Sandfly®

Agentless Linux Security

Linux Malware from Simple to Sophisticated

Craig H. Rowland
Founder, CEO
@CraigHRowland
www.sandflysecurity.com

I’m a Linux Malware Connoisseur

Menu of Effective Linux Malware

Simple and does one thing really well.

Small and respects system resources.

Hides, but doesn’t try to outsmart itself.

Can be quickly deployed with little risk.

Malware Scorecard

Sophistication - How hard is it to pull off?

Effectiveness - How well does it work?

Stealth - How well does it hide?

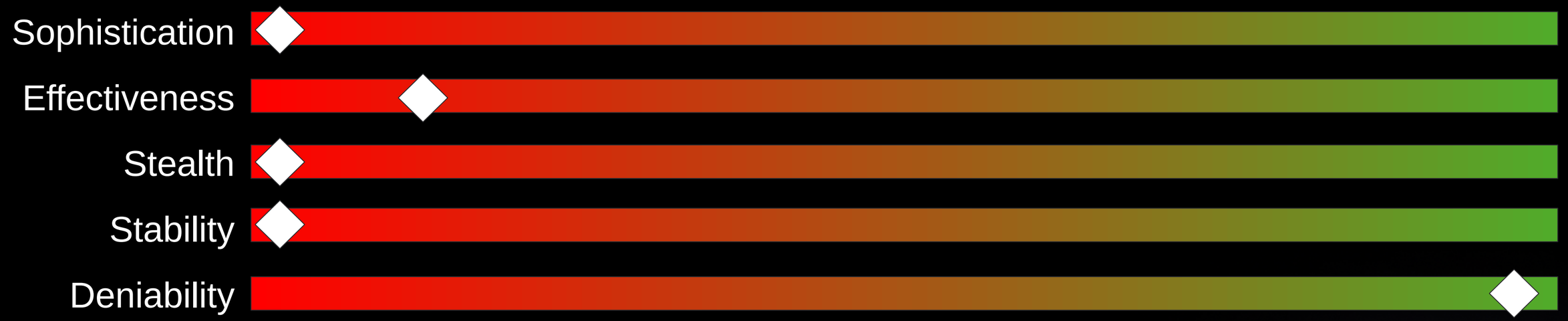
Stability - Can it run without drawing attention to itself?

Deniability - Is it common or unique?

Beginner

Cryptominers and Botnets

Cryptominers and Botnets



Cryptominers and Botnets

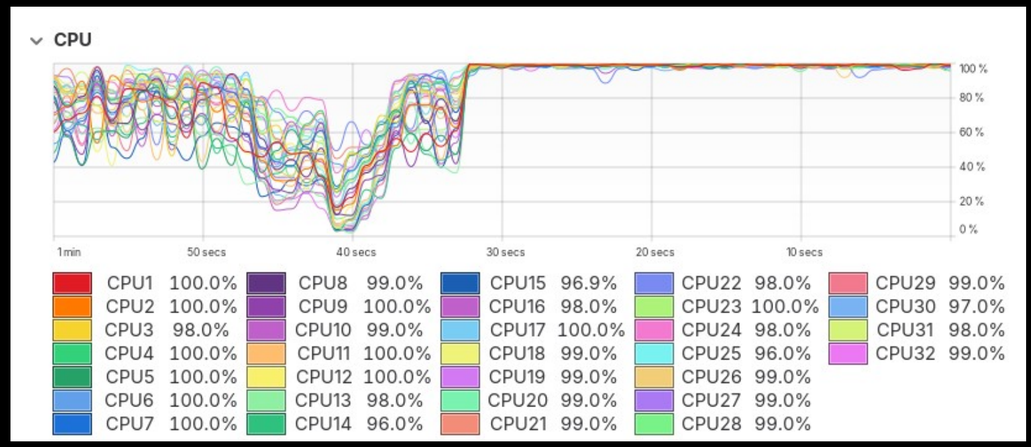
CPU/Bandwidth hit and run.

Targets consumer and SOHO devices.

Extremely obvious, but may have secrets.

A free security audit.

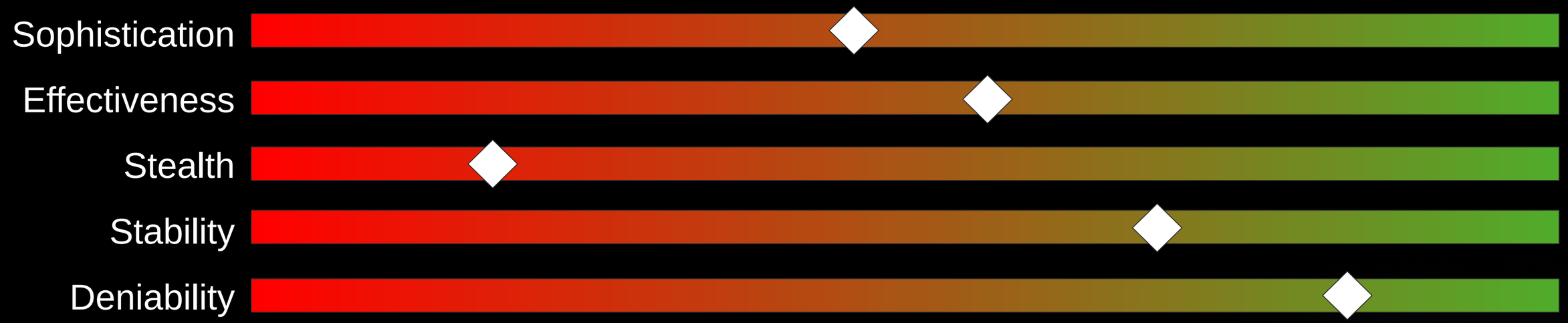
They got it onto the box somehow!



Intermediate

Command and Control (C2) Framework

Command and Control (C2) Framework



Command and Control (C2) Framework

Red teams and turnkey hacking groups.

Feature-laden and bloated.

Can bypass exfiltration controls.

They got it onto the box somehow!

Command and Control (C2) Framework Capabilities

File Operations
Shell Access
Process Manipulation
Credential Harvesting
Keyboard/Screen Capture
Network Pivoting
Exploit Plug-Ins

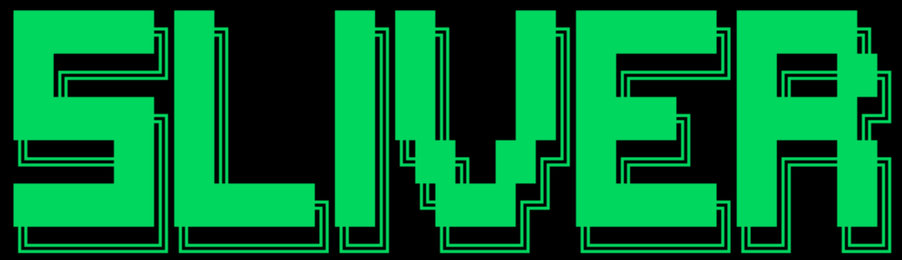
SLIVER
FRAMEWORK

MERLIN

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

Command and Control (C2) Framework

```
root@sandfly-attacker:~# sliver
Connecting to 127.0.0.1:31337 ...
```




```
All hackers gain hidden agenda
[*] Server v1.7.3 - 3bbaf805104dcc4a75414ee0084e8de50702cad4
[*] Welcome to the sliver shell, please type 'help' for options

[127.0.0.1] sliver > sessions

 ID         Transport   Remote Address          Hostname         Username   Operating System   Health
========== =========== ====================== ================ ========== ================== =========
 ab48c7ce   mtls        157.230.226.120:60672   sandfly-victim   root       linux/amd64        [ALIVE]

[127.0.0.1] sliver >
```

Command and Control (C2) Framework

```
 ID          Transport   Remote Address          Hostname         Username   Operating System   Health
========== =========== ====================== ================ ========== ================== =========
 ab48c7ce   mtls        157.230.226.120:60672   sandfly-victim   root       linux/amd64        [ALIVE]

[127.0.0.1] sliver > use ab48c7ce

[*] Active session demo (ab48c7ce-8e54-4425-916e-86b38e5f51f3)
[127.0.0.1] sliver (demo) >
[127.0.0.1] sliver (demo) > ls

/root (11 items, 60.6 MiB)
==========================
drwx------  root:root  .                       <dir>     Tue Apr 28 00:57:11 +0000 2026
-rw-------  root:root  .bash_history           104 B     Tue Apr 28 01:11:48 +0000 2026
-rw-r--r--  root:root  .bashrc                 3.0 KiB   Mon Apr 22 13:04:27 +0000 2024
drwx------  root:root  .cache                  <dir>     Mon Apr 27 23:55:39 +0000 2026
-rw-r--r--  root:root  .cloud-locale-test.skip 0 B       Tue Apr 28 01:12:06 +0000 2026
drwx------  root:root  .config                 <dir>     Mon Apr 27 23:58:02 +0000 2026
-rw-r--r--  root:root  .profile                161 B     Mon Apr 22 13:04:27 +0000 2024
drwx------  root:root  .ssh                    <dir>     Mon Apr 27 23:53:22 +0000 2026
-rw-r--r--  root:root  .wget-hsts              185 B     Tue Apr 28 00:24:13 +0000 2026
-rwx------  root:root  demo                    29.9 MiB  Tue Apr 28 00:58:38 +0000 2026
-rwx------  root:root  test                    30.6 MiB  Tue Apr 28 00:54:01 +0000 2026


[127.0.0.1] sliver (demo) >
```

Huge size. Yuck!

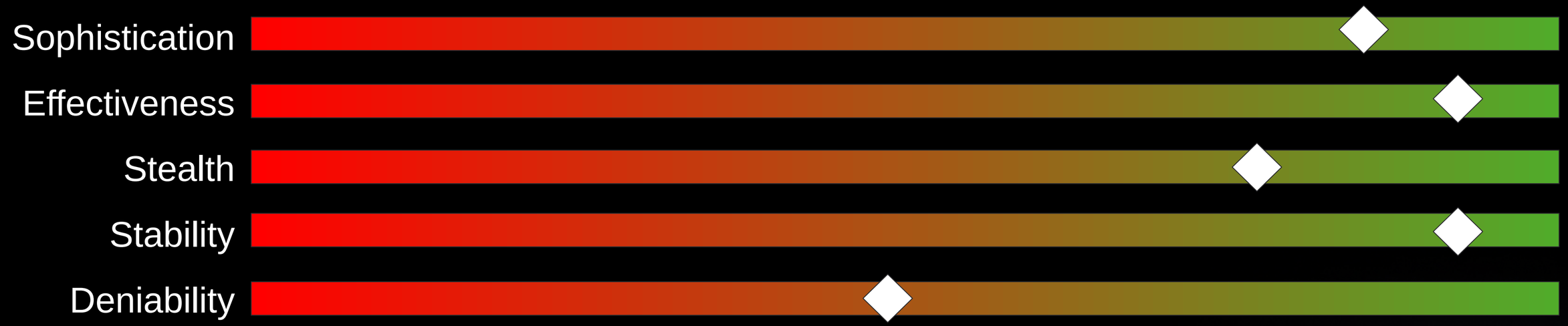
What is the biggest problem with C2 frameworks?

C2 Frameworks Are Overdressed For the Occasion

Expert

Network Implants and Backdoors

Network Implants and Backdoors



Network Implants and Backdoors

Focused features.

Enough stealth to hide for a long time.

These users mean business.

They got it onto the box somehow!

Well-Known Network Implants and Backdoors

TCP/UDP Backdoors

ICMP Backdoors

Alternate Protocol Backdoors (SCTP)

SSH/PAM Backdoors

Network Implant Common Features

Magic Packet Activation

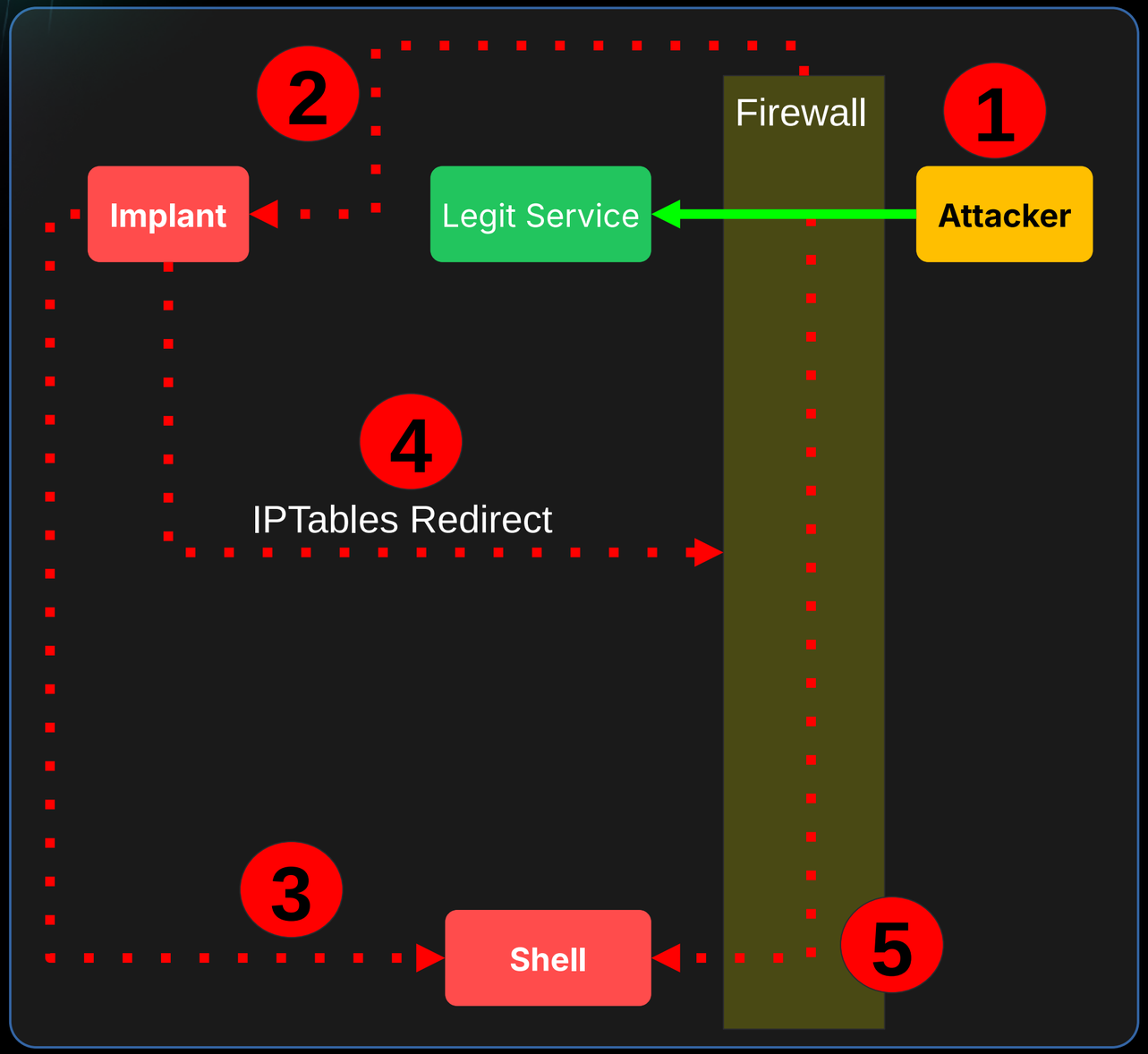
Covert Channel Communications

Remote Access

Lateral Movement

Anti-Forensics

Network Implants and Backdoors: BPFDoor Magic Packet



1. Attacker sends packet to any port with **magic number**.
2. **Implant** sees packet before firewall can reject.
3. Implant starts **shell** on TCP port.
4. Reconfigures firewall to **redirect** attacker to shell.
5. Traffic appears to go to legit port but is **rerouted** to shell.

Spot BPFDoor - Simple Evasion

```
root           1  0.0  1.1 166280 11392 ?        Ss   Sep10   0:02 /sbin/init
root         335  0.0  2.0  40040 19892 ?        S<s  Sep10   0:00 /lib/systemd/systemd-journald
root         372  0.0  2.7 289312 27100 ?        SLsl Sep10   0:06 /sbin/multipathd -d -s
systemd+     450  0.0  0.6  89352  6456 ?        Ssl  Sep10   0:00 /lib/systemd/systemd-timesyncd
systemd+     525  0.0  0.8  16116  8252 ?        Ss   Sep10   0:00 /lib/systemd/systemd-networkd
systemd+     544  0.0  1.3  25648 12948 ?        Ss   Sep10   0:00 /lib/systemd/systemd-resolved
root         568  0.0  0.6  22724  6236 ?        Ss   Sep10   0:00 /lib/systemd/systemd-udevd
root         626  0.0  0.2   7284  2744 ?        Ss   Sep10   0:00 /usr/sbin/cron -f -P
message+     628  0.0  0.4   8580  4756 ?        Ss   Sep10   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         630  0.0  0.5 1299308 5508 ?        Ssl  Sep10   0:00 /opt/digitalocean/bin/droplet-agent
root         635  0.0  1.9  33084 18856 ?        Ss   Sep10   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
syslog       636  0.0  0.5 222400  5640 ?        Ssl  Sep10   0:00 /usr/sbin/rsyslogd -n -iNONE
root         638  0.0  2.8 1245368 28416 ?       Ssl  Sep10   0:05 /usr/lib/snapd/snapd
root         640  0.0  0.7  15500  7552 ?        Ss   Sep10   0:00 /lib/systemd/systemd-logind
root         650  0.0  0.1   6216  1100 ttyS0    Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,57600,38400,9600 ttyS0 vt220
root         653  0.0  0.1   6172  1080 tty1     Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         678  0.0  0.9  15420  9228 ?        Ss   Sep10   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        3333  0.0  1.1  17188 11072 ?        Ss   Sep11   0:00  \_ sshd: root@pts/2
root        3385  0.0  0.5   9280  5420 pts/2    Ss+  Sep11   0:00  |   \_ -bash
root        3986  0.0  1.1  17188 11072 ?        Ss   00:03   0:00  \_ sshd: root@pts/4
root        4038  0.0  0.5   9148  5172 pts/4    Ss   00:03   0:00      \_ -bash
root        4054  0.0  0.3  10888  3584 pts/4    R+   00:04   0:00          \_ ps -auxwwf
root         686  0.0  2.1 110084 21348 ?        Ssl  Sep10   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root        2123  0.0  2.0 295960 20428 ?        Ssl  Sep11   0:00 /usr/libexec/packagekitd
root        2127  0.0  0.7 234492  6904 ?        Ssl  Sep11   0:00 /usr/libexec/polkitd --no-debug
root        3204  0.0  0.9  17040  9804 ?        Ss   Sep11   0:00 /lib/systemd/systemd --user
root        3205  0.0  0.3 169336  3764 ?        S    Sep11   0:00  \_ (sd-pam)
root        3306  0.0  0.1   2792  1300 ?        Ss   Sep11   0:00 /sbin/udevd -d
root        3976  0.0  0.1   2792  1336 pts/3    Ss   00:03   0:00 /usr/libexec/postfix/master
root        3985  0.0  0.1   2888  1000 pts/3    S+   00:03   0:00  \_ qmgr -l -t fifo -u
root@sandflysecurity:/root #
```

Sandfly Security®

Spot BPFDoor - Running Instance

```
root           1  0.0  1.1 166280 11392 ?        Ss   Sep10   0:02 /sbin/init
root         335  0.0  2.0  40040 19892 ?        S<s  Sep10   0:00 /lib/systemd/systemd-journald
root         372  0.0  2.7 289312 27100 ?        SLsl Sep10   0:06 /sbin/multipathd -d -s
systemd+     450  0.0  0.6  89352  6456 ?        Ssl  Sep10   0:00 /lib/systemd/systemd-timesyncd
systemd+     525  0.0  0.8  16116  8252 ?        Ss   Sep10   0:00 /lib/systemd/systemd-networkd
systemd+     544  0.0  1.3  25648 12948 ?        Ss   Sep10   0:00 /lib/systemd/systemd-resolved
root         568  0.0  0.6  22724  6236 ?        Ss   Sep10   0:00 /lib/systemd/systemd-udevd
root         626  0.0  0.2   7284  2744 ?        Ss   Sep10   0:00 /usr/sbin/cron -f -P
message+     628  0.0  0.4   8580  4756 ?        Ss   Sep10   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         630  0.0  0.5 1299308 5508 ?        Ssl  Sep10   0:00 /opt/digitalocean/bin/droplet-agent
root         635  0.0  1.9  33084 18856 ?        Ss   Sep10   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
syslog       636  0.0  0.5 222400  5640 ?        Ssl  Sep10   0:00 /usr/sbin/rsyslogd -n -iNONE
root         638  0.0  2.8 1245368 28416 ?       Ssl  Sep10   0:05 /usr/lib/snapd/snapd
root         640  0.0  0.7  15500  7552 ?        Ss   Sep10   0:00 /lib/systemd/systemd-logind
root         650  0.0  0.1   6216  1100 ttyS0    Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,57600,38400,9600 ttyS0 vt220
root         653  0.0  0.1   6172  1080 tty1     Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         678  0.0  0.9  15420  9228 ?        Ss   Sep10   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        3333  0.0  1.1  17188 11072 ?        Ss   Sep11   0:00  \_ sshd: root@pts/2
root        3385  0.0  0.5   9280  5420 pts/2    Ss+  Sep11   0:00  |   \_ -bash
root        3986  0.0  1.1  17188 11072 ?        Ss   00:03   0:00  \_ sshd: root@pts/4
root        4038  0.0  0.5   9148  5172 pts/4    Ss   00:03   0:00      \_ -bash
root        4054  0.0  0.3  10888  3584 pts/4    R+   00:04   0:00          \_ ps -auxwwf
root         686  0.0  2.1 110084 21348 ?        Ssl  Sep10   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root        2123  0.0  2.0 295960 20428 ?        Ssl  Sep11   0:00 /usr/libexec/packagekitd
root        2127  0.0  0.7 234492  6904 ?        Ssl  Sep11   0:00 /usr/libexec/polkitd --no-debug
root        3204  0.0  0.9  17040  9804 ?        Ss   Sep11   0:00 /lib/systemd/systemd --user
root        3205  0.0  0.3 169336  3764 ?        S    Sep11   0:00  \_ (sd-pam)
root        3306  0.0  0.1   2792  1300 ?        Ss   Sep11   0:00 /sbin/udevd -d
root        3976  0.0  0.1   2792  1336 pts/3    Ss   00:03   0:00 /usr/libexec/postfix/master
root        3985  0.0  0.1   2888  1000 pts/3    S+   00:03   0:00  \_ qmgr -l -t fifo -u
root@sandflysecurity:/root #
```

No elaborate tricks, just simple tradecraft gets the job done.

Spot BPFDoor - Shell Spawned

```
root           1  0.0  1.1 166280 11392 ?        Ss   Sep10   0:02 /sbin/init
root         335  0.0  2.0  40040 19892 ?        S<s  Sep10   0:00 /lib/systemd/systemd-journald
root         372  0.0  2.7 289312 27100 ?        SLsl Sep10   0:06 /sbin/multipathd -d -s
systemd+     450  0.0  0.6  89352  6456 ?        Ssl  Sep10   0:00 /lib/systemd/systemd-timesyncd
systemd+     525  0.0  0.8  16116  8252 ?        Ss   Sep10   0:00 /lib/systemd/systemd-networkd
systemd+     544  0.0  1.3  25648 12948 ?        Ss   Sep10   0:00 /lib/systemd/systemd-resolved
root         568  0.0  0.6  22724  6236 ?        Ss   Sep10   0:00 /lib/systemd/systemd-udevd
root         626  0.0  0.2   7284  2744 ?        Ss   Sep10   0:00 /usr/sbin/cron -f -P
message+     628  0.0  0.4   8580  4756 ?        Ss   Sep10   0:00 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         630  0.0  0.5 1299308 5508 ?        Ssl  Sep10   0:00 /opt/digitalocean/bin/droplet-agent
root         635  0.0  1.9  33084 18856 ?        Ss   Sep10   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
syslog       636  0.0  0.5 222400  5640 ?        Ssl  Sep10   0:00 /usr/sbin/rsyslogd -n -iNONE
root         638  0.0  2.8 1245368 28416 ?       Ssl  Sep10   0:05 /usr/lib/snapd/snapd
root         640  0.0  0.7  15500  7552 ?        Ss   Sep10   0:00 /lib/systemd/systemd-logind
root         650  0.0  0.1   6216  1100 ttyS0    Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,57600,38400,9600 ttyS0 vt220
root         653  0.0  0.1   6172  1080 tty1     Ss+  Sep10   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         678  0.0  0.9  15420  9228 ?        Ss   Sep10   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        3333  0.0  1.1  17188 11072 ?        Ss   Sep11   0:00  \_ sshd: root@pts/2
root        3385  0.0  0.5   9280  5420 pts/2    Ss+  Sep11   0:00  |   \_ -bash
root        3986  0.0  1.1  17188 11072 ?        Ss   00:03   0:00  \_ sshd: root@pts/4
root        4038  0.0  0.5   9148  5172 pts/4    Ss   00:03   0:00      \_ -bash
root        4054  0.0  0.3  10888  3584 pts/4    R+   00:04   0:00          \_ ps -auxwwf
root         686  0.0  2.1 110084 21348 ?        Ssl  Sep10   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root        2123  0.0  2.0 295960 20428 ?        Ssl  Sep11   0:00 /usr/libexec/packagekitd
root        2127  0.0  0.7 234492  6904 ?        Ssl  Sep11   0:00 /usr/libexec/polkitd --no-debug
root        3204  0.0  0.9  17040  9804 ?        Ss   Sep11   0:00 /lib/systemd/systemd --user
root        3205  0.0  0.3 169336  3764 ?        S    Sep11   0:00  \_ (sd-pam)
root        3306  0.0  0.1   2792  1300 ?        Ss   Sep11   0:00 /sbin/udevd -d
root        3976  0.0  0.1   2792  1336 pts/3    Ss   00:03   0:00 /usr/libexec/postfix/master
root        3985  0.0  0.1   2888  1000 pts/3    S+   00:03   0:00  \_ qmgr -l -t fifo -u
root@sandflysecurity:/root #
```

Does standard and reverse shell depending on packet received.

