ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 22 / 30 · C2 INFRASTRUCTURE

Shared Team C2 Consoles

SuperShell, AdaptixC2, Caldera and Viper in the Open

How browser shell consoles, plugin teamservers and emulation planners are deployed, and which of them to block

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

718 / 537
Endpoints and distinct hosts across ten team C2 and emulation frameworks

34 / 25
Confirmed C2 endpoints and the addresses they sit on (SuperShell, ToShellC2, Metasploit, Meterpreter)

18
Confirmed addresses published for blocking; 7 addresses in one German business-ISP cluster are withheld

180
SuperShell endpoints; 2 confirmed on port 8888, 169 suspected in one Hong Kong cluster

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

How browser shell consoles, plugin teamservers and emulation planners are deployed, and which of them to block

01	Executive Summary	04
02	Ten Frameworks, Three Workflows	07
03	Browser Shell Consoles and Metasploit Workbenches	10
04	Plugin Teamservers and Emulation Planners	14
05	Container Stacks and an Exposed Metasploit Directory	18
06	Look-Alikes: What Not to Block	21
07	What Defenders Should Do	24
08	Detection Rules	26
09	Indicators	29
10	Scope and Limits	32
11	Sources	34
A	Indicators of compromise (18)	36
B	Detection rules (4 files)	37

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 718 endpoints on 537 hosts running ten team command-and-control (C2) and adversary-emulation frameworks. Only 34 endpoints, on 25 addresses, are confirmed C2: SuperShell, ToShellC2, Metasploit and Meterpreter. Caldera, AdaptixC2 and the rest stay on watchlists, because labs, appliances and mail servers look alike. Block the 18 published confirmed addresses, and pair port alerts with in-memory process signals.

01

CHAPTER 01

Executive Summary

IN SHORT

In a two-week observation window ending 18 November 2026, Odin by Brandefense mapped 718 endpoints on 537 hosts running ten team command-and-control (C2) and adversary-emulation frameworks. Only 34 endpoints, on 25 addresses, are confirmed C2: SuperShell, ToShellC2, Metasploit and Meterpreter. Caldera, AdaptixC2 and the rest stay on watchlists, because labs, appliances and mail servers look alike. Block the 18 published confirmed addresses, and pair port alerts with in-memory process signals.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Team C2 frameworks let several operators share one attack server. They bundle reverse shells, payload builders, a task database and a web or desktop console into one Docker stack. This report maps where these consoles run, how each framework works, and which listeners are safe to block.

1. **Browser shell consoles hold all 34 confirmed C2 endpoints.**
   SuperShell (2), ToShellC2 (10), Metasploit (17) and Meterpreter (5) make up the confirmed set. Viper, a browser front end for Metasploit, sits on top of these. These consoles wrap reverse SSH and Metasploit sessions in shared web terminals.

2. **Plugin teamservers move post-exploitation into memory.**
   AdaptixC2 runs on 101 endpoints, 35 of them on its default port 4321. It loads listener and agent plugins and runs Beacon Object Files (BOFs) in memory. PyramidC2 uses signed Python interpreters to load offensive packages without writing them to disk.

3. **Emulation planners and look-alikes need watchlists, not blocks.**
   MITRE Caldera shows 257 endpoints, but 239 are banner look-alikes on a security vendor's address space. The other 18 sit on cloud hosts. Purple teams run the same Caldera agents, so no Caldera address is published.

Three Decisions for Leaders

1. **Block confirmed shell consoles, watch dual-use tools.** Block the 18 published confirmed SuperShell, ToShellC2, Metasploit and Meterpreter addresses, and re-check them after 30 days. Route Caldera, Starkiller and unconfirmed AdaptixC2 listeners to analyst watchlists.
2. **Join network alerts with memory signals.** Connect workstation traffic to teamserver ports (3001, 3232, 4321, 8888, 18081) with memory allocation, unbacked .NET module loads or signed Python network activity within ten minutes.
3. **Register and lock down your own emulation servers.** List every sanctioned Caldera, Viper, Empire and Metasploit host in your SIEM allowlists. Put their consoles behind mutual TLS or a VPN, and turn off directory listing on staging servers.

The Study in Numbers

Number	What it is
718 / 537	Endpoints and distinct hosts across ten team C2 and emulation frameworks
34 / 25	Confirmed C2 endpoints and the addresses they sit on (SuperShell, ToShellC2, Metasploit, Meterpreter)
18	Confirmed addresses published for blocking; 7 addresses in one German business-ISP cluster are withheld
180	SuperShell endpoints; 2 confirmed on port 8888, 169 suspected in one Hong Kong cluster
101 / 89	AdaptixC2 endpoints and hosts; 35 endpoints use default port 4321
257 / 239	MITRE Caldera endpoints, and how many of them are vendor banner look-alikes
569	Entries in an exposed Metasploit installation directory on one unattributed server

How to use this report.

Security leaders can read Chapter 1, Chapter 6 and Chapter 7. SOC and detection engineers should start with Chapters 7 to 9. CTI analysts will find framework and infrastructure detail in Chapters 2 to 5.

02

CHAPTER 02

Ten Frameworks, Three Workflows

IN SHORT

The 718 endpoints fall into three working styles: browser shell consoles, plugin teamservers and automated emulation planners. Grouping them this way shows how a shared team splits shell handling, modular evasion and lateral planning.

INSIDE THIS CHAPTER

The ten frameworks 08

Status across all endpoints 08

Where they run 08

02 Ten Frameworks, Three Workflows

Defenders often expect a reverse shell to look like a raw `netcat` stream. Modern team frameworks look different. They package shell multiplexers, compilers, a task database and role-based web consoles in Docker Compose stacks. Several operators then share the same stack at once. What the targets of these servers experienced is not visible from the server side.

Figure 1 is an analytical model. It groups the frameworks into three workflows that meet at the target's memory. It does not show one actor commanding all three.

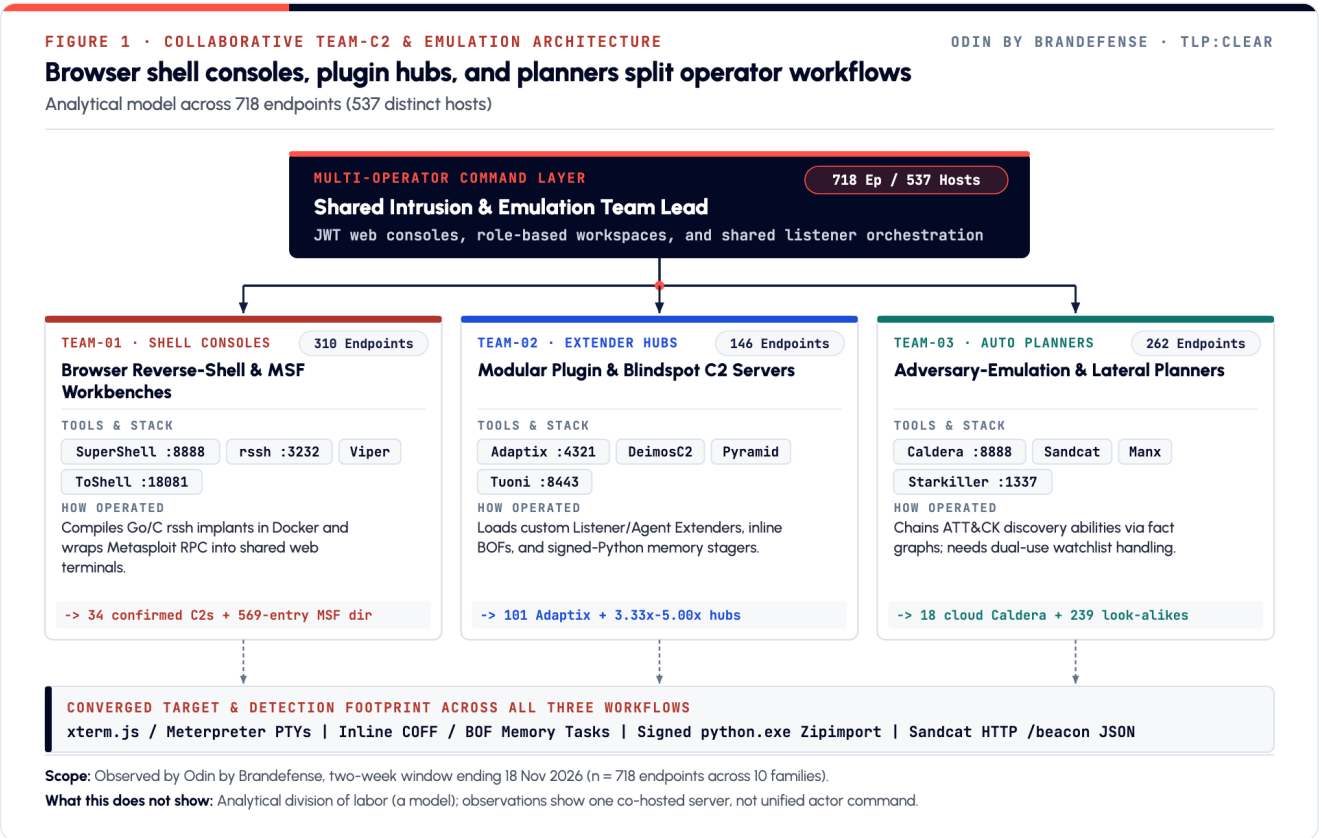


Figure 1: Browser shell consoles, plugin hubs, and planners split operator workflows

The ten frameworks

Endpoints count each distinct address and port once. Viper has no endpoints of its own, because it drives Metasploit and Meterpreter listeners rather than exposing its own implant protocol.

