ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 26 / 30 · COMMODITY MALWARE

Tax Lures to Hidden Desktops
PureRAT, ShadowHVNC and XenoRAT Infrastructure

How a Form 1120 tax-lure workbench, Chrome DevTools cookie theft and hidden-desktop DLLs sit beside multi-port RAT and loader fleets

Two-week observation window ending 19 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

172
C2 endpoints across twelve families, on 131 hosts

35
Confirmed C2 endpoints on 26 hosts; the other 137 stay on watchlists

61
PureRAT endpoints on 38 hosts; 44 of them on ports 56001 to 56003

8
ShadowHVNC endpoints, all on port 443; 5 on DEDIK SERVICES LIMITED

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

How a Form 1120 tax-lure workbench, Chrome DevTools cookie theft and hidden-desktop DLLs sit beside multi-port RAT and loader fleets

01	Executive Summary	04
02	The Ecosystem at a Glance	07
03	PureRAT, ShadowHVNC and XenoRAT Fleets	10
04	The Form1120 Workbench: Tax Lures, Cookie Theft and Hidden Desktops	14
05	Loaders, Confirmed Controllers and Co-Staged RAT Kits	18
06	What Not to Block	22
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 (19)	36
B	Detection rules (4 files)	37

IN SHORT

Odin by Brandefense mapped 172 command-and-control (C2) endpoints on 131 hosts across twelve remote access, loader and stealer families. Of these, 35 endpoints on 26 hosts are confirmed. Beside them sits an exposed Russian staging server with 212 files: corporate tax lures, hidden-desktop DLLs and scripts that relaunch Chrome to read session cookies. Block the confirmed controllers, keep PureRAT and ShadowHVNC candidates on watchlists, and alert when scripts relaunch browsers with a remote debugging port.

01

CHAPTER 01

Executive Summary

IN SHORT

Odin by Brandefense mapped 172 command-and-control (C2) endpoints on 131 hosts across twelve remote access, loader and stealer families. Of these, 35 endpoints on 26 hosts are confirmed. Beside them sits an exposed Russian staging server with 212 files: corporate tax lures, hidden-desktop DLLs and scripts that relaunch Chrome to read session cookies. Block the confirmed controllers, keep PureRAT and ShadowHVNC candidates on watchlists, and alert when scripts relaunch browsers with a remote debugging port.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Remote access trojans (RATs) give an operator control of a Windows workstation. Hidden-desktop tools, known as HVNC (hidden virtual network computing), let the operator use the victim's browser on an invisible second desktop. This report maps where these controllers listen and what one exposed staging server shows about attack preparation.

1. **PureRAT and ShadowHVNC use two different hosting patterns.**
   PureRAT has 61 endpoints on 38 hosts, and 44 of them sit on sequential ports 56001 to 56003. ShadowHVNC has 8 endpoints, all on port 443, and 5 of them sit on one offshore VPS provider, DEDIK SERVICES LIMITED.

2. **One staging server links IRS tax lures to cookie theft and hidden desktops.**
   The server holds a 1,392,428-byte `Form1120.pdf` that is byte-identical to a raw payload file, `.pdf.lnk` shortcut lures, five hidden-desktop DLL builds and scripts that relaunch Chrome with remote debugging. These are staged files. Nothing shows they were used against a target.

3. **Confirmed loader and RAT controllers sit next to false-positive traps.**
   The 35 confirmed endpoints belong to Emotet (28), XenoRAT (2), OrcusRAT (2), SerpentStealer (2) and ChaosRAT (1). Three suspected Emotet listeners share a Dutch registrar's FTP hosting, and two Emotet nodes outside the confirmed 35 sit on a dynamic China Unicom network. These five belong on watchlists, not block lists.

Three Decisions for Leaders

1. **Block confirmed controllers and keep candidates on watchlists.** Block the confirmed C2 addresses in this report. Keep uncorroborated PureRAT and ShadowHVNC listeners, FTP collisions and dynamic telecom addresses on time-bound watchlists.
2. **Lock down browser remote debugging.** Alert when PowerShell, Windows Script Host or an unsigned program relaunches Chrome, Edge or Brave with `--remote-debugging-port`. Set the browser policy that turns remote debugging off on managed workstations.
3. **Inspect tax-season attachments and high-port TLS egress.** Block `.pdf.lnk` double-extension shortcuts at the mail gateway. Watch outbound connections to ports 56001 to 56003 and 57003.

The Study in Numbers

Number	What it is
172	C2 endpoints across twelve families, on 131 hosts
35	Confirmed C2 endpoints on 26 hosts; the other 137 stay on watchlists
61	PureRAT endpoints on 38 hosts; 44 of them on ports 56001 to 56003
8	ShadowHVNC endpoints, all on port 443; 5 on DEDIK SERVICES LIMITED
212	Files on one exposed staging server, spanning tax lures, HVNC DLLs and Chrome cookie scripts
1,392,428	Bytes in the `Form1120.pdf` file that is byte-identical to `Form1120.bin`
5	Listeners held on watchlists despite a match: 3 FTP collisions and 2 dynamic telecom addresses

How to use this report.

Leaders can read Chapters 1, 6 and 7. SOC and detection engineers should start with Chapters 7 to 9. CTI analysts will find fleet and workbench detail in Chapters 2 to 5.

02

CHAPTER 02

The Ecosystem at a Glance

IN SHORT

Twelve families split into four roles: loaders and stealers, multi-port RATs, hidden-desktop tools, and a staging workbench. No host carries more than one family, so the four roles are an analytical model, not a single actor.

INSIDE THIS CHAPTER

Four roles, not one group 07

Counts by family 07

Where the endpoints sit 08

02 The Ecosystem at a Glance

Four roles, not one group

Modern workstation intrusions rarely rely on one tool. Operators combine upstream loaders and stealers, multi-port RATs, and session-bypass tools such as HVNC and Chrome DevTools Protocol (CDP) cookie scripts.

Figure 1 groups the 172 endpoints and the staging server into four cells. The cells are an analytical model of functional roles. None of the 131 hosts carries two families, so we make no claim that one group runs all twelve.

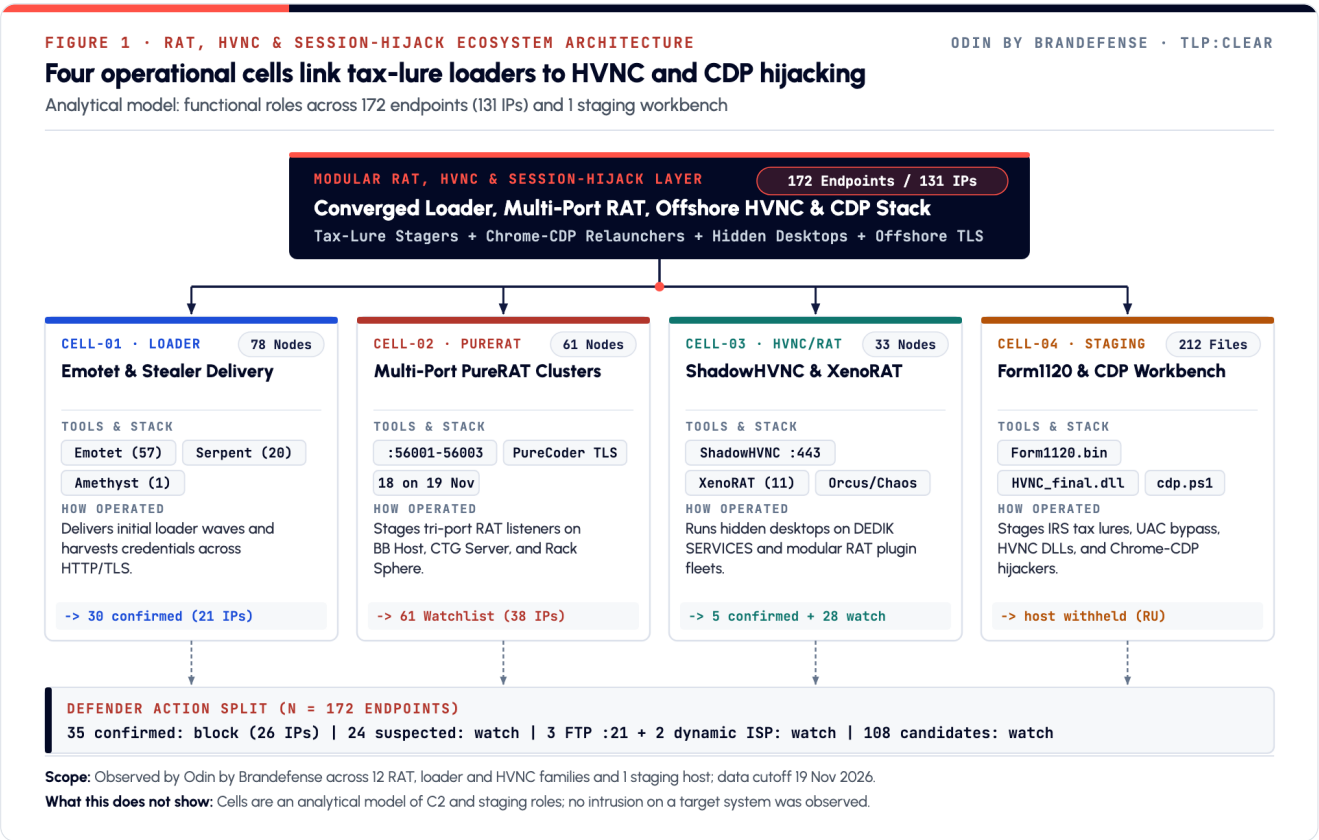


Figure 1: Four operational cells link tax-lure loaders to HVNC and CDP hijacking (analytical model)