Sandfly Security®

SSH Backdoor Common Features

Magic Password Shell

Password Stealer

Non-Resident Code

SSH Backdoors

ENCRYPTED

****

S3kretPa55

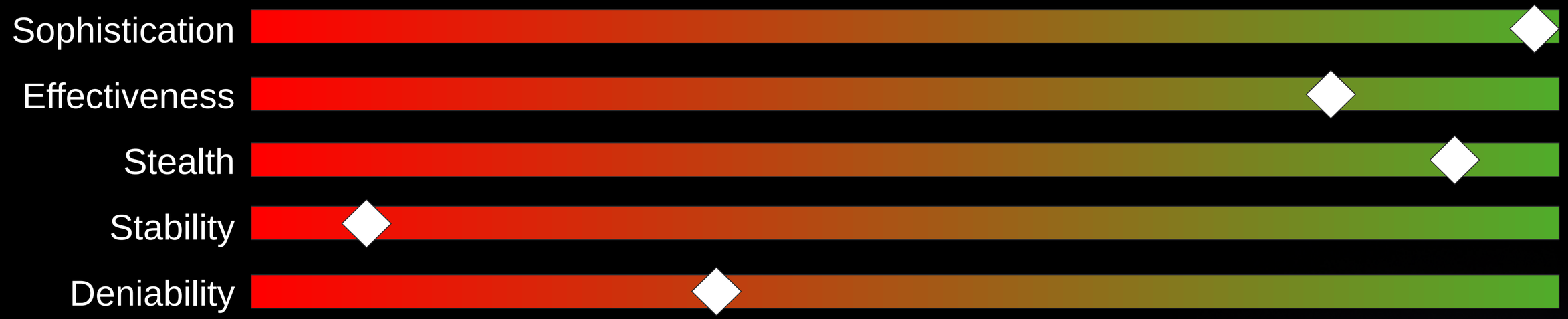
S3kretPa55

Sandfly Security®

Elite

Stealth Rootkits

Stealth Rootkits



Stealth Rootkits

Theory

Pinnacle of stealth and evasive tradecraft.

Stealth Rootkits

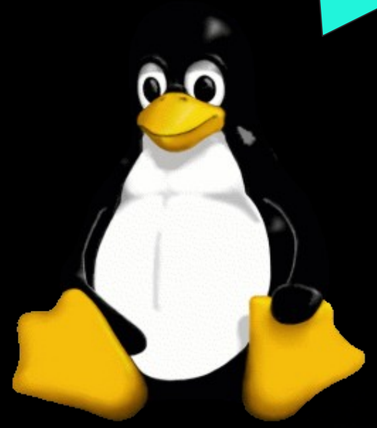
Reality

A stealth rootkit is a lawyer.

Stealth Rootkits

Give me data.

No Rootkit



Here you go.

Data

Stealth Rootkits

Give me data.

Let me consult my lawyer.

Rootkit

Altered Data

Data

Sandfly Security®

Stealth Rootkits - Complex Reality

Style	Compatibility	Stealth	Stability	Deployment	Risk/Reward
Loadable Kernel Module (LKM)					
Enhanced BPF (eBPF)					
io_uring					

Work well in targeted instances.

Evasive.

Expensive and a pain to deploy.

Can outsmart itself.

They got it onto the box somehow!

Stealth Rootkits - Rootkit Impacts

System Crashes

Performance Impacts

Updates Break System

Weird and Unexplained Network Activity

Stealth Rootkits - Detection

Directory and File Inconsistencies

Hidden Modules

Stealth Processes Decloaking

System Performance Impacts

Stealth Rootkits - Full Presentation

https://sandflysecurity.com/blog/linux-stealth-rootkit-hunting-presentation

Stealth Rootkits - Automated Detection

process_running_hidden_stealth

Alert | Lvl 5 | Latest

T1547.006 | defense_evasion | persistence | default_active | exploit.backdoor | exploit.rootkit | process

The process with PID `2129` is trying to hide. It has made itself invisible from listing in the /proc filesystem or system process listing tools. A stealth rootkit may have cloaked this PID to conceal it is operating on the remote host and forensic details may be masked. The host should be investigated directly with focus on the /proc/PID directory for unusual appearance, lack of being present, missing data, or other details that can indicate the process is being maliciously hidden. Other alerts on the host may reveal more details about the activity.

