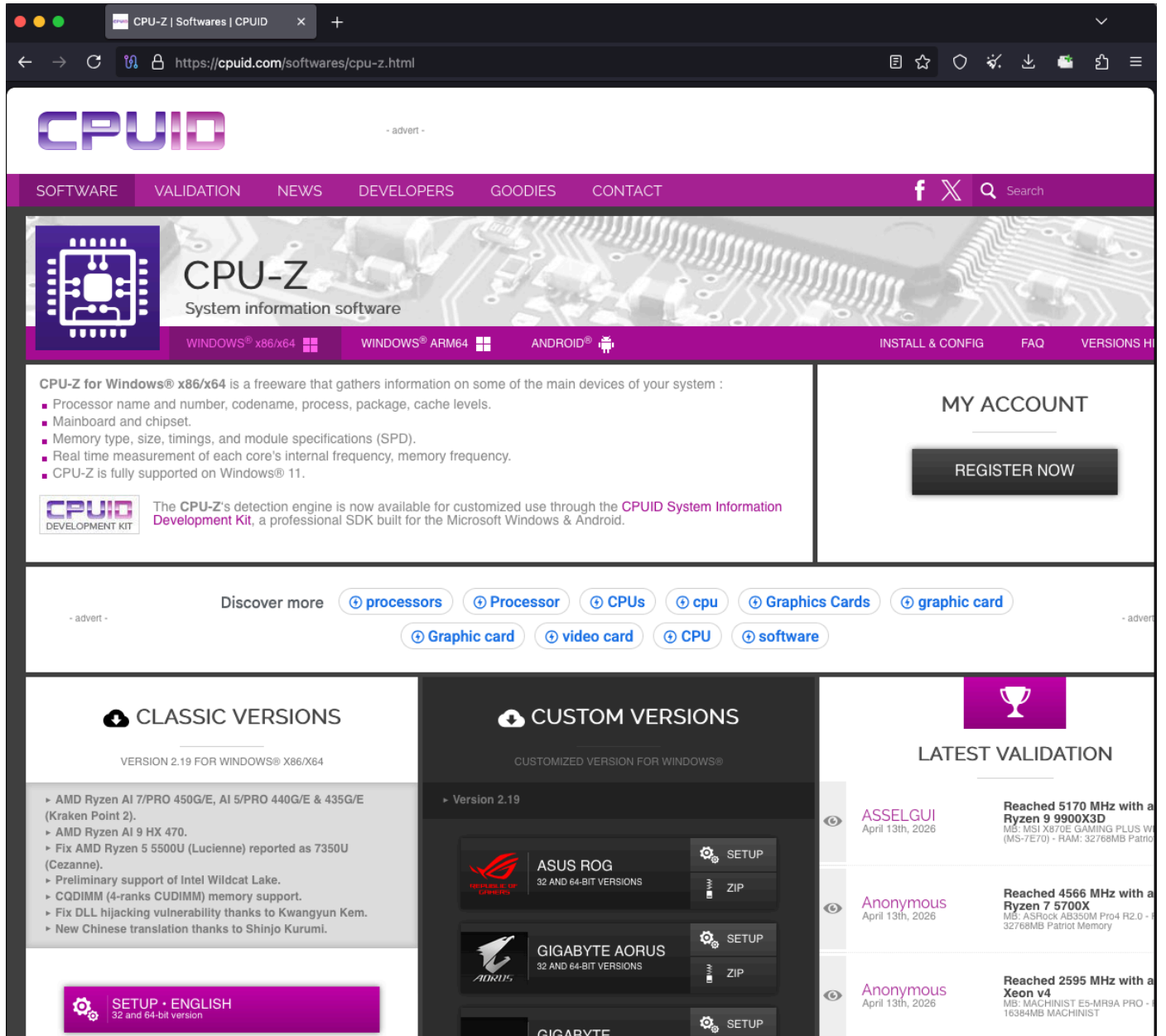


[Op Report] Trojanized CPU-Z Delivers STXRAT, Steals Credentials, and Exfils Data Through a Hidden QEMU VM

 blog.deception.pro/blog/cpuz-trojan-stxrat-purelogs-data-exfil-april-2026

MalBeacon

April 13, 2026



The screenshot shows the CPUID CPU-Z website. The header includes the CPUID logo and navigation links: SOFTWARE, VALIDATION, NEWS, DEVELOPERS, GOODIES, CONTACT. A search bar is also present. The main content area features a large CPU-Z logo and the text 'System information software'. Below this, there are tabs for WINDOWS® x86/x64, WINDOWS® ARM64, and ANDROID®. The left sidebar lists features of CPU-Z for Windows® x86/x64, such as processor name, mainboard, memory, and real-time frequency measurement. The right sidebar has a 'MY ACCOUNT' section with a 'REGISTER NOW' button. The main content area is divided into three sections: 'CLASSIC VERSIONS' (listing various AMD Ryzen and Intel processors), 'CUSTOM VERSIONS' (showing ASUS ROG and GIGABYTE AORUS versions), and 'LATEST VALIDATION' (displaying benchmark results for ASSELGUI, Anonymous, and Xeon v4).

Tags: CPU-Z, Trojan, STXRAT, PureLogs, RClone, Qemu, Data Exfiltration

Executive Summary

Between April 10 and April 15, 2026, a [Deception.Pro](https://blog.deception.pro) persistent operation captured a complete, multi-stage intrusion chain initiated via a trojanized CPU-Z hardware utility installer. The campaign delivered STXRAT via DLL side-loading, followed by PureLogs Stealer for credential

harvesting and PureHVNC for remote interactive access, culminating in two-plus days of covert data exfiltration routed through a locally-hosted QEMU Alpine Linux virtual machine as a network proxy.

This operation is notable for several reasons:

- It represents the first confirmed observed full post-exploitation chain following initial STXRAT infection for this campaign — while the initial trojanized CPU-Z delivery was previously documented by security vendors and flagged on X by ThreatrayLabs, no subsequent activity beyond STXRAT staging had been publicly reported.
- The threat actor employed sophisticated defense evasion: DLL side-loading into a signed binary, dynamic in-memory .NET compilation via csc.exe and InstallUtil, browser credential theft from isolated Chrome and Edge processes under calc.exe, and a QEMU-based VM to proxy exfiltration traffic.
- Data exfiltration via rclone serving a local WebDAV share tunneled through the QEMU Alpine VM ran continuously for approximately 54 hours (April 10 – April 12).
- Suricata telemetry from decrypted TLS PCAPs confirmed PureLogs Stealer C2

Despite public industry reporting stating otherwise, the threat actor demonstrated a high degree of operational sophistication, combining living-off-the-land (LOTL) binaries, sandbox evasion, and layered C2 infrastructure to maximize persistence and minimize detection surface.

Environment at a Glance

- **Replica Role:** Cloud Solutions Architect
- **Replica Organization:** Market-leading cloud-native AI platform firm
- **Industry:** Technology & IT Services
- **Topology:** Microsoft Active Directory environment with **1,000+ endpoints** and **500+ users**.
- **Replica Location:** United States
- **Observed duration:** ~12 days (Feb 3–Feb 16, 2026)
- **Sensor Stack:** LimaCharlie EDR, Suricata (EVE JSON & Decrypted TLS)
- **Infection Vector:** Trojanized CPU-Z 2.19 installer Zip (DLL side-loaded)
- **Primary Threat Families:** STXRAT, PