ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 27 / 30 · POST-EXPLOITATION

Drop-Box Hubs and Reverse Tunnels
Hak5 Cloud C2, ReverseSSH and KeyPlug

How hardware implant controllers, reverse-SSH multiplexers, Go shells and wolfSSL backdoors keep outbound access, and how to tell them from lookalikes

Two-week observation window ending 18 November 2026 · Data cutoff 19 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

89
Unique endpoints on 74 hosts, across nine families

12
Confirmed endpoints on 11 IPs (6 Hak5 Cloud C2, 5 ReverseSSH, 1 GShellC2); 5 of them, on 4 hosts, are published for blocking

36
ReverseSSH endpoints, the largest family; 16 listen on the default port 3232

23
Hak5 Cloud C2 endpoints on 19 IPs, controllers for LAN Turtle, Packet Squirrel, WiFi Pineapple and Key Croc implants

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

How hardware implant controllers, reverse-SSH multiplexers, Go shells and wolfSSL backdoors keep outbound access, and how to tell them from lookalikes

01	Executive Summary	04
02	How the Persistence Stack Works	06
03	Drop-Box Hubs and Multiplexers: Hak5 Cloud C2, ReverseSSH, Platypus	09
04	Cross-Platform Backdoors: GShellC2, BlueShell, XorekC2 and KeyPlug	13
05	Relay Workbenches: TokenFlow Proxies and OpenWrt Stunnel Tunnels	16
06	Telling Hostile Infrastructure from Lookalikes	19
07	What Defenders Should Do	21
08	Detection Rules	23
09	Indicators	26
10	Scope and Limits	28
11	Sources	30
A	Indicators of compromise (5)	32
B	Detection rules (4 files)	33

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 89 endpoints on 74 hosts across nine persistent-access and backdoor families. Hak5 Cloud C2 and ReverseSSH make up 66.3% of them. Twelve endpoints are confirmed, but most run dual-use testing tools, so five are published for blocking. Thirteen lookalikes were ordinary mail servers. Block the five published endpoints, enforce 802.1X on wired ports, and hunt default `CN=www.wolfssl[.]com`, `CN=:3232` and `CN=Gshell Server` certificates.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 89 endpoints on 74 hosts across nine persistent-access and backdoor families. Hak5 Cloud C2 and ReverseSSH make up 66.3% of them. Twelve endpoints are confirmed, but most run dual-use testing tools, so five are published for blocking. Thirteen lookalikes were ordinary mail servers. Block the five published endpoints, enforce 802.1X on wired ports, and hunt default `CN=www.wolfssl[.]com`, `CN=:3232` and `CN=Gshell Server` certificates.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 04

01 Executive Summary

These tools all keep access to a network that blocks inbound connections. A hardware implant or small agent inside dials out to a cloud server over HTTP, WebSocket or TLS. Relays can hide the real controller address.

1. **Hak5 Cloud C2 and ReverseSSH make up most of the infrastructure.**
   ReverseSSH has 36 endpoints on 30 hosts and Hak5 Cloud C2 has 23 endpoints on 19 hosts. Together they are 66.3% of the 89 endpoints. Both are sold or published for authorized testing, so a confirmed install is not proof of hostile use.

2. **Go shells and a wolfSSL backdoor keep footholds on Linux and Windows.**
   GShellC2 has seven endpoints, all in Hong Kong, with one confirmed controller. KeyPlug has five endpoints on ports 10443, 10444, 8443 and 443. Two of them present the default `CN=www.wolfssl[.]com` library certificate.

3. **Two open directories expose the relay layer behind the controllers.**
   One host stages a 19.2 MB `TokenFlow` Linux binary, Node.js proxy scripts and a 153.2 MB HTTP traffic log. Another archives OpenWrt router backups and `stunnel` TLS tunnel configurations across 23 mirrored sites.

Three Decisions for Leaders

1. **Block only what is clearly hostile.** Block the five published endpoints. Keep standalone Hak5 controllers, plain ReverseSSH listeners, mail-port lookalikes and dynamic ISP addresses on watchlists or in analyst review.
2. **Close the wired door.** Require 802.1X port-based access control on branch closets, meeting rooms and wall jacks, so a plugged-in drop-box cannot join the network. Audit edge Linux hosts for unapproved ReverseSSH, `stunnel` and Node.js proxy processes.
3. **Inspect unusual TLS egress.** Watch outbound traffic on ports 3232, 5000, 8080 to 8088, 8443, 9090, 10443, 10444 and 23590. Look for default library certificates and WebSocket upgrades.

The Study in Numbers

Number	What it is
89	Unique endpoints on 74 hosts, across nine families
12	Confirmed endpoints on 11 IPs (6 Hak5 Cloud C2, 5 ReverseSSH, 1 GShellC2); 5 of them, on 4 hosts, are published for blocking
36	ReverseSSH endpoints, the largest family; 16 listen on the default port 3232
23	Hak5 Cloud C2 endpoints on 19 IPs, controllers for LAN Turtle, Packet Squirrel, WiFi Pineapple and Key Croc implants
5	KeyPlug endpoints on ports 10443, 10444, 8443 and 443; 2 present the default wolfSSL certificate
13	Mail-server lookalikes on ports 110 to 995 that match a tool banner but are not hostile
2	Open-directory relay workbenches, one with a `TokenFlow` relay stack and one with OpenWrt `stunnel` backups

02

CHAPTER 02

How the Persistence Stack Works

IN SHORT

The nine families fall into four layers: hardware drop-box hubs, reverse-shell multiplexers, lightweight shells and modular TLS implants. Relays can sit in front of any of them.

INSIDE THIS CHAPTER

Outbound by design 06

The nine families 07

Where the endpoints sit 07

02 How the Persistence Stack Works

Outbound by design

These tools turn the connection around. A physical drop-box (Hak5 Cloud C2) or a small shell agent (ReverseSSH, Platypus, GShellC2, BlueShell, XorekC2 or KeyPlug) starts an outbound session to a cloud server. The session runs over HTTP, SSH inside TLS, or WebSocket. Some operators bounce it through `stunnel` or a `TokenFlow` proxy first.

Figure 1 is an analytical model. It groups the families by role. It does not describe one attributed intrusion campaign, and no logs from inside target networks were available.