Seen 1 time on sfly-d-diamorphine (10.124.32.6).

Severity: 5

First Seen: 2026-04-30T06:18:56Z

Last Seen: 2026-04-30T06:18:56Z

View Sandfly | Analyze Result

dirs_cloaked_entry_bin

Alert | Lvl 5 | Latest

T1014 | T1547.006 | T1564.001 | defense_evasion | persistence | default_active | directory | exploit.rootkit

The directory `/usr/bin/` contains an entry, `/usr/bin/diamorphine_secret_dir`, that does not appear when retrieving the directory entries using normal tools (e.g. what you would see with 'ls'). This is a strong indication that a malicious stealth rootkit kernel module is hiding something from view.

Seen 1 time on sfly-d-diamorphine (10.124.32.6).

Severity: 5

First Seen: 2026-04-30T06:18:44Z

Last Seen: 2026-04-30T06:18:44Z

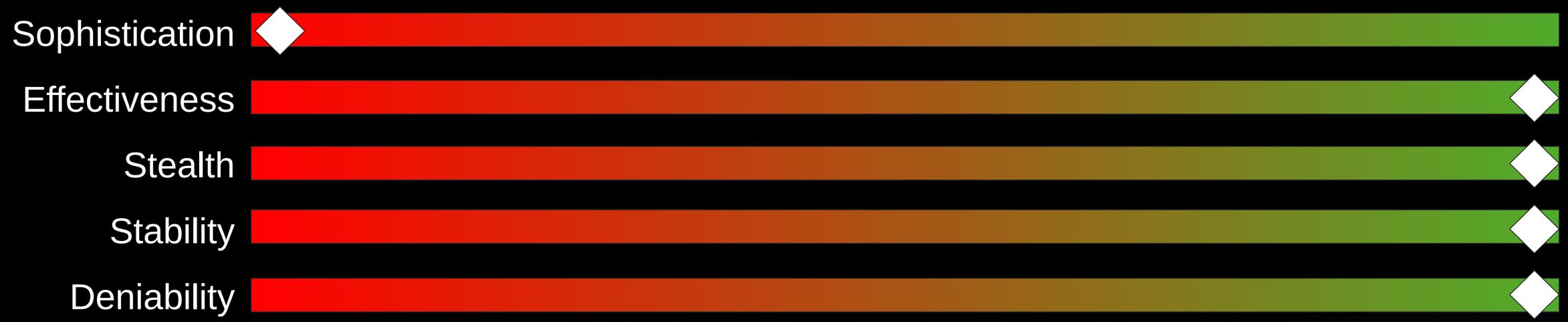
View Sandfly | Analyze Result

Super Elite

Super Elite - Compromised Credentials

Sandfly Security®

Compromised Credentials



Compromised Credentials

Malware Common Goal is to
Steal Credentials

Compromised Credentials - Why?

No need for elaborate exploit.

Blends in with normal users.

Installing implants is a cakewalk.

Risk is mainly that credentials may be rotated.

Compromised Credentials

Ransomware gang encrypted network from a webcam to bypass EDR

By Bill Toulas

March 6, 2025 03:31 PM 5

Weak and default credentials allow Linux compromise.

Compromised Credentials

```
root@sandflysecurity:/ # find / -name "id_ed25519" 2>/dev/null
/home/root/.ssh/id_ed25519
/home/root/.ssh/old/id_ed25519
/home/backups/.ssh/id_ed25519
```

Step 1: Simple command to find credentials lying about.

Compromised Credentials

```
root@sandflysecurity:/ # cat ~backups/.ssh/known_hosts
192.168.1.2 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5…ZTNcM65oH+wyDii3mjSN
10.2.2.2 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAID…1Mp2FkhrnTx4Kf7PI
…

root@sandflysecurity:/ # cat ~/.ssh/config
Host 192.168.1.2
     HostName backups.example.com
     User backups
     Port 22
     IdentityFile /home/backups/.ssh/id_ed25519

root@sandflysecurity:/ # last
backups pts/7    192.168.1.79     Tue Apr 21 13:48 - 13:48  (00:00)
…
```

Step 2: Look at system files and audit logs to find new systems to target.

Closing

Simple malware gets the job done.

Clumsy malware is stealth malware if you aren’t looking.

Regardless of malware type, they got on the box somehow.

Sandfly®

Agentless Linux Security

Craig H. Rowland
Founder, CEO
@CraigHRowland
www.sandflysecurity.com

Thank you.