ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 52 / 30 · C2 INFRASTRUCTURE

Gamaredon and PlugX Candidates
Port-53 Listeners and Regional RATs

How 1,421 examined endpoints across five feed-labelled families split into 1,251 cloud hunt leads, 170 withheld CDN and telecom rows, and deployable wire and TLS detections

Prepared November 2026
Full Report · Public edition · Version 1.1

0 / 1,421
Confirmed cloud C2 addresses for standalone IP blocking after withholding a Chinanet port 3389 host

563 / 564
Gamaredon-labelled endpoints on HTTPS port 443 across 517 /24 subnets (361 on DigitalOcean)

31 / 281
PlugX-labelled endpoints on port 53, including 28 multi-port hosts and 5 serving TLS on port 53

107 / 552
GhOstRAT-labelled endpoints on port 14994 (96 in Hong Kong and 8 in Japan)

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

How 1,421 examined endpoints across five feed-labelled families split into 1,251 cloud hunt leads, 170 withheld CDN and telecom rows, and deployable wire and TLS detections

01	Executive Summary	04
02	Four Infrastructure Groups, One Analytical Model	07
03	Gamaredon-Labelled HTTPS Candidates and PlugX Port-53 Listeners	10
04	Gh0stRAT Port-14994 Clusters and Cross-Family Certificate Reuse	13
05	Hong Kong Subnet Bursts, Dense /24 Clusters, and njRAT	16
06	Why Static IP Block Lists Misfire Across All Five Families	19
07	What Defenders Should Do	21
08	Detection Rules	23
09	Indicators	26
10	Scope and Limits	29
11	Sources	31
A	Indicators of compromise (8)	33
B	Detection rules (4 files)	34

IN SHORT

Odin by Brandefense reviewed 1,421 historical feed records across 1,261 hosts and 942 `/24` subnets spanning five upstream feed labels: Gamaredon, PlugX, Gh0stRAT, NDragonRAT, and njRAT. Zero endpoints held up for standalone firewall IP blocking after reviewing the sole feed-confirmed host on a Chinese broadband carrier exposing Remote Desktop. Stop blocking raw feed lists by IP address, restrict direct port 53 traffic to internal DNS forwarders, and alert on non-DNS framing and conserved RAT headers.

01

CHAPTER 01

Executive Summary

IN SHORT

Odin by Brandefense reviewed 1,421 historical feed records across 1,261 hosts and 942 `/24` subnets spanning five upstream feed labels: Gamaredon, PlugX, Gh0stRAT, NDragonRAT, and njRAT. Zero endpoints held up for standalone firewall IP blocking after reviewing the sole feed-confirmed host on a Chinese broadband carrier exposing Remote Desktop. Stop blocking raw feed lists by IP address, restrict direct port 53 traffic to internal DNS forwarders, and alert on non-DNS framing and conserved RAT headers.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Threat intelligence feeds often label virtual servers with espionage or remote access trojan (RAT) names from a single self-signed certificate, TLS server fingerprint, or port banner. Loading raw candidate lists into perimeter firewalls disrupts content delivery networks (CDNs), cuts off broadband customers, and misses rotating proxy relays.

1. **Gamaredon candidates scatter port-443 endpoints across 517 subnets while colliding with Akamai edges.**

   Across 564 Gamaredon-labelled endpoints, 563 listen on HTTPS port 443 across 517 `/24` subnets, 479 of them single-host, led by 361 DigitalOcean servers and 22 self-signed `CN=Elastics` certificates. Another 106 rows sit on Akamai edge networks and 5 on European telecom carriers.

2. **PlugX-labelled candidates expose TCP port 53 alongside web ports on commercial cloud hosts.**

   Out of 281 PlugX-labelled endpoints on 158 hosts, 31 hosts expose port 53 and 28 bind HTTP or HTTPS ports at the same time. Five port 53 hosts complete TLS handshakes directly on TCP port 53 instead of DNS-over-TLS port 853.

3. **Gh0stRAT and NDragonRAT clusters concentrate inside Hong Kong and South Korean server subnets.**

   Gh0stRAT accounts for 552 endpoints, placing 107 on port 14994 and reusing `CN=DcRat` certificates across 11 endpoints on 9 hosts. Its sole feed-confirmed row sits on Chinanet Remote Desktop port 3389. On 21 November 2026, five new NDragonRAT port 8080 listeners were recorded on Hong Kong provider CTG Server Limited, including four in one `/24` subnet.

Three Decisions for Leaders

1. **Keep uncorroborated espionage and RAT feed lists out of automatic IP block lists.** Use cyber threat intelligence to route cloud candidates to network and endpoint hunting while withholding Akamai, Cloudflare, telecom carriers, and Remote Desktop or mail-port collisions from firewall blocks.
2. **Enforce strict protocol validation on outbound UDP and TCP port 53.** Block direct port 53 connections outside internal DNS forwarders, and alert whenever TCP port 53 carries HTTP verbs or TLS handshakes.
3. **Detect conserved wire framing, self-signed certificate templates, and script HTTPS connections.** Alert on Gh0stRAT zlib headers, njRAT pipe-delimited frames, self-signed `CN=Elastics` and `CN=DcRat` certificates, and Windows Script Host outbound HTTPS traffic.

The Study in Numbers

Number	What it is
1,421 / 1,261	Global feed-labelled sightings and examined endpoints across 1,261 hosts and 942 `/24` subnets
0 / 1,421	Confirmed cloud C2 addresses for standalone IP blocking after withholding a Chinanet port 3389 host
1,251 / 170	Commercial cloud endpoints kept for hunting (1,251) vs withheld telecom and CDN rows (170)
563 / 564	Gamaredon-labelled endpoints on HTTPS port 443 across 517 `/24` subnets (361 on DigitalOcean)
31 / 281	PlugX-labelled endpoints on port 53, including 28 multi-port hosts and 5 serving TLS on port 53
107 / 552	Gh0stRAT-labelled endpoints on port 14994 (96 in Hong Kong and 8 in Japan)
8	Published hunt indicators in Appendix A: 8 JARM fingerprints (0 IPv4 addresses and 0 hashes)

How to use this report.

Security leaders can focus on Chapters 1, 6, and 7. Network and Windows architects should read Chapters 3, 4, 5, and 7. SOC analysts and detection engineers should start with Chapters 5, 8, and 9. CTI analysts will find hosting, `/24` subnet, and TLS detail in Chapters 2 through 6.

02

CHAPTER 02

Four Infrastructure Groups, One Analytical Model

IN SHORT

Zero hosts appear in more than one family across the 1,261 hosts in this study, and only one Hong Kong `/24` subnet holds two families. We group the five upstream feed labels into four infrastructure roles as an analytical model for defenders, not as one threat actor. Hunt each role with separate protocol and TLS checks.

INSIDE THIS CHAPTER

Why zero IP addresses are published for blocking 08

Where the endpoints sit 08

02 Four Infrastructure Groups, One Analytical Model

Upstream feeds assign labels (`aptgamaredon`, `plugx`, `gh0strat`, `ndragonrat`, `njrat`) from TLS certificate fields, JARM fingerprints, or port banners. Those labels show which signature matched a host; they do not establish state sponsorship or operator identity. Eleven endpoints tagged `gh0strat` serve the default self-signed `CN=DcRat` certificate across 9 hosts, showing how commodity RAT certificates cross feed rules.

Host comparison confirms zero shared hosts across the five families (`564 + 515 + 158 + 18 + 6 = 1,261` hosts). The study spans 942 distinct `/24` blocks from 943 family-subnet pairs. One Hong Kong CTG Server Limited `/24` holds both a Gh0stRAT and an NDragonRAT port 8080 host. Figure 1 presents the four groups as an analytical model.