Framework	What it is	Endpoints (hosts)	Ports per host	Confirmed
MITRE Caldera	Automated emulation planner	257 (135)	1.90x	0
SuperShell	Browser reverse-SSH console	180 (180)	1.00x	2
AdaptixC2	Plugin-based teamserver	101 (89)	1.13x	0
Metasploit	Exploit and C2 framework	75 (65)	1.15x	17
ToShellC2	Browser shell controller	37 (33)	1.12x	10
DeimosC2	Go and Vue team C2	30 (6)	5.00x	0
Meterpreter	Staged implant handler	18 (18)	1.00x	5
PyramidC2	Signed-Python in-memory C2	10 (3)	3.33x	0
TuoniC2	Containerized plugin C2	5 (4)	1.25x	0
Starkiller	Multi-operator Empire console	5 (5)	1.00x	0

The per-framework host counts add up to 538, not 537. One Alibaba Cloud server in China runs both AdaptixC2 and ToShellC2.

Status across all endpoints

Status	Endpoints	Share
Confirmed C2	34	4.7%
Suspected C2	541	75.3%
Candidate	138	19.2%
Dynamic consumer ISP, short watchlist	4	0.6%
Dual-use emulation tooling	1	0.1%

Where they run

Browser shell consoles cluster in East and Southeast Asia. SuperShell places 171 of 180 endpoints (95.0%) in Hong Kong and 6 in China. ToShellC2 places 26 of 37 (70.3%) in China (14) and Hong Kong (12).

AdaptixC2 and Metasploit spread across Western and Asian VPS providers alike.

Framework	Top countries (endpoints)
AdaptixC2	US 19, HK 15, CN 13, SG 10, RU 7, DE 5
Metasploit	DE 19, HK 11, MA 8, SG 7, FR 5, US 5, AU 5

03

CHAPTER 03

Browser Shell Consoles and Metasploit Workbenches

IN SHORT

Browser shell platforms account for all 34 confirmed C2 endpoints. They wrap reverse-SSH tunnels and Metasploit RPC sessions in shared web dashboards, so one server serves a whole team.

INSIDE THIS CHAPTER

SuperShell and its embedded rssh listener 10

ToShellC2 11

Viper, Metasploit and Meterpreter 11

03 Browser Shell Consoles and Metasploit Workbenches

Browser consoles remove manual listener work. A single Docker command brings up a web terminal (`xterm.js`), payload cross-compilers, SOCKS5 pivots and a file browser. Operators log in through a JWT-protected portal and share live shells with each other.

Figure 2 maps each framework from server port to implant behaviour, target surface and the matching detection rule.

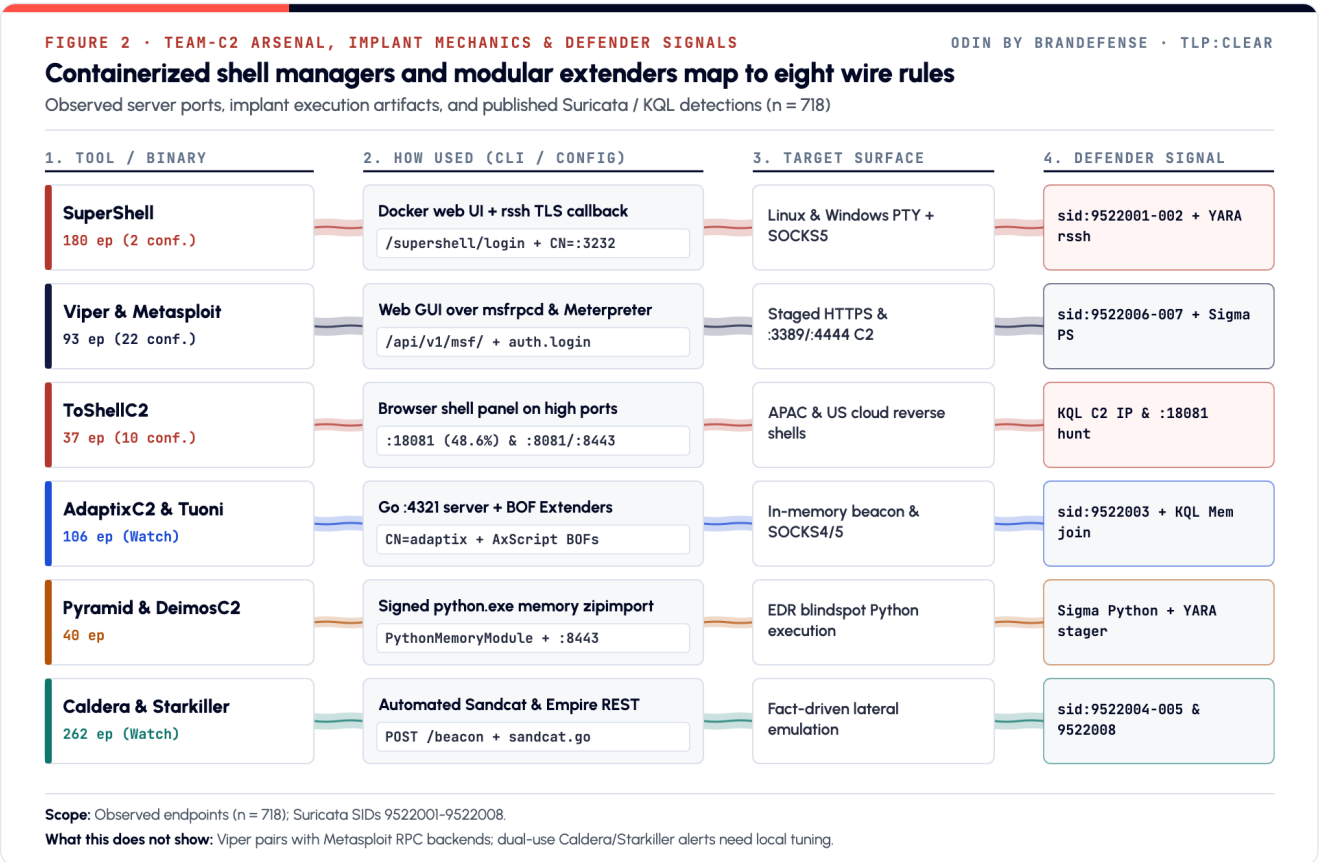


Figure 2: Containerized shell managers and modular extenders map to eight wire rules

SuperShell and its embedded rssh listener

SuperShell (`tdragon6/supershell`) bundles a Flask and Nginx management portal with a reverse SSH (`rssh`) multiplexer.

Component	Default	Detail
Web portal	Port 8888	JWT login under `/supershell/login`
`rssh` listener	Port 3232	TLS-wrapped SSH with a self-signed certificate `CN=:3232`
Implant builder	In the browser	Statically linked Go or C implants for Windows and Linux

The implant dials out over TLS-wrapped SSH. The operator gets a browser terminal, file transfer, SOCKS5 tunnelling and shellcode injection. No inbound port needs to be open on the target.

The 180 SuperShell endpoints fall into three groups.

Group	Endpoints	Ports and TLS	Hosting	Status
Confirmed consoles	2	8888	Shenzhen Tencent (CN), Cloudie Limited (HK)	Block
Hong Kong 443 cluster	169	443, JARM prefixes `21d14d..` and `3fd3fd..`	LUOGELANG (FRANCE) LIMITED (HK)	Suspected, watchlist
Other candidates	8 candidate + 1 suspected	8888 (7), 18888 (1), 8443 (1); `CN=:3232` on 2	Alibaba, Tencent, Huawei, Cloudie	Watchlist

The two confirmed consoles are 111.229.193[.]140:8888 and 103.115.57[.]195:8888.

Two candidate consoles in China present SuperShell's default `rssh` certificate `CN=:3232`. They share JARM `3fd3fd20d3fd3fd00043d3fd3fd43d5ecfbe778b06e32b538bd51f24eb7398`. A third candidate uses a Chinese-language certificate name meaning "inventory management system". Their addresses are withheld.

ToShellC2

ToShellC2 is a lightweight web reverse-shell panel. It shows 37 endpoints on 33 hosts. Port 18081 carries 18 candidates (48.6%), and port 8081 carries 4 confirmed endpoints.

Ten ToShellC2 endpoints on 8 addresses are confirmed. Two of these servers listen on two ports each.

Endpoint	Hosting	Note
186.244.231[.]115:80 and :8080	CLOUDVALLEY SDN. BHD. (US)	Dual-port controller
185.207.154[.]238:8081 and :8443	Cloudie Limited (HK)	Dual-port, third-party certificate subject withheld
186.244.215[.]55:443	Uscloud Inc (US)	`CN=fileserver`

The full list of confirmed ToShellC2 addresses is in Chapter 9.