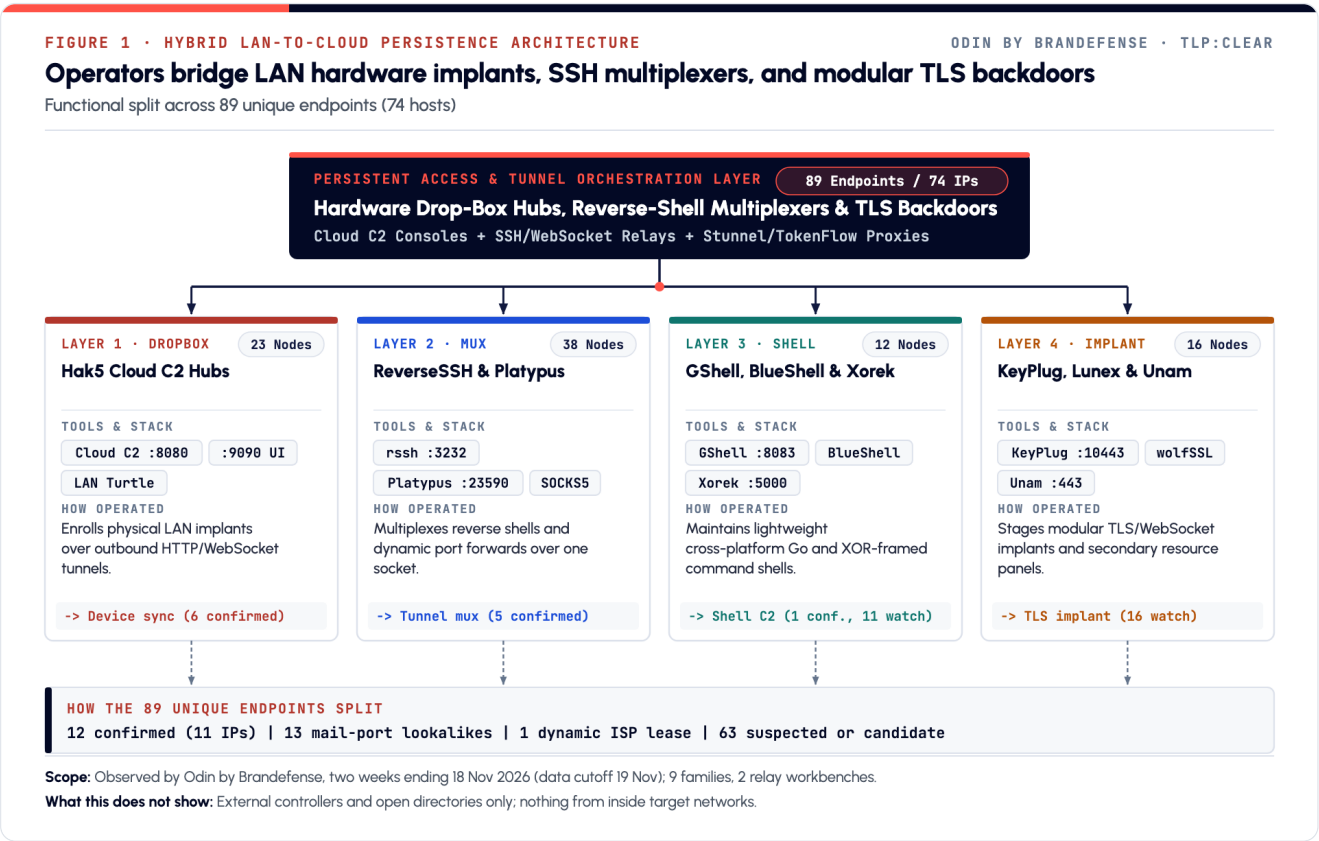


Figure 1: Operators bridge LAN hardware implants, SSH multiplexers, and modular TLS backdoors

The nine families

The study covers 89 unique endpoints on 74 hosts. No host runs two families. Twelve hosts run one family on several ports.

Family	Role	Endpoints (hosts)	Confirmed	Mail lookalikes	Dynamic ISP	Suspected	Candidates
ReverseSSH	ReverseSSH multiplexer	36 (30)	5	8	1	3	19
Hak5 Cloud C2	Hardware drop-box hub	23 (19)	6	5	0	5	7
Unam	Cryptominer web panel	8 (7)	0	0	0	1	7
GShellC2	Go reverse-shell controller	7 (5)	1	0	0	0	6
KeyPlug	Modular C++ TLS backdoor	5 (4)	0	0	0	0	5
Lunex	Secondary TLS listener	3 (3)	0	0	0	0	3
BlueShell	Go TLS backdoor	3 (2)	0	0	0	0	3
Platypus	Go reverse-shell multiplexer	2 (2)	0	0	0	0	2
XorekC2	Port 5000 XOR shell	2 (2)	0	0	0	0	2
Total		**89 (74)**	**12**	**13**	**1**	**9**	**54**

Where the endpoints sit

Six countries lead. The country totals need care, because benign mail servers inflate two of them.

Country	Endpoints	Share	Note
Hong Kong	18	20.2%	Includes all 7 GShellC2 endpoints
United States	17	19.1%	
Netherlands	13	14.6%	5 are mail ports on one host
Italy	8	9.0%	All 8 are mail-server lookalikes
China	7	7.9%	
Germany	6	6.7%	

The 12 confirmed endpoints all sit on dedicated cloud and VPS hosting. DigitalOcean has 3, Amazon AWS 2 and Latitude.sh 2 (two ports on one host). netcup, Shenzhen Tencent, Scloud, HK Kwaifong and HK Lightlayer have one each.

CHAPTER 03

Drop-Box Hubs and Multiplexers: Hak5 Cloud C2, ReverseSSH, Platypus

IN SHORT

Hardware implants and multiplexed SSH tunnels give an operator the same thing: a durable outbound control channel with built-in SOCKS pivoting. Hak5 Cloud C2, ReverseSSH and Platypus account for 61 of the 89 endpoints (68.5%).

INSIDE THIS CHAPTER

Hak5 Cloud C2 09
ReverseSSH 10
Platypus 11

03 Drop-Box Hubs and Multiplexers: Hak5 Cloud C2, ReverseSSH, Platypus

Figure 2 maps each family to its ports, default certificates, target surface and detection.

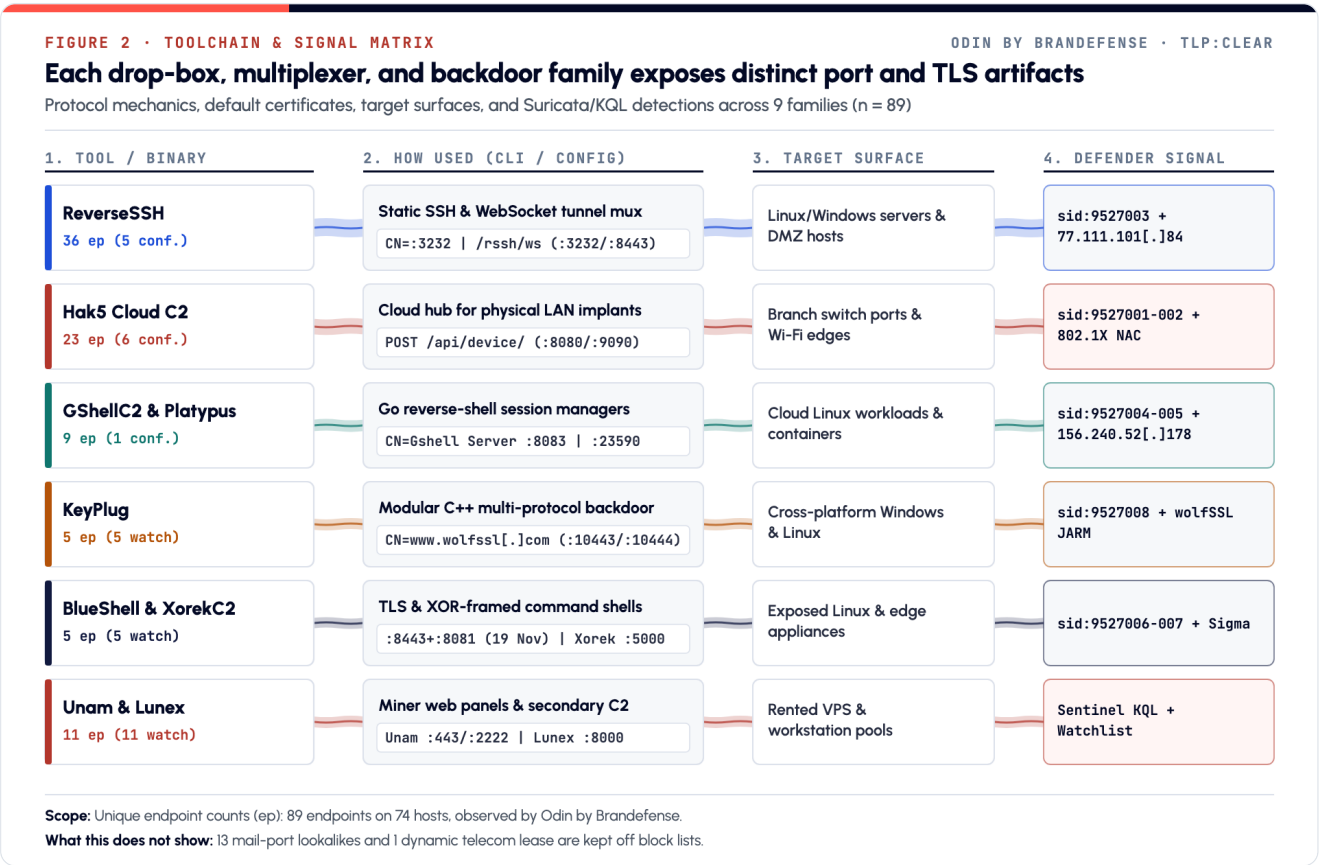


Figure 2: Each drop-box, multiplexer, and backdoor family exposes distinct port and TLS artifacts

Hak5 Cloud C2

Hak5 Cloud C2 (`c2-community` or `c2-pro`) manages the vendor's implants: LAN Turtle, Packet Squirrel, WiFi Pineapple, Key Croc and Screen Crab. A device plugged into an unattended Ethernet jack beacons out over HTTP or WebSocket. It can then open a reverse SSH shell with no inbound firewall rule.

The fleet holds 23 endpoints on 19 IPs.

Port	Endpoints
8080	5
80	4
9090	2
443	2
8088	1
8095, 8834, 31010, 3389	Candidates, one each
110, 143, 465, 993, 995	5 mail-port lookalikes on one host

Six controllers on dedicated cloud hosting are confirmed as Hak5 Cloud C2. Hak5 sells this product to penetration testers, so a standalone controller does not show hostile use. We publish only the one controller with a second, independent offensive signal.

Endpoint	Hosting	Port	Certificate and JARM	Status
146.190.211[.]163	DigitalOcean (US)	8088	HTTP	Published for blocking. Monograph 12 documents a separate GoPhish phishing server on the same host
Address withheld	netcup (DE)	8080	Certificate domain withheld	Analyst review
Address withheld	Amazon AWS (GB)	80	Certificate domain withheld	Analyst review
Address withheld	Amazon AWS (US)	8080	HTTP	Analyst review
Two addresses withheld	DigitalOcean (US)	9090	A pair sharing one certificate and one JARM	Analyst review

Three more Hak5 instances present self-signed `CN=pentest` certificates. They sit on Amazon AWS in France (443), Microsoft Azure in Ireland (3389) and Amazon AWS in Germany (443). The certificate suggests an authorized red-team engagement, so their addresses are withheld.

ReverseSSH

ReverseSSH (`rssh`) builds an SSH server into one static binary. The binary dials out over TCP, TLS, HTTP or WebSocket, by default to port 3232. Through that one socket the operator gets a shell, SOCKS5 proxying (`-D`) and SFTP file transfer.

The fleet holds 36 endpoints on 30 hosts. Sixteen listen on 3232. Eight of those present a self-signed `CN=:3232` certificate, and seven share the JARM `3fd3fd20d3fd3fd00043d3fd3fd43d5ecfbe778b06e32b538bd51f24eb7398`.

Five ReverseSSH endpoints on dedicated cloud hosting are confirmed. ReverseSSH is an open-source tool used by testers too. We publish the two hosts that wrap SSH in TLS under a self-signed certificate named after their own `IP:port`, matching Monograph 12. The two plain HTTP listeners stay in analyst review.

