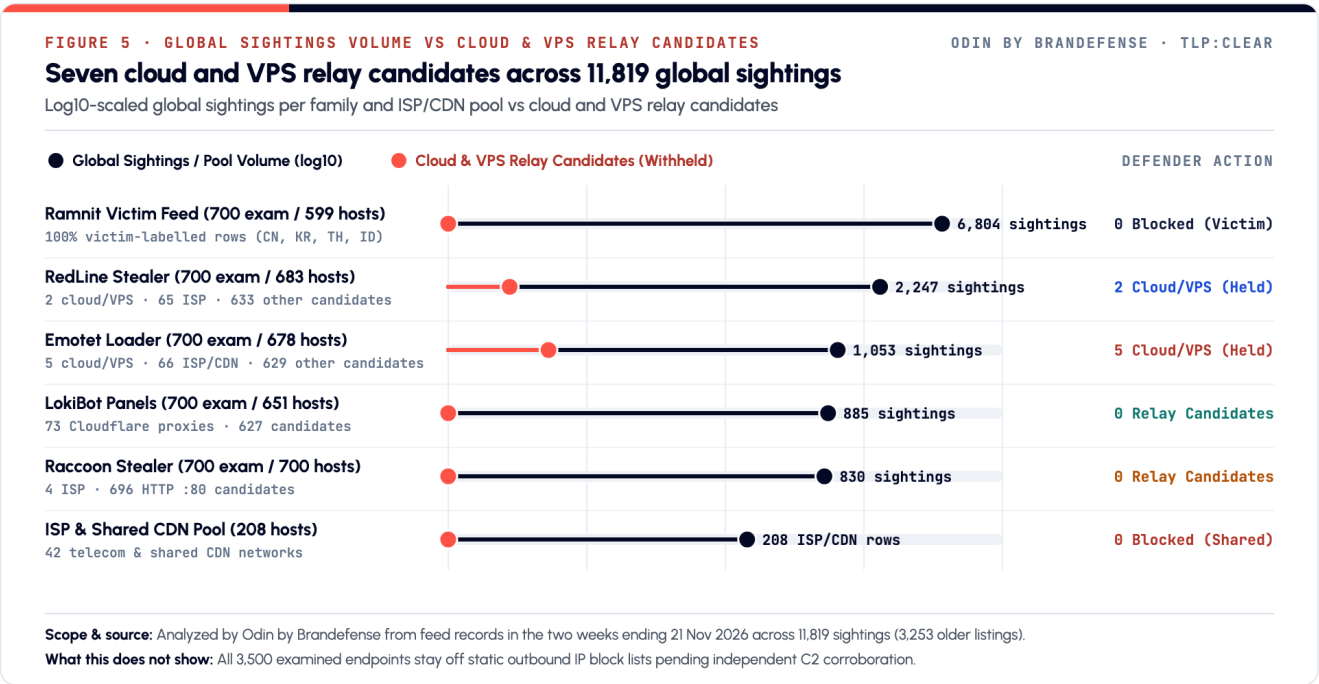


Figure 5: Seven cloud and VPS relay candidates across 11,819 global sightings

Group in our analysis	Feed "confirmed"	Feed "suspected"	Feed "candidate"	Total rows	Hosts	Share	Action
Cloud and VPS relay candidates	7	0	0	7	6	0.20%	Withhold IP; hunt with wire and endpoint rules
Other unverified candidates	21	30	2,534	2,585	2,498	73.86%	Withhold; hunt with wire and endpoint rules
Subscriber ISPs and shared CDNs	2	5	201	208	208	5.94%	Withhold; protect broadband users and Cloudflare
Victim-labelled Ramnit rows	4	15	681	700	599	20.00%	Withhold; never block victim-classified feeds

Why 27 of 34 feed-confirmed rows failed collision checks

Twenty-seven of the 34 upstream "confirmed" records (79.4%) failed initial collision review. Four were victim-labelled Ramnit hosts on port 21 (three in China) and port 8443 (one in Thailand), and two were Emotet-labelled broadband telecom rows in southern China.

Two more were Dutch port 3389 Remote Desktop collisions at RootLayer Web Services Ltd., while six Huawei Cloud port 443 and 8443 financial-lure rows lacked Emotet C2 traffic. The final 13 rows included six Alibaba Cloud port 443 rows from one uncorroborated batch. Seven HTTP port 80 and 8010 rows at JSC Selectel and Data Storage Center JSC also lacked handshake verification.