Viper, Metasploit and Meterpreter

Viper (`FunnyWolf/Viper`) puts a React and Ant Design multi-operator interface and an ATT&CK module runner on top of Metasploit. It talks to the Metasploit RPC daemon `msfrpcd`, which accepts `auth.login` calls over MessagePack.

Across 75 Metasploit endpoints (65 hosts) and 18 Meterpreter endpoints (18 hosts), 22 are confirmed C2. They form three groups.

Group	Confirmed endpoints	Addresses	Detail
German dual-port cluster on a business ISP	14 (7 addresses)	Withheld	Each binds Metasploit listeners on 443 and 80 and shares one third-party company certificate
Metasploit team listeners on 3001	3	77.83.36[.]163 (Layer7 Networks, SC), 185.254.199[.]160 (SOLLUTIUM EU, NL), 77.91.71[.]99 (hosting network, IL)	Standalone 3001 listeners
Meterpreter handlers	5	See table below	Includes one handler on the RDP port

Meterpreter handler	Hosting	Note
65.38.121[.]42:3389	BL Networks (RO)	TLS Meterpreter on the RDP port, `CN=6a47718162def1c`
181.215.18[.]135:8443	Datacamp (HK)	Reverse-HTTPS handler
190.2.184[.]47:4444	MASTER DA WEB (BR)	Default Meterpreter port
8.148.31[.]135:4446	Alibaba Cloud (CN)	Non-default TCP port
154.89.152[.]104:10003	CLOUDVALLEY (HK)	High-port handler

Binding Meterpreter to 3389 makes the traffic look like Remote Desktop at a glance. Four more suspected Meterpreter hosts on Tencent Cloud port 443 share the default cloud image certificate `CN=VM-0-4-centos`. They stay on the watchlist.

04

CHAPTER 04

Plugin Teamservers and Emulation Planners

IN SHORT

AdaptixC2, DeimosC2, PyramidC2 and TuoniC2 (146 endpoints) favour loadable plugins, in-memory BOFs and signed-Python loaders. Caldera and Starkiller (262 endpoints) automate ATT&CK-style lateral planning. All 408 stay on watchlists.

INSIDE THIS CHAPTER

AdaptixC2 14

PyramidC2, TuoniC2 and DeimosC2 15

MITRE Caldera and Starkiller 15

04 Plugin Teamservers and Emulation Planners

Plugin teamservers separate the core server from its transport and implant modules. An operator can swap HTTP, SMB, DNS or TCP listeners without rebuilding the backend. This also makes static signatures age quickly.

Figure 3 is a synthesized model built from the public documentation of each tool. It shows six protocol and memory steps and the defender signal for each. No single intrusion log links all six steps.

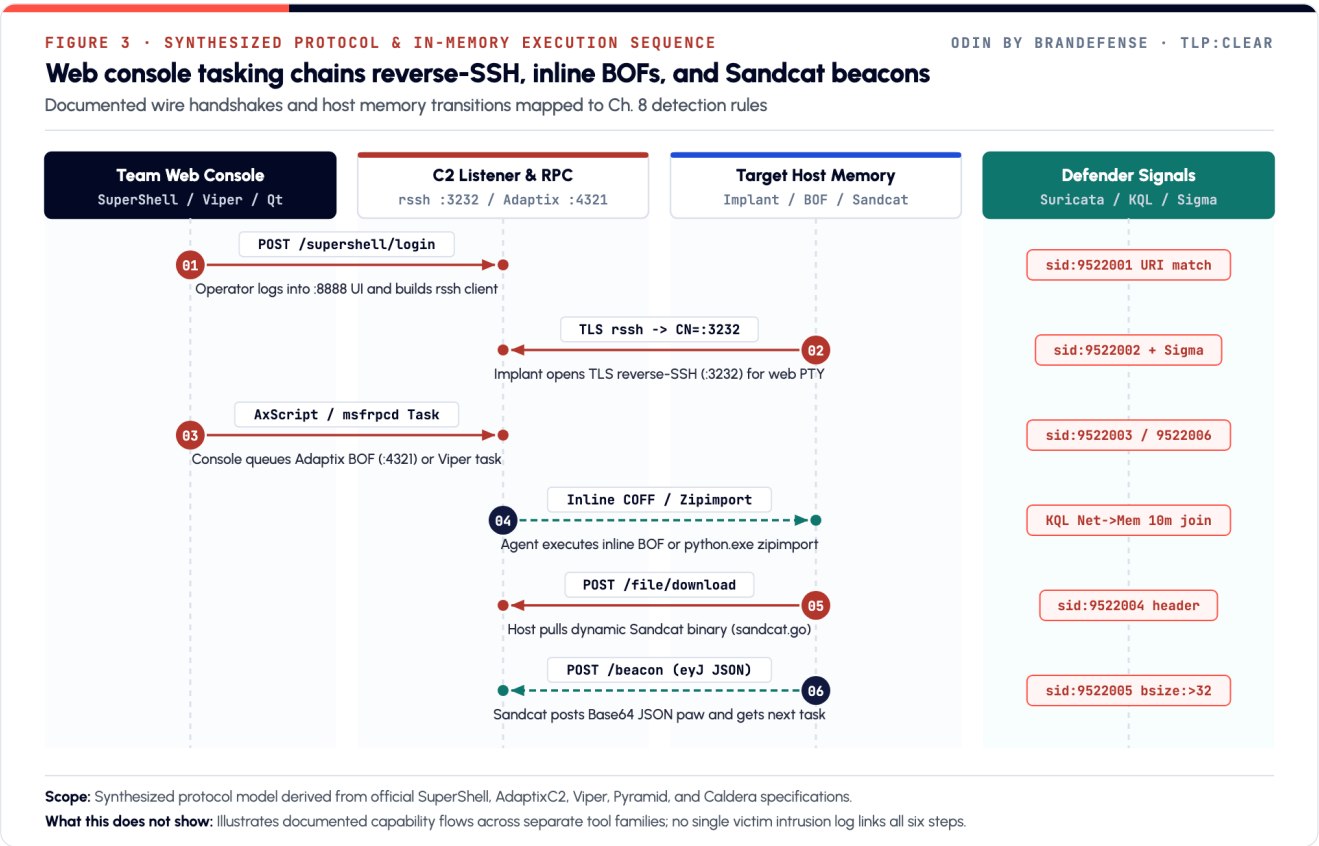


Figure 3: Web console tasking chains reverse-SSH, inline BOFs, and Sandcat beacons

AdaptixC2

AdaptixC2 pairs a Go teamserver with a C++ and Qt operator client. It loads protocols and implants as "Extenders" (`ExtenderListener` and `ExtenderAgent`), scripted in `AxScript`. Operators can run BOFs inline (`execute bof`) and pivot through SOCKS4 or SOCKS5.

The 101 AdaptixC2 endpoints on 89 hosts break down as 32 suspected, 68 candidates and 1 node on a dynamic Chinanet line. None is confirmed.

Signal	Endpoints
Default port 4321	35 (34.7%)
Port 443 / 4444 / 8443 / 4443 / 43211	7 / 6 / 4 / 3 / 3
Go TLS JARM `29d29d00000000000043d43d00043dc3b2afa8a5ec09b510a8559aff7899fb`	21
`CN=localhost`	11
`CN=adaptix` / `CN=adaptix.local` / `CN=adaptix-server`	4 / 2 / 1
Spoofed `CN=AnyDesk Client` (US)	1

Default certificates give many deployments away. Some servers also bind several ports: one host in India uses 4444, 4445 and 50003, and one in Switzerland uses 4322 and 4323. A DigitalOcean host in Singapore pairs the 4321 management port with a 4444 beacon port. These addresses are withheld.

PyramidC2, TuoniC2 and DeimosC2

Framework	Endpoints (hosts)	How it works	What we saw
PyramidC2	10 (3), 3.33x	Uses signed `python.exe` or `pythonw.exe` to fetch and import offensive packages (such as BloodHound and `secretsdump`) in memory through `zipimport` and `PythonMemoryModule`, with no `.pyd` DLL on disk	An Akamai US listener on 8080; a three-port host on a German consumer ISP; a six-port OVH host in France whose other five ports are mail ports
TuoniC2	5 (4), 1.25x	Dockerized red-team suite with plugins	All 4 TLS instances on 8443 (RU, DE, TR) share `CN=localhost` and JARM `07d3fd16d21d21d00042d43d00041ddb04deffa1705e2edc44cae1ed24a4da`; the Russian host also exposes 12702
DeimosC2	30 (6), 5.00x	Go and Vue team C2	1 German candidate on 8443; the other 29 are mail and FTP ports on 5 OVH hosts in Canada and Chile (see Chapter 6)

PyramidC2 is built to work inside endpoint detection blind spots. A signed Python interpreter is often trusted, so the loaded code inherits that trust.

MITRE Caldera and Starkiller

MITRE Caldera automates post-compromise decisions. It pairs a Go HTTP agent, Sandcat (also written `54ndc47`), and a TCP reverse-shell agent, Manx, with planners driven by collected facts.

1. The target sends `POST /file/download` with the header `file: sandcat.go`.
2. The server compiles a fresh Go binary that embeds the `server` and `group` values, so the agent's command line can stay clean.
3. The agent then exchanges Base64-encoded JSON (starting with `eyJ`) over `POST /beacon` and receives its next task.