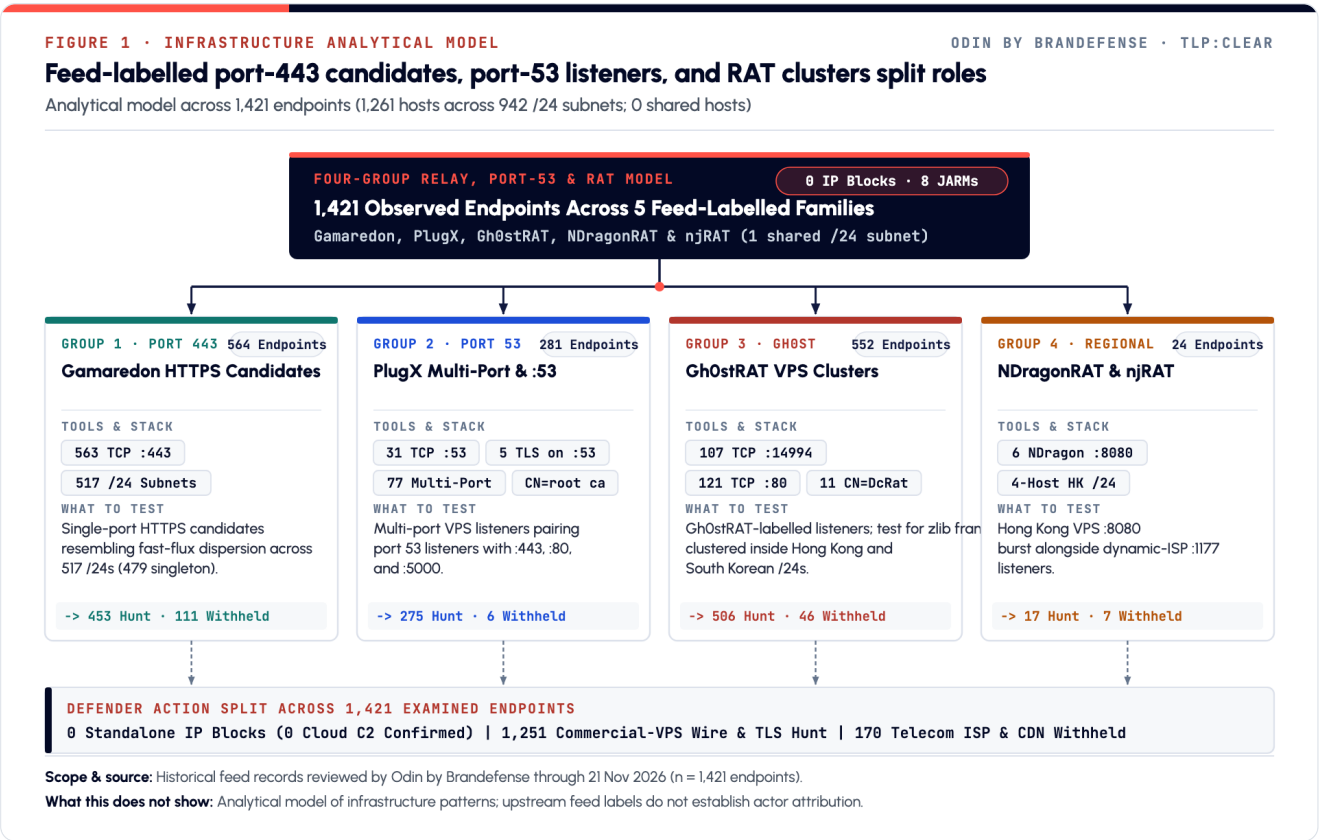


Figure 1: Feed-labelled port-443 candidates, port-53 listeners, and RAT clusters split roles (analytical model)

Group	Feed labels	Endpoints	Hosts	/24 s	Defender action
Port-443 relay candidates	Gamaredon	564	564	517	Hunt `CN=Elastics` certs and script HTTPS fan-out; withhold 106 Akamai rows
Port-53 cloud listeners	PlugX	281	158	122	Block workstation port 53; inspect TCP 53 for HTTP or TLS framing
Port-14994 RAT clusters	Gh0stRAT	552	515	283	Hunt `Gh0st` + zlib `|78 9c|` and `CN=DcRat`; withhold 46 telecom rows
HK `/24` burst and port 1177	NDragonRAT, njRAT	24	24	21	Hunt port 1177 `|00|lv` frames and HK port 8080 clusters; withhold 7 ISP rows

Why zero IP addresses are published for blocking

Upstream feeds marked 1,406 endpoints as candidates (98.9%), 14 as suspected (10 PlugX, 4 Gh0stRAT), and 1 as confirmed. Reviewing that sole feed-confirmed record (13 November 2026 under Gh0stRAT) showed that it sits on Chinanet, a Chinese broadband carrier, on TCP port 3389 for Windows Remote Desktop Protocol (RDP).

Broadband hosts exposing RDP are potential victims or third parties rather than cloud C2 servers. That host and 169 other telecom ISP and CDN rows are withheld (170 total, 12.0%). All 1,251 commercial cloud candidates (88.0%) also stay withheld because banner matches alone do not confirm malicious ownership.

Where the endpoints sit

Hong Kong leads across 33 countries, with 393 endpoints (27.7%). The United States has 272 (19.1%), China 141 (9.9%), and Canada and South Korea each have 84 (5.9%). Next are the Netherlands (68), the United Kingdom (59), India (57), Japan (56), Germany (48), Singapore (25), and Taiwan (22).

Network provider	Role	Endpoints	Family breakdown	Handling
DigitalOcean, LLC	Cloud VPS hosting	361	Gamaredon (361, 64.0% of family)	Protocol and TLS hunt
CTG Server Limited	Commercial VPS (HK, SG)	137	Gh0stRAT (129), NDragonRAT (6), PlugX (2)	Protocol and TLS hunt
Akamai International and Connected Cloud	Shared CDN edge networks	106	Gamaredon (65 + 41)	Withheld (do not block)
MOACK[.]Co[.]LTD	Server hosting (KR)	65	Gh0stRAT (65, port 80 `/24` clusters)	Protocol and TLS hunt
BGPNET Global ASN	Commercial VPS (HK, JP)	52	PlugX (30, 4 on port 53), Gh0stRAT (22)	Protocol and TLS hunt
The Constant Company, LLC	Cloud VPS hosting	48	PlugX (30, 5 on port 53), Gamaredon (18)	Protocol and TLS hunt
Shenzhen Tencent Computer Systems	Cloud hosting (CN, HK)	42	Gh0stRAT (36), PlugX (5), njRAT (1)	Protocol and TLS hunt
Naruto	Commercial VPS (HK, JP)	34	Gh0stRAT (34, 27 on port 14994)	Protocol and TLS hunt
Amazon[.]com, Inc.	Hyperscale cloud	27	PlugX (25, 6 on port 53), Gh0stRAT (1), njRAT (1)	Protocol and TLS hunt
Chinanet, CHINANET, and CHINA UNICOM	Broadband telecom ISPs	37	Gh0stRAT (37 of 46 withheld rows)	Withheld (do not block)

CHAPTER 03

Gamaredon-Labelled HTTPS Candidates and PlugX Port-53 Listeners

IN SHORT

Gamaredon candidates (564 endpoints) and PlugX candidates (281 endpoints on 158 hosts) use opposite cloud designs. Gamaredon-labelled records place 563 of 564 endpoints on port 443 across 517 `/24` subnets. Of those subnets, 479 hold one host. Nearly half of PlugX-labelled hosts expose two to five ports, including 31 listeners on port 53. Block direct workstation port 53 traffic and inspect allowed port 53 sessions for HTTP or TLS payloads.

INSIDE THIS CHAPTER

Gamaredon: 99.8% port 443 dispersion and Akamai edge collisions 10

PlugX: multi-port VPS stacks and port-53 listener verification 11

03 Gamaredon-Labelled HTTPS Candidates and PlugX Port-53 Listeners

CISA and MITRE ATT&CK (G0047) report that Gamaredon uses fast-flux DNS (T1568.001) to rotate domain records across short-lived cloud proxies (T1090.002) polled by VBScript and HTA scripts (T1218.005). PlugX (S0013) side-loads DLLs via signed Windows binaries. It cycles C2 sessions across HTTPS (443), HTTP (80, 8080), 5000, and port 53 (T1571 ; DNS-protocol use is not established in this sample). Figure 2 maps all five families to their detections.

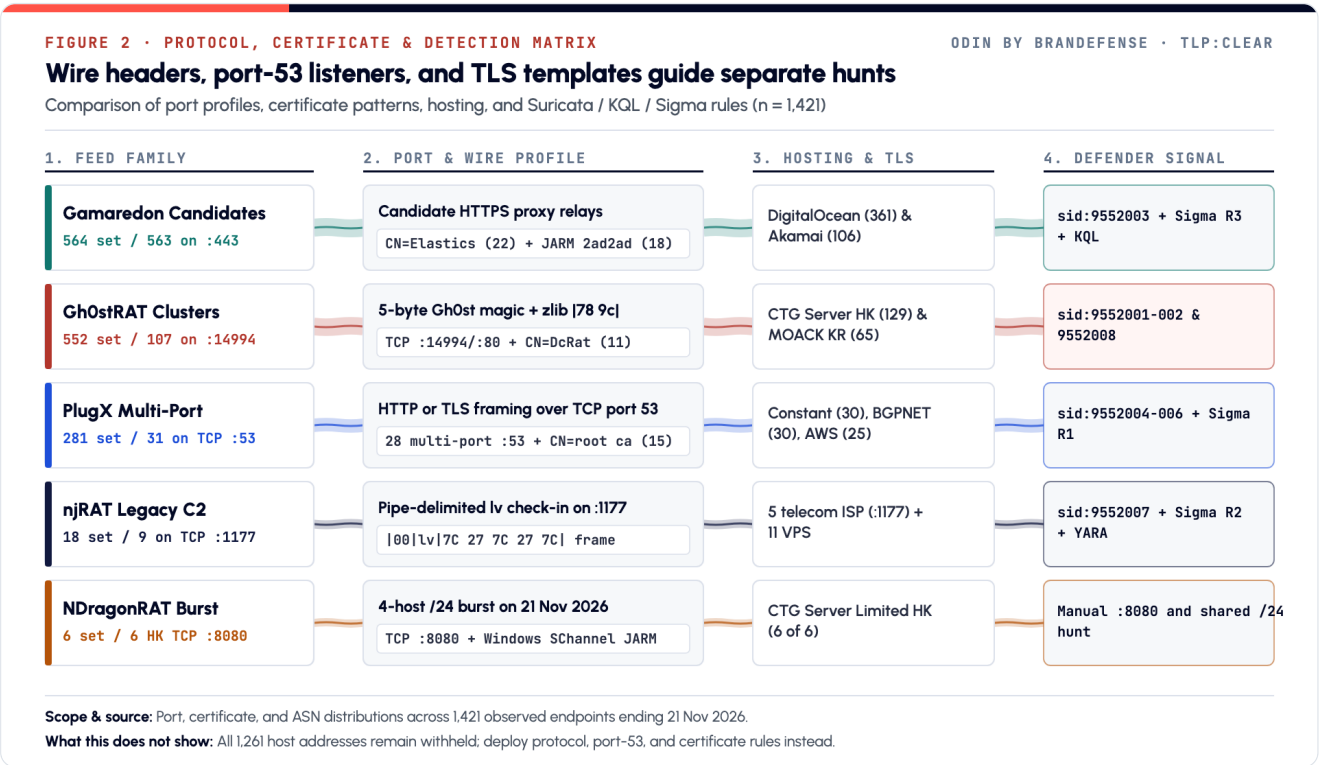


Figure 2: Wire headers, port-53 listeners, and TLS templates guide separate hunts