Four other ways to read the 3,493 non-relay endpoints

1. **Pre-existing services on victim-labelled hosts (700 Ramnit rows on 599 hosts).** Some victim-labelled hosts expose up to nine ports, including 21, 80, 81, 82, 88, 8081, 8088, and 9201. The ports may serve FTP, cameras, or web traffic. Individual infection or sinkhole status was not verified.
2. **Dynamic broadband NAT and telecom ISP listings (114 telecom ISP rows).** Subscriber-network rows (57 RedLine port 25920 leases in Uruguay and 45 Emotet-labelled telecom leases) sit on residential carrier ranges where individual infection or proxy status was not verified.
3. **Shared CDN anycast proxies and edge caches (94 Cloudflare and Akamai rows).** Operators place 73 LokiBot PHP panels behind Cloudflare because blocking shared anycast IPs breaks legitimate websites.
4. **Reassigned VPS addresses, Windows SChannel overlaps, and RDP servers (2,585 candidates).** Older Raccoon (2025) and LokiBot (May 2026) VPS listings, shared Windows SChannel JARMs, and port 3389 servers require endpoint or payload corroboration.

07

CHAPTER 07

What Defenders Should Do

IN SHORT

This chapter lists the actions defenders should take, in priority order.

07 What Defenders Should Do

Perimeter firewall and network security

- [ ] Do not import raw Emotet, RedLine, Raccoon, LokiBot, or Ramnit feed IPv4 addresses into static firewall block lists without an independent protocol, beacon, or endpoint signal.
- [ ] Keep Cloudflare, Akamai Connected Cloud, residential telecom ISP ranges, and victim-classified Ramnit feeds out of automated firewall deny lists.

SOC and endpoint detection

- [ ] Deploy the six Suricata 7 signatures in Chapter 8 on perimeter and SSL-inspection links. Those rules alert on RedLine `IRemoteEndpoint` SOAP envelopes, LokiBot `/PvqDq929BSx_A_D_M_I_N_a.php` and `/fre.php` posts, Emotet bare-IPv4 multipart POSTs, and Raccoon `/config` check-ins behind Cloudflare or ISP NAT.
- [ ] Run the Sentinel KQL hunt and two Sigma rules across Windows endpoint logs. Isolate hosts when `regsvr32.exe` or `rundll32.exe` connects to public Emotet ports (80, 443, 2083, 8010, 8080, 8443) or `.NET` and script utilities open RedLine high ports (1912, 5800, 16383, 25920, 27667, 49157, 55123, 55615).
- [ ] Scan unpacked binaries, sandbox drops, and memory dumps with the three YARA rules for RedLine WCF contracts, LokiBot `Charon; Inferno` gates, and Raccoon `/config` parameters.

Threat intelligence management

- [ ] Strip `victim`-categorized botnet feeds (Ramnit), standalone Windows SChannel JARMs, and port 3389 Remote Desktop collisions out of firewall External Dynamic Lists.

CHAPTER 08

Detection Rules

IN SHORT

This chapter describes each published rule and where to deploy it.

INSIDE THIS CHAPTER

How the Suricata, KQL, Sigma, and YARA rules work 26

08 Detection Rules

The full rules are in Appendix B. The Suricata file passes a static syntax check with zero problems. The rules were not loaded on live Suricata, Sentinel Kusto, Sigma, or YARA engines for this edition, so test and tune them before enabling automated isolation.

Rule file	What it catches
`odin_emotet_redline_raccoon_and_lokibot_c2.rules`	Suricata 7 (6 rules): RedLine WCF SOAP headers and bodies, LokiBot PHP panel and `fre.php` posts, Emotet bare-IPv4 multipart POSTs, and Raccoon `/config` check-ins
`sentinel_loader_stealer_c2_and_victim_noise_hunt.kql`	Microsoft Sentinel and Defender XDR: `regsvr32.exe` / `rundll32.exe` Emotet port egress and `.NET` or script binaries hitting RedLine high ports
`sigma_loader_stealer_relays_and_wcf_beacons.yml`	Sigma (2 Windows network rules): `regsvr32.exe` / `rundll32.exe` reaching Emotet ports, and `.NET` or script binaries reaching RedLine WCF ports
`odin_emotet_redline_raccoon_and_lokibot_artifacts.yar`	YARA (3 rules): RedLine `IRemoteEndpoint` WCF configs, LokiBot `Charon; Inferno` and `fre.php` stagers, and Raccoon `/config` check-ins

How the Suricata, KQL, Sigma, and YARA rules work

SID or Rule	Looks for	Action
SID 9551001	HTTP `POST` with `SOAPAction` `IRemoteEndpoint` header	RedLine WCF SOAP header
SID 9551002	XML SOAP envelope calling `CheckConnect`, `ScanResult`, or `GetArguments`	RedLine WCF SOAP body
SID 9551003	HTTP URI `/PvqDq929BSx_A_D_M_I_N_a.php`	LokiBot PHP admin panel
SID 9551004	HTTP `POST` to `/fre.php` with `Charon; Inferno` User-Agent	LokiBot credential gate
SID 9551005	Multipart `POST` to bare IPv4 `Host` without `Referer` or `Origin`	Emotet HTTP beacon (hunt)
SID 9551006	HTTP `POST` to `/config` containing `bot_id` and `config_id`	Raccoon config check-in
Sigma Rule 1	Exact `regsvr32.exe` or `rundll32.exe` reaching public Emotet ports	High (contain loader)
Sigma Rule 2	Exact `.NET` or script host reaching RedLine WCF high ports	High (contain stealer)
YARA Rules 1 to 3	Bounded (<2 MB) RedLine WCF, LokiBot Charon, and Raccoon `/config` payloads	Hunt / Contain

The Sentinel KQL query looks back seven days across `DeviceNetworkEvents` and `DeviceProcessEvents`. It correlates outbound `regsvr32.exe` and `rundll32.exe` connections on Emotet ports. It also checks `.NET` or script connections on RedLine WCF ports, excluding exact lab hostnames in `ApprovedRedTeamHosts`.

Tactic	Technique	Study observation	Detection
Resource Development	T1583.003 Virtual Private Server	Cloud and VPS relay candidates across DigitalOcean, Hetzner, and AWS	8 JARM indicators; Sigma 1, 2; Sentinel KQL
Resource Development	T1583.005 Botnet	66 Emotet-labelled ISP/edge rows and 700 Ramnit victim-labelled nodes	Feed quarantine; Sigma 1
Defense Evasion	T1218.010 / T1218.011 Regsvr32 and Rundll32	Emotet DLL loader network activity	Sigma 1; Sentinel KQL
Command and Control	T1071.001 Web Protocols	RedLine SOAP, LokiBot `/fre.php`, Raccoon `/config`, Emotet POST	SIDs 9551001 to 9551006; YARA 1 to 3
Command and Control	T1573.002 Asymmetric Cryptography	Emotet port 443 and RedLine port 49157 TLS relay candidates	8 JARM indicators; Sentinel KQL
Credential Access	T1555.003 Credentials from Web Browsers	RedLine, Raccoon, and LokiBot browser password theft	SIDs 9551001 to 9551004, 9551006; Sigma 2; YARA 1 to 3

09

CHAPTER 09

Indicators

IN SHORT

This chapter lists the published indicators and explains what stays withheld.

INSIDE THIS CHAPTER

JARM fingerprints and wire signatures to hunt 29

09 Indicators

Appendix A holds 8 published indicators: 8 TLS JARM fingerprints used for hunting. All six cloud and VPS IPv4 addresses remain withheld because no independent C2 beacon is documented. They cover seven address-and-port entries; one German DigitalOcean droplet had ports 80 and 8010.

The other 3,493 examined endpoints are also withheld. There are no file hashes in this report. Five text-only HTTP and SOAP wire signatures also appear below.

Type	Count	Where to use it
TLS JARM fingerprints (Appendix A)	8	TLS hunting paired with endpoint process logs; never block on a JARM alone
HTTP and SOAP wire signatures (text-only)	5	Suricata and HTTP proxy rules (`sid:9551001` to 9551006)
Withheld cloud and VPS relay candidates (6 unique IPv4s)	7	Withheld pending independent protocol or beacon signal; do not block

JARM fingerprints and wire signatures to hunt

Indicator	Family	Context
`29d29d07d29d29d21c29d29d29d29dce2e4c8c53174ecbf5529ce7584d5518`	Emotet	Upstream-confirmed US AWS port 443 endpoint (address withheld)
`2ad2ad0002ad2ad0002ad2ad2ad2ade1a3c0d7ca6ad8388057924be83dfc6a`	Emotet	Seen across 96 cloud and broadband telecom rows
`29d29d00029d29d21c29d29d29d29d8da29ade5a975f32a8d3f61299c69dc4`	Emotet	Shared across four Alibaba Cloud port 443 candidate endpoints
`2ad2ad16d2ad2ad00042d42d0000008fe5654c9239cdb4052d3ab65a579afa`	Emotet	Huawei Cloud port 443 financial-lure certificate cluster
`14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532`	RedLine Stealer	Windows SChannel JARM on 55 rows including 13 victim-labelled Ramnit rows
`26d26d16d26d26d22c26d26d26d26dfd9c9d14e4f4f67f94f0359f8b28f532`	Ramnit	Windows JARM on 47 rows including 31 victim-labelled Ramnit rows and 14 RedLine rows
`2ad2ad16d2ad2ad22c2ad2ad2ad2adfd9c9d14e4f4f67f94f0359f8b28f532`	RedLine Stealer	Windows SChannel JARM on 43 rows including 11 victim-labelled Ramnit rows
`29d3fd00029d29d21c42d43d00041df61f6b5fa6973e9fa14c8155669c6633`	Raccoon Stealer	Linux Nginx JARM across 21 RedLine, 16 Raccoon, and 1 LokiBot candidates
`hxxp://tempuri[.]org/IRemoteEndpoint/`	RedLine Stealer	Text-only WCF `SOAPAction` header contract; SIDs 9551001, 9551002
`/PvqDq929BSx_A_D_M_I_N_a.php`	LokiBot	Text-only PHP C2 administration panel URI; SID 9551003
`/fre.php`	LokiBot	Text-only Charon binary credential submission gate; SID 9551004
`/config`	Raccoon Stealer	Text-only HTTP `POST` check-in path (`bot_id` , `config_id`); SID 9551006
`Content-Type: multipart/form-data`	Emotet	Text-only bare-IPv4 HTTP `POST` without `Referer` ; SID 9551005

We withhold all 3,500 examined endpoints across 3,311 hosts. These include 7 uncorroborated relay rows on 6 hosts, 700 Ramnit rows on 599 hosts, and 208 ISP/CDN rows on 208 hosts. The other 2,585 candidates span 2,498 hosts; unverified certificate domains and Windows machine hostnames are also withheld.

10

CHAPTER 10

Scope and Limits

IN SHORT

This chapter sets out what the evidence can show and what it cannot.

10 Scope and Limits

- **Observation window.** Findings cover a two-week observation window ending 21 November 2026. Earlier dates on 3,253 examined records (including Raccoon Stealer through December 2025 and LokiBot through May 2026) are upstream feed listing dates, not continuous monitoring by Odin by Brandefense.
- **Feed labels are not attribution.** Malware family names and verification tags come from upstream feeds. Because independent protocol or beacon corroboration is not documented for the seven cloud and VPS relay candidates (six IPv4 addresses), all 3,500 examined endpoints remain withheld from public block lists.
- **Analytical model.** Zero hosts span two families across all 3,311 hosts. Figures 1 and 3 present an analytical model of loader, stealer, and victim-feed collisions rather than a unified threat group.
- **No victim or subscriber hosts contacted.** Odin by Brandefense did not interact with Ramnit victim-labelled machines or consumer broadband routers, and all 3,311 examined hosts remain withheld.
- **Rule validation.** Detection rules were verified statically and were not loaded on live production engines for this edition.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. MITRE ATT&CK. S0367 Emotet. https://attack.mitre.org/software/S0367/ (verified 21 November 2026)
2. MITRE ATT&CK. S1240 RedLine Stealer. https://attack.mitre.org/software/S1240/ (verified 21 November 2026)
3. MITRE ATT&CK. S1148 Raccoon Stealer. https://attack.mitre.org/software/S1148/ (verified 21 November 2026)
4. MITRE ATT&CK. S0447 Lokibot. https://attack.mitre.org/software/S0447/ (verified 21 November 2026)
5. CISA. Alert AA20-280A: Emotet Malware. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a (verified 21 November 2026)
6. CISA. Alert AA20-266A: LokiBot Malware. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-266a (verified 21 November 2026)
7. Europol EC3. World's most dangerous malware EMOTET disrupted through global action. https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (verified 21 November 2026)
8. Europol EC3. Botnet [Ramnit] taken down through international law enforcement cooperation. https://www.europol.europa.eu/media-press/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation (verified 21 November 2026)
9. MITRE ATT&CK. T1583.005 Acquire Infrastructure: Botnet. https://attack.mitre.org/techniques/T1583/005/ (verified 21 November 2026)
10. Salesforce Engineering. JARM: active TLS server fingerprinting. https://github.com/salesforce/jarm (verified 21 November 2026)

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

Appendix A lists the indicators published for this study. Appendix B carries every published detection rule in full.

INSIDE

A. Indicators of compromise (8) 36

B. Detection rules (4 files) 37

A Indicators of Compromise

Values are defanged for display. The CSV, JSON and STIX files on the online edition carry the raw values. Values the report marks as withheld are not listed.

ID	Type	Indicator	Port	Context	Action
R51-IOC-01	JARM	29d29d07d29d29d21c29d29d29d29dce2e4c8c53174ecbf5529ce7584d5518	443	emotet · TLS fingerprint on upstream-confirmed US AWS port 443 endpoint (address withheld)	HUNT
R51-IOC-02	JARM	2ad2ad0002ad2ad0002ad2ad2ad2ade1a3c0d7ca6ad8388057924be83dfc6a	443	emotet · Dominant Emotet TLS fingerprint across 96 cloud and broadband telecom rows	HUNT
R51-IOC-03	JARM	29d29d00029d29d21c29d29d29d29d8da29ade5a975f32a8d3f61299c69dc4	443	emotet · TLS fingerprint shared across four Alibaba Cloud port 443 candidate endpoints	HUNT
R51-IOC-04	JARM	2ad2ad16d2ad2ad00042d42d0000008fe5654c9239cdb4052d3ab65a579afa	443	emotet · TLS fingerprint on Huawei Cloud port 443 financial-lure certificate cluster	HUNT
R51-IOC-05	JARM	14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532	443	redlinestealer · Windows SChannel TLS fingerprint across 55 endpoints including 13 Ramnit victim-labelled rows	HUNT
R51-IOC-06	JARM	26d26d16d26d26d22c26d26d26d26dfd9c9d14e4f4f67f94f0359f8b28f532	8443	ramnit · Windows TLS fingerprint across 47 endpoints including 31 Ramnit victim-labelled rows and 14 RedLine candidates	HUNT
R51-IOC-07	JARM	2ad2ad16d2ad2ad22c2ad2ad2ad2adfd9c9d14e4f4f67f94f0359f8b28f532	443	redlinestealer · Windows SChannel TLS fingerprint across 43 endpoints including 11 Ramnit victim-labelled rows	HUNT
R51-IOC-08	JARM	29d3fd00029d29d21c42d43d00041df61f6b5fa6973e9fa14c8155669c6633	443	raccoonstealer · Linux Nginx TLS fingerprint shared across 21 RedLine, 16 Raccoon, and 1 LokiBot candidates	HUNT

B Detection Rules

Each rule file loads in its own engine (YARA-X, Suricata 7, Kusto, pySigma). Tune thresholds and allow-lists to your environment before alerting or blocking. The same files can be downloaded from the online edition.

odin_emotet_redline_raccoon_and_lokibot_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 51 / 52 Bounded YARA Detection Suite
   Covers: RedLine Stealer .NET WCF IRemoteEndpoint client stubs, LokiBot PHP panel
           and Charon HTTP submission stagers, and Raccoon Stealer HTTP /config
           check-in payloads.
   Classification: TLP:CLEAR
*/

rule ODIN_RedLine_Stealer_WCF_SOAP_Client_Config {
    meta:
        author = "Odin by Brandefense"
        monograph = "51 / 52"
        date = "2026-11-21"
        action = "hunt_and_contain"
        description = "Matches RedLine Stealer .NET Windows Communication Foundation IRemoteEndpoint SOAP
contract and tasking strings"
    strings:
        $contract = "IRemoteEndpoint" ascii wide
        $ns1 = "http://tempuri.org/" ascii wide
        $ns2 = "BasicHttpBinding" ascii wide
        $op1 = "CheckConnect" ascii wide
        $op2 = "EnvironmentSettings" ascii wide
        $op3 = "ScanResult" ascii wide
        $op4 = "GetArguments" ascii wide
    condition:
        filesize < 2MB and $contract and 1 of ($ns*) and 2 of ($op*)
}

rule ODIN_LokiBot_PHP_Panel_And_Charon_Gate_Strings {
    meta:
        author = "Odin by Brandefense"
        monograph = "51 / 52"
        date = "2026-11-21"
        action = "hunt_and_contain"
        description = "Matches LokiBot binary credential stealer Charon User-Agent and fre.php or admin panel
gate artifacts"
    strings:
        $uri1 = "/fre.php" ascii wide
        $uri2 = "PvqDq929BSx_A_D_M_I_N_a.php" ascii wide
        $ua1 = "Charon; Inferno" ascii wide
        $ua2 = "Mozilla/4.08 [en]" ascii wide
        $db1 = "sqlite3_open" ascii
        $hdr1 = "application/octet-stream" ascii wide
        $hdr2 = "HTTP/1.0" ascii wide
    condition:
        filesize < 2MB and 1 of ($uri*) and 1 of ($ua*) and 1 of ($db1, $hdr1, $hdr2)
}

rule ODIN_Raccoon_Stealer_V2_HTTP_Config_Checkin {
    meta:
        author = "Odin by Brandefense"
        monograph = "51 / 52"
        date = "2026-11-21"
        action = "hunt_and_contain"
        description = "Matches Raccoon Stealer C/C++ HTTP POST /config check-in parameters alongside browser
credential store targets"
    strings:
        $cfg1 = "/config" ascii wide
        $cfg2 = "bot_id" ascii wide
        $cfg3 = "config_id" ascii wide
```

```
        $brw1 = "Login Data" ascii wide
        $brw2 = "Web Data" ascii wide
        $brw3 = "sqlite3_column_blob" ascii
    condition:
        filesize < 2MB and all of ($cfg*) and 1 of ($brw*)
}
```

odin_emotet_redline_raccoon_and_lokibot_c2.rules

SURICATA

```
# Odin by Brandefense - Monograph 51 / 52 Suricata 7.x Detection Suite
# Coverage: RedLine Stealer .NET WCF SOAP beacons, LokiBot PHP panel and Charon binary
#           submission gates, Emotet Epoch bare-IPv4 HTTP POST check-ins, and Raccoon
#           Stealer HTTP /config check-ins
# Classification: TLP:CLEAR

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN [R51] RedLine Stealer WCF IRemoteEndpoint SOAPAction
Header"; flow:established,to_server; http.method; bsize:4; content:"POST"; http.header; bsize:>42;
content:"SOAPAction: |22|http://tempuri.org/IRemoteEndpoint/"; fast_pattern; classtype:trojan-activity; sid:
9551001; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN [R51] RedLine Stealer WCF XML Envelope CheckConnect or
ScanResult Body"; flow:established,to_server; http.method; bsize:4; content:"POST"; http.request_body; bsize:>64;
content:"<s:Envelope xmlns:s=|22|http://schemas.xmlsoap.org/soap/envelope/|22|>"; fast_pattern;
content:"IRemoteEndpoint"; pcre:"/<(CheckConnect|EnvironmentSettings|ScanResult|GetArguments)\b/";
classtype:trojan-activity; sid:9551002; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress,
tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN [R51] LokiBot PHP C2 Administration Panel URI Request";
flow:established,to_server; http.uri; bsize:>27; content:"/PvqDq929BSx_A_D_M_I_N_a.php"; fast_pattern;
classtype:trojan-activity; sid:9551003; rev:1; metadata:created_at 2026_11_21, deployment perimeter_and_proxy,
tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN [R51] LokiBot Charon Binary Credential Submission POST
to fre.php"; flow:established,to_server; http.method; bsize:4; content:"POST"; http.uri; bsize:>7; content:"/
fre.php"; fast_pattern; http.user_agent; bsize:>14; content:"Charon|3B| Inferno"; classtype:trojan-activity; sid:
9551004; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress, tactic exfiltration;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,443,8010,8080,8443] (msg:"ODIN [R51] HUNT Emotet Epoch Multipart
POST to Bare IPv4 Host Without Referer"; flow:established,to_server; http.method; bsize:4; content:"POST";
http.content_type; bsize:>19; content:"multipart/form-data"; fast_pattern; http.host; pcre:"/^\d{1,3}(?:\.
\d{1,3}){3}(?::(?:80|443|8010|8080|8443))?$/"; http.header_names; content:!"Referer"; content:!"Origin";
classtype:trojan-activity; sid:9551005; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress,
policy behavioral_hunt, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN [R51] Raccoon Stealer HTTP POST Check-In to /config
Endpoint"; flow:established,to_server; http.method; bsize:4; content:"POST"; http.uri; bsize:7; content:"/
config"; fast_pattern; http.request_body; bsize:>24; pcre:"/(?=.*bot_id)(?=.*config_id)/s"; classtype:trojan-
activity; sid:9551006; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress, tactic
command_and_control;)
```

sentinel_loader_stealer_c2_and_victim_noise_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 51 / 52 Microsoft Sentinel & Defender XDR Hunt
// Correlates outbound regsvr32/rundll32 Emotet loader egress on Epoch relay ports and
// scripting/.NET binaries initiating RedLine WCF high-port beacons while keeping
// uncorroborated feed IPs, subscriber ISPs, and Ramnit victim-labelled networks off
// static IP blocklists
// Classification: TLP:CLEAR

let Lookback = 7d;
let ApprovedRedTeamHosts = dynamic(["REDTEAM-LOADER-LAB-01", "PURPLE-SIM-WIN-01"]);
let EmotetLoaderBinaries = dynamic([
    @"c:\windows\system32\regsvr32.exe",
    @"c:\windows\syswow64\regsvr32.exe",
```

```
    @"c:\windows\system32\rundll32.exe",
    @"c:\windows\syswow64\rundll32.exe"
]);
let StealerHostBinaries = dynamic([
    @"c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe",
    @"c:\windows\microsoft.net\framework64\v4.0.30319\msbuild.exe",
    @"c:\windows\microsoft.net\framework\v4.0.30319\regasm.exe",
    @"c:\windows\microsoft.net\framework64\v4.0.30319\regasm.exe",
    @"c:\windows\microsoft.net\framework\v4.0.30319\vbc.exe",
    @"c:\windows\microsoft.net\framework64\v4.0.30319\vbc.exe",
    @"c:\windows\microsoft.net\framework\v4.0.30319\installutil.exe",
    @"c:\windows\microsoft.net\framework64\v4.0.30319\installutil.exe",
    @"c:\windows\system32\windowspowershell\v1.0\powershell.exe",
    @"c:\windows\syswow64\windowspowershell\v1.0\powershell.exe",
    @"c:\windows\system32\wscript.exe",
    @"c:\windows\system32\mshta.exe"
]);
let EmotetRelayPorts = dynamic([80, 443, 2083, 8010, 8080, 8443]);
let RedLineHighPorts = dynamic([1912, 5800, 16383, 25920, 27667, 49157, 55123, 55615]);
let SuspiciousLoaderProcs = DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedRedTeamHosts))
    | extend ProcPathLower = tolower(FolderPath)
    | where ProcPathLower in (EmotetLoaderBinaries) or ProcPathLower in (StealerHostBinaries)
    | project ProcTime = Timestamp, DeviceId, DeviceName, ProcFile = FileName, FolderPath, ProcessCommandLine;
DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where RemoteIPType == "Public"
    | where not(DeviceName in~ (ApprovedRedTeamHosts))
    | extend InitPathLower = tolower(InitiatingProcessFolderPath)
    | where (InitPathLower in (EmotetLoaderBinaries) and RemotePort in (EmotetRelayPorts))
        or (InitPathLower in (StealerHostBinaries) and RemotePort in (RedLineHighPorts))
    | summarize
        NetFirstSeen = min(Timestamp),
        NetLastSeen = max(Timestamp),
        DistinctRemoteIps = dcount(RemoteIP),
        EmotetLoaderHits = countif(InitPathLower in (EmotetLoaderBinaries) and RemotePort in (EmotetRelayPorts)),
        RedLinePortHits = countif(InitPathLower in (StealerHostBinaries) and RemotePort in (RedLineHighPorts)),
        SampleEndpoints = make_set(strcat(RemoteIP, ":", tostring(RemotePort)), 12),
        ConnectionCount = count()
        by DeviceId, DeviceName, InitiatingProcessFileName, InitiatingProcessFolderPath
    | join kind=leftouter (SuspiciousLoaderProcs) on DeviceId, DeviceName
    | extend AlertAction = case(
        EmotetLoaderHits > 0 and isnotempty(ProcessCommandLine), "CONTAIN_EMOTET_DLL_LOADER_EGRESS",
        RedLinePortHits > 0 and isnotempty(ProcessCommandLine), "CONTAIN_REDLINE_WCF_HIGH_PORT_BEACON",
        EmotetLoaderHits > 0, "HUNT_REGSVR32_RUNDLL32_EPOCH_PORT_EGRESS",
        "HUNT_DOTNET_HOST_REDLINE_WCF_PORT"
    )
    | sort by NetLastSeen desc
    | project NetFirstSeen, NetLastSeen, ProcTime, DeviceName, AlertAction, InitiatingProcessFileName,
InitiatingProcessFolderPath, ProcFile, ProcessCommandLine, SampleEndpoints, DistinctRemoteIps, ConnectionCount
```

sigma_loader_stealer_relays_and_wcf_beacons.yml

SIGMA

```
title: Windows Regsvr32 or Rundll32 Connecting to Emotet Epoch Relay Ports
id: 9b5128a0-4c19-4d83-8a51-005100000002
status: experimental
description: Detects regsvr32.exe or rundll32.exe initiating public outbound network sessions on Emotet Epoch
HTTP and TLS relay ports (80, 443, 2083, 8010, 8080, 8443), catching broadband proxy beacons without static ISP
blocklists.
author: Odin by Brandefense
date: 2026-11-21
modified: 2026-11-21
references:
  - https://attack.mitre.org/software/S0367/
  - https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a
logsource:
  category: network_connection
```

```
    product: windows
  detection:
    selection_proc:
      Image:
        - 'C:\Windows\System32\regsvr32.exe'
        - 'C:\Windows\SysWOW64\regsvr32.exe'
        - 'C:\Windows\System32\rundll32.exe'
        - 'C:\Windows\SysWOW64\rundll32.exe'
    selection_net:
      Initiated: 'true'
      DestinationPort:
        - 80
        - 443
        - 2083
        - 8010
        - 8080
        - 8443
    filter_private_dest:
      DestinationIsIpv6: 'false'
      DestinationIp|cidr:
        - '10.0.0.0/8'
        - '172.16.0.0/12'
        - '192.168.0.0/16'
        - '127.0.0.0/8'
    filter_approved_lab:
      ComputerName:
        - 'REDTEAM-LOADER-LAB-01'
        - 'PURPLE-SIM-WIN-01'
    condition: selection_proc and selection_net and not 1 of filter_*
  falsepositives:
    - Signed Windows shell extensions making legitimate HTTPS calls when verified by exact DLL path in EDR
  level: high
  tags:
    - attack.defense-evasion
    - attack.t1218.010
    - attack.t1218.011
    - attack.command-and-control
  ---
  title: Windows .NET or Scripting Host Connecting to RedLine WCF High Ports
  id: 9b5128a0-4c19-4d83-8a51-005100000003
  status: experimental
  description: Detects .NET framework compilation or hollowing target binaries and Windows script hosts initiating
  outbound connections on recurring RedLine Stealer WCF ports (1912, 5800, 16383, 25920, 27667, 49157, 55123,
  55615).
  author: Odin by Brandefense
  date: 2026-11-21
  modified: 2026-11-21
  references:
    - https://attack.mitre.org/software/S1240/
  logsource:
    category: network_connection
    product: windows
  detection:
    selection_proc:
      Image:
        - 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe'
        - 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe'
        - 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe'
        - 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe'
        - 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe'
        - 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\vbc.exe'
        - 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe'
        - 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe'
        - 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe'
        - 'C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe'
        - 'C:\Windows\System32\wscript.exe'
        - 'C:\Windows\System32\mshta.exe'
    selection_net:
      Initiated: 'true'
      DestinationPort:
        - 1912
        - 5800
```

```
      - 16383
      - 25920
      - 27667
      - 49157
      - 55123
      - 55615
  filter_approved_lab:
    ComputerName:
      - 'REDTEAM-LOADER-LAB-01'
      - 'PURPLE-SIM-WIN-01'
  condition: selection_proc and selection_net and not filter_approved_lab
falsepositives:
  - Authorized purple-team simulation hosts listed by exact hostname in filter_approved_lab
level: high
tags:
  - attack.command-and-control
  - attack.t1071.001
  - attack.t1555.003
```

ODIN

About Odin Research

Odin Research is the public research series of Odin by Brandefense. It documents adversary infrastructure seen on the internet and turns each finding into indicators and detection rules that defenders can use. Victims and third parties stay anonymous, addresses appear only for confirmed adversary infrastructure, and no working attack code is published.

Odin is the agentic analyst inside the Brandefense threat intelligence platform, which unifies Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management.

Online edition, indicators and rules · brandefense.io/odin-research/reports/loader-and-stealer-feeds/
Short Read · brandefense.io/odin-research/blog/emotet-and-ramnit-feeds/
Defense Kit · brandefense.io/odin-research/defense-kit/