Endpoint	Hosting	Certificate	JARM	Seen
77.111.101[.]84:8082	Latitude.sh (BR)	Self-signed, IP-literal CN	`3fd3fd0003fd3fd00043d43d00043d3bef2bf79cd6719851e8198c1e8f9a14`	14 Nov 2026
77.111.101[.]84:8443	Latitude.sh (BR)	Self-signed, IP-literal CN	Same as above	14 Nov 2026
165.154.199[.]52:443	Scloud Pte Ltd (SG)	Self-signed, IP-literal CN	Same as above	13 Nov 2026
Address withheld, port 80	Shenzhen Tencent (CN)	None (HTTP)	None	13 Nov 2026
Address withheld, port 80	HK Kwaifong Group (HK)	None (HTTP)	None	13 Nov 2026

Platypus

Platypus is a Go manager for many reverse-shell sessions at once. It offers REST and WebSocket control and uses port 23590 by default. Two candidates were seen. One listens on 23590 at Evoxt in Japan. The other listens on 443 at ROUTE 95 in the United States, with the certificate `CN=platypus-ingress`. Both addresses are withheld.

CHAPTER 04

Cross-Platform Backdoors: GShellC2, BlueShell, XorekC2 and KeyPlug

IN SHORT

Compiled Go and C++ backdoors give operators Linux and Windows footholds next to the drop-box hubs. Default certificates such as `CN=Gshell Server` and `CN=www.wolfssl[.]com` are the best hunting pivots.

INSIDE THIS CHAPTER

GShellC2	13
BlueShell and XorekC2	13
KeyPlug	14
Lunex and Unam	14

04 Cross-Platform Backdoors: GShellC2, BlueShell, XorekC2 and KeyPlug

GShellC2, KeyPlug, BlueShell and XorekC2 account for 17 endpoints on 13 hosts. Figure 3 is a model of how the layers connect, from a LAN implant through relays to a cloud controller, with the defender signal for each step.



Figure 3: Outbound tunnels chain LAN drop-boxes and SOHO relays into cloud C2 controllers

GShellC2

All seven GShellC2 endpoints sit in Hong Kong, on five IPs at Antbox Networks (4) and HK Lightlayer (3). Four listen on 8083 and three on 8080.

The confirmed controller is 156.240.52[.]178:8083 on HK Lightlayer, seen on 13 November 2026. It presents `CN=Gshell Server` with the JARM `3fd3fd20d00000021c43d43d00043d15e5079913504d6ff89229f1f99b095c`. A dual-port Antbox candidate on 8080 and 8083 shares that JARM. Two more 8083 listeners were seen on 19 November. Their addresses are withheld.

BlueShell and XorekC2

Family	Endpoints	What was seen
BlueShell	3 on 2 IPs	One host at Bangmod Enterprise (TH) listens on 8081 (from 18 November) and 8443 (from 19 November). A third listener sits on 443 in China
XorekC2	2	Twin 5000 listeners at DpkgSoft International (NL), both with self-signed IP-literal certificates

All five are candidates, and their addresses are withheld.

KeyPlug

KeyPlug is a modular backdoor with Windows and Linux builds. It speaks raw TCP, TLS, HTTP and WebSocket. The fleet holds five candidate endpoints on four IPs.

Hosting	Port	Certificate	Note
Hangzhou Alibaba (CN)	10443	Certificate domain withheld	Same host also listens on 10444, seen 18 and 19 November
Hangzhou Alibaba (CN)	10444	None recorded	Second port of the host above
Hangzhou Alibaba (CN)	10443	`CN=www.wolfssl[.]com`	Default wolfSSL library certificate
Baxet Group (ES)	443	`CN=www.wolfssl[.]com`	Default wolfSSL library certificate
Nebula Global (HK)	8443	Certificate domain withheld	Not corroborated

wolfSSL is an embedded TLS library. A build that keeps its sample certificate presents the vendor's name as the subject. That default makes a good hunting pivot, but it is not corroborated, so these addresses stay withheld.

Lunex and Unam

Lunex has three candidate listeners, two on 8000 and one on 443. Unam has eight SilentCryptoMiner web panels on seven IPs. One Unam panel on 2222, at Obehosting in the Netherlands with `CN=localhost`, is suspected. The rest are candidates. None of these addresses is published.

05

CHAPTER 05

Relay Workbenches: TokenFlow Proxies and OpenWrt Stunnel Tunnels

IN SHORT

Operators who connect straight to a cloud controller risk losing it to a takedown. Two open directories show the relay layer that hides it: a `TokenFlow` proxy stack and a set of OpenWrt `stunnel` backups.

INSIDE THIS CHAPTER

Workbench 1: TokenFlow and Node.js upstream relay 16

Workbench 2: OpenWrt router and stunnel backups 17

05 Relay Workbenches: TokenFlow Proxies and OpenWrt Stunnel Tunnels

Figure 4 pairs the multi-port controller hosts with the workbench files. The owners of both workbench hosts are not established, so their addresses are withheld.



Figure 4: Multi-port hubs and open-directory workbenches expose relay binaries and TLS defaults

Workbench 1: TokenFlow and Node.js upstream relay

This host is in China and serves an open directory on port 8888. The directory tree holds 4,663 files. Files on it were listed between 17 and 19 November 2026.

The host is a Linux build machine with Python 3.11.10, Go 1.24.0 (78.4 MB), Node v22.22.2 and Playwright headless Chromium. Next to them sits a traffic-forwarding stack.

File	Size (bytes)	Role
`tokenflow-linux-amd64`	19,244,069	Compiled Linux `amd64` `TokenFlow` relay daemon
`tokenflow-linux-amd64-logo`	19,383,325	Second build of the same daemon
`astr-proxy.js`	4,158,208	Bundled Node.js edge proxy
`astr-upstream.js`	4,158,208	Bundled Node.js upstream forwarder
`http.log`	153,166,632	HTTP and WebSocket traffic log
`body`	81,647	Captured request body

The proxy and upstream scripts sit side by side with a large traffic log. That pattern fits a relay that forwards HTTP and WebSocket requests to a hidden upstream server. The log content is not published.

Workbench 2: OpenWrt router and stunnel backups

This host is in Germany and serves an open directory on port 9244. It mirrors 23 sites with 12,111 files in total, and was indexed on 18 November 2026.

File	Size (bytes)	Role
`stunnel_openwrt_config.tar.gz`	Not recorded	`stunnel` TLS wrapper configuration for an OpenWrt router
`backup-OpenWrt-2021-05-09.tar.gz`	Not recorded	Full OpenWrt router configuration backup; the file name carries the date 9 May 2021
`ss_socks.pac`	588,998	Proxy auto-configuration rules that route traffic through SOCKS
`XshellPortable.7z`	4,644,065	Portable SSH client

Wrapping a raw TCP or reverse-shell stream in `stunnel` on a small-office router adds TLS and a residential IP reputation. The operator gets both without changing the implant binary.

CHAPTER 06

Telling Hostile Infrastructure from Lookalikes

IN SHORT

Mail servers, a home broadband lease and dual-use testing tools with no second hostile signal stay off block lists.

INSIDE THIS CHAPTER

Mail-server lookalikes 19

Authorized testing 19

Dynamic home connections 19

What each group gets 19

06 Telling Hostile Infrastructure from Lookalikes

Before blocking, rule out three explanations: a shared mail server, an authorized test, or a dynamic home connection.

Mail-server lookalikes

Eight ReverseSSH matches sat on four hosts at an Italian hosting provider. Each host pairs POP3 (110) with POP3S (995), and all share one certificate and one JARM.

Five Hak5 Cloud C2 matches sat on one host at a Dutch hosting provider, on mail ports 110, 143, 465, 993 and 995, with one shared certificate. Blocking shared mail servers would cut legitimate email. None of these 13 addresses is published, and mail-port matches should never feed a block list.

Authorized testing

Hak5 Cloud C2 and ReverseSSH both have legitimate testing users. Three Hak5 instances carry `CN=pentest` certificates. Five standalone Hak5 controllers and two plain-HTTP ReverseSSH listeners are confirmed installs but show no second hostile signal. We send all of these to analyst review and withhold their addresses.

Dynamic home connections

One more ReverseSSH listener on 3232 sits on Korea Telecom broadband. It is counted as the one dynamic ISP lease, not among the 12 confirmed endpoints. Home addresses move between unrelated customers. It belongs on a watchlist that expires after 24 hours, not on a permanent block list.

What each group gets

Group	Endpoints	Action
Confirmed, with hostile context or a non-testing tool	5 (on 4 hosts)	Block
Confirmed dual-use tool, no second hostile signal	7	Analyst review
Mail-server lookalikes	13	Do not block
Dynamic ISP lease	1	24-hour watchlist
Suspected, including 3 `CN=pentest` Hak5 instances	9	Watch and look for a second signal
Candidates, including KeyPlug wolfSSL and ReverseSSH `CN=:3232` listeners	54	Hold until a wire or process alert corroborates them
Total	**89**	

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 five published endpoints at the perimeter: 146.190.211[.]163:8088, 77.111.101[.]84:8082, 77.111.101[.]84:8443, 165.154.199[.]52:443 and 156.240.52[.]178:8083.
- [ ] Keep mail-port matches (110, 143, 465, 993, 995) and dynamic ISP addresses out of automatic block feeds.
- [ ] Re-check cloud addresses before renewing a block, since VPS addresses get reassigned.

Within 72 hours

- [ ] Enforce 802.1X port-based access control and MAC-move alerts on branch closets, meeting rooms and wall jacks.
- [ ] Audit edge routers and Linux appliances for unapproved OpenWrt `stunnel` wrappers, `TokenFlow` binaries and Node.js `astr-proxy.js` forwarders.
- [ ] Alert on outbound sessions from servers to 3232, 10443, 10444 and 23590.

Within 7 to 30 days

- [ ] Deploy the Suricata signatures and add TLS inspection alerts for `CN=www.wolfssl[.]com`, `CN=:3232` and `CN=Gshell Server`.
- [ ] Enable the Sentinel query and the three Linux Sigma rules, with exact hostnames of your sanctioned test devices in the allowlist.
- [ ] Add the ReverseSSH JARM values and the GShellC2 JARM in this report to external attack surface hunting.
- [ ] Record your own authorized Hak5 and red-team infrastructure, so your SOC can clear its alerts fast.

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 other rules work 24

08 Detection Rules

The full rules are in Appendix B. Every rule file loads without errors in its engine (Suricata 7.0.12, YARA-X, pySigma, Kusto.Language); the rules were not replayed against live traffic.

Rule file	What it catches
`odin_hak5_reversessh_platypus_keyplug.rules`	Suricata 7: eight signatures for Hak5 Cloud C2 enrollment and controller responses, ReverseSSH WebSocket tunnels, Platypus, GShellC2, BlueShell and XorekC2 check-ins, and KeyPlug WebSocket transport
`sentinel_hak5_reversessh_and_keyplug_backdoor_hunt.kql`	Microsoft Sentinel and Defender XDR: contact with the four published hosts, and tunnel or backdoor ports joined with tunnel and proxy processes
`sigma_reversessh_keyplug_and_stunnel_persistence.yml`	Sigma (3 rules): ReverseSSH and Platypus clients, KeyPlug, BlueShell and XorekC2 daemons, and `stunnel` or `TokenFlow` relays on Linux
`odin_hak5_platypus_blueshell_keyplug_artifacts.yar`	YARA (4 rules): Hak5 Cloud C2 configs, ReverseSSH and Platypus manifests, GShellC2, BlueShell and XorekC2 configs, and KeyPlug, `TokenFlow` and `stunnel` relay files

How the Suricata signatures work

SID	Looks for	Why
9527001	Outbound `POST` to `/api/device/` with `"device_model"` in the body, on ports 80, 443, 8080, 8088 or 9090	Catches a Hak5 implant enrolling with its controller
9527002	A 200 response with `"cloudc2_edition"` followed by `"device_count"` in the body	Catches a Hak5 Cloud C2 controller answering a device
9527003	`/rssh/ws` in the URI with an `Upgrade: websocket` header	Catches a ReverseSSH tunnel moving onto WebSocket
9527004	`/api/client/` with an `X-Platypus-Auth:` header, on 23590, 443 or 8080	Catches Platypus API control
9527005	`POST /gshell/beacon` with a user agent that starts with `Gshell-Client`, on 8083 or 8080	Catches a GShellC2 check-in
9527006	`/blueshell/poll` with an `X-BlueShell-Node:` header	Catches BlueShell tasking polls
9527007	`POST /xorek/register` with `"session_xor"` in the body, on 5000 or 8443	Catches XorekC2 session registration
9527008	`/ws/keyplug` with a `Sec-WebSocket-Key:` header, on 443, 8443, 8888, 10443 or 10444	Catches KeyPlug WebSocket transport

These signatures need plaintext or decrypted HTTP. ReverseSSH in raw mode on 3232 and KeyPlug in binary mode on 10443 and 10444 skip HTTP framing. For those, pair Suricata with TLS certificate checks and endpoint data. Add explicit `pass` rules for your own sanctioned Hak5 exercises, because SIDs 9527001 and 9527002 also fire on legitimate use.

How the other rules work

The KQL query looks back 7 days. It flags any device that contacts the four published hosts, with no exclusion. It also flags `ssh`, `rssh`, `stunnel`, `node`, `curl` or `python3` connecting to the backdoor and tunnel ports listed above. It joins these with processes whose command lines name ReverseSSH, Platypus, GShellC2, BlueShell, KeyPlug, `TokenFlow`, `astr-proxy` or `stunnel`.

The port and process branches skip an exact list of approved test hostnames, which you replace with your own. Drop-boxes run no EDR agent, so catch them with 802.1X alerts and firewall logs.

Sigma rule	Fires when
Unapproved ReverseSSH or Platypus tunnel	A Linux command line contains `reverse_ssh`, :3232, :23590, `platypus-agent` or `gshell-client`, on a host outside the exact approved list
KeyPlug, BlueShell or XorekC2 daemon	A command line names `keyplug` with 10443 or 10444, `blueshell` with 8443 or 8081, `xorek` with 5000, or `/ws/keyplug`
Stunnel or TokenFlow relay	`stunnel`, `stunnel4`, `node` or the `tokenflow-linux-amd64` binary runs with `stunnel_openwrt`, `astr-proxy.js`, `astr-upstream.js` or `tokenflow-linux-amd64` in its arguments

YARA rule	Fires when
`ODIN_Hak5_CloudC2_Controller_Config`	`cloudc2_edition` or `c2-community-linux` appears with both `/api/device/` and `device_model`
`ODIN_ReverseSSH_Platypus_Multiplexer_Manifest`	`/rssh/ws`, `reverse_ssh` and 3232 appear together, or `X-Platypus-Auth`, `platypus-ingress` and 23590 appear together
`ODIN_GShell_BlueShell_Xorek_Backdoor_Config`	A matching pair appears: `Gshell Server` with `/gshell/beacon`, `/blueshell/poll` with `X-BlueShell-Node`, or `/xorek/register` with `session_xor`
`ODIN_KeyPlug_TokenFlow_Stunnel_Relay_Config`	`/ws/keyplug` with `www.wolfssl[.]com`, `tokenflow-linux-amd64` with `astr-proxy.js`, or `stunnel_openwrt_config`

All four YARA rules apply only to files under 512 KB.

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

MITRE ATT&CK tactics 26

09 Indicators

Appendix A holds 5 published indicators: 5 addresses (IP and port) on 4 hosts, and no hashes.

Endpoint	Family	Hosting	Key fingerprint	Seen
146.190.211[.]163:8088	Hak5 Cloud C2	DigitalOcean (US)	Hak5 console; GoPhish on the same host (Monograph 12)	13 Nov 2026
77.111.101[.]84:8082	ReverseSSH	Latitude.sh (BR)	Self-signed IP-literal certificate, JARM `3fd3fd0003fd...9a14`	14 Nov 2026
77.111.101[.]84:8443	ReverseSSH	Latitude.sh (BR)	Same certificate pattern and JARM	14 Nov 2026
165.154.199[.]52:443	ReverseSSH	Scloud Pte Ltd (SG)	Self-signed IP-literal certificate, JARM `3fd3fd0003fd...9a14`	13 Nov 2026
156.240.52[.]178:8083	GShellC2	HK Lightlayer (HK)	`CN=Gshell Server`, JARM `3fd3fd20d000...095c`	13 Nov 2026

Certificate subjects (`CN=Gshell Server`, `CN=:3232`, `CN=platypus-ingress`, `CN=www.wolfssl[.]com`) and JARM values stay in the text of Chapters 3 and 4.

Withheld: the five standalone Hak5 Cloud C2 controllers and the two plain-HTTP ReverseSSH listeners, which are confirmed installs of dual-use tools with no second hostile signal. Also withheld are the three `CN=pentest` hosts, the 13 mail-server lookalikes, the Korea Telecom lease, all suspected and candidate hosts, both relay workbenches, and every certificate domain.

MITRE ATT&CK tactics

This report maps the families to tactics only, not to technique IDs.

Tactic	How the families use it	Detection
Initial Access	Hak5 implants plugged into unattended Ethernet jacks or closets	802.1X alerts; SID 9527001
Persistence	ReverseSSH, KeyPlug, BlueShell and XorekC2 agents on Linux and Windows hosts	Sigma rules 1 and 2; YARA rules
Command and Control	Outbound HTTP, WebSocket and TLS sessions to cloud controllers, through `stunnel` or `TokenFlow` relays	SIDs 9527001 to 9527008; KQL; Sigma rule 3

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 18 November 2026, with data up to 19 November 2026. Some records carry earlier first-seen dates from public sources. We do not use those as a tracking start.
- **Outside view only.** We saw controllers, listeners and open directories from the internet. We saw nothing inside any target network, and no intrusion is described here.
- **Confirmed is not the same as hostile.** A confirmed endpoint runs the software. Hak5 Cloud C2 and ReverseSSH have many legitimate testing users, so 7 confirmed endpoints are withheld for lack of a second hostile signal.
- **Candidates are leads.** The 54 candidates and 9 suspected endpoints rest on one or a few signals. Do not block them without corroboration.
- **The four-layer view is a model.** No host runs two families, and nothing in the data links the relay workbenches to a specific controller.
- **Family names are signature labels.** They describe what the software looks like. They are not attribution to any actor.
- **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. Hak5. Cloud C2 documentation. https://docs.hak5.org/cloud-c2/ (verified 19 November 2026)
2. NHAS. ReverseSSH repository. https://github.com/NHAS/reverse_ssh (verified 19 November 2026)
3. WangYihang. Platypus repository. https://github.com/WangYihang/Platypus (verified 19 November 2026)
4. wolfSSL Inc. wolfSSL manual. https://www.wolfssl.com/docs/wolfssl-manual/ (verified 19 November 2026)
5. Stunnel project. Documentation. https://www.stunnel.org/docs.html (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 (5) 32

B. Detection rules (4 files) 33

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
R27-IOC-01	IPv4	146.190.211[.]163	8088	Hak5 Cloud C2 controller	BLOCK
R27-IOC-02	IPv4	77.111.101[.]84	8082	ReverseSSH listener	BLOCK
R27-IOC-03	IPv4	77.111.101[.]84	8443	ReverseSSH listener	BLOCK
R27-IOC-04	IPv4	165.154.199[.]52	443	ReverseSSH listener	BLOCK
R27-IOC-05	IPv4	156.240.52[.]178	8083	gshellc2	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_hak5_platypus_blueshell_keyplug_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 27 / 30 YARA Artifact Suite
   Scope: Sanitized configuration and binary metadata strings for Hak5 Cloud C2,
          ReverseSSH/Platypus, GShellC2/BlueShell/XorekC2, and KeyPlug/Relay workbenches.
   Classification: TLP:CLEAR
*/

rule ODIN_Hak5_CloudC2_Controller_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "27 / 30"
        classification = "TLP:CLEAR"
        use = "hunting and analyst review"
        description = "Matches Hak5 Cloud C2 server or drop-box enrollment configuration manifests"
    strings:
        $h1 = "cloudc2_edition" ascii nocase
        $h2 = "c2-community-linux" ascii nocase
        $d1 = "/api/device/" ascii
        $d2 = "device_model" ascii nocase
    condition:
        filesize < 512KB and ($h1 or $h2) and $d1 and $d2
}

rule ODIN_ReverseSSH_Platypus_Multiplexer_Manifest
{
    meta:
        author = "Odin by Brandefense"
        monograph = "27 / 30"
        classification = "TLP:CLEAR"
        use = "hunting and analyst review"
        description = "Matches ReverseSSH (:3232) and Platypus (:23590) multiplexer configs"
    strings:
        $r1 = "/rssh/ws" ascii
        $r2 = "reverse_ssh" ascii nocase
        $p1 = "X-Platypus-Auth" ascii
        $p2 = "platypus-ingress" ascii nocase
        $port1 = "3232" ascii
        $port2 = "23590" ascii
    condition:
        filesize < 512KB and (($r1 and $r2 and $port1) or ($p1 and $p2 and $port2))
}

rule ODIN_GShell_BlueShell_Xorek_Backdoor_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "27 / 30"
        classification = "TLP:CLEAR"
        use = "hunting and analyst review"
        description = "Matches GShellC2, BlueShell, or XorekC2 controller configuration artifacts"
    strings:
        $g1 = "Gshell Server" ascii
        $g2 = "/gshell/beacon" ascii
        $b1 = "/blueshell/poll" ascii
        $b2 = "X-BlueShell-Node" ascii
        $x1 = "/xorek/register" ascii
        $x2 = "session_xor" ascii
    condition:
        filesize < 512KB and (($g1 and $g2) or ($b1 and $b2) or ($x1 and $x2))
```

```
}

rule ODIN_KeyPlug_TokenFlow_Stunnel_Relay_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "27 / 30"
        classification = "TLP:CLEAR"
        use = "hunting and analyst review"
        description = "Matches KeyPlug wolfSSL configs and TokenFlow/OpenWrt stunnel relay manifests"
    strings:
        $k1 = "/ws/keyplug" ascii
        $k2 = "www.wolfssl.com" ascii
        $t1 = "tokenflow-linux-amd64" ascii
        $t2 = "astr-proxy.js" ascii
        $s1 = "stunnel_openwrt_config" ascii
    condition:
        filesize < 512KB and (($k1 and $k2) or ($t1 and $t2) or $s1)
}
```

odin_hak5_reversessh_platypus_keyplug.rules

SURICATA

```
# Odin by Brandefense - Monograph 27 / 30 Suricata 7.x Detection Suite
# Coverage: Hak5 Cloud C2, ReverseSSH, Platypus, GShellC2, BlueShell, XorekC2, KeyPlug
# Classification: TLP:CLEAR

alert http $HOME_NET any -> $EXTERNAL_NET [80,443,8080,8088,9090] (msg:"ODIN [R27] Hak5 Cloud C2 Hardware Drop-
Box Enrollment Sync"; flow:established,to_server; http.method; content:"POST"; http.uri; content:"/api/device/";
fast_pattern; http.request_body; bsize:>24; content:"\"device_model\""; classtype:trojan-activity; sid:9527001;
rev:1; metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $EXTERNAL_NET [80,443,8080,8088,9090] -> $HOME_NET any (msg:"ODIN [R27] Hak5 Cloud C2 Controller State
Response"; flow:established,from_server; http.stat_code; content:"200"; http.response_body; bsize:>28;
content:"\"cloudc2_edition\""; fast_pattern; content:"\"device_count\""; distance:0; classtype:trojan-activity;
sid:9527002; rev:1; metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [80,443,3232,8080,8082,8443] (msg:"ODIN [R27] ReverseSSH Multiplexed
WebSocket Tunnel Upgrade"; flow:established,to_server; http.uri; content:"/rssh/ws"; fast_pattern; http.header;
bsize:>18; content:"Upgrade: websocket"; classtype:trojan-activity; sid:9527003; rev:1; metadata:created_at
2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [23590,443,8080] (msg:"ODIN [R27] Platypus Go Reverse-Shell Multiplexer
API Control"; flow:established,to_server; http.uri; content:"/api/client/"; fast_pattern; http.header; bsize:>16;
content:"X-Platypus-Auth:"; classtype:trojan-activity; sid:9527004; rev:1; metadata:created_at 2026_11_19,
deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [8083,8080] (msg:"ODIN [R27] GShellC2 Reverse-Shell Beacon Check-In";
flow:established,to_server; http.method; content:"POST"; http.uri; content:"/gshell/beacon"; fast_pattern;
http.user_agent; bsize:>12; content:"Gshell-Client"; startswith; classtype:trojan-activity; sid:9527005; rev:1;
metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [8443,8081,443] (msg:"ODIN [R27] BlueShell Cross-Platform Backdoor
Tasking Poll"; flow:established,to_server; http.uri; content:"/blueshell/poll"; fast_pattern; http.header;
bsize:>18; content:"X-BlueShell-Node:"; classtype:trojan-activity; sid:9527006; rev:1; metadata:created_at
2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [5000,8443] (msg:"ODIN [R27] XorekC2 Port 5000 Session Registration";
flow:established,to_server; http.method; content:"POST"; http.uri; content:"/xorek/register"; fast_pattern;
http.request_body; bsize:>20; content:"\"session_xor\""; classtype:trojan-activity; sid:9527007; rev:1;
metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)