Caldera shows 257 endpoints on 135 hosts. Chapter 6 explains why 239 of them are look-alikes.

Five Starkiller nodes run multi-user consoles for PowerShell Empire (MITRE S0363), which logs operators in through `/api/v2/users/login`. Two use the Empire REST port 1337 (US and FI). Three use port 80 on OVH in France.

05

CHAPTER 05

Container Stacks and an Exposed Metasploit Directory

IN SHORT

Port layouts and one open directory show how team C2 backends are packaged on cloud servers. An unattributed server in India exposed the full internal Metasploit installation tree.

INSIDE THIS CHAPTER

The exposed Metasploit installation 18

Co-hosting and multi-port layouts 19

05 Container Stacks and an Exposed Metasploit Directory

A port banner shows which listener answers. A directory tree or a multi-port layout shows how the server was built. Figure 4 is a composite view across separate servers. It combines the SuperShell, `rssh`, AdaptixC2 and Caldera layers with the exposed Metasploit tree.

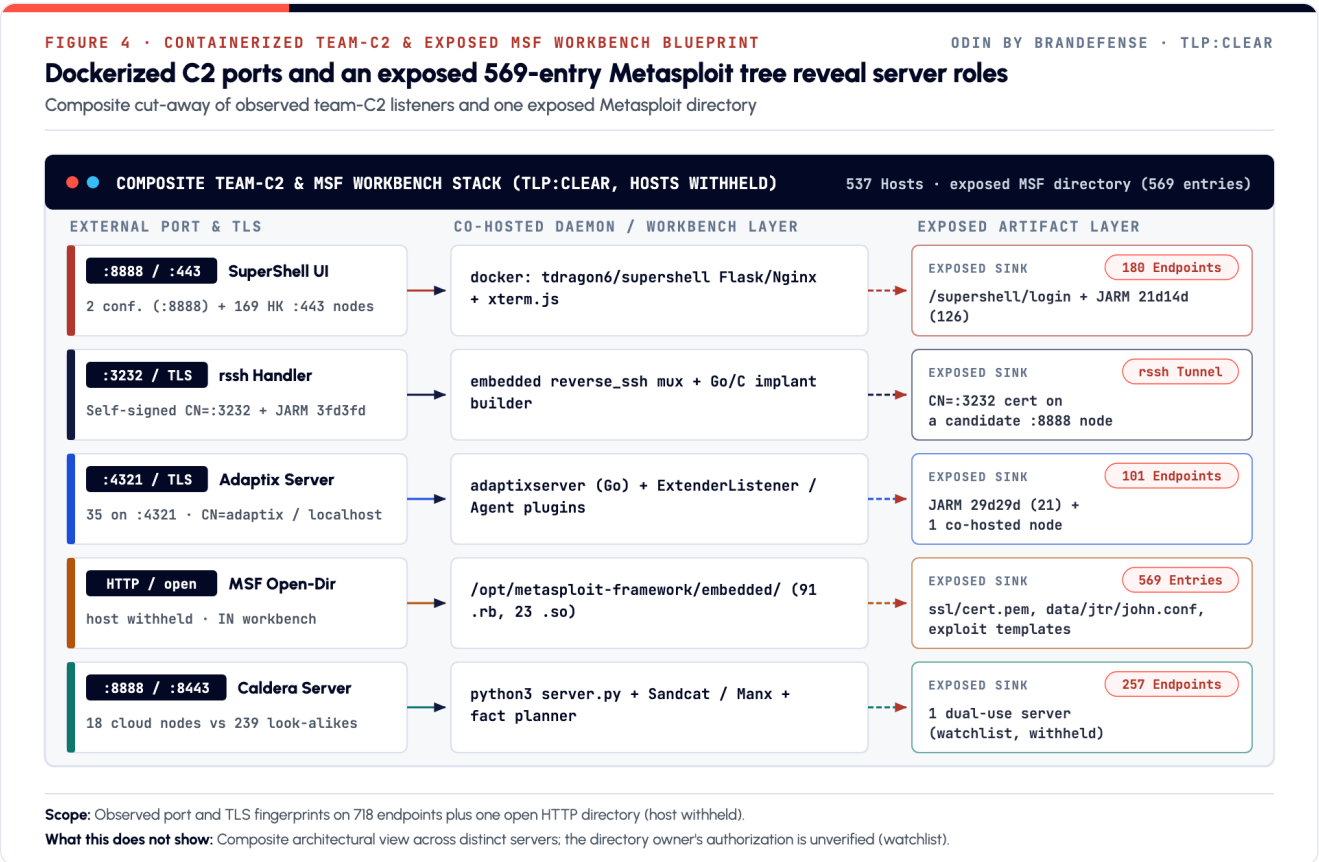


Figure 4: Dockerized C2 ports and an exposed 569-entry Metasploit tree reveal server roles

The exposed Metasploit installation

A server on an Indian hosting network ran an unauthenticated HTTP directory listing on a non-standard port. It exposed the internal Omnibus installation directory of the Rapid7 Metasploit Framework, `/opt/metasploit-framework/embedded/`. The listing reports 58 directory sites holding 7,064 files. This report describes 569 of those entries. The table shows the largest file types among them; smaller groups are not broken out.

An exposed framework installation could belong to an unhardened security lab, a scanner or an attack staging server. The owner's authorization is unknown, so the address, port and file hashes are withheld.

File type	Entries	Share	What it is
No extension (ELF binaries)	237	41.7%	Embedded PostgreSQL and terminal tools, such as `bin/pg_restore`, `bin/pgbench`, `bin/pg_waldump` and `bin/tic`
`.rb`	91	16.0%	Ruby framework libraries, exploit support code and `msfrpcd` runtime modules
`.so` and versioned libraries	43	7.6%	23 `.so` files plus 20 versioned links, such as `plpgsql.so`, `liblzma.so` and `libncurses.so`
`.txt`, `.md`, `.rdoc`	38	6.7%	Framework documentation (20, 12 and 6)
`.h` and `.a`	35	6.2%	OpenSSL and ncurses headers, plus 10 static libraries such as `lib/libpgtypes.a`
`.pem`, `.conf` and exploit data	15+	2.6%+	TLS root bundles, John the Ripper rule files and exploit templates

The tree tells defenders three things.

1. **A database-backed install.** Files such as `pg_restore`, `pg_receivewal` and `lib/postgresql/plpgsql.so` belong to a full Metasploit workspace. Such a workspace can hold shared host tables, captured credentials and Viper session state.
2. **Cracking rules next to exploits.** The John the Ripper rule files `john.conf` (117,142 bytes) and `dumb32.conf` (100,781 bytes) sit beside the framework's exploit templates.
3. **A common exposure mistake.** The most likely explanation is a quick Python HTTP server started from a parent directory during a file transfer. That publishes the whole framework tree by accident.

Co-hosting and multi-port layouts

Across all 718 endpoints, one server runs two different frameworks. It sits on Hangzhou Alibaba Advertising (CN) and binds AdaptixC2 on 60001 beside ToShellC2 on 18081. Its address is withheld.

Another 14 servers run one framework on several ports, not counting vendor and mail look-alikes.

Layout	Servers	Detail
Confirmed dual-port Metasploit	7	The German business-ISP cluster, each with 443 and 80 (withheld)
Confirmed dual-port ToShellC2	2	186.244.231[.]115 (80 and 8080) and 185.207.154[.]238 (8081 and 8443)
Candidate ToShellC2	1	Singapore host on 80, 8080 and 28443 (withheld)
AdaptixC2 and TuoniC2 teamservers	4	India (4444, 4445, 50003), Switzerland (4322, 4323), Singapore DigitalOcean (4321 with 4444), Russia TuoniC2 (8443 web admin with 12702 implant delivery); all withheld

CHAPTER 06

Look-Alikes: What Not to Block

IN SHORT

Raw C2 lists mix real listeners with security appliances, mail servers, scanner consoles and sanctioned purple-team labs. Only 34 of 718 endpoints are confirmed; the other 684 (95.3%) belong on watchlists.

INSIDE THIS CHAPTER

Six sources of false positives 21

06 Look-Alikes: What Not to Block

Feeding raw Caldera, DeimosC2 or Metasploit lists into an automatic firewall block creates real business risk. Figure 5 compares each framework's endpoint count with its confirmed count.

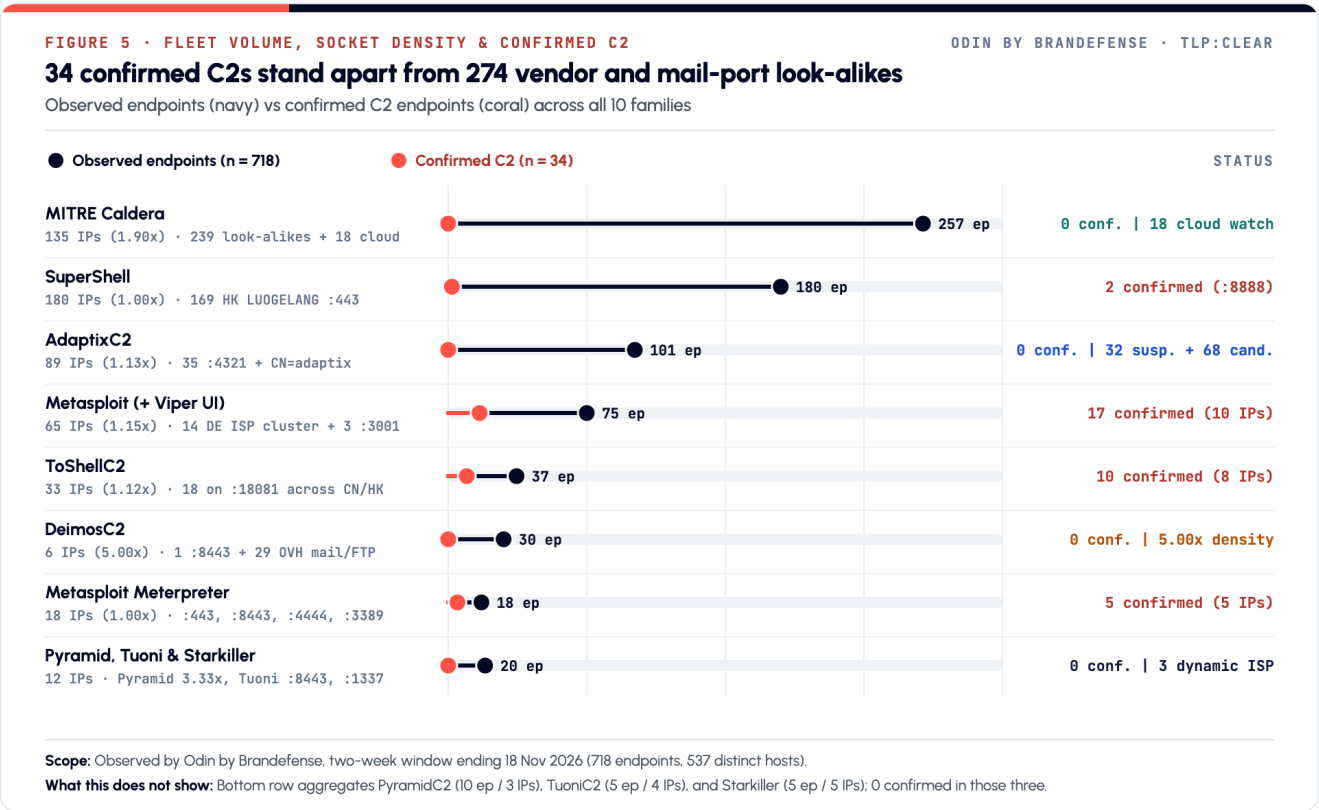


Figure 5: 34 confirmed C2s stand apart from 274 vendor and mail-port look-alikes

Six sources of false positives

Source	Endpoints	Why it is not a C2	What to do
Security-vendor banner look-alikes in the Caldera list	239	Upstream HTTP and TLS fingerprints collide with the vendor's own cloud and appliance services	Do not block
Sanctioned purple-team Caldera and Starkiller servers	18 cloud Caldera + 5 Starkiller	Purple teams and attack-simulation vendors run the same unmodified Sandcat and Empire servers	Watchlist
Mail and FTP ports	35	Standard mail and FTP services match Go and OpenSSL JARM patterns	Do not block
Vulnerability-management and Metasploit Pro consoles	1 + 19 on port 3790	A scanner console certificate, or the Metasploit Pro admin interface, is not a hostile handler	Watchlist unless paired with stager delivery
One-provider SuperShell cluster	169	Shared JARMs on one Hong Kong network, with nothing beyond port and JARM tying them to SuperShell	Watchlist
Dynamic consumer ISP lines	4	Addresses rotate between unrelated customers	24-hour watchlist

Vendor look-alikes. The 239 Caldera look-alikes sit on 117 US hosts in Fortinet corporate address space, which is a fingerprint collision and not Caldera activity. Their ports are 443 (117), 80 (114), 16018 (5) and 8080 (3). One certificate subject repeats on 236 of them.

The 18 cloud Caldera servers.

Removing the look-alikes leaves 18 Caldera endpoints on 18 hosts: 13 on AWS, 2 on DigitalOcean, 2 on Alibaba and 1 on TT DOTCOM. Fourteen use the default port 8888, and one uses 8443. One DigitalOcean server in Germany matches the Caldera protocol and is held as dual-use tooling.

Mail and FTP ports.

The 35 rows split as 29 DeimosC2 rows on 5 OVH hosts in Canada and Chile, 5 PyramidC2 rows on one OVH host in France, and 1 Caldera row on Alibaba. The ports are 21, 110, 143, 465, 587, 993 and 995. Removing them leaves the DeimosC2 candidate on 8443 and the five PyramidC2 web listeners on four ports: 443 (two hosts), 8080, 61380 and 80.

Dynamic ISP lines. The four rows are 1 AdaptixC2 node on Chinanet, 2 PyramidC2 rows on Deutsche Telekom and 1 TuoniC2 node on Turk Telekom. Their addresses 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 traffic to the 18 published confirmed addresses in Chapter 9. Re-check each one after 30 days, since cloud addresses get reassigned.
- [ ] Send any match on the German business-ISP Metasploit cluster pattern (dual 443 and 80 listeners behind one company certificate) to analyst review, not the block list.
- [ ] Keep Caldera, Starkiller, AdaptixC2, DeimosC2, PyramidC2 and TuoniC2 listeners on watchlists, not block lists.
- [ ] Put dynamic consumer ISP addresses on a 24-hour watchlist.

Within 72 hours

- [ ] Deploy the eight Suricata signatures behind TLS inspection and at perimeter TLS monitoring points. Add `pass` rules for your documented purple-team addresses first.
- [ ] Schedule the Sentinel query and the three Sigma rules to catch inline BOFs, Sandcat, `rssh` and Pyramid loaders.
- [ ] Turn off HTTP directory listing on every staging and build server.

Within 7 to 30 days

- [ ] Restrict signed `python.exe` and `pythonw.exe` with WDAC or AppLocker on non-developer workstations. Alert on interpreter connections to ports 3001, 3232, 4321, 8888 and 18081.
- [ ] Keep a formal register of sanctioned Caldera, Viper, Empire and Metasploit hosts. Put their consoles behind mutual TLS or a VPN.
- [ ] Before you auto-block any external C2 list, filter out vendor appliance banners, mail and FTP ports (21, 110, 143, 465, 587, 993, 995), scanner console certificates and dynamic ISP lines.

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
MITRE ATT&CK mapping 27

08 Detection Rules

The full rules are in Appendix B. Together they cover wire, certificate, process and file signals.

Rule file	What it catches
`odin_supershell_adaptix_caldera_metasploit.rules`	Suricata 7: eight signatures for SuperShell, AdaptixC2, Caldera Sandcat, Viper, Metasploit RPC and Starkiller traffic
`sentinel_supershell_caldera_sandcat_and_bof_hunt.kql`	Microsoft Sentinel and Defender XDR: contact with confirmed C2 addresses, console URIs, interpreter egress, and egress followed by in-memory activity
`sigma_sandcat_supershell_and_meterpreter_execution.yml`	Sigma (3 rules): Caldera agents, SuperShell `rssh` callbacks, and Meterpreter or Pyramid in-memory stagers
`odin_supershell_adaptix_caldera_pyramid_implants.yar`	YARA (4 rules): SuperShell, AdaptixC2, Caldera agent and PyramidC2 stager files

How the Suricata signatures work

SID	Looks for	Why
9522001	Outbound URI starting `/supershell/` followed by `login`, `client`, `shell`, `compile` or `mem`	Catches use of a SuperShell web console
9522002	TLS certificate subject `CN=:3232` from an external server	Catches the default SuperShell `rssh` listener
9522003	TLS certificate subject `CN=adaptix`, `CN=adaptix.local` or `CN=adaptix-server`	Catches default AdaptixC2 teamservers
9522004	Outbound `POST /file/download` with `sandcat.go` in the headers	Catches a Caldera Sandcat agent download (dual-use, policy alert)
9522005	Outbound `POST /beacon` with a body starting `eyJ`	Catches Sandcat Base64 JSON check-ins (dual-use, policy alert)
9522006	URI starting `/api/v1/msf/`	Catches Viper workbench API use
9522007	`auth.login` in a request to `/api/` on ports 55552, 55553, 60000 or 3790	Catches Metasploit RPC logins
9522008	Outbound `POST /api/v2/users/login`	Catches Starkiller and Empire v2 operator logins (dual-use, policy alert)

The URI and body rules need TLS inspection to see HTTPS traffic. The certificate rules work on passive perimeter monitoring. Operators who replace the default `CN=:3232` or `CN=adaptix` certificates evade SIDs 9522002 and 9522003, so pair them with the Sentinel query.

How the other rules work

The KQL query looks back 14 days. It has three branches.

1. **Network.** It flags devices that contact the 18 confirmed C2 addresses in Appendix A. It also flags console URIs such as `/supershell/` and `/api/v1/msf/`, and script interpreters (`python.exe`, `powershell.exe`, `rundll32.exe`) connecting to team C2 ports.

2. **Process.** It flags command lines with both `-server` and `-group`, or with markers such as `sandcat.go`, `54ndc47`, `PythonMemoryModule` or `ExtenderAgent`.
3. **Network then memory.** It joins a network hit with remote thread creation, memory allocation, AMSI script content or an unbacked .NET module load on the same device within 10 minutes.

An exact-hostname allowlist excludes sanctioned purple-team machines, but never hides contact with a confirmed C2 address. Treat Caldera and Starkiller hits as hunting leads.

Sigma rule	Fires when
Caldera Sandcat and Manx execution (Windows)	A command line has `-server http` with `-group`, or names `sandcat.go`, `54ndc47` or `manx.go`
SuperShell `rssh` callback (Linux)	A command line names `tdragon6/supershell`, `/supershell/login` or `SSH-2.0-rssh`, or an `rssh` client dials `-d host:3232`, 8888 or 18888
Meterpreter and Pyramid stagers (Windows)	PowerShell decodes Base64 with `VirtualAlloc`, `CreateThread` or a named pipe; or signed Python combines a memory loader with `urllib.request` or `http.client`

Each Sigma rule carries an exact-hostname allowlist for sanctioned lab machines.

YARA rule	Fires when
`ODIN_SuperShell_RSSH_Implant_And_Console`	Two SuperShell strings appear together (such as `tdragon6/supershell`, `/supershell/login`, `SSH-2.0-rssh`); files under 25 MB
`ODIN_AdaptixC2_Extender_And_Beacon_Config`	Three of `AdaptixC2`, `ExtenderListener`, `ExtenderAgent`, `AxScript` and `execute bof`; files under 15 MB
`ODIN_Caldera_Sandcat_And_Manx_Agent`	Three of `sandcat.go`, `54ndc47`, `/file/download`, `contact_http` and `listenP2P`; files under 20 MB
`ODIN_PyramidC2_Python_InMemory_Stager`	`PythonMemoryModule` or `BG_LOAD` with two of `zipimport`, `urllib.request` and `VirtualAlloc`; files under 5 MB

MITRE ATT&CK mapping

Technique	How these tools use it	Detection
T1071.001 Application Layer Protocol: Web Protocols	Sandcat HTTP beacons, Viper and Starkiller REST APIs	SIDs 9522004 to 9522008; Sigma Caldera rule
T1572 Protocol Tunneling	SuperShell reverse SSH over TLS with SOCKS5 pivots	SID 9522002; Sigma `rssh` rule
T1055 Process Injection	Inline BOFs, Meterpreter stagers and shellcode injection	KQL network-then-memory branch; Sigma stager rule
T1059.006 Command and Scripting Interpreter: Python	PyramidC2 in-memory loading through signed Python	Sigma stager rule; YARA PyramidC2 rule

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

Confirmed C2 addresses 29

JARM values for hunting 30

09 Indicators

Appendix A holds 18 published indicators: 18 confirmed C2 addresses to block. The 2 JARM values appear in this report only, for TLS hunting. The JARM values belong to suspected and candidate nodes and are not block indicators. The seven addresses of the German business-ISP cluster, six watchlist entries and all file hashes are withheld.

Type	Count
Confirmed C2 addresses in Appendix A (block)	18
Confirmed addresses withheld (German business-ISP cluster)	7
JARM values for TLS hunting only (not block indicators)	2
Watchlist entries (addresses withheld)	6
File hashes (SHA-256)	0 published; 8 withheld

The six withheld watchlist entries are the exposed Metasploit directory, the dual-use Caldera server, a default AdaptixC2 teamserver, the co-hosted AdaptixC2 and ToShellC2 server, a SuperShell candidate with `CN=:3232`, and the dual-port TuoniC2 server. The eight SHA-256 values come from stock Metasploit files on the unattributed server, so they are withheld.

Confirmed C2 addresses

Endpoint	Framework	Hosting (country)	Key fingerprint	Seen
111.229.193[.]40:8888	SuperShell	Shenzhen Tencent (CN)	SuperShell web console	13 Nov 2026
103.115.57[.]95:8888	SuperShell	Cloudie Limited (HK)	SuperShell web console	13 Nov 2026
206.119.189[.]208:8081	ToShellC2	SonderCloud (US)	Shell console on 8081	13 Nov 2026
186.244.231[.]115:8080	ToShellC2	CLOUDVALLEY (US)	Also 80	13 Nov 2026
186.244.215[.]55:443	ToShellC2	Uscloud Inc (US)	`CN=fileserver`, JARM `3fd3fd0003fd3fd00043d43d00043d3bef2bf79cd6719851e8198c1e8f9a14`	13 Nov 2026
45.192.109[.]17:80	ToShellC2	cognetcloud INC (HK)	HTTP console	13 Nov 2026
8.138.248[.]246:8081	ToShellC2	Alibaba Cloud (CN)	Listener on 8081	13 Nov 2026
185.207.154[.]238:8443	ToShellC2	Cloudie Limited (HK)	Also 8081; same JARM as above	13 Nov 2026
83.229.120[.]101:8081	ToShellC2	LUCIDACLOUD (HK)	Listener on 8081	13 Nov 2026
43.160.243[.]229:443	ToShellC2	Shenzhen Tencent (SG)	TLS listener	13 Nov 2026

Endpoint	Framework	Hosting (country)	Key fingerprint	Seen
181.215.18[.]135:8443	Meterpreter	Datacamp (HK)	Reverse-HTTPS handler, JARM `07d19d12d21d21d07c42d43d000000f50d155305214cf247147c43c0f1a823`	13 Nov 2026
65.38.121[.]42:3389	Meterpreter	BL Networks (RO)	`CN=6a47718162def1c` on the RDP port, JARM `14d14d16d14d14d08c14d14d14d14dfd9c9d14e4f4f67f94f0359f8b28f532`	13 Nov 2026
190.2.184[.]47:4444	Meterpreter	MASTER DA WEB (BR)	Default handler port	14 Nov 2026
8.148.31[.]135:4446	Meterpreter	Alibaba Cloud (CN)	TCP handler	13 Nov 2026
154.89.152[.]104:10003	Meterpreter	CLOUDVALLEY (HK)	High-port handler	13 Nov 2026
77.83.36[.]163:3001	Metasploit	Layer7 Networks (SC)	Team listener	14 Nov 2026
185.254.199[.]160:3001	Metasploit	SOLLUTIUM EU (NL)	Team listener	13 Nov 2026
77.91.71[.]99:3001	Metasploit	Hosting network (IL)	Team listener	13 Nov 2026

The seven-address German cluster (14 endpoints, each address on 443 and 80) sits on a business ISP and shares one third-party company certificate. That pattern also fits an authorized testing firm or lab, so its addresses are withheld. With it and the second ports on 186.244.231[.]115 and 185.207.154[.]238, the table above accounts for all 34 confirmed endpoints.

JARM values for hunting

JARM	Framework	Use
`29d29d00000000000043d43d00043dc3b2afa8a5ec09b510a8559aff7899fb`	AdaptixC2	Go teamserver TLS fingerprint on 21 listeners; hunt, do not block alone
`3fd3fd20d3fd3fd00043d3fd3fd43d5ecfbe778b06e32b538bd51f24eb7398`	SuperShell	Default `rssh` TLS fingerprint, seen with `CN=:3232` on candidate consoles in China; hunt, do not block alone

Supporting fingerprints: the certificate subjects `CN=:3232`, `CN=adaptix`, `CN=adaptix.local`, `CN=adaptix-server`, `CN=fileserver` and `CN=6a47718162def1c`.

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. Some records carry earlier first-seen dates from public sources; we do not treat those as a tracking start.
- **Server side only.** These observations show what runs on attacker-side servers. They do not show which targets were reached or what happened on them.
- **Confirmed is a high bar.** Only 34 of 718 endpoints are confirmed, and 18 of their addresses are published. One confirmed cluster is withheld because it may belong to an authorized tester. Suspected and candidate endpoints are leads, not block entries.
- **Dual-use tools.** Caldera, Starkiller, Empire, Metasploit and Viper are used legitimately by red and purple teams. A listener alone does not prove hostile intent.
- **The workflow model is a model.** The three-workflow grouping in Figure 1 and the six-step sequence in Figure 3 are analytical. Nothing here links the frameworks to one actor.
- **The exposed directory.** The Metasploit tree shows a full installation. It does not show who ran it or whether it was used against anyone.
- **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. tdragon6. SuperShell repository. https://github.com/tdragon6/Supershell (verified 20 November 2026)
2. Adaptix-Framework. AdaptixC2 repository. https://github.com/Adaptix-Framework/AdaptixC2 (verified 20 November 2026)
3. MITRE Caldera documentation, plugin library (Sandcat and Manx agents). https://caldera.readthedocs.io/en/latest/Plugin-library.html (verified 20 November 2026)
4. FunnyWolf. Viper repository. https://github.com/FunnyWolf/Viper (verified 20 November 2026)
5. Rapid7. Metasploit documentation. https://docs.rapid7.com/metasploit/ (verified 20 November 2026)
6. shell-dot. Tuoni repository. https://github.com/shell-dot/tuoni (verified 20 November 2026)
7. naksyn. Pyramid repository. https://github.com/naksyn/Pyramid (verified 20 November 2026)
8. MITRE ATT&CK. Empire, S0363. https://attack.mitre.org/software/S0363/ (verified 20 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 (18) 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
R22-IOC-01	IPv4	111.229.193[.]40	8888	SuperShell console	BLOCK
R22-IOC-02	IPv4	103.115.57[.]95	8888	SuperShell console	BLOCK
R22-IOC-03	IPv4	206.119.189[.]208	8081	ToShellC2 console	BLOCK
R22-IOC-04	IPv4	186.244.231[.]115	8080	ToShellC2 console	BLOCK
R22-IOC-05	IPv4	186.244.215[.]55	443	ToShellC2 console	BLOCK
R22-IOC-06	IPv4	45.192.109[.]17	80	ToShellC2 console	BLOCK
R22-IOC-07	IPv4	8.138.248[.]246	8081	ToShellC2 console	BLOCK
R22-IOC-08	IPv4	185.207.154[.]238	8443	ToShellC2 console	BLOCK
R22-IOC-09	IPv4	83.229.120[.]101	8081	ToShellC2 console	BLOCK
R22-IOC-10	IPv4	43.160.243[.]229	443	ToShellC2 console	BLOCK
R22-IOC-11	IPv4	181.215.18[.]135	8443	Metasploit / Meterpreter handler	BLOCK
R22-IOC-12	IPv4	65.38.121[.]42	3389	Metasploit / Meterpreter handler	BLOCK
R22-IOC-13	IPv4	190.2.184[.]47	4444	Metasploit / Meterpreter handler	BLOCK
R22-IOC-14	IPv4	8.148.31[.]135	4446	Metasploit / Meterpreter handler	BLOCK
R22-IOC-15	IPv4	154.89.152[.]104	10003	Metasploit / Meterpreter handler	BLOCK
R22-IOC-16	IPv4	77.83.36[.]163	3001	Metasploit server	BLOCK
R22-IOC-17	IPv4	185.254.199[.]160	3001	Metasploit server	BLOCK
R22-IOC-18	IPv4	77.91.71[.]99	3001	Metasploit server	BLOCK

B Detection Rules

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

odin_supershell_adaptix_caldera_metasploit.rules

SURICATA

```
# Odin by Brandefense - Report #22 Suricata 7.x Team-C2, SuperShell, AdaptixC2, Caldera & Metasploit Suite
# Classification: TLP:CLEAR
# Scope Note: Network HTTP/TLS offload and C2 RPC signatures (sid:9522001-9522008).
#             Pair dual-use Caldera and Starkiller alerts with sanctioned purple-team host allowlists.

# 1. SuperShell Browser-Native Console API & Implant Compilation Route (/supershell/)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-C2 SuperShell Browser Console API Request (/
supershell/)"; flow:established,to_server; http.uri; content:"/supershell/"; startswith; fast_pattern; bsize:>12;
pcre:"/^\/supershell\/(?:login|client|shell|compile|mem)/i"; metadata:created_at 2026_11_19, tactic
command_and_control; classtype:trojan-activity; sid:9522001; rev:1;)

# 2. SuperShell Embedded Reverse-SSH (rssh) Default TLS Certificate Subject (CN=:3232)
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-C2 SuperShell Embedded rssh Default TLS Subject (CN=:
3232)"; flow:established,from_server; tls.cert_subject; content:"CN=:3232"; fast_pattern; bsize:>7;
metadata:created_at 2026_11_19, tactic command_and_control; classtype:trojan-activity; sid:9522002; rev:1;)

# 3. AdaptixC2 Default Teamserver TLS Certificate Subject (CN=adaptix / CN=adaptix.local / CN=adaptix-server)
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-C2 AdaptixC2 Default Teamserver TLS Certificate Subject";
flow:established,from_server; tls.cert_subject; content:"CN=adaptix"; nocase; fast_pattern; bsize:>9; pcre:"/
CN=adaptix(?:\.local|-server)?(?:,|$)/i"; metadata:created_at 2026_11_19, tactic command_and_control;
classtype:trojan-activity; sid:9522003; rev:1;)

# 4. MITRE Caldera Sandcat Dynamic Agent Compilation & Download Header (file: sandcat.go)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-DUALUSE MITRE Caldera Sandcat Dynamic Payload Download";
flow:established,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/file/download"; bsize:14;
http.header; content:"sandcat.go"; nocase; fast_pattern; metadata:created_at 2026_11_19, tactic
command_and_control; classtype:policy-violation; sid:9522004; rev:1;)

# 5. MITRE Caldera Sandcat Base64 JSON Profile Check-In (POST /beacon)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-DUALUSE MITRE Caldera Sandcat HTTP Beacon Check-In (/
beacon)"; flow:established,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/beacon"; bsize:7;
fast_pattern; http.request_body; content:"eyJ"; startswith; bsize:>32; metadata:created_at 2026_11_19, tactic
command_and_control; classtype:policy-violation; sid:9522005; rev:1;)

# 6. Viper Multi-Operator Metasploit Browser Workbench REST API (/api/v1/msf/)
alert http any any -> any any (msg:"ODIN-C2 Viper Multi-Operator Metasploit Workbench API Access";
flow:established,to_server; http.uri; content:"/api/v1/msf/"; startswith; fast_pattern; bsize:>11;
metadata:created_at 2026_11_19, tactic command_and_control; classtype:trojan-activity; sid:9522006; rev:1;)

# 7. Metasploit RPC Daemon (msfrpcd) MessagePack Authentication Handshake (auth.login)
alert http any any -> any [55552,55553,60000,3790] (msg:"ODIN-C2 Metasploit RPC Daemon (msfrpcd) auth.login
Call"; flow:established,to_server; http.uri; content:"/api/"; startswith; bsize:>4; http.request_body;
content:"auth.login"; fast_pattern; bsize:>12; metadata:created_at 2026_11_19, tactic command_and_control;
classtype:trojan-activity; sid:9522007; rev:1;)

# 8. Starkiller / PowerShell Empire REST v2 Operator Authentication (/api/v2/users/login)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-DUALUSE Starkiller / Empire v2 REST API Login";
flow:established,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/api/v2/users/login";
fast_pattern; bsize:19; metadata:created_at 2026_11_19, tactic command_and_control; classtype:policy-violation;
sid:9522008; rev:1;)
```

odin_supershell_adaptix_caldera_pyramid_implants.yar

YARA

```
/*
   Odin by Brandefense - Report #22 YARA Implant, Extender & Staging Suite
   Classification: TLP:CLEAR
   Scope: SuperShell rssh implants/configs, AdaptixC2 Extender/Beacon manifests,
          MITRE Caldera Sandcat/Manx stagers, and Pyramid signed-Python memory loaders.
*/

rule ODIN_SuperShell_RSSH_Implant_And_Console
{
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-19"
        tlp = "CLEAR"
        description = "Detects SuperShell containerized web console artifacts and compiled rssh reverse-SSH
implants"
    strings:
        $s1 = "tdragon6/supershell" ascii nocase
        $s2 = "/supershell/login" ascii nocase
        $s3 = "SSH-2.0-rssh" ascii
        $s4 = "compile_client" ascii
        $s5 = ":3232" ascii
    condition:
        filesize < 25MB and (2 of ($s1, $s2, $s3, $s4)) and ($s3 or $s5 or $s1)
}

rule ODIN_AdaptixC2_Extender_And_Beacon_Config
{
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-19"
        tlp = "CLEAR"
        description = "Detects AdaptixC2 teamserver JSON profiles, ExtenderListener/ExtenderAgent plugins, and
AxScript BOF tasking"
    strings:
        $a1 = "AdaptixC2" ascii nocase
        $a2 = "ExtenderListener" ascii
        $a3 = "ExtenderAgent" ascii
        $a4 = "AxScript" ascii
        $a5 = "execute bof" ascii nocase
    condition:
        filesize < 15MB and 3 of ($a*)
}

rule ODIN_Caldera_Sandcat_And_Manx_Agent
{
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-19"
        tlp = "CLEAR"
        description = "Detects MITRE Caldera Sandcat (54ndc47) and Manx agent binaries or dynamic delivery
headers"
    strings:
        $c1 = "sandcat.go" ascii nocase
        $c2 = "54ndc47" ascii
        $c3 = "/file/download" ascii
        $c4 = "contact_http" ascii
        $c5 = "listenP2P" ascii
    condition:
        filesize < 20MB and 3 of ($c*)
}

rule ODIN_PyramidC2_Python_InMemory_Stager
{
    meta:
        author = "Odin by Brandefense"
        date = "2026-11-19"
        tlp = "CLEAR"
        description = "Detects Pyramid Living-off-the-Blindspot Python memory-import stagers and
```

```
PythonMemoryModule loaders"
    strings:
        $p1 = "PythonMemoryModule" ascii
        $p2 = "zipimport" ascii
        $p3 = "urllib.request" ascii
        $p4 = "VirtualAlloc" ascii
        $p5 = "BG_LOAD" ascii
    condition:
        filesize < 5MB and ($p1 or $p5) and 2 of ($p2, $p3, $p4)
}
```