Gamaredon: 99.8% port 443 dispersion and Akamai edge collisions

Upstream feed entries for Gamaredon carry record dates ending on 24 April 2025. Their port and subnet layout resembles published Gamaredon fast-flux patterns, but this sample does not establish DNS rotation or actor attribution:

- **Single-port HTTPS focus.** Exactly 563 of 564 endpoints (99.8%) listen on TCP 443, with one port 80 host in the Netherlands and zero multi-port hosts.
- **Wide /24 spread.** The 564 hosts span 517 /24 subnets: 479 hold 1 host (92.6%), 29 hold 2, 9 hold 3, and zero hold 4 or more.
- **DigitalOcean droplets vs Akamai edges.** DigitalOcean hosts 361 endpoints (64.0%), followed by Constant (18), Unitas Global (18), and BL Networks (17) across the US (191), Canada (83), the Netherlands (59), India (57), the UK (55), and Germany (42). Another 106 rows (18.8%) sit on Akamai International (65) and Akamai Connected Cloud (41) plus 5 European telecom rows, which sit on shared CDN networks and should not be blocked from feed labels alone.

- **Self-signed `CN=Elastics` certificates.** Alongside 370 entries without a certificate subject and 144 custom-domain certificates, 22 port 443 hosts present self-signed `CN=Elastics`. Sixteen of those 22 share JARM `2ad2ad0002ad2ad22c42d42d0000008a5941c13f67e0c0a2c8a36bfeef6920` (18 total), tied with custom-domain candidate JARM `27d40d40d00040d00042d43d000000d2e61cae37a985f75ecafb81b33ca523` (18).

PlugX: multi-port VPS stacks and port-53 listener verification

Among 281 PlugX endpoints on 158 hosts in 122 `/24` subnets, Hong Kong leads with 125 (44.5%). The US has 49 (17.4%), Japan 44 (15.7%), and Singapore 14 (5.0%). Seventy-seven hosts (48.7%) expose two to five ports together, a pattern defenders can review with external attack surface management. These multi-port hosts include 41 two-port, 27 three-port, 8 four-port, and 1 five-port servers.

Port 443 holds 96 endpoints (34.2%), 80 holds 45 (16.0%), **port 53 holds 31 hosts (11.0%)**, 5000 holds 29 (10.3%), and 8080 holds 16 (5.7%). Smaller sets bind 5080 (6), 12345 (6), 8000 (5), 8443 (5), and 21 (5). Fifteen TLS endpoints serve self-signed `CN=root ca`, with 12 sharing JARM `07d0bd16d21d21d07c07d0bd07d21dd7fc4c7c6ef19b77a4ca0787979cdc13` (XNNET 9, Cogent 3).

Ten PlugX endpoints across nine hosts carried an upstream `suspected` label between 13 and 19 November 2026. Eight sit on Amazon[.]com, CTG Server Limited, Alibaba, Shenzhen Tencent (8000 and stacked 1033/8254), Hetzner (443, `CN=root ca`), and Nocix (53). One port 49154 row sits on withheld ISP Korea Telecom.

Port-53 check	Observed across 31 PlugX port-53 hosts	Defender takeaway
Cloud VPS hosting	30 sit on cloud ASNs (Amazon[.]com 6, Constant 5, BGPNET 4, Gigabit 3, PEG TECH 2, Nocix 1) and 1 on Cloudflare London	Separates rented cloud hosts from home lines while keeping Cloudflare withheld
TLS directly on TCP 53	5 PlugX hosts (US, KR, HK, EE) plus 1 Gh0stRAT host (HK) complete TLS handshakes on TCP 53; 2 share JARM `29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787`	DNS-over-TLS normally uses TCP 853; TLS on TCP 53 is a non-DNS hunt signal, not proof of a PlugX tunnel (SID 9552006)
Multi-port stacking	28 of 31 hosts (90.3%) co-expose 55 companion ports: 443 (22), 80 (17), 8080 (10), 12345 (2), 21 (2), 8000 (1), 8443 (1)	Matches PlugX builder profiles binding identical listeners across 53, 80, 443, 8080
Resolver overlap	26 hosts expose plain port 53 without TLS, which web panels running `named` or `dnsmasq` can also create	Block workstation port 53 and inspect forwarder TCP 53 for `HTTP/1.1` or TLS

04

CHAPTER 04

Gh0stRAT Port-14994 Clusters and Cross-Family Certificate Reuse

IN SHORT

Gh0stRAT accounts for 552 examined endpoints on 515 hosts across 283 `/24` subnets, led by Hong Kong (262), China (134), and South Korea (79). Port 14994 holds 107 commercial-VPS endpoints, and 11 endpoints across 9 hosts serve self-signed `CN=DcRat` certificates. Alert on the 5-byte `Gh0st` header plus zlib `|78 9c|` stream and keep broadband RDP and mail ports out of firewall blocks.

INSIDE THIS CHAPTER

Port 14994 concentration in Hong Kong and Japan 13

04 Gh0stRAT Port-14994 Clusters and Cross-Family Certificate Reuse

Gh0stRAT (`S0032`) variants keep a conserved binary wire header: a 5-byte ASCII tag (`Gh0st`), two 4-byte length fields, and a `zlib` payload (`0x78 0x9c`) at byte offset 13. Figure 3 models how fast-flux polling, port-53 listeners, and RAT frames cross network layers.

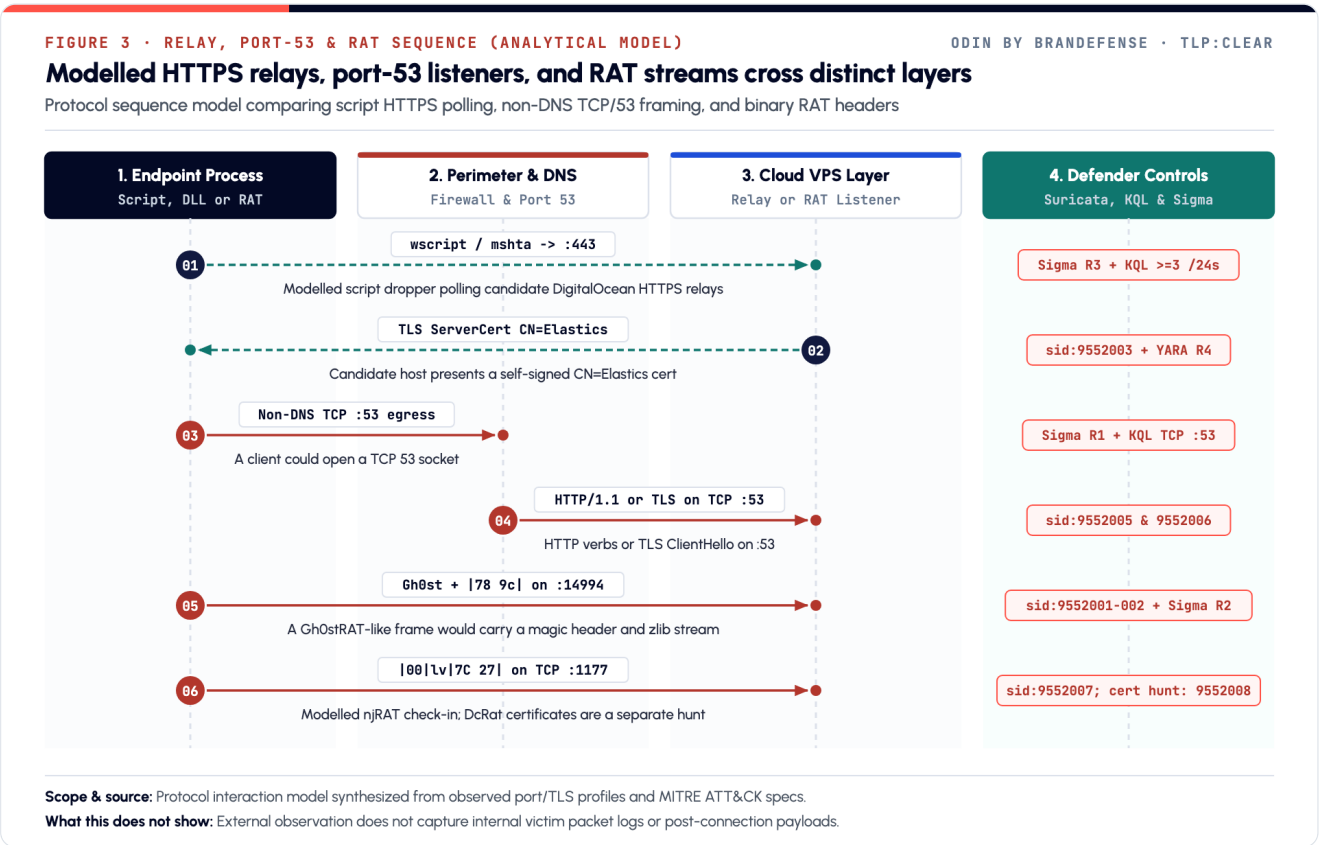


Figure 3: Modelled HTTPS relays, port-53 listeners, and RAT streams cross distinct layers (analytical model)

Port 14994 concentration in Hong Kong and Japan

Across 552 Gh0stRAT endpoints on 515 hosts (28 seen in November 2026), four ports hold 364 endpoints (65.9%). These are 80 (121, 21.9%), **14994 (107 hosts, 19.4%)**, 443 (77, 13.9%), and 8080 (59, 10.7%). Secondary ports include 8000 (29), 3456 (15), 9999 (13), 2100 (11), and 10086 (7).

Hong Kong holds 96 of the 107 port 14994 hosts (89.7%) and Japan holds 8 (7.5%), led by CTG Server Limited (52) and Naruto (27). Twenty-seven port 14994 endpoints match JARM `3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763` and 25 match Windows SChannel JARM `14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532`.

Sub-slice	Endpoints and hosts	Detail	Defender takeaway
`CN=DcRat` reuse	11 endpoints on 9 hosts (443: 8, 80: 2, 8000: 1)	7 in one KR/HK `/24`, 3 in one CTG Server HK `/24`; 10 share JARM `22b22b00022b22b22b22b22b22bd3b67dd3674d9af9dd91c1955a35d0e9`	Alert on `CN=DcRat` server certificates (SID 9552008)
Telecom and RDP	46 endpoints on 44 hosts	Includes sole feed-confirmed row on Chinanet port 3389 (13 November 2026) and Chunghwa Telecom port 8443	Withhold broadband carriers and RDP port 3389 from blocks
Mail-port host	3 endpoints on 1 host (465, 993, 995)	Upstream-suspected CTG Server HK host (14 November 2026) serving SMTPS, IMAPS, and POP3S	Require `Gh0st` wire payload matches before blocking mail ports

05

CHAPTER 05

Hong Kong Subnet Bursts, Dense /24 Clusters, and njRAT

IN SHORT

Commercial VPS resellers in Hong Kong and South Korea pack RAT candidates into single `/24` blocks, including 25 `/24` clusters (187 endpoints) and a four-host NDragonRAT burst. Legacy njRAT splits instead between scattered VPS hosts and broadband lines on port 1177, so hunt port 1177 delimiters and `/24` VPS bursts.

INSIDE THIS CHAPTER

The 21 November 2026 NDragonRAT burst on CTG Server Limited 16

Top 25 dense `/24` clusters vs scattered njRAT port-1177 hosts 17

05 Hong Kong Subnet Bursts, Dense /24 Clusters, and njRAT

Figure 4 contrasts PlugX multi-port stacks, Gh0stRAT port 14994 clusters, and NDragonRAT's Hong Kong `/24` burst with withheld telecom and CDN rows.

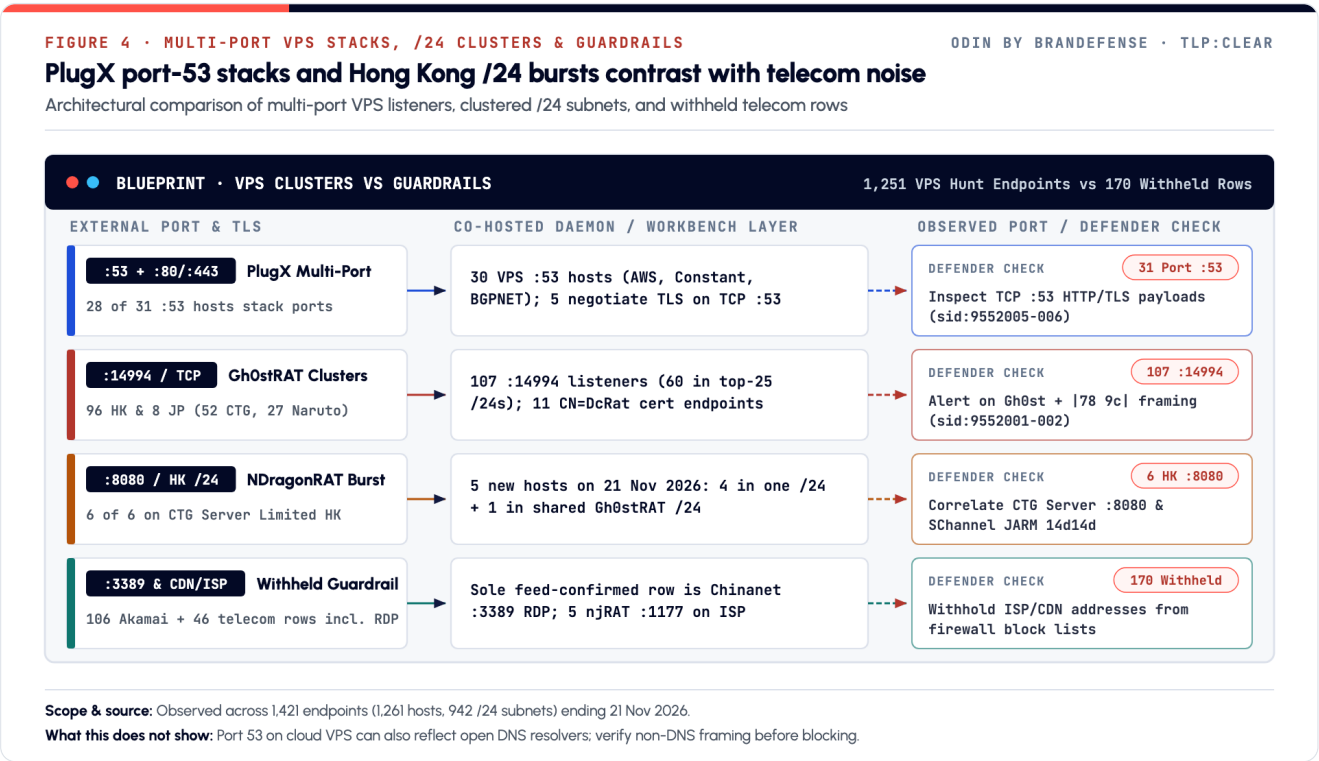


Figure 4: PlugX port-53 stacks and Hong Kong /24 bursts contrast with telecom noise

The 21 November 2026 NDragonRAT burst on CTG Server Limited

All 6 NDragonRAT endpoints sit in **Hong Kong on CTG Server Limited TCP port 8080**. One host was observed from 17 to 20 November 2026 with JARM `21d14d00021d21d00042d43d00000091f9827a8676a9d9f27d421962a09b5d` (shared with 9 Gh0stRAT endpoints).

On 21 November 2026, five new port 8080 hosts were recorded on CTG Server Limited. Four sit together inside one `/24` subnet, with one serving a default Windows host certificate and SChannel JARM `14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532`. The fifth sits inside the sole `/24` subnet shared with a Gh0stRAT port 8080 candidate.

Top 25 dense `/24` clusters vs scattered njRAT port-1177 hosts

Across the study, 29 groups split by family, `/24` subnet, port and country hold 4 or more endpoints (203 endpoints, including NDragonRAT's four-host group). The top 25 dense `/24` clusters total **187 endpoints (13.2%)** across 24 unique `/24` subnets:

Cluster group	`/24` clusters	Port(s)	Providers and locations	Endpoints
Korean HTTP clusters	6 (Gh0stRAT)	80	MOACK[.]Co[.]LTD KR (16, 11, 7, 7, 6) and BGP Network KR (5)	52
Asian port-14994 clusters	7 (Gh0stRAT)	14994	CTG Server HK (10, 10, 9, 5), Naruto HK/JP (13, 6), BGPNET HK (7)	60
HK and KR HTTPS clusters	6 (Gh0stRAT)	443	CTG Server HK (10, 7, 6, 4), BGPNET HK (9), BGP Network KR (7, `CN=DcRat`)	43
HK, SG, and CN clusters	3 (Gh0stRAT)	80, 9999	NetLab Global HK (11), Hubei Feixun CN (5), CTG Server SG (4)	20
HK PlugX HTTPS clusters	3 (PlugX)	443	CNSERVERS LLC HK (4) and Netsec Limited HK (4 and 4)	12

NjRAT (`S0385`, 18 hosts across 18 `/24` subnets in 12 countries, with upstream record dates ending on 21 October 2026) shows zero `/24` clustering. Nine endpoints (50.0%) use default port **1177**, alongside 8080 (3) and singletons on 6522, 7070, 7077, 22 (SSH on PT Telekomunikasi Indonesia), 443, and 5000.

Five port 1177 hosts sit on dynamic subscriber telecom lines: four on PALTEL and one on Saudi Telecom. One port 6522 host sits on Free SAS, bringing withheld telecom rows to 7. Suricata SID 9552007 catches njRAT's `|00|lv|'|'|` check-in frame regardless of IP churn.

CHAPTER 06

Why Static IP Block Lists Misfire Across All Five Families

IN SHORT

Zero endpoints out of 1,421 examined records belong on an automated IP block list. Blocking unverified espionage and RAT feeds disrupts Akamai and Cloudflare edges and broadband subscribers without verifying candidate relays or port-53 listeners. Validate protocol framing before containment.

INSIDE THIS CHAPTER

Four reasons raw feed blocking fails here 19

06 Why Static IP Block Lists Misfire Across All Five Families

Figure 5 compares total observed endpoints with the 1,251 commercial-VPS hunt endpoints across all five families.

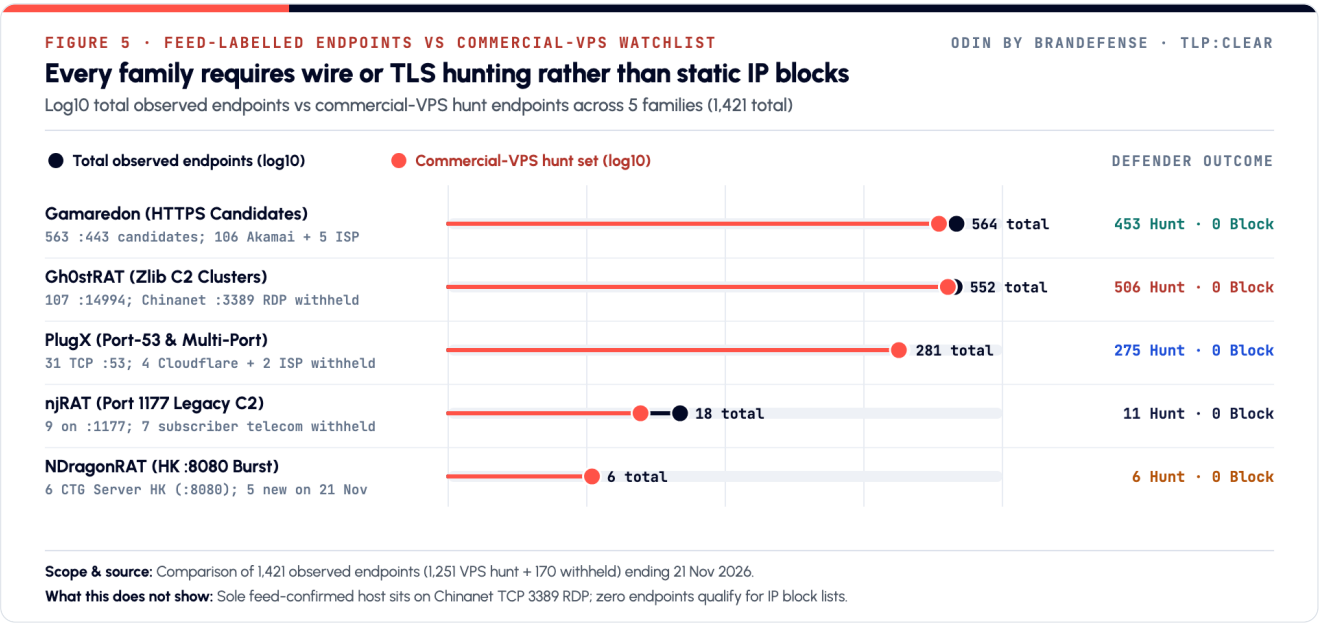


Figure 5: Every family requires wire or TLS hunting rather than static IP blocks

Family	Observed	Hosts	Block	Commercial-VPS hunt set	Withheld telecom and CDN rows
Gamaredon	564	564	0	453 (361 DigitalOcean, 22 `CN=Elastics`)	111 (106 Akamai + 5 EU telecom)
GhOstRAT	552	515	0	506 (107 port 14994, 11 `CN=DcRat`)	46 (telecom rows incl. Chinanet port 3389 RDP)
PlugX	281	158	0	275 (30 VPS port 53, 15 `CN=root ca`)	6 (4 Cloudflare + 2 telecom ISPs)
njRAT	18	18	0	11 (4 VPS port 1177, 3 port 8080)	7 (4 PALTEL + Saudi Telecom + Free + Telkom)
NDragonRAT	6	6	0	6 (6 CTG Server HK port 8080)	0

Four reasons raw feed blocking fails here

1. **Shared CDN edge networks (110 rows).** The feed labels 106 Akamai CDN rows as Gamaredon candidates, and 4 PlugX rows point to Cloudflare London.
2. **Broadband dynamic DNS and RDP collisions (60 rows).** Telecom carriers hold 46 GhOstRAT rows (including Chinanet port 3389 RDP), 7 njRAT rows, 5 Gamaredon rows, and 2 PlugX rows.
3. **Shared OS TLS stacks across all five families.** JARM `14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532` spans 75 endpoints across all five families (64 GhOstRAT, 6 Gamaredon, 3 PlugX, 1 NDragonRAT, 1 njRAT), and `3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763` spans 89 endpoints across three families, fingerprinting stock Windows SChannel and OpenSSL VPS stacks.
4. **Open DNS resolvers and mail daemons on VPS hosts.** Plain port 53 and mail ports (465, 993, 995) require wire payload verification before enforcement.

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

DNS and perimeter firewall

- [ ] Block direct outbound UDP and TCP port 53 traffic from workstations and servers outside internal DNS forwarders (`RFC 1035`).
- [ ] Inspect allowed TCP port 53 trunks with NIDS signatures so HTTP requests or TLS handshakes over port 53 trigger investigation before containment.

Windows endpoints and script hosts

- [ ] Block `wscript.exe`, `cscript.exe`, and `mshta.exe` from opening direct internet connections on port 443 via host firewall or Attack Surface Reduction rules.
- [ ] Audit and block unsigned DLL side-loading via `rundll32.exe` or `regsvr32.exe` in `C:\ProgramData\` and `C:\Windows\Temp\`.

Network detection and threat intelligence

- [ ] Deploy the Suricata, Sentinel KQL, Sigma, and YARA rules in Chapter 8 with exact-hostname allowlists for corporate DNS forwarders and sandboxes.
- [ ] Keep Akamai, Cloudflare, telecom ISPs, RDP port 3389, mail ports (465, 993, 995), and JARM-only matches out of automatic firewall block lists.

CHAPTER 08

Detection Rules

IN SHORT

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

INSIDE THIS CHAPTER

How the Suricata signatures work 23

How the KQL, Sigma, and YARA rules work 23

MITRE ATT&CK mapping 24

08 Detection Rules

The full rules are in Appendix B. Suricata `7.0.12` (`suricata -T`) loaded all eight signatures with 0 errors and `lint_suricata.py` found 0 problems. Sentinel KQL, Sigma (3 rules), and YARA (4 rules) passed static syntax, modifier, and fixture checks without live engine replay on our build host. Test and tune them locally before automated isolation.

Rule file	What it catches
`odin_gamaredon_fastflux_plugx_dns_and_rat_c2.rules`	Suricata 7: eight signatures for Gh0stRAT zlib headers, `CN=Elastics`, `CN=root ca`, and `CN=DcRat` certs, HTTP or TLS on TCP 53, and njRAT port 1177 frames
`sentinel_fastflux_plugx_dns_and_rat_hunt.kql`	Microsoft Sentinel and Defender XDR: non-resolver TCP 53 egress, ports 1177 and 14994, script HTTPS `/24` fan-out, and writable-path DLL staging
`sigma_plugx_port53_gamaredon_script_and_rat_ports.yml`	Sigma (3 rules): Windows non-DNS outbound TCP 53 connections, ports 14994 or 1177, and `wscript` / `cscript` / `mshta` outbound HTTPS traffic
`odin_gh0strat_plugx_njrat_and_gamaredon_artifacts.yar`	YARA (4 rules): Gh0stRAT zlib PE implants, PlugX side-loaded loaders, njRAT .NET clients, and Gamaredon VBS/HTA droppers

How the Suricata signatures work

SID	Looks for	Why
9552001	Outbound TCP 14994 stream starting with `Gh0st` and zlib `|78 9c|` at offset 13	Classic Gh0stRAT binary framing on its primary VPS port
9552002	Outbound `Gh0st` + zlib header on ports 80, 443, 2100, 3456, 8000, 8080, 9999, 10086	Catches Gh0stRAT masquerading on web and alternate ports
9552003	Inbound port 443 server cert with subject and issuer containing the same CN (`CN=Elastics`)	Flags Gamaredon-labelled `CN=Elastics` candidate certs (22 rows)
9552004	Inbound port 443 or 8443 server cert with subject and issuer containing the same CN (`CN=root ca`)	Hunt signal for PlugX-labelled `CN=root ca` certs (15 rows; alert-only)
9552005	Outbound `HTTP/1.1` `GET`, `POST`, `PUT`, or `HEAD` request over TCP 53	Flags HTTP requests on TCP 53 for non-DNS protocol investigation
9552006	Outbound TLS `ClientHello` (`|16 03|` + `|01 00|`) over TCP 53	Flags TLS ClientHello on TCP 53 for non-DNS protocol investigation (5 PlugX, 1 Gh0stRAT)
9552007	Outbound TCP 1177 stream with `|00|lv|7C 27 7C 27 7C|` within 16 bytes	Catches njRAT 0.7d pipe-delimited check-in frames
9552008	Inbound server cert with subject and issuer containing the same CN (`CN=DcRat`)	Catches DcRat and cross-family cert reuse (11 Gh0stRAT rows)

How the KQL, Sigma, and YARA rules work

The Sentinel KQL query correlates seven days of `DeviceNetworkEvents` and `DeviceProcessEvents`. It flags non-DNS processes opening outbound TCP 53 sockets, connections to ports 1177 or 14994, and `wscript.exe`, `cscript.exe`, or `mshta.exe` reaching three or more `/24` subnets over port 443.

It also catches `rundll32.exe` or `regsvr32.exe` staging in `C:\ProgramData\` or `C:\Windows\Temp\`. Exact allowlists cover only `CORP-DNS-FWD-01` /02, `SEC-SANDBOX-WIN-01`, `SEC-NETLAB-LNX-01`, and exact system DNS binary paths.

Sigma rule	Level	Fires when
Non-Resolver Process Initiating Outbound TCP Port 53 Connection	High	Windows TCP 53 egress outside exact `dns.exe` / `svchost.exe` paths and `CORP-DNS-FWD-01` /02
Outbound Connection to Characteristic Gh0stRAT Port 14994 or njRAT Port 1177	High	Windows host outside `SEC-SANDBOX-WIN-01` connects to TCP 14994 or 1177
Windows Script Host or MSHTA Initiating Outbound HTTPS Connection	High	Exact `System32` or `SysWOW64` `wscript.exe`, `cscript.exe`, or `mshta.exe` connects to TCP 443

YARA rule	Fires when
`ODIN_Gh0stRAT_Magic_Zlib_Implant`	PE under 5 MB combines `Gh0st` and zlib `1.1.4` or `{ 78 9C }` with two manager classes
`ODIN_PlugX_Sideloaded_Payload_Loader`	PE under 4 MB combines `GULP`, `PLUG`, or `boot.ldr` with `RtlDecompressBuffer`, `VirtualAlloc`, and WinInet/DNS APIs
`ODIN_njRAT_DotNet_Port1177_Client`	.NET PE under 2 MB combines `mscoree.dll` and `|'|'|` with `0.7d` or 1177 and firewall strings
`ODIN_Gamaredon_VBS_FastFlux_Relay_Dropper`	Script under 1 MB combines `WScript.Shell` / `FileSystemObject`, `XMLHTTP` / `WinHttp`, `ADODB.Stream`, and `wscript` / `mshta`

MITRE ATT&CK mapping

Tactic	Technique	How it shows up	Detection
Resource Development	T1583.003 Virtual Private Server	361 DigitalOcean droplets, 137 CTG Server HK and 65 MOACK[.]Co[.]LTD rows, 4-host HK `/24` burst	SIDs 9552001 to 9552008; 8 JARMs
Command and Control	T1568.001 Fast Flux DNS	563 Gamaredon-labelled port-443 candidates across 517 `/24`s (479 single-host) and 22 `CN=Elastics` certs	SID 9552003; KQL; Sigma rule 3
Command and Control	T1571 Non-Standard Port	Gh0stRAT 14994 (107), njRAT 1177 (9), PlugX TCP 53 (31) and 5000 (29)	SIDs 9552001, 9552005 to 9552007
Defense Evasion	T1218.005 Mshta	Gamaredon VBS/HTA HTTPS droppers and PlugX writable-folder DLL side-loading	Sigma rule 3; KQL; YARA rules 2 and 4

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

JARM fingerprints to hunt (in Appendix A) 26

Other indicators (text only) 27

09 Indicators

Appendix A holds 8 published indicators: 0 IPv4 addresses, 0 file hashes, and 8 JARM fingerprints. Eight more wire, certificate, and port-cluster markers appear in this report only. All 1,261 distinct host addresses across the 1,421 examined endpoints are withheld.

Type	Count	Where to use it
Network addresses and file hashes (Appendix A)	0	Zero addresses or hashes are published because no cloud host met C2 block criteria
TLS JARM fingerprints (Appendix A)	8	TLS hunting only; never block on a JARM fingerprint alone
Wire, certificate, and port markers (text only)	8	Suricata, Sentinel KQL, Sigma, and YARA hunting

JARM fingerprints to hunt (in Appendix A)

JARM	Family	Context
`2ad2ad0002ad2ad22c42d42d0000008a5941c13f67e0c0a2c8a36bfeef6920`	Gamaredon	Shared by 18 HTTPS endpoints, including 16 of 22 self-signed `CN=Elastics` candidates
`27d40d40d00040d00042d43d000000d2e61cae37a985f75ecafb81b33ca523`	Gamaredon, GhOstRAT	TLS fingerprint across 20 feed-labelled endpoints (19 on port 443, one on port 2100)
`07d0bd16d21d21d07c07d0bd07d21dd7fc4c7c6ef19b77a4ca0787979cdc13`	PlugX	Shared by 13 commercial-VPS endpoints, including 12 of 15 `CN=root ca` listeners
`2ad2ad0002ad2ad22c2ad2ad2ad2ad703dc1bf20eb9604decefea997eabff7`	PlugX	Seen on 11 PlugX-labelled endpoints across six ports, none on port 443
`29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787`	PlugX	Shared by 2 of 5 PlugX-labelled hosts serving TLS on TCP 53, plus one port 80 and one port 443 endpoint
`3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763`	GhOstRAT, PlugX, Gamaredon	Leading TLS stack across 89 endpoints (86 GhOstRAT, 27 on port 14994)
`14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532`	All 5 families	Windows SChannel TLS stack across 75 endpoints across all five labels
`22b22b00022b22b22b22b22b22b22bd3b67dd3674d9af9dd91c1955a35d0e9`	GhOstRAT	Shared by 16 endpoints, including 10 of 11 `CN=DcRat` certificate endpoints

Other indicators (text only)

Indicator	Type	Where to hunt
`Gh0st` + zlib `|78 9c|` at offset 13	Binary C2 header	Suricata SIDs 9552001 and 9552002; YARA rule 1
`CN=Elastics`	TLS subject and issuer (22 rows)	Suricata SID 9552003 on inbound TCP 443
`CN=root ca`	TLS subject and issuer (15 rows)	Suricata SID 9552004 (alert-only hunt)
`CN=DcRat`	TLS subject and issuer (11 rows)	Suricata SID 9552008 across TLS ports
`HTTP/1.1` or TLS `ClientHello` on TCP 53	Non-DNS port-53 investigation signal	Suricata SIDs 9552005 and 9552006; Sigma rule 1; KQL
`|00|lv|7C 27 7C 27 7C|`	njRAT check-in frame	Suricata SID 9552007 and YARA rule 3
TCP 14994	Gh0stRAT VPS port (107 rows)	Suricata SID 9552001; Sigma rule 2; KQL
TCP 53 + 80 + 443 + 8080	Multi-port PlugX stack (28 hosts)	Attack-surface and egress correlation

Withheld: all 1,261 distinct host addresses across the 1,421 examined endpoints, plus unverified custom certificate domains, workstation hostnames, and brand-lure certificate strings.

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

- **Window.** The records have last-seen dates from 13 June 2023 through 21 November 2026. Upstream feed entries for Gamaredon carry record dates ending on 24 April 2025, and njRAT entries carry record dates ending on 21 October 2026.
- **Feed labels are not attribution.** Family names come from upstream rules matching certificates, JARM hashes, or port banners and do not establish state sponsorship.
- **Analytical model.** Zero hosts overlap across the five families, and the single shared Hong Kong `/24` subnet sits on a commercial VPS reseller. Figures 1 and 3 show an analytical model, not one actor.
- **No victim packet logs.** External records do not capture victim traffic or confirm whether non-TLS port 53 hosts ran PlugX or open DNS software.
- **Rule validation.** Suricata `7.0.12` loaded all eight rules (`suricata -T`, 0 errors; `lint_suricata.py`, 0 problems). Sentinel KQL, Sigma, and YARA passed static checks without live engine replay on our build host.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. MITRE ATT&CK. G0047 Gamaredon Group. https://attack.mitre.org/groups/G0047/ (verified 21 November 2026)
2. MITRE ATT&CK. S0013 PlugX. https://attack.mitre.org/software/S0013/ (verified 21 November 2026)
3. MITRE ATT&CK. S0032 gh0st RAT. https://attack.mitre.org/software/S0032/ (verified 21 November 2026)
4. MITRE ATT&CK. S0385 njRAT. https://attack.mitre.org/software/S0385/ (verified 21 November 2026)
5. CISA, NSA, FBI, and International Partners. Advisory AA25-093A: Fast Flux: A National Security Threat. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a (verified 21 November 2026)
6. CISA, FBI, and NSA. Advisory AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a (verified 21 November 2026)
7. MITRE ATT&CK. T1568.001 Dynamic Resolution: Fast Flux DNS. https://attack.mitre.org/techniques/T1568/001/ (verified 21 November 2026)
8. MITRE ATT&CK. T1571 Non-Standard Port. https://attack.mitre.org/techniques/T1571/ (verified 21 November 2026)
9. IETF. RFC 1035: Domain Names - Implementation and Specification. https://www.rfc-editor.org/rfc/rfc1035 (verified 21 November 2026)
10. Salesforce Engineering. JARM: An Active Transport Layer Security (TLS) Server Fingerprinting Tool. 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) 33

B. Detection rules (4 files) 34

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
R52-IOC-01	JARM	2ad2ad0002ad2ad22c42d42d0000008a5941c13f67e0c0a2c8a36bfeef6920	443	aptgamaredon · shared by 18 HTTPS endpoints including 16 of 22 self-signed CN=Elastics candidates	HUNT
R52-IOC-02	JARM	27d40d40d00040d00042d43d000000d2e61cae37a985f75ecafb81b33ca523	443	aptgamaredon and gh0strat · TLS fingerprint across 20 feed-labelled candidates (19 on port 443, one on port 2100)	HUNT
R52-IOC-03	JARM	07d0bd16d21d21d07c07d0bd07d21dd7fc4c7c6ef19b77a4ca0787979cdc13	443	plugx · shared by 13 commercial VPS endpoints including 12 of 15 self-signed CN=root ca listeners	HUNT
R52-IOC-04	JARM	2ad2ad0002ad2ad22c2ad2ad2ad2ad703dc1bf20eb9604decefea997eabff7	5000	plugx · seen on 11 PlugX-labelled endpoints across six ports; six use port 5000 and none use port 443	HUNT
R52-IOC-05	JARM	29d29d00029d29d00042d43d00041dd469afa8cfbe5e42c631eb3fc55d6787	53	plugx · seen on four PlugX-labelled endpoints: two on port 53, one on port 80, and one on port 443	HUNT
R52-IOC-06	JARM	3fd3fd0003fd3fd21c42d42d000000bdfc58c9a46434368cf60aa440385763	14994	gh0strat, plugx and aptgamaredon · leading TLS stack across 89 endpoints including 27 on port 14994	HUNT
R52-IOC-07	JARM	14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532	14994	all five families · shared Windows SChannel TLS stack across 75 endpoints	HUNT
R52-IOC-08	JARM	22b22b00022b22b22b22b22b22bd3b67dd3674d9af9dd91c1955a35d0e9	443	gh0strat · shared by 16 endpoints including 10 of 11 self-signed CN=DcRat certificate servers	HUNT

B Detection Rules

Each rule file loads in its own engine (Suricata 7, YARA-X, 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_gamaredon_fastflux_plugx_dns_and_rat_c2.rules

SURICATA

```
# Odin by Brandefense - Monograph 52 / 52 Suricata 7.x Detection Suite
# Scope: Gh0stRAT 5-byte magic + zlib C2 framing, Gamaredon CN=Elastics TLS server certs,
#        PlugX CN=root ca TLS certs and non-DNS HTTP/TLS framing on TCP port 53,
#        njRAT pipe-delimited framing on TCP 1177, and cross-family CN=DcRat TLS reuse.
# Classification: TLP:CLEAR

alert tcp $HOME_NET any -> $EXTERNAL_NET 14994 (msg:"ODIN R52 Gh0stRAT - Outbound Magic Header and Zlib C2 Stream
on Port 14994"; flow:to_server,established; content:"Gh0st"; depth:5; fast_pattern; content:"|78 9c|"; distance:
8; within:2; classtype:command-and-control; metadata:malware_family Gh0stRAT, deployment Perimeter,
signature_severity Critical, created_at 2026_11_21; sid:9552001; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET [80,443,2100,3456,8000,8080,9999,10086] (msg:"ODIN R52 Gh0stRAT -
Outbound Magic Header and Zlib Frame on Alternate C2 Port"; flow:to_server,established; content:"Gh0st"; depth:5;
fast_pattern; content:"|78|"; distance:8; within:1; pcre:"/^Gh0st.{8}\x78[\x01\x9c\xda]/s"; classtype:command-
and-control; metadata:malware_family Gh0stRAT, deployment Perimeter, signature_severity Critical, created_at
2026_11_21; sid:9552002; rev:1;)
alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ODIN R52 Gamaredon Hunt - Subject and Issuer Contain
CN=Elastics"; flow:to_client,established; tls.cert_subject; content:"CN=Elastics"; nocase; fast_pattern;
tls.cert_issuer; content:"CN=Elastics"; nocase; classtype:trojan-activity; metadata:malware_family Gamaredon,
deployment Perimeter, signature_severity High, created_at 2026_11_21; sid:9552003; rev:1;)
alert tls $EXTERNAL_NET [443,8443] -> $HOME_NET any (msg:"ODIN R52 PlugX Hunt - Subject and Issuer Contain
CN=root ca"; flow:to_client,established; tls.cert_subject; content:"CN=root ca"; nocase; fast_pattern;
tls.cert_issuer; content:"CN=root ca"; nocase; classtype:trojan-activity; metadata:malware_family PlugX,
deployment Perimeter, signature_severity Medium, created_at 2026_11_21; sid:9552004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ODIN R52 Hunt - HTTP Request on TCP Port 53";
flow:to_server,established; http.protocol; content:"HTTP/1.1"; bsize:8; fast_pattern; http.method; pcre:"/
^(?:GET|POST|PUT|HEAD)$/"; classtype:non-standard-protocol; metadata:deployment Perimeter, signature_severity
High, created_at 2026_11_21; sid:9552005; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"ODIN R52 Hunt - TLS ClientHello on TCP Port 53";
flow:to_server,established; content:"|16 03|"; depth:2; content:"|01 00|"; distance:3; within:2; fast_pattern;
classtype:non-standard-protocol; metadata:deployment Perimeter, signature_severity High, created_at 2026_11_21;
sid:9552006; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET 1177 (msg:"ODIN R52 njRAT C2 - Outbound Pipe-Delimited Check-In Frame on
TCP 1177"; flow:to_server,established; content:"|00|lv|7C 27 7C 27 7C|"; depth:16; fast_pattern;
classtype:command-and-control; metadata:malware_family njRAT, deployment Perimeter, signature_severity Critical,
created_at 2026_11_21; sid:9552007; rev:1;)
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN R52 Commodity RAT - Inbound Subject and Issuer Contain
CN=DcRat"; flow:to_client,established; tls.cert_subject; content:"CN=DcRat"; nocase; fast_pattern;
tls.cert_issuer; content:"CN=DcRat"; nocase; classtype:command-and-control; metadata:malware_family
DcRat_Gh0stRAT, deployment Perimeter, signature_severity High, created_at 2026_11_21; sid:9552008; rev:1;)
```

odin_gh0strat_plugx_njrat_and_gamaredon_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 52 / 52 YARA Detection Suite
   Scope: Gh0stRAT zlib-framed Windows implants, PlugX side-loaded payload loaders,
          njRAT .NET TCP 1177 clients, and Gamaredon VBS/HTA fast-flux script droppers.
   Classification: TLP:CLEAR
*/

rule ODIN_Gh0stRAT_Magic_Zlib_Implant
{
    meta:
        author = "Odin by Brandefense"
        description = "Detects Gh0stRAT Windows PE implants combining the 5-byte Gh0st packet magic, zlib
compression routines, and remote desktop or keylogger manager strings"
        reference = "https://attack.mitre.org/software/S0032/"
```

```
        date = "2026-11-21"
        tlp = "CLEAR"
    strings:
        $magic = "Gh0st" ascii
        $zlib_ver = "1.1.4" ascii
        $zlib_hdr = { 78 9C }
        $m1 = "ScreenSpy" ascii wide
        $m2 = "KeyboardManager" ascii wide
        $m3 = "ShellManager" ascii wide
    condition:
        uint16(0) == 0x5A4D and filesize < 5120KB and $magic and ($zlib_ver or $zlib_hdr) and 2 of ($m*)
}

rule ODIN_PlugX_Sideloaded_Payload_Loader
{
    meta:
        author = "Odin by Brandefense"
        description = "Detects PlugX DLL side-loading modules combining characteristic header/config markers with
LZNT1 decompression and WinInet or DNS resolution APIs"
        reference = "https://attack.mitre.org/software/S0013/"
        date = "2026-11-21"
        tlp = "CLEAR"
    strings:
        $tag1 = "GULP" ascii
        $tag2 = "PLUG" ascii
        $tag3 = "boot.ldr" ascii wide nocase
        $api1 = "RtlDecompressBuffer" ascii
        $api2 = "VirtualAlloc" ascii
        $net1 = "HttpSendRequestA" ascii
        $net2 = "HttpSendRequestW" ascii
        $net3 = "DnsQuery_A" ascii
    condition:
        uint16(0) == 0x5A4D and filesize < 4096KB and 1 of ($tag*) and $api1 and $api2 and 1 of ($net*)
}

rule ODIN_njRAT_DotNet_Port1177_Client
{
    meta:
        author = "Odin by Brandefense"
        description = "Detects njRAT .NET implants featuring the default pipe-quote field delimiter, firewall
bypass command strings, and 0.7d/1177 client artifacts"
        reference = "https://attack.mitre.org/software/S0385/"
        date = "2026-11-21"
        tlp = "CLEAR"
    strings:
        $dotnet = "mscoree.dll" ascii
        $delim = "|'|'|" ascii wide
        $ver1 = "0.7d" ascii wide
        $ver2 = "1177" ascii wide
        $fw1 = "netsh firewall add allowedprogram" ascii wide nocase
        $fw2 = "SEE_MASK_NOZONECHECKS" ascii wide
    condition:
        uint16(0) == 0x5A4D and filesize < 2048KB and $dotnet and $delim and 1 of ($ver*) and 1 of ($fw*)
}

rule ODIN_Gamaredon_VBS_FastFlux_Relay_Dropper
{
    meta:
        author = "Odin by Brandefense"
        description = "Detects Gamaredon-style VBScript and HTA stage-1 droppers polling HTTPS fast-flux relays
via XMLHTTP/WinHttp and staging payloads with ADODB.Stream"
        reference = "https://attack.mitre.org/groups/G0047/"
        date = "2026-11-21"
        tlp = "CLEAR"
    strings:
        $sh1 = "WScript.Shell" ascii wide nocase
        $sh2 = "Scripting.FileSystemObject" ascii wide nocase
        $http1 = "MSXML2.XMLHTTP" ascii wide nocase
        $http2 = "WinHttp.WinHttpRequest.5.1" ascii wide nocase
        $stream = "ADODB.Stream" ascii wide nocase
```

```
        $exec1 = "wscript.exe" ascii wide nocase
        $exec2 = "mshta.exe" ascii wide nocase
    condition:
        filesize < 1024KB and 1 of ($sh*) and 1 of ($http*) and $stream and 1 of ($exec*)
}
```

sentinel_fastflux_plugx_dns_and_rat_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 52 / 52 Microsoft Sentinel & Defender XDR Hunt
// Correlates non-resolver TCP port 53 connections, Gh0stRAT port 14994 and njRAT port 1177 sessions,
// script-interpreter HTTPS fast-flux relay fan-out across /24 subnets, and PlugX DLL side-loading paths.
// Uses exact hostname and exact system-binary allowlists only.

let Lookback = 7d;
let RatOperatorPorts = dynamic([1177, 14994]);
let ApprovedDnsForwarders = dynamic(["CORP-DNS-FWD-01", "CORP-DNS-FWD-02"]);
let ApprovedLabHosts = dynamic(["SEC-SANDBOX-WIN-01", "SEC-NETLAB-LNX-01"]);
let SystemDnsBinaries = dynamic([
    @"C:\Windows\System32\dns.exe",
    @"C:\Windows\System32\svchost.exe",
    "/usr/sbin/named",
    "/usr/sbin/unbound",
    "/usr/lib/systemd/systemd-resolved"
]);
let ScriptRelayInterpreters = dynamic([
    @"C:\Windows\System32\wscript.exe",
    @"C:\Windows\System32\cscript.exe",
    @"C:\Windows\System32\mshta.exe",
    @"C:\Windows\SysWOW64\wscript.exe",
    @"C:\Windows\SysWOW64\cscript.exe",
    @"C:\Windows\SysWOW64\mshta.exe"
]);
let NetSignals =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where ActionType in ("ConnectionSuccess", "ConnectionAttempt")
    | where isnotempty(RemoteIP) and RemoteIPType == "Public"
    | where not(DeviceName in~ (ApprovedLabHosts))
    | extend RemoteSubnet24 = strcat(extract(@"^(\d+\.\d+\.\d+)\.\d+$", 1, RemoteIP), ".0/24")
    | extend IsNonResolverTcp53 = RemotePort == 53 and Protocol =~ "Tcp"
        and not(DeviceName in~ (ApprovedDnsForwarders))
        and not(InitiatingProcessFolderPath in~ (SystemDnsBinaries))
    | extend IsCharacteristicRatPort = RemotePort in (RatOperatorPorts)
    | extend IsScriptHttpsRelay = RemotePort == 443 and InitiatingProcessFolderPath in~ (ScriptRelayInterpreters)
    | where IsNonResolverTcp53 or IsCharacteristicRatPort or IsScriptHttpsRelay
    | summarize
        FirstNetSeen = min(Timestamp),
        LastNetSeen = max(Timestamp),
        NonResolverTcp53Hits = countif(IsNonResolverTcp53),
        RatPortHits = countif(IsCharacteristicRatPort),
        ScriptHttpsSubnets = dcountif(RemoteSubnet24, IsScriptHttpsRelay),
        SampleEndpoints = make_set(strcat(RemoteIP, ":", tostring(RemotePort)), 10)
      by DeviceId, DeviceName;
let ProcSignals =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedLabHosts))
    | extend IsScriptDropper = FolderPath in~ (ScriptRelayInterpreters)
        and ProcessCommandLine has_any (".vbs", ".hta", ".lnk")
    | extend IsWritableDllStaging = ProcessCommandLine has_any (@"C:\ProgramData\", @"C:\Windows\Temp\")
        and ProcessCommandLine has_any ("rundll32.exe", "regsvr32.exe")
    | where IsScriptDropper or IsWritableDllStaging
    | summarize
        FirstProcSeen = min(Timestamp),
        ScriptDropperHits = countif(IsScriptDropper),
        WritableStagingHits = countif(IsWritableDllStaging),
        SampleCommands = make_set(ProcessCommandLine, 5)
      by DeviceId, DeviceName;
```

```
NetSignals
| join kind=fullouter ProcSignals on DeviceId
| extend HostName = coalesce(DeviceName, DeviceName1)
| extend NonResolverTcp53Hits = coalesce(NonResolverTcp53Hits, 0),
         RatPortHits = coalesce(RatPortHits, 0),
         ScriptHttpsSubnets = coalesce(ScriptHttpsSubnets, 0),
         ScriptDropperHits = coalesce(ScriptDropperHits, 0),
         WritableStagingHits = coalesce(WritableStagingHits, 0)
| where NonResolverTcp53Hits > 0 or RatPortHits > 0 or ScriptHttpsSubnets >= 3 or (ScriptDropperHits > 0 and
WritableStagingHits > 0)
| extend RecommendedAction = case(
    NonResolverTcp53Hits > 0 and WritableStagingHits > 0, "INVESTIGATE_TCP53_AND_WRITABLE_PATH_ACTIVITY",
    RatPortHits > 0, "INVESTIGATE_14994_OR_1177_SESSION",
    ScriptHttpsSubnets >= 3, "INVESTIGATE_SCRIPT_HTTPS_FANOUT",
    NonResolverTcp53Hits > 0, "INVESTIGATE_NON_RESOLVER_TCP53_EGRESS",
    "HUNT_SCRIPT_OR_WRITABLE_DLL_SIDELOAD"
  )
| project
    HostName,
    RecommendedAction,
    NonResolverTcp53Hits,
    RatPortHits,
    ScriptHttpsSubnets,
    ScriptDropperHits,
    WritableStagingHits,
    FirstNetSeen,
    LastNetSeen,
    SampleEndpoints,
    SampleCommands
| order by NonResolverTcp53Hits desc, RatPortHits desc, ScriptHttpsSubnets desc
```

sigma_plugx_port53_gamaredon_script_and_rat_ports.yml

SIGMA

```
title: Non-Resolver Process Initiating Outbound TCP Port 53 Connection
id: 7b49e210-8a52-4f91-9d01-520000000001
status: experimental
description: Detects non-DNS Windows processes establishing outbound TCP connections on port 53 for non-DNS
protocol investigation.
author: Odin by Brandefense
date: 2026-11-21
references:
  - https://attack.mitre.org/software/S0013/
  - https://attack.mitre.org/techniques/T1571/
logsource:
  category: network_connection
  product: windows
detection:
  selection:
    Initiated: 'true'
    Protocol: 'tcp'
    DestinationPort: 53
  filter_system_dns:
    Image:
      - 'C:\Windows\System32\dns.exe'
      - 'C:\Windows\System32\svchost.exe'
  filter_dns_forwarders:
    ComputerName:
      - 'CORP-DNS-FWD-01'
      - 'CORP-DNS-FWD-02'
  condition: selection and not 1 of filter_*
falsepositives:
  - Dedicated DNS administration workstations running dig or nslookup zone checks over TCP
level: high
tags:
  - attack.command_and_control
  - attack.t1571
---
title: Outbound Connection to Characteristic Gh0stRAT Port 14994 or njRAT Port 1177
```

```
id: 7b49e210-8a52-4f91-9d01-520000000002
status: experimental
description: Detects outbound TCP connections to characteristic Gh0stRAT listener port 14994 or default njRAT
listener port 1177.
author: Odin by Brandefense
date: 2026-11-21
references:
  - https://attack.mitre.org/software/S0032/
  - https://attack.mitre.org/software/S0385/
logsource:
  category: network_connection
  product: windows
detection:
  selection:
    Initiated: 'true'
    Protocol: 'tcp'
    DestinationPort:
      - 14994
      - 1177
  filter_sandbox:
    ComputerName:
      - 'SEC-SANDBOX-WIN-01'
  condition: selection and not filter_sandbox
falsepositives:
  - Custom internal applications bound to port 14994 or 1177 on documented servers
level: high
tags:
  - attack.command_and_control
  - attack.t1571
---
title: Windows Script Host or MSHTA Initiating Outbound HTTPS Connection
id: 7b49e210-8a52-4f91-9d01-520000000003
status: experimental
description: Detects wscript.exe, cscript.exe, or mshta.exe initiating direct outbound TCP 443 sessions
consistent with Gamaredon VBS and HTA fast-flux HTTPS relay polling.
author: Odin by Brandefense
date: 2026-11-21
references:
  - https://attack.mitre.org/groups/G0047/
  - https://attack.mitre.org/techniques/T1568/001/
logsource:
  category: network_connection
  product: windows
detection:
  selection:
    Initiated: 'true'
    Protocol: 'tcp'
    DestinationPort: 443
    Image:
      - 'C:\Windows\System32\wscript.exe'
      - 'C:\Windows\System32\cscript.exe'
      - 'C:\Windows\System32\mshta.exe'
      - 'C:\Windows\SysWOW64\wscript.exe'
      - 'C:\Windows\SysWOW64\cscript.exe'
      - 'C:\Windows\SysWOW64\mshta.exe'
  filter_sandbox:
    ComputerName:
      - 'SEC-SANDBOX-WIN-01'
  condition: selection and not filter_sandbox
falsepositives:
  - Legacy enterprise logon scripts fetching HTTPS resources via Windows Script Host
level: high
tags:
  - attack.command_and_control
  - attack.t1568.001
  - attack.t1218.005
```

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/gamaredon-and-plugx-candidates/
Short Read · brandefense.io/odin-research/blog/gamaredon-and-plugx-candidates/
Defense Kit · brandefense.io/odin-research/defense-kit/