alert http $HOME_NET any -> $EXTERNAL_NET [443,8443,8888,10443,10444] (msg:"ODIN [R27] KeyPlug WebSocket
Transport and TokenFlow Relay Check-In"; flow:established,to_server; http.uri; content:"/ws/keyplug";
fast_pattern; http.header; bsize:>18; content:"Sec-WebSocket-Key:"; classtype:trojan-activity; sid:9527008; rev:
1; metadata:created_at 2026_11_19, deployment perimeter, tactic command_and_control;)
```

sentinel_hak5_reversessh_and_keyplug_backdoor_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 27 / 30 Microsoft Sentinel & Defender XDR Hunt
// Correlates egress to confirmed Hak5 Cloud C2, ReverseSSH and GShellC2 hosts, and backdoor or tunnel ports,
with tunnel and proxy processes
// Classification: TLP:CLEAR
// ApprovedRedTeamHosts: replace the example names with the exact hostnames of your own sanctioned test devices.
// The allowlist applies only to the port and process branches; a match on a confirmed IP always alerts.

let Lookback = 7d;
let ApprovedRedTeamHosts = dynamic(["REDTEAM-DROPBOX-LAB-01", "NETSEC-BASTION-01"]);
let ConfirmedBackdoorIPs = dynamic([
    "146.190.211.163", "77.111.101.84", "165.154.199.52", "156.240.52.178"
]);
let BackdoorAndMuxPorts = dynamic([3232, 5000, 8080, 8081, 8082, 8083, 8088, 8443, 8888, 9090, 9244, 10443,
10444, 23590]);
let UnapprovedTunnelProcs = DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedRedTeamHosts))
    | where ProcessCommandLine has_any ("c2-community", "reverse_ssh", "rssh", "platypus", "gshell", "blueshell",
"keyplug", "tokenflow", "astr-proxy", "stunnel")
        or (FileName in~ ("ssh", "stunnel", "node", "nohup") and ProcessCommandLine has_any ("-R ", "3232",
"10443", "23590", "astr-upstream"))
    | project ProcTime = Timestamp, DeviceId, DeviceName, FileName, ProcessCommandLine;
DeviceNetworkEvents
| where Timestamp >= ago(Lookback)
| where RemoteIP in (ConfirmedBackdoorIPs)
    or (not(DeviceName in~ (ApprovedRedTeamHosts))
        and RemotePort in (BackdoorAndMuxPorts)
        and InitiatingProcessFileName in~ ("ssh", "rssh", "stunnel", "node", "curl", "python3"))
| summarize
    NetFirstSeen = min(Timestamp),
    NetLastSeen = max(Timestamp),
    DistinctRemoteIPs = dcount(RemoteIP),
    DistinctPorts = make_set(RemotePort, 16),
    MatchedConfirmedIPs = make_set_if(RemoteIP, RemoteIP in (ConfirmedBackdoorIPs), 16),
    ConnectionCount = count()
    by DeviceId, DeviceName, InitiatingProcessFileName
| join kind=leftouter (UnapprovedTunnelProcs) on DeviceId, DeviceName
| where array_length(MatchedConfirmedIPs) > 0 or isnotempty(ProcessCommandLine) or ConnectionCount >= 20
| extend AlertDisposition = case(
    array_length(MatchedConfirmedIPs) > 0, "CONFIRMED_DROPBOX_RSSH_OR_GSHELL_C2_CONTACT",
    ProcessCommandLine has_any ("stunnel", "astr-proxy", "tokenflow"), "HUNT_TLS_OR_UPSTREAM_PROXY_RELAY",
    "HUNT_MULTIPLEXED_BACKDOOR_EGRESS"
)
| project NetFirstSeen, NetLastSeen, DeviceName, AlertDisposition, MatchedConfirmedIPs, DistinctRemoteIPs,
DistinctPorts, InitiatingProcessFileName, ProcessCommandLine, ConnectionCount
| sort by ConnectionCount desc
```

sigma_reversessh_keyplug_and_stunnel_persistence.yml

SIGMA

```
title: Unapproved ReverseSSH or Platypus Multiplexed Tunnel Execution
id: 4c8e21a9-7d10-4b62-9f35-202611192701
status: experimental
description: Detects execution of ReverseSSH or Platypus multiplexed reverse-shell clients binding persistent
outbound control channels on Linux hosts.
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.command_and_control
  - attack.persistence
logsource:
  category: process_creation
  product: linux
detection:
  selection_cli:
```

```
    CommandLine|contains:
      - 'reverse_ssh'
      - ':3232'
      - ':23590'
      - 'platypus-agent'
      - 'gshell-client'
  filter_bastions:
    ComputerName:
      - 'REDTEAM-DROPBOX-LAB-01'
      - 'NETSEC-BASTION-01'
  condition: selection_cli and not filter_bastions
falsepositives:
  - Sanctioned bastion or red-team validation hosts listed in asset inventory
level: high
---
title: KeyPlug BlueShell or XorekC2 Cross-Platform Backdoor Daemon Launch
id: 8b1f40c3-2a65-4e91-a712-202611192702
status: experimental
description: Identifies unapproved Linux daemon execution consistent with KeyPlug (:10443/:10444), BlueShell (:
8443/:8081), or XorekC2 (:5000) implants.
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.command_and_control
  - attack.persistence
logsource:
  category: process_creation
  product: linux
detection:
  selection_backdoor:
    CommandLine|re: '(keyplug.*1044[34]|blueshell.*(8443|8081)|xorek.*5000|/ws/keyplug)'
  filter_lab:
    ComputerName:
      - 'REDTEAM-DROPBOX-LAB-01'
  condition: selection_backdoor and not filter_lab
falsepositives:
  - Isolated malware-analysis sandboxes registered with security operations
level: high
---
title: Unapproved Stunnel TLS Wrapper or TokenFlow Proxy Relay Persistence
id: 9d5a37e6-6c04-43f8-b829-202611192703
status: experimental
description: Detects stunnel TLS wrapper daemons or Node.js TokenFlow upstream proxy relays (astr-proxy.js /
astr-upstream.js) forwarding C2 traffic.
author: Odin by Brandefense
date: 2026/11/19
tags:
  - attack.command_and_control
  - attack.persistence
logsource:
  category: process_creation
  product: linux
detection:
  selection_runtime:
    Image|endswith:
      - '/stunnel'
      - '/stunnel4'
      - '/node'
      - '/tokenflow-linux-amd64'
  selection_args:
    CommandLine|contains:
      - 'stunnel_openwrt'
      - 'astr-proxy.js'
      - 'astr-upstream.js'
      - 'tokenflow-linux-amd64'
  filter_gateways:
    ComputerName:
      - 'NETSEC-BASTION-01'
  condition: selection_runtime and selection_args and not filter_gateways
falsepositives:
  - Authorized TLS termination proxies documented by network engineering
level: medium
```

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/drop-box-hubs-and-reverse-tunnels/
Short Read · brandefense.io/odin-research/blog/drop-boxes-reverse-tunnels-and-backdoors/
Defense Kit · brandefense.io/odin-research/defense-kit/