sentinel_supershell_caldera_sandcat_and_bof_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Report #22 Sentinel & Defender XDR Team-C2, Sandcat & BOF Hunt
// Classification: TLP:CLEAR
let Lookback = 14d;
let CorrelationWindow = 10m;
// Placeholder host names: replace with your own approved hosts.
let ApprovedPurpleTeamHosts = dynamic(["SRV-PURPLE-CALDERA01", "WKSTN-REDTEAM-01"]);
let ConfirmedTeamC2Ips = dynamic([
    "111.229.193.40", "103.115.57.95", "206.119.189.208", "186.244.231.115", "186.244.215.55",
    "45.192.109.17", "8.138.248.246", "185.207.154.238", "83.229.120.101", "43.160.243.229",
    "181.215.18.135", "65.38.121.42", "190.2.184.47", "8.148.31.135", "154.89.152.104",
    "77.83.36.163", "185.254.199.160", "77.91.71.99"
]);
let TeamC2Ports = dynamic([3001, 3232, 3790, 4321, 4444, 4446, 8888, 12702, 18081, 18888]);
let TeamC2Net =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback) and ActionType == "ConnectionSuccess"
    | where RemoteIPType == "Public"
    // Purple-team allowlist never hides contact with a confirmed C2 address
    | where RemoteIP in (ConfirmedTeamC2Ips) or not(DeviceName in~ (ApprovedPurpleTeamHosts))
    | where RemoteIP in (ConfirmedTeamC2Ips)
        or RemoteUrl has_any ("/supershell/", "/file/download", "/api/v1/msf/", "/api/v2/users/login")
        or (InitiatingProcessFileName in~ ("python.exe", "pythonw.exe", "powershell.exe", "pwsh.exe",
"rundll32.exe") and RemotePort in (TeamC2Ports))
    | project DeviceName, NetTime = Timestamp, InitiatingProcessFileName, RemoteIP, RemotePort, RemoteUrl;
let MemoryAndBofEvents =
    DeviceEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedPurpleTeamHosts))
    | where ActionType in ("CreateRemoteThreadApiCall", "VirtualAllocApiCall", "AmsiScriptContent",
"ClrUnbackedModuleLoaded")
    | project DeviceName, MemTime = Timestamp, MemAction = ActionType, MemFile = InitiatingProcessFileName,
AdditionalFields;
union isfuzzy=true
(
    TeamC2Net
    | extend Timestamp = NetTime,
             HuntSignal = case(
                 RemoteIP in (ConfirmedTeamC2Ips), "Confirmed_SuperShell_ToShell_Or_Metasploit_C2_Egress",
                 RemoteUrl has_any ("/supershell/", "/api/v1/msf/"), "Browser_Console_Or_Viper_Workbench_URI",
                 RemoteUrl has_any ("/file/download", "/api/v2/users/login"),
"Preliminary_Caldera_Or_Starkiller_DualUse_Egress",
                 "Suspicious_Interpreter_To_TeamC2_Listener_Port"
             ),
             ArtifactDetail = strcat(RemoteIP, ":", tostring(RemotePort), " (", coalesce(RemoteUrl,
"direct_socket"), ")")
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName = InitiatingProcessFileName,
ArtifactDetail
),
(
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedPurpleTeamHosts))
    | where (ProcessCommandLine contains " -server " and ProcessCommandLine contains " -group ")
        or ProcessCommandLine has_any ("sandcat.go", "54ndc47", "tdragon6/supershell", "PythonMemoryModule",
"ExtenderAgent")
```

```
        or (FileName in~ ("python.exe", "pythonw.exe") and ProcessCommandLine has_all ("zipimport",
"urllib.request"))
    | extend HuntSignal = "Sandcat_SuperShell_Or_Pyramid_InMemory_Process",
             ArtifactDetail = ProcessCommandLine
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName, ArtifactDetail
),
(
    TeamC2Net
    | join kind=inner (MemoryAndBofEvents) on DeviceName
    | where MemTime between (NetTime .. (NetTime + CorrelationWindow))
    | extend Timestamp = MemTime,
             HuntSignal = "TeamC2_Egress_Followed_By_InMemory_BOF_Or_Injection",
             ArtifactDetail = strcat(RemoteIP, ":", tostring(RemotePort), " -> ", MemAction, " by ", MemFile)
    | project Timestamp, DeviceName, HuntSignal, InitiatingProcessFileName, FileName = MemFile, ArtifactDetail
)
| summarize
    FirstSeen = min(Timestamp),
    LastSeen = max(Timestamp),
    EventCount = count(),
    SampleIndicators = make_set(ArtifactDetail, 5)
    by DeviceName, HuntSignal, InitiatingProcessFileName, FileName
| order by EventCount desc
```

sigma_sandcat_supershell_and_meterpreter_execution.yml

SIGMA

```
title: MITRE Caldera Sandcat and Manx Agent Execution
id: 22a9b4c1-7d31-4e82-9a14-8f12c3049501
status: experimental
description: Detects command-line invocation or dynamic compilation flags of MITRE Caldera Sandcat (54ndc47) and
Manx agents outside approved purple-team hosts.
author: Odin by Brandefense
date: 2026/11/19
references:
  - https://caldera.readthedocs.io/en/latest/Plugin-library.html
logsource:
  category: process_creation
  product: windows
detection:
  selection_cli_pair:
    CommandLine|contains:
      - ' -server http'
      - ' -server https'
  selection_group:
    CommandLine|contains: ' -group '
  selection_agent_markers:
    CommandLine|contains:
      - 'sandcat.go'
      - '54ndc47'
      - 'manx.go'
  filter_approved_purple_team:
    # Placeholder host names: replace with your own approved hosts.
    ComputerName:
      - 'SRV-PURPLE-CALDERA01'
      - 'WKSTN-REDTEAM-01'
  condition: ((selection_cli_pair and selection_group) or selection_agent_markers) and not
filter_approved_purple_team
falsepositives:
  - Sanctioned MITRE Caldera purple-team exercises on hosts not yet added to filter_approved_purple_team
level: high
tags:
  - attack.command_and_control
  - attack.t1071.001
  - attack.execution
---
title: SuperShell rssh Implant Callback and Containerized Server Launch
id: 22a9b4c1-7d31-4e82-9a14-8f12c3049502
status: experimental
description: Detects execution of SuperShell reverse-SSH (rssh) implants dialing out to default :3232/:8888
```

```
listeners or unauthorized tdragon6/supershell container launches.
author: Odin by Brandefense
date: 2026/11/19
references:
  - https://github.com/tdragon6/Supershell
logsource:
  category: process_creation
  product: linux
detection:
  selection_container_or_bin:
    CommandLine|contains:
      - 'tdragon6/supershell'
      - '/supershell/login'
      - 'SSH-2.0-rssh'
  selection_rssh_callback:
    CommandLine|re: '(?:rssh|reverse_ssh).*\s-d\s+[A-Za-z0-9_.-]+:(?:3232|8888|18888)\b'
  filter_approved_redteam:
    # Placeholder host names: replace with your own approved hosts.
    Hostname:
      - 'SRV-REDTEAM-DOCKER01'
  condition: (selection_container_or_bin or selection_rssh_callback) and not filter_approved_redteam
falsepositives:
  - Authorized red-team infrastructure testing on dedicated lab hosts
level: high
tags:
  - attack.command_and_control
  - attack.t1572
  - attack.t1071.004
---
title: Meterpreter Reflective Stager and Pyramid Signed-Python Memory Loader
id: 22a9b4c1-7d31-4e82-9a14-8f12c3049503
status: experimental
description: Detects PowerShell reflective Meterpreter stagers and Pyramid Living-off-the-Blindspot signed Python
interpreters staging in-memory dependencies.
author: Odin by Brandefense
date: 2026/11/19
references:
  - https://github.com/naksyn/Pyramid
  - https://docs.rapid7.com/metasploit/
logsource:
  category: process_creation
  product: windows
detection:
  selection_py_bin:
    Image|endswith:
      - '\python.exe'
      - '\pythonw.exe'
  selection_py_mem:
    CommandLine|contains:
      - 'PythonMemoryModule'
      - 'zipimport'
      - 'VirtualAlloc'
  selection_py_net:
    CommandLine|contains:
      - 'urllib.request'
      - 'http.client'
  selection_msf_ps:
    Image|endswith:
      - '\powershell.exe'
      - '\pwsh.exe'
    CommandLine|contains:
      - 'FromBase64String'
    CommandLine|re: '(?:VirtualAlloc|CreateThread|\\\\\.\\pipe\\[A-Za-z0-9]{6,16})'
  filter_dev_build:
    # Placeholder host names: replace with your own approved hosts.
    ComputerName:
      - 'SRV-PYBUILD-CI01'
  condition: ((selection_py_bin and selection_py_mem and selection_py_net) or selection_msf_ps) and not
filter_dev_build
falsepositives:
  - Custom Python packaging tools using zipimport alongside urllib on developer CI runners
```

```
  level: high
  tags:
    - attack.defense_evasion
    - attack.t1055
    - attack.t1059.006
```

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/shared-team-c2-consoles/
Short Read · brandefense.io/odin-research/blog/shared-attack-consoles/
Defense Kit · brandefense.io/odin-research/defense-kit/