Counts by family

An endpoint is one IP address and port.

Family	Role	Endpoints	Hosts	Endpoints per host	Confirmed	Watchlist
PureRAT	Multi-port .NET RAT and HVNC client	61	38	1.61	0	61 candidates
Emotet	Modular loader	57	45	1.27	28	24 suspected, 3 FTP collisions, 2 dynamic ISP
SerpentStealer	Credential and token stealer	20	14	1.43	2	18 candidates
XenoRAT	Plugin-based C# RAT	11	11	1.00	2	9 candidates

Family	Role	Endpoints	Hosts	Endpoints per host	Confirmed	Watchlist
ShadowHVNC	Hidden-desktop C2	8	8	1.00	0	8 candidates
ChaosRAT	Cross-platform admin trojan	3	3	1.00	1	1 with open directory, 1 candidate
OrcusRAT	Modular remote admin trojan	3	3	1.00	2	1 candidate
SectopRAT	Hidden-desktop and browser RAT	3	3	1.00	0	3 candidates on 15647
PhantomRAT	TLS remote access trojan	2	2	1.00	0	2 candidates on 443
SparkRAT	Cross-platform Go RAT	2	2	1.00	0	2 candidates on 8000
AmethystStealer	.NET browser stealer	1	1	1.00	0	1 candidate on 443
NDragonRAT	High-port HTTP and TLS RAT	1	1	1.00	0	1 candidate on 8080
Total		**172**	**131**		**35**	**137**

Of the 131 hosts, 36 bind more than one port: 16 for PureRAT, 12 for Emotet, 6 for SerpentStealer and 2 for other families.

Where the endpoints sit

Seven countries lead.

Country	Endpoints	Share
United States	48	27.9%
China	20	11.6%
Germany	16	9.3%
Netherlands	16	9.3%
Hong Kong	11	6.4%
Brazil	11	6.4%
Singapore	11	6.4%

Hosting differs by role. ShadowHVNC clusters on one offshore provider, PureRAT on regional VPS hosts, and confirmed Emotet controllers on large clouds.

03

CHAPTER 03

PureRAT, ShadowHVNC and XenoRAT Fleets

IN SHORT

PureRAT spreads listeners across sequential high ports on regional VPS hosts. ShadowHVNC hides on port 443 with one offshore provider. XenoRAT has two confirmed TLS controllers and a candidate whose certificate imitates a browser name.

INSIDE THIS CHAPTER

PureRAT: three ports per host 10

ShadowHVNC: all on port 443 11

XenoRAT: two confirmed controllers 11

03 PureRAT, ShadowHVNC and XenoRAT Fleets

Even when the payload is packed or side-loaded, each family leaves its own transport and TLS signals. Figure 2 maps six capability groups to their wire signals and to the matching rules in Chapter 8.

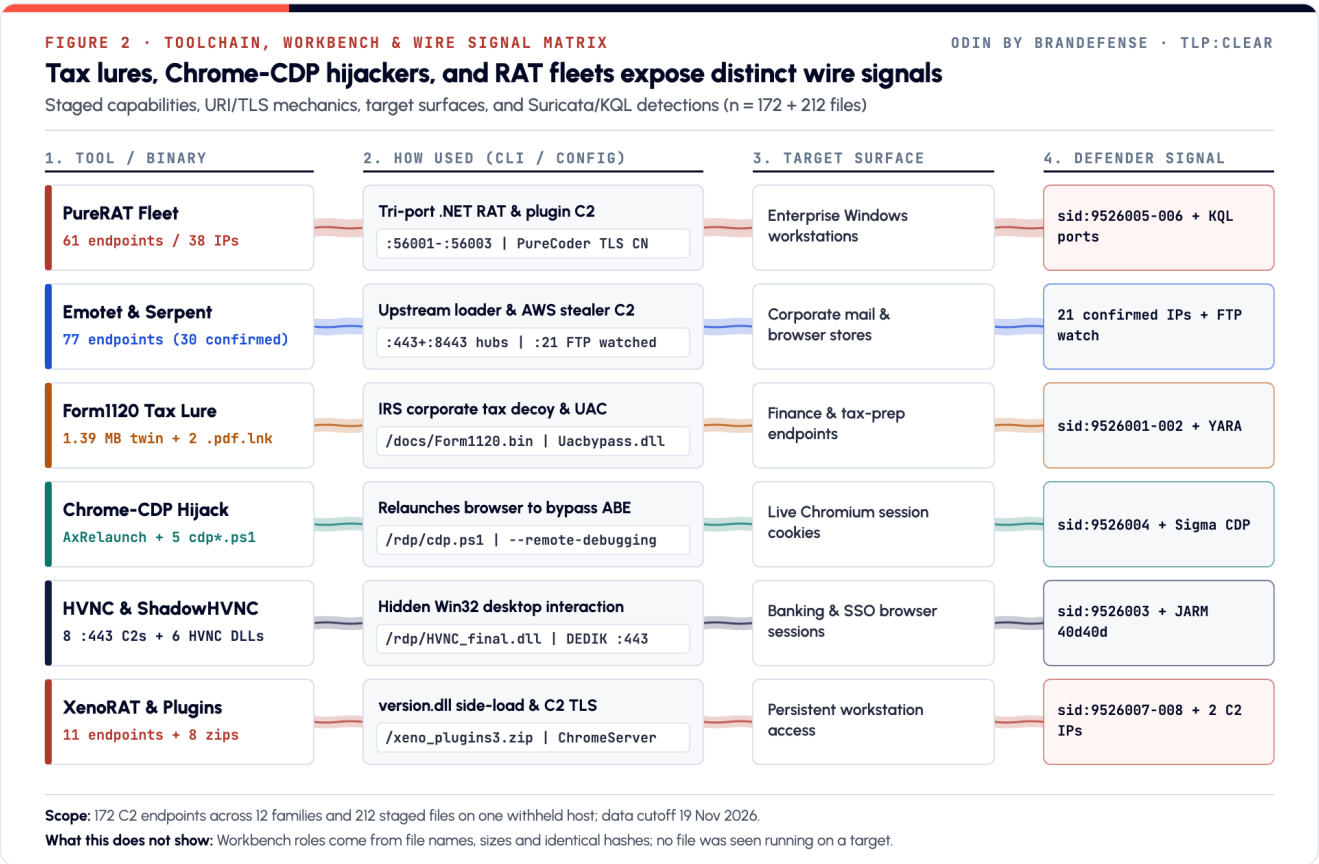


Figure 2: Tax lures, Chrome-CDP hijackers, and RAT fleets expose distinct wire signals

PureRAT: three ports per host

PureRAT is sold in the PureCoder commercial malware line, next to PureHVNC and PureLogs. It has the highest port-to-host density in this study: 61 endpoints on 38 hosts.

Operators often open sequential high ports instead of one web port. The likely purpose is to separate client check-ins, live desktop streams and plugin traffic.

Port	PureRAT endpoints
56002	17
56003	14
56001	13
443	5
442, 6767	2 each
1337, 4443, 7500, 7777, 55004, 55005, 55009, 57003	1 each

Ports 56001 to 56003 carry 44 of the 61 endpoints (72.1%). Five hosts bind all three ports at once, on BB Host LTDA (Brazil), RACK SPHERE HOSTING S.A. (Netherlands) and Tier.Net Technologies (United States). Another 11 hosts bind two of them. Of the 61 endpoints, 18 on 11 hosts were first seen on 19 November 2026.

Two TLS certificates point to the vendor: a PureCoder-branded API hostname on Contabo and the subject `PureRAT Agent` on CTG Server.

Hosting (country)	Ports	TLS subject and JARM prefix	First seen
Contabo Inc. (US)	57003	PureCoder API hostname (withheld) · `2ad2ad15d2ad2ad0`	19 Nov 2026
CTG Server Limited (HK)	443	`PureRAT Agent` · `22b22b07b22b22b2`	18 Nov 2026
BB Host LTDA (BR)	56001 to 56003	Raw TCP, three sockets	19 Nov 2026
BB Host LTDA (BR)	56001 to 56003	Raw TCP, three sockets	19 Nov 2026
RACK SPHERE HOSTING S.A. (NL)	56001 to 56003	Raw TCP, three sockets	19 Nov 2026
CTG Server Limited (HK)	56001, 56002	Dual-port host, paired with a second CTG address	19 Nov 2026
CTG Server Limited (JP)	56001, 56002	Domain withheld · `1dd40d40d00040d0`	18 Nov 2026
OVH SAS (SG)	56002, 56003	Domain withheld · `15d3fd16d29d29d0`	17 Nov 2026

All 61 PureRAT endpoints are candidates. Each rests on a port and TLS pattern without a confirmed C2 protocol match, so their addresses are withheld.

ShadowHVNC: all on port 443

ShadowHVNC binds only TCP port 443. This blends interactive hidden-desktop traffic into normal HTTPS egress.

Hosting provider	Countries	Endpoints
DEDIK SERVICES LIMITED	Germany (3), United States (1), Netherlands (1)	5
The Constant Company, LLC	United States	2
Heymman Servers Corporation	United States	1

Five of the eight (62.5%) sit on DEDIK SERVICES LIMITED. Two of the nodes present self-signed certificates with the IP address as the common name. Both share JARM `40d40d40d00000000043d43d00043d6aff5ab0f4fc31897186312c9e639319`.

JARM is a fingerprint of how a server answers TLS handshakes. A shared JARM groups servers built the same way, but it is not enough to block on. All eight ShadowHVNC endpoints are candidates, and their addresses are withheld.

XenoRAT: two confirmed controllers

XenoRAT has 11 endpoints on 11 hosts. Two dedicated Asian VPS nodes are confirmed TLS controllers: 156.239.225[.]62:443 on CORENET CLOUD (HK) and 111.90.147[.]147:443 on Shinjiru Technology (MY).

The other nine are candidates on ports 443, 4444, 5333, 8080, 8123 and 50607. Two of them, on port 4444 in France and the United States, were first seen on 19 November 2026.

One candidate on a Belgian broadband network listens on port 5333. Its certificate subject is `CN=ChromeServer`, a name that imitates the browser. It shares JARM `22b22b00022b22b22b22b22b22b22bd3b67dd3674d9af9dd91c1955a35d0e9` with an OrcusRAT candidate on port 8080 that presents `CN=Orcus Server`. The shared fingerprint is a lead, not proof of a shared operator.

04

CHAPTER 04

The Form1120 Workbench: Tax Lures, Cookie Theft and Hidden Desktops

IN SHORT

An open directory on a Russian server, port 8080, held 212 staged files between 16 and 18 November 2026. They combine IRS Form 1120 tax lures, privilege escalation, DLL side-loading, five hidden-desktop builds and Chrome cookie-theft scripts.

INSIDE THIS CHAPTER

What the server held 14

Stage 1: tax-season delivery 15

Stage 2: elevation, firewall and side-loading 15

Stage 3: hidden desktops 16

Stages 4 and 5: defeating Chrome App-Bound Encryption 16

04 The Form1120 Workbench: Tax Lures, Cookie Theft and Hidden Desktops

Listeners show where controllers sit. An open staging server shows how operators build lures and work around endpoint and browser defenses. The server's address is withheld.

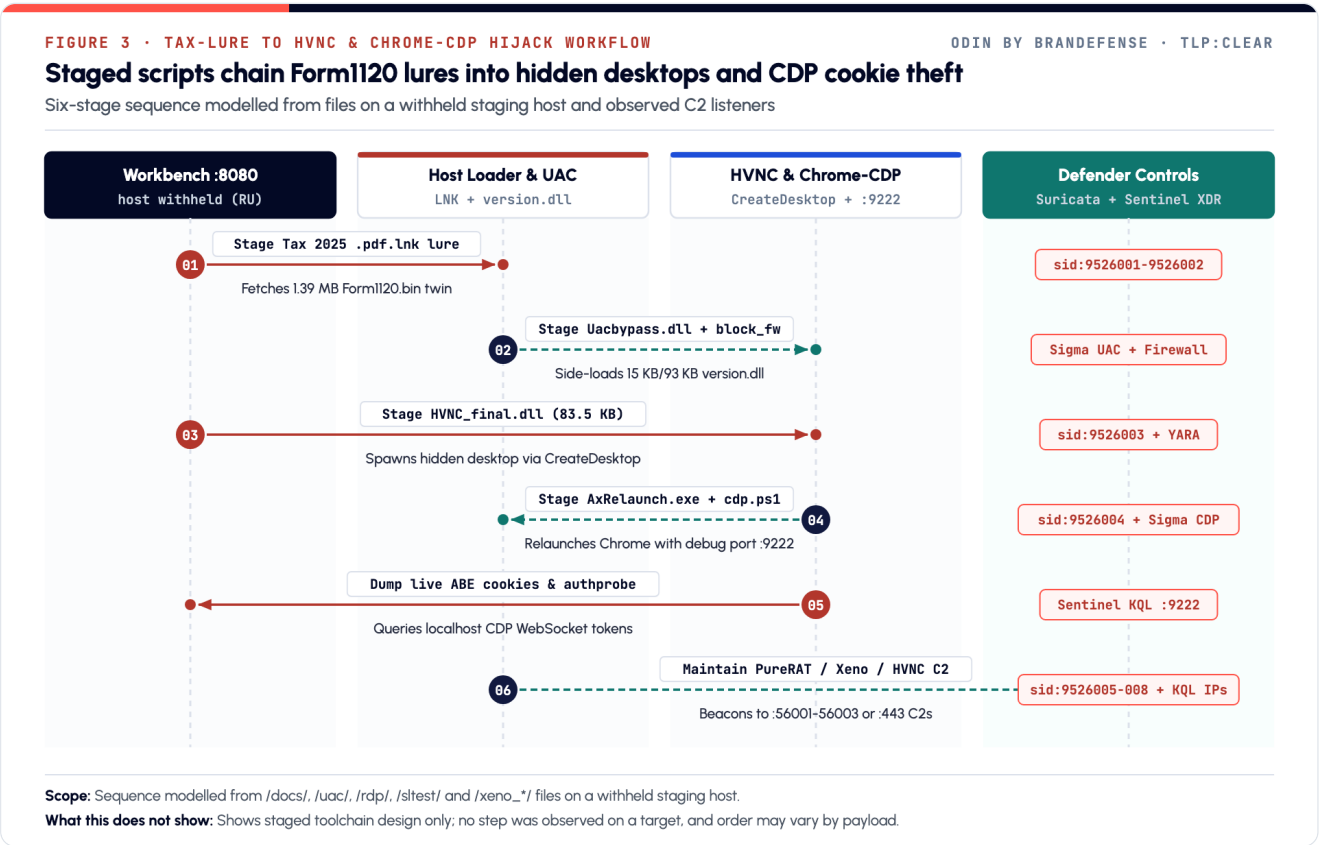


Figure 3: Staged scripts chain Form1120 lures into hidden desktops and CDP cookie theft (modelled sequence)

What the server held

Of the 212 files, 90 have SHA-256 values on record. Those 90 include 23 DLLs, 23 PowerShell scripts, 16 raw shellcode `.bin` files, 13 ZIP archives, 8 Windows executables and 4 VB.NET client sources.

Figure 3 lays out a six-stage sequence modelled from these files. No step was observed on a target system, and the real order may vary by payload.

Stage 1: tax-season delivery

The file names target corporate finance and accounting staff ahead of year-end tax work. IRS Form 1120 is the U.S. Corporation Income Tax Return.

File	Size (bytes)	What it is
`/docs/Form1120.pdf` and `/docs/Form1120.bin`	1,392,428	Byte-identical pair; the `.pdf` is a raw payload, not a tax form
`/rdp/Tax Documents 2025.pdf.lnk`	1,245	Shortcut with a double extension, posing as a PDF
`/rdp/relaunch2.pdf.lnk`	3,258	Second `.pdf.lnk` shortcut
`/rdp/deliver.vbs`	1,543	Visual Basic script stager
`/rdp/sacloader.b64`	5,464	Base64-encoded loader

The two `Form1120` files share one SHA-256 value. So the `.pdf` file is the same raw payload under a document extension. The likely aim is to slip past URL and proxy filters that trust `.pdf` names.

Stage 2: elevation, firewall and side-loading

File	Size (bytes)	What it is
`/uac/Uacbypass.dll`	19,968	User Account Control (UAC) bypass module
`/block_fw.ps1`	3,331	Host firewall tampering script
`/hidden_launch.exe`	15,872	Launcher for hidden processes
`/sltest/mstsc.exe`	1,114,112	Copy of the Microsoft Remote Desktop client
`/sltest/version.dll`	93,375	Proxy DLL, byte-identical to `/rdp/version_new_fresh.dll`
`/sltest/version_orig.dll`	55,192	Original `version.dll` kept for forwarding
`/sltest/shell.bin`	53,868	Shellcode loaded by the proxy

DLL side-loading (MITRE ATT&CK T1574.002) works by placing a fake `version.dll` next to a trusted program. When the program starts, Windows loads the fake DLL first. Here the trusted program is a copy of `mstsc.exe` outside `System32`.

The same pattern repeats in five sibling directories, four of them named `/xeno_*/`. Each pairs an 85,100-byte `shell.bin` with a 15,360-byte `version.dll`. Four of these `version.dll` files share one SHA-256 value.

Stage 3: hidden desktops

HVNC takes a different route. It does not move cookies off the host. Instead it calls the Windows `CreateDesktop` and `SetThreadDesktop` functions to open an invisible second desktop. There it starts a cloned browser profile and uses the victim's own IP address, device fingerprint and active sign-in sessions.

File	Size (bytes)	Build
`/hvnc_test.dll`	59,904	First test build
`/rdp/hvnc_new.dll`	60,416	Second build
`/rdp/HVNC_patched.dll`	75,264	Patched build
`/rdp/HVNC_mark3.dll`	76,288	`mark3` build
`/rdp/HVNC_final.dll`	83,456	Final build

Related files sit next to the five builds: `/rdp/hijack_standalone.dll` (1,078,272 bytes), `/rdp/hvx.dll` (10,752), `/rdp/uia_test.exe` (6,656), `/rdp/payload_uia.bin` (55,296) and `/rdp/desks.ps1` (2,395). The `uia` names point to Windows UI Automation, which lets code drive a window without a visible user.

The growing file sizes suggest an operator iterating on one module. We infer each file's purpose from its name, size and any identical hashes.

Stages 4 and 5: defeating Chrome App-Bound Encryption

In mid-2024 Google added App-Bound Encryption (ABE) to Chrome on Windows. ABE ties the cookie encryption key to a system service that checks which program is asking. Stealers that read the `Cookies` database from disk no longer get usable cookies.

The `/rdp/` folder shows an operator testing a way around this. The idea is to ask the real, signed browser for its cookies. The scripts relaunch Chrome with a remote debugging port and request cookies over a local WebSocket through the Chrome DevTools Protocol (CDP) call `Network.getAllCookies`.

Files	Sizes (bytes)	Purpose by name and size
`abtest.ps1`, `abtest2.ps1`, `get_abkey.ps1`	3,071 / 2,433 / 365	Test ABE key boundaries
`AxRelaunch.cs`, `AxRelaunch.exe`	1,207 / 4,096	C# browser relauncher; the `.exe` is byte-identical to `ax.dll`
`cdp.ps1`, `cdp_real.ps1`, `cdp_real2.ps1`, `cdp_real3.ps1`	1,641 / 1,980 / 1,813 / 2,333	CDP cookie requests
`check_cdp.ps1`, `dump_cookies.ps1`	272 / 441	Check the debug port and save cookies
`authprobe.ps1` to `authprobe4.ps1`	1,615 to 1,919	Test whether stolen sessions still work
`expiry_dump.exe`	1,065,984	Cookie expiry dumper

For defenders, a script or small unsigned program that starts Chrome with `--remote-debugging-port` is a strong signal. So is PowerShell connecting to local port 9222.

05

CHAPTER 05

Loaders, Confirmed Controllers and Co-Staged RAT Kits

IN SHORT

Emotet supplies 28 of the 35 confirmed endpoints, on 19 cloud hosts. The staging server also holds full XWorm, XenoRAT and Remcos kits, so the operator keeps several implant families ready.

INSIDE THIS CHAPTER

Confirmed Emotet controllers 18

Other confirmed controllers 19

Three RAT kits on one server 20

05 Loaders, Confirmed Controllers and Co-Staged RAT Kits

Operators of hidden-desktop and cookie-theft tools often buy access from loader botnets, then add commodity RAT panels for backup. Figure 4 shows the staging server's folders next to the multi-port C2 clusters.



Figure 4: Workbench directory trees and tri-port hubs reveal iterative operator builds

Confirmed Emotet controllers

Emotet has 57 endpoints on 45 hosts. Of these, 28 HTTP and HTTPS endpoints on 19 dedicated cloud addresses are confirmed. Nine hosts carry two confirmed ports each. The three Huawei Cloud hosts share one certificate (domain withheld) and the JARM prefix `2ad2ad16d2ad2ad0`. The three Alibaba hosts were confirmed on 18 November 2026.

Address	Ports	Hosting (country)
1.95.216[.]95	443, 8443	Huawei Cloud (CN)
1.95.144[.]27	443, 8443	Huawei Cloud (CN)
1.94.25[.]210	443, 8443	Huawei Cloud (CN)
8.130.115[.]156	443	Hangzhou Alibaba (CN)
8.130.122[.]123	443	Hangzhou Alibaba (CN)
8.130.159[.]214	443	Hangzhou Alibaba (CN)
64.227.189[.]225	80, 443	DigitalOcean (IN)

Address	Ports	Hosting (country)
167.71.229[.]25	80, 443	DigitalOcean (IN)
128.199.131[.]70	80, 443	DigitalOcean (SG)
142.93.158[.]102	80, 443	DigitalOcean (CA)
167.172.183[.]165	80, 8010	DigitalOcean (DE)
185.232.107[.]206	80, 8010	Data Storage Center JSC (RU)
91.206.14[.]212	80	JSC Selectel (RU)
185.137.233[.]37	80	JSC Selectel (RU)
185.137.233[.]198	80	JSC Selectel (RU)
188.246.224[.]196	80	JSC Selectel (RU)
178.57.77[.]87	80	Data Storage Center JSC (RU)
159.203.173[.]129	80	DigitalOcean (US)
138.197.111[.]250	80	DigitalOcean (US)

Other confirmed controllers

Seven confirmed endpoints belong to other families.

Family	Endpoint	Hosting (country)	Note
XenoRAT	156.239.225[.]62:443	CORENET CLOUD (HK)	TLS controller
XenoRAT	111.90.147[.]147:443	Shinjiru Technology (MY)	TLS controller
OrcusRAT	165.22.243[.]96:443	DigitalOcean (SG)	TLS controller
OrcusRAT	Address withheld, port 8086	UK consumer broadband (Virgin Media)	Custom TCP port; see Chapter 6
ChaosRAT	93.127.160[.]122:80	23M GmbH (DE)	HTTP controller
SerpentStealer	13.216.143[.]112:80	Amazon AWS (US)	Confirmed 18 Nov 2026
SerpentStealer	23.22.63[.]150:80	Amazon AWS (US)	HTTP collector

Two more clusters stay on watchlists. A ChaosRAT candidate on DigitalOcean (US), port 8080, shares its host with an exposed open directory. Three SectopRAT candidates on port 15647 sit on NForce (NL), Flyservers (HU) and Data Campus (NL), and share the JARM prefix `14d14d16`.

Three RAT kits on one server

The staging server holds builders, panels and loaders for three RAT families at once. That points to redundancy: if one implant is caught, another is ready.

Family	Files	Sizes (bytes)
XWorm	`/XWorm6v.zip` (version 6), `/XWormV5.6_panel.zip`, `/XWormV3.1_clean.exe`	43,798,746 / 25,644,229 / 7,278,080
XWorm	Four VB client sources (`/xw56_desig.vb`, `/xworm56_client.vb`, `/xw56_desig2.vb`, `/client.vb`)	78 to 87 KB each
XWorm	`/find_xworm_reg.ps1` (registry persistence finder), `/xwprobe_host.exe`	1,018 / 113,152
XenoRAT	`/xeno_plugins3.zip`, `/implant_xeno.zip`, `/xeno_plugins2.zip`, `/xeno_plugins_renamed.zip`	1,133,184 / 638,010 / 237,927 / 102,164
XenoRAT	Five archives of about 86 KB: `/xeno_inj.zip`, `/xeno_nobypass.zip`, `/xeno_desig.zip`, `/xeno_hide.zip`, `/xeno_mini.zip`	About 86 KB each
Remcos	`/rdp/shell_remcos.bin`, `/rdp/version_remcos.dll`	660,480 / 27,136
Shellcode	`/rdp/shell_rp.bin`, `/rdp/shell_debug.bin`, `/rdp/shell_amsi.bin`	10.37 MB / 10.35 MB / 77,420

The five XenoRAT archives match the `/xeno_*/` side-loading folders described in Chapter 4.

06

CHAPTER 06

What Not to Block

IN SHORT

A match is not always a hostile host. Shared FTP hosting, rotating telecom addresses, old cloud addresses and uncorroborated candidates all need corroboration before anyone blocks them.

INSIDE THIS CHAPTER

Who runs the staging server 22

06 What Not to Block

Of the 172 endpoints, 35 (20.3%) are confirmed. The other 137 belong on watchlists for one of the reasons below.

Group	Endpoints	Why not block	Suggested action
Suspected Emotet listeners on a Dutch registrar's shared hosting	3	They sit beside ordinary FTP on port 21; blocking would hit the registrar's customers	Watchlist about 72 hours; never alert on port 21 alone
Emotet nodes on China Unicom Guangdong	2	Subscriber addresses move between unrelated customers	Watchlist about 24 hours; addresses withheld
ChaosRAT candidate with an open directory	1	Open directory; not yet corroborated	Watchlist about 7 days
Uncorroborated candidates, including all 61 PureRAT and 8 ShadowHVNC endpoints	107	Feed label only; not corroborated	Watchlist about 72 hours
Suspected Emotet listeners	24	Feed label only; not corroborated	Watch for a second signal

Eighteen of the SerpentStealer candidates are on Amazon AWS. Their records are older feed entries, and cloud addresses that old have likely moved to other AWS customers. Only the two SerpentStealer collectors confirmed in November 2026 are in the block set.

One confirmed OrcusRAT controller sits on a UK consumer broadband network. We withhold its address. Defenders who track it should block only its custom port 8086 and recheck ownership every 14 to 30 days.

Who runs the staging server

We weighed two explanations for the Russian staging server.

Hypothesis	For	Against	Verdict
H1: Criminal intrusion staging	Cracked XWorm 5.6 and 6 panels, Remcos shellcode and IRS tax lures sit together	No campaign or victim tie was observed	Most likely
H2: Authorized red-team server	Custom C# relauncher and HVNC test builds look like offensive research	Red teams rarely stage cracked commercial RAT panels beside tax lures	Less likely

The file mix fits financially motivated intrusion staging better than a scoped red-team exercise. Either way, an internal workstation that fetches `/docs/Form1120.*`, `/rdp/HVNC_*` or `/rdp/cdp*.ps1` should be isolated and examined. Because the owner is not established, the server's address and file hashes are withheld.

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

Within 24 hours

- [ ] Block the 25 confirmed C2 addresses published in this report. Chapter 9 explains which confirmed addresses are published and which are withheld. Review cloud and AWS addresses every 30 days, since providers reassign them.
- [ ] Keep the FTP collisions, dynamic telecom addresses and all PureRAT and ShadowHVNC candidates on watchlists, not block lists.

Within 72 hours

- [ ] Block `.pdf.lnk` double-extension shortcuts and tax-themed `.vbs` and `.b64` attachments at the mail gateway and with Windows Attack Surface Reduction rules.
- [ ] Set the Chrome and Edge policy `RemoteDebuggingAllowed` to false on managed workstations. This stops user-space scripts from opening a CDP debug socket.
- [ ] Alert on outbound connections to ports 56001 to 56003 and 57003 from workstation processes.

Within 7 to 30 days

- [ ] Deploy the three Sigma rules and four YARA rules for HVNC DLLs, `Uacbypass.dll` and `mstsc.exe` running outside `System32`.
- [ ] Load the eight Suricata signatures for tax-lure fetches, HVNC and CDP file downloads, and RAT certificate subjects.
- [ ] Schedule the Sentinel hunt with an exact list of approved Playwright, Puppeteer or Selenium hosts. Never use wildcard exclusions.

08

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 26

How the other rules work 26

08 Detection Rules

The full rules are in Appendix B.

Rule file	What it catches
`odin_purerat_shadowhvnc_xenorat_cdp.rules`	Suricata 7: eight signatures for tax-lure fetches, HVNC and CDP file downloads, XenoRAT plugin archives and RAT certificate subjects
`sentinel_form1120_hvnc_cdp_and_purerat_hunt.kql`	Microsoft Sentinel and Defender XDR: contact with confirmed C2 addresses, PureRAT high ports, local CDP sockets and workbench process markers
`sigma_hvnc_dll_uacbypass_and_chrome_cdp_hijack.yml`	Sigma (3 rules): browser relaunch with a debug port, HVNC and UAC bypass DLLs or side-loaded `mstsc.exe`, and tax-lure or firewall-script execution
`odin_hvnc_form1120_xenorat_purerat_artifacts.yar`	YARA (4 rules): HVNC DLLs, CDP cookie scripts, Form1120 stagers, and XenoRAT or PureRAT plugin and config markers

How the Suricata signatures work

SID	Looks for	Why
9526001	Outbound `GET` with `/docs/Form1120.` in the URI	Catches the tax-lure payload pair being fetched
9526002	Outbound `GET` with a URI ending in `.pdf.lnk`	Catches the double-extension shortcut lure (T1204.002)
9526003	Outbound `GET` for `/rdp/HVNC_` followed by `.dll`	Catches hidden-desktop DLL downloads
9526004	Outbound `GET` for `/rdp/cdp` followed by `.ps1`	Catches CDP cookie-script downloads
9526005	TLS certificate subject containing `purecoder` from PureRAT ports or 443	Catches PureCoder-branded PureRAT listeners
9526006	TLS certificate subject `PureRAT Agent`	Catches the default PureRAT agent certificate
9526007	TLS certificate subject `ChromeServer` from ports 443, 4444, 5333 or 8080	Catches the XenoRAT browser-name certificate
9526008	Outbound `GET` for `/xeno_plugins` followed by `.zip`	Catches XenoRAT plugin archive downloads

TLS 1.3 encrypts the server certificate. Against TLS 1.3 listeners, SIDs 9526005 to 9526007 will not fire. Pair them with JARM hunting in your attack surface tools or with endpoint socket data from the KQL hunt. Exempt detonation sandboxes from SID 9526002.

How the other rules work

The KQL hunt has a 7-day lookback. It flags devices that contact any of the 25 confirmed C2 addresses, or that connect to PureRAT and related ports (55004, 55005, 55009, 56001 to 56003, 57003, 15647, 4444, 5333, 8086). It also flags PowerShell or `AxRelaunch.exe` talking to local port 9222.

The hunt then joins process events that name workbench files such as `Form1120`, `HVNC_final` or `cdp_real`, or a script host relaunching a browser with `--remote-debugging-port=`. An exact approved-host list applies to the port and process branches only. It never hides contact with a confirmed C2 address.

Sigma rule	Fires when
Chromium forced relaunch with remote debugging port	Chrome, Edge or Brave starts with `--remote-debugging-port=` or `--remote-allow-origins=`, and the parent is PowerShell, `cmd.exe`, `wscript.exe`, `AxRelaunch.exe` or `hidden_launch.exe` (T1539)
HVNC DLL, UAC bypass and `version.dll` side-loading	A command line names `Uacbypass.dll`, an `HVNC_*.dll` build, `hijack_standalone.dll` or a proxy `version.dll`, or `mstsc.exe` starts from any path other than `System32` or `SysWOW64` (T1574.002, T1548.002)
Tax-lure `.pdf.lnk` execution and firewall tampering	A command line names `Form1120`, the two `.pdf.lnk` lures, `sacloader.b64` or `block_fw.ps1` (T1204.002, T1562.004)

Sigma exclusions name exact hosts only. Replace them with your own QA and lab machines.

YARA rule	Fires when
`ODIN_HVNC_HiddenDesktop_DLL_Strings`	A file under 2 MB holds `CreateDesktopA` or `CreateDesktopW`, `SetThreadDesktop` and `PrintWindow`, plus one HVNC build name
`ODIN_Chrome_CDP_Cookie_Hijack_PowerShell`	A script under 512 KB holds a debug-port or `/json/version` marker, a cookie call (`Network.getAllCookies` or `Storage.getCookies`) and `AxRelaunch` or `dump_cookies`
`ODIN_Form1120_TaxLure_Delivery_Stager`	A file names `Form1120.bin` or `Form1120.pdf` together with a `.pdf.lnk` lure, `sacloader.b64` or `Uacbypass.dll`
`ODIN_XenoRAT_PureRAT_Plugin_Loader_Config`	`xeno_plugins` with `ChromeServer` or `version_new_fresh.dll`; or `PureRAT Agent`; or `purecoder` with one of the XenoRAT markers

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

Confirmed endpoints in Appendix A 29

MITRE ATT&CK mapping 30

09 Indicators

Appendix A holds 19 published indicators: 19 confirmed C2 addresses and no file hashes. Six more confirmed Emotet addresses are listed in Chapter 5 and in the KQL rule only, which brings the published confirmed addresses to 25.

Type	Count	Where
Confirmed C2 addresses (with port)	19	Appendix A and this report
Additional confirmed Emotet addresses	6	This report and the KQL rule
Withheld confirmed address (UK consumer broadband)	1	Not published
Watchlist endpoints	137	Not published; counts and hosting only
Staging-server file hashes	0 published	Withheld; names and sizes in Chapter 4

Supporting fingerprints for hunting: certificate subjects `PureRAT Agent`, `ChromeServer` and `Orcus Server`; the ShadowHVNC JARM `40d40d40d00000000043d43d00043d6aff5ab0f4fc31897186312c9e639319`; and the XenoRAT and OrcusRAT JARM `22b22b00022b22b22b22b22b22b22bd3b67dd3674d9af9dd91c1955a35d0e9`.

Confirmed endpoints in Appendix A

Endpoint	Family	Hosting (country)	Seen
156.239.225[.]62:443	XenoRAT	CORENET CLOUD (HK)	13 Nov 2026
111.90.147[.]147:443	XenoRAT	Shinjiru Technology (MY)	13 Nov 2026
165.22.243[.]96:443	OrcusRAT	DigitalOcean (SG)	13 Nov 2026
93.127.160[.]122:80	ChaosRAT	23M GmbH (DE)	13 Nov 2026
13.216.143[.]112:80	SerpentStealer	Amazon AWS (US)	18 Nov 2026
23.22.63[.]150:80	SerpentStealer	Amazon AWS (US)	13 Nov 2026
8.130.115[.]156:443	Emotet	Hangzhou Alibaba (CN)	18 Nov 2026
8.130.122[.]123:443	Emotet	Hangzhou Alibaba (CN)	18 Nov 2026
8.130.159[.]214:443	Emotet	Hangzhou Alibaba (CN)	18 Nov 2026
1.95.216[.]95:443	Emotet	Huawei Cloud (CN)	16 Nov 2026
1.95.144[.]27:443	Emotet	Huawei Cloud (CN)	16 Nov 2026
1.94.25[.]210:443	Emotet	Huawei Cloud (CN)	16 Nov 2026
91.206.14[.]212:80	Emotet	JSC Selectel (RU)	14 Nov 2026
185.232.107[.]206:80	Emotet	Data Storage Center JSC (RU)	13 Nov 2026
185.137.233[.]37:80	Emotet	JSC Selectel (RU)	13 Nov 2026
64.227.189[.]225:443	Emotet	DigitalOcean (IN)	13 Nov 2026

Endpoint	Family	Hosting (country)	Seen
128.199.131[.]70:443	Emotet	DigitalOcean (SG)	13 Nov 2026
167.172.183[.]165:80	Emotet	DigitalOcean (DE)	13 Nov 2026
142.93.158[.]102:443	Emotet	DigitalOcean (CA)	13 Nov 2026

Withheld: the UK broadband OrcusRAT address, the staging server's address and its file hashes, the two China Unicom addresses, the three FTP-collision hosts, and every suspected or candidate address. Certificate domains seen only on unconfirmed servers, including the PureCoder API hostname, are withheld too.

MITRE ATT&CK mapping

Tactic	Technique	How it shows here	Detection
Initial Access / Execution	T1204.002 User Execution: Malicious File	`.pdf.lnk` tax lures and the `Form1120.pdf` payload	SIDs 9526001, 9526002; Sigma tax-lure rule; YARA Form1120 rule
Privilege Escalation	T1548.002 Bypass User Account Control	`Uacbypass.dll`	Sigma HVNC and UAC rule
Defense Evasion	T1574.002 Hijack Execution Flow: DLL Side-Loading	Proxy `version.dll` beside `mstsc.exe` and in `/xeno_*/` folders	Sigma HVNC and UAC rule; YARA XenoRAT rule
Defense Evasion	T1562.004 Impair Defenses: Disable or Modify System Firewall	`block_fw.ps1`	Sigma tax-lure rule
Credential Access	T1539 Steal Web Session Cookie	CDP relaunch scripts and `Network.getAllCookies`	SID 9526004; Sigma CDP rule; YARA CDP rule; KQL port 9222 branch

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 findings cover a two-week observation window ending 19 November 2026. Some records are older feed entries, such as the SerpentStealer candidates on AWS; no dates are given for them. We do not use those as a tracking start.
- **Infrastructure, not intrusions.** This report describes C2 listeners and staged files. We observed no intrusion on a target system and make no claim about victims.
- **Staged is not used.** The staging server's files show intent and tooling. Their purposes are inferred from file names, sizes and identical hashes. Nothing shows the files were run against a target.
- **Candidates are leads.** All PureRAT and ShadowHVNC endpoints are candidates. Do not block them without corroboration.
- **Family names.** A family label names the software a listener matches. It is not attribution to a named group, and the four-cell view in Figure 1 is an analytical model.
- **First-seen dates are not build dates.** Eighteen PureRAT endpoints were first seen on 19 November 2026. That date is a first observation, not the date the operator set them up.
- **Rule testing.** Every published rule file loads without errors in its engine (Suricata 7.0.12, YARA-X, pySigma and Microsoft's Kusto.Language analyzer, checked on 20 November 2026). The rules were not replayed against live traffic, so test and tune them in your own environment before production use.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. Chrome DevTools Team. Chrome DevTools Protocol. https://chromedevtools.github.io/devtools-protocol/ (verified 19 November 2026)
2. Google Security Blog. Improving the security of Chrome cookies on Windows. https://security.googleblog.com/2024/07/improving-security-of-chrome-cookies-on.html (verified 19 November 2026)
3. Microsoft Learn. CreateDesktopA function (winuser.h). https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-createdesktopa (verified 19 November 2026)
4. MITRE ATT&CK. T1574.002 Hijack Execution Flow: DLL Side-Loading. https://attack.mitre.org/techniques/T1574/002/ (verified 19 November 2026)
5. Internal Revenue Service. About Form 1120, U.S. Corporation Income Tax Return. https://www.irs.gov/forms-pubs/about-form-1120 (verified 19 November 2026)
6. OISF. Suricata 7.0 User Guide, HTTP keywords. https://docs.suricata.io/en/suricata-7.0.0/rules/http-keywords.html (verified 19 November 2026)
7. Salesforce Engineering. Easily identify malicious servers on the internet with JARM. https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a/ (verified 19 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 (19) 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
R26-IOC-01	IPv4	156.239.225[.]62	443	xenorat	BLOCK
R26-IOC-02	IPv4	111.90.147[.]147	443	xenorat	BLOCK
R26-IOC-03	IPv4	165.22.243[.]96	443	orcusrat	BLOCK
R26-IOC-04	IPv4	93.127.160[.]122	80	chaosrat	BLOCK
R26-IOC-05	IPv4	13.216.143[.]112	80	serpentstealer	BLOCK
R26-IOC-06	IPv4	23.22.63[.]150	80	serpentstealer	BLOCK
R26-IOC-07	IPv4	8.130.115[.]156	443	emotet	BLOCK
R26-IOC-08	IPv4	8.130.122[.]123	443	emotet	BLOCK
R26-IOC-09	IPv4	8.130.159[.]214	443	emotet	BLOCK
R26-IOC-10	IPv4	1.95.216[.]95	443	emotet	BLOCK
R26-IOC-11	IPv4	1.95.144[.]27	443	emotet	BLOCK
R26-IOC-12	IPv4	1.94.25[.]210	443	emotet	BLOCK
R26-IOC-13	IPv4	91.206.14[.]212	80	emotet	BLOCK
R26-IOC-14	IPv4	185.232.107[.]206	80	emotet	BLOCK
R26-IOC-15	IPv4	185.137.233[.]37	80	emotet	BLOCK
R26-IOC-16	IPv4	64.227.189[.]225	443	emotet	BLOCK
R26-IOC-17	IPv4	128.199.131[.]70	443	emotet	BLOCK
R26-IOC-18	IPv4	167.172.183[.]165	80	emotet	BLOCK
R26-IOC-19	IPv4	142.93.158[.]102	443	emotet	BLOCK

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_hvnc_form1120_xenorat_purerat_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 26 / 30 YARA Artifact Suite
   Scope: Bounded detection rules for Hidden-Desktop (HVNC) DLLs, Chrome-CDP cookie
          hijackers, Form1120 tax-lure stagers, and XenoRAT/PureRAT plugin configs.
   Classification: TLP:CLEAR
*/

rule ODIN_HVNC_HiddenDesktop_DLL_Strings
{
    meta:
        author = "Odin by Brandefense"
        monograph = "26 / 30"
        classification = "TLP:CLEAR"
        action = "isolate host and review"
        description = "Matches Win32 hidden-desktop creation and workbench HVNC DLL markers"
    strings:
        $api1 = "CreateDesktopA" ascii
        $api2 = "CreateDesktopW" ascii
        $api3 = "SetThreadDesktop" ascii
        $api4 = "PrintWindow" ascii
        $hv1 = "HVNC_final" ascii wide nocase
        $hv2 = "HVNC_mark3" ascii wide nocase
        $hv3 = "HVNC_patched" ascii wide nocase
        $hv4 = "hijack_standalone" ascii wide nocase
    condition:
        filesize < 2MB and (($api1 or $api2) and $api3 and $api4) and 1 of ($hv*)
}

rule ODIN_Chrome_CDP_Cookie_Hijack_PowerShell
{
    meta:
        author = "Odin by Brandefense"
        monograph = "26 / 30"
        classification = "TLP:CLEAR"
        action = "isolate host and review"
        description = "Matches PowerShell or C# browser relaunch scripts abusing Chrome DevTools Protocol cookie
extraction"
    strings:
        $cdp1 = "--remote-debugging-port=" ascii wide nocase
        $cdp2 = "/json/version" ascii wide nocase
        $ws1 = "Network.getAllCookies" ascii wide
        $ws2 = "Storage.getCookies" ascii wide
        $ax1 = "AxRelaunch" ascii wide nocase
        $ax2 = "dump_cookies" ascii wide nocase
    condition:
        filesize < 512KB and ($cdp1 or $cdp2) and ($ws1 or $ws2) and ($ax1 or $ax2)
}

rule ODIN_Form1120_TaxLure_Delivery_Stager
{
    meta:
        author = "Odin by Brandefense"
        monograph = "26 / 30"
        classification = "TLP:CLEAR"
        action = "quarantine file and review"
        description = "Matches corporate tax-lure delivery scripts and LNK/VBS stagers referencing Form1120 and
UAC bypass modules"
    strings:
        $tx1 = "Form1120.bin" ascii wide nocase
        $tx2 = "Form1120.pdf" ascii wide nocase
```

```
        $ln1 = "Tax Documents 2025.pdf.lnk" ascii wide nocase
        $ln2 = "sacloader.b64" ascii wide nocase
        $uac = "Uacbypass.dll" ascii wide nocase
    condition:
        filesize < 2MB and ($tx1 or $tx2) and ($ln1 or $ln2 or $uac)
}

rule ODIN_XenoRAT_PureRAT_Plugin_Loader_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "26 / 30"
        classification = "TLP:CLEAR"
        action = "analyst review"
        description = "Matches XenoRAT side-loading plugin manifests and PureRAT and PureCoder brand markers"
    strings:
        $xe1 = "xeno_plugins" ascii wide nocase
        $xe2 = "ChromeServer" ascii wide
        $pr1 = "purecoder" ascii wide nocase
        $pr2 = "PureRAT Agent" ascii wide
        $sl1 = "version_new_fresh.dll" ascii wide nocase
    condition:
        filesize < 2MB and (($xe1 and ($xe2 or $sl1)) or $pr2 or ($pr1 and ($xe2 or $sl1)))
}
```

odin_purerat_shadowhvnc_xenorat_cdp.rules

SURICATA

```
# Odin by Brandefense - Monograph 26 / 30 Suricata 7.x Detection Suite
# Coverage: Form1120 Tax-Lure Stagers, HVNC DLLs, Chrome-CDP Hijackers, PureRAT, and XenoRAT
# Classification: TLP:CLEAR

alert http $HOME_NET any -> $EXTERNAL_NET [80,8080,8000] (msg:"ODIN [R26] Corporate Tax-Lure Form1120 Payload
Twin HTTP Retrieval"; flow:established,to_server; http.method; content:"GET"; http.uri; bsize:>14; content:"/
docs/Form1120."; fast_pattern; classtype:trojan-activity; sid:9526001; rev:1; metadata:created_at 2026_11_19,
deployment perimeter, tactic initial_access;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,8080,8000] (msg:"ODIN [R26] Masqueraded Corporate Tax PDF-LNK
Stager HTTP Download"; flow:established,to_server; http.method; content:"GET"; http.uri; bsize:>12;
content:".pdf.lnk"; endswith; fast_pattern; classtype:trojan-activity; sid:9526002; rev:1; metadata:created_at
2026_11_19, deployment perimeter, tactic initial_access;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,8080,8000] (msg:"ODIN [R26] Workbench Hidden-Desktop HVNC DLL
Module HTTP Fetch"; flow:established,to_server; http.method; content:"GET"; http.uri; bsize:>13; content:"/rdp/
HVNC_"; fast_pattern; content:".dll"; distance:0; classtype:trojan-activity; sid:9526003; rev:1;
metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,8080,8000] (msg:"ODIN [R26] Chrome-CDP Session Hijacker PowerShell
Script Staging Fetch"; flow:established,to_server; http.method; content:"GET"; http.uri; bsize:>11; content:"/
rdp/cdp"; fast_pattern; content:".ps1"; distance:0; classtype:credential-theft; sid:9526004; rev:1;
metadata:created_at 2026_11_19, deployment perimeter, tactic credential_access;)

alert tls $EXTERNAL_NET [56001,56002,56003,57003,443] -> $HOME_NET any (msg:"ODIN [R26] PureRAT PureCoder Vendor
TLS Certificate Subject Observed"; flow:established,from_server; tls.cert_subject; content:"purecoder"; nocase;
fast_pattern; classtype:command-and-control; sid:9526005; rev:2; metadata:created_at 2026_11_19, deployment
perimeter, tactic command_and_control;)

alert tls $EXTERNAL_NET [442,443,56001,56002,56003] -> $HOME_NET any (msg:"ODIN [R26] PureRAT Default Agent TLS
Certificate Subject Handshake"; flow:established,from_server; tls.cert_subject; bsize:>12; content:"PureRAT
Agent"; fast_pattern; classtype:command-and-control; sid:9526006; rev:1; metadata:created_at 2026_11_19,
deployment perimeter, tactic command_and_control;)

alert tls $EXTERNAL_NET [443,4444,5333,8080] -> $HOME_NET any (msg:"ODIN [R26] XenoRAT ChromeServer Masquerade
TLS Certificate Handshake"; flow:established,from_server; tls.cert_subject; bsize:>11; content:"ChromeServer";
fast_pattern; classtype:command-and-control; sid:9526007; rev:1; metadata:created_at 2026_11_19, deployment
perimeter, tactic command_and_control;)
```

```
alert http $HOME_NET any -> $EXTERNAL_NET [80,8080,8000] (msg:"ODIN [R26] XenoRAT Modular Plugin Archive Open-Directory Retrieval"; flow:established,to_server; http.method; content:"GET"; http.uri; bsize:>16; content:"/xeno_plugins"; fast_pattern; content:".zip"; distance:0; classtype:trojan-activity; sid:9526008; rev:1; metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)
```

sentinel_form1120_hvnc_cdp_and_purerat_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 26 / 30 Microsoft Sentinel & Defender XDR Hunt
// Correlates confirmed C2 egress, PureRAT tri-port clusters, Form1120 tax lures, HVNC DLLs, and Chrome-CDP hijacks
// Classification: TLP:CLEAR
// The host allowlist applies only to the port and process branches. Contact with a confirmed C2 address always alerts.

let Lookback = 7d;
let ApprovedAdminHosts = dynamic(["QA-BROWSER-TEST-01", "E2E-PLAYWRIGHT-RUNNER-01", "REDTEAM-LAB-WIN-01"]);
let ConfirmedC2IPs = dynamic([
    "1.94.25.210", "1.95.144.27", "1.95.216.95", "111.90.147.147",
    "128.199.131.70", "13.216.143.112", "138.197.111.250", "142.93.158.102",
    "156.239.225.62", "159.203.173.129", "165.22.243.96", "167.172.183.165",
    "167.71.229.25", "178.57.77.87", "185.137.233.198", "185.137.233.37",
    "185.232.107.206", "188.246.224.196", "23.22.63.150", "64.227.189.225",
    "8.130.115.156", "8.130.122.123", "8.130.159.214",
    "91.206.14.212", "93.127.160.122"
]);
let PureRatAndRatPorts = dynamic([55004, 55005, 55009, 56001, 56002, 56003, 57003, 15647, 4444, 5333, 8086]);
let WorkbenchMarkers = @"(?i)(Form1120|Tax Documents 2025\.pdf\.lnk|relaunch2\.pdf\.lnk|Uacbypass\.dll|HVNC_final|HVNC_mark3|HVNC_patched|hijack_standalone\.dll|AxRelaunch|cdp_real|block_fw\.ps1)";
let SuspiciousWorkbenchProcs = DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAdminHosts))
    | where ProcessCommandLine matches regex WorkbenchMarkers
        or (FileName in~ ("chrome.exe", "msedge.exe", "brave.exe") and ProcessCommandLine contains "--remote-debugging-port=" and InitiatingProcessFileName in~ ("powershell.exe", "pwsh.exe", "cmd.exe", "wscript.exe", "AxRelaunch.exe"))
    | project ProcTime = Timestamp, DeviceId, DeviceName, InitiatingProcessFileName, FileName, ProcessCommandLine;
DeviceNetworkEvents
| where Timestamp >= ago(Lookback)
| where RemoteIP in (ConfirmedC2IPs)
    or (not(DeviceName in~ (ApprovedAdminHosts)) and RemotePort in (PureRatAndRatPorts))
    or (not(DeviceName in~ (ApprovedAdminHosts)) and RemotePort == 9222 and RemoteIP in ("127.0.0.1", "::1") and InitiatingProcessFileName in~ ("powershell.exe", "pwsh.exe", "AxRelaunch.exe"))
| summarize
    NetFirstSeen = min(Timestamp),
    NetLastSeen = max(Timestamp),
    DistinctRemoteIPs = dcount(RemoteIP),
    DistinctPorts = make_set(RemotePort, 16),
    MatchedC2IPs = make_set_if(RemoteIP, RemoteIP in (ConfirmedC2IPs), 16),
    ConnectionCount = count()
    by DeviceId, DeviceName, InitiatingProcessFileName
| join kind=leftouter (SuspiciousWorkbenchProcs) on DeviceId, DeviceName
| where array_length(MatchedC2IPs) > 0 or isnotempty(ProcessCommandLine) or set_has_element(DistinctPorts, 56001) or set_has_element(DistinctPorts, 56002) or set_has_element(DistinctPorts, 56003)
| extend AlertAction = case(
    array_length(MatchedC2IPs) > 0, "BLOCK_CONFIRMED_RAT_OR_LOADER_C2",
    ProcessCommandLine matches regex @"(?i)(--remote-debugging-port=|HVNC_|Form1120|Uacbypass\.dll)", "ISOLATE_HVNC_OR_CHROME_CDP_HIJACK",
    "HUNT_PURERAT_HIGH_PORT_EGRESS"
)
| project NetFirstSeen, NetLastSeen, DeviceName, AlertAction, MatchedC2IPs, DistinctRemoteIPs, DistinctPorts, InitiatingProcessFileName, ProcessCommandLine, ConnectionCount
| sort by ConnectionCount desc
```

sigma_hvnc_dll_uacbypass_and_chrome_cdp_hijack.yml

SIGMA

```
title: Chromium Forced Relaunch With Remote Debugging Port for CDP Session Hijack
id: 3a71f09c-6d2e-49b8-a105-202611192601
status: experimental
description: Detects PowerShell, WScript, or custom C# launchers (such as AxRelaunch.exe and cdp.ps1) relaunching
Chromium browsers with --remote-debugging-port to bypass App-Bound Encryption and dump live session cookies.
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.credential_access
  - attack.t1539
logsource:
  category: process_creation
  product: windows
detection:
  selection_browser:
    Image|endswith:
      - '\chrome.exe'
      - '\msedge.exe'
      - '\brave.exe'
  selection_cdp_flags:
    CommandLine|contains:
      - '--remote-debugging-port='
      - '--remote-allow-origins='
  selection_parent:
    ParentImage|endswith:
      - '\powershell.exe'
      - '\pwsh.exe'
      - '\cmd.exe'
      - '\wscript.exe'
      - '\AxRelaunch.exe'
      - '\hidden_launch.exe'
  filter_approved_qa:
    ComputerName:
      - 'QA-BROWSER-TEST-01'
      - 'E2E-PLAYWRIGHT-RUNNER-01'
  condition: selection_browser and selection_cdp_flags and selection_parent and not filter_approved_qa
falsepositives:
  - Dedicated QA browser automation hosts listed in ComputerName allowlists
level: high
---
title: Hidden Desktop HVNC DLL Injection UAC Bypass and Version DLL Side-Loading
id: 8c52b41e-90f3-4e64-b812-202611192602
status: experimental
description: Detects execution or rundll32/PowerShell loading of workbench HVNC hidden-desktop modules
(HVNC_final.dll, HVNC_mark3.dll, HVNC_patched.dll, hijack_standalone.dll), Uacbypass.dll, or non-system mstsc.exe
side-loading harnesses.
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.defense_evasion
  - attack.privilege_escalation
  - attack.t1574.002
  - attack.t1548.002
logsource:
  category: process_creation
  product: windows
detection:
  selection_artifacts:
    CommandLine|contains:
      - 'Uacbypass.dll'
      - 'HVNC_final.dll'
      - 'HVNC_mark3.dll'
      - 'HVNC_patched.dll'
      - 'hijack_standalone.dll'
      - 'version_new_fresh.dll'
      - 'version_remcos.dll'
  selection_mstsc_sideload:
    Image|endswith: '\mstsc.exe'
```

```
  filter_system_mstsc:
    Image:
      - 'C:\Windows\System32\mstsc.exe'
      - 'C:\Windows\SysWOW64\mstsc.exe'
  filter_redteam_lab:
    ComputerName:
      - 'REDTEAM-LAB-WIN-01'
  condition: (selection_artifacts or (selection_mstsc_sideload and not filter_system_mstsc)) and not
filter_redteam_lab
falsepositives:
  - Authorized adversary-simulation lab hosts registered with SOC operations
level: high
---
title: Corporate Tax-Lure PDF-LNK Execution and Host Firewall Tampering
id: 5e94a17d-2c8b-43f1-9d60-202611192603
status: experimental
description: Identifies execution chains referencing corporate tax lures (Form1120.pdf, Form1120.bin, Tax
Documents 2025.pdf.lnk) or companion host firewall suppression scripts (block_fw.ps1).
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.initial_access
  - attack.defense_evasion
  - attack.t1204.002
  - attack.t1562.004
logsource:
  category: process_creation
  product: windows
detection:
  selection_lure_or_fw:
    CommandLine|contains:
      - 'Form1120.bin'
      - 'Form1120.pdf'
      - 'Tax Documents 2025.pdf.lnk'
      - 'relaunch2.pdf.lnk'
      - 'sacloader.b64'
      - 'block_fw.ps1'
  filter_redteam_lab:
    ComputerName:
      - 'REDTEAM-LAB-WIN-01'
  condition: selection_lure_or_fw and not filter_redteam_lab
falsepositives:
  - Sanctioned malware analysis sandboxes processing corporate tax lure samples
level: high
```

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/tax-lures-to-hidden-desktops/
Short Read · brandefense.io/odin-research/blog/tax-lures-hidden-desktops-and-cookie-theft-around-purerat/
Defense Kit · brandefense.io/odin-research/defense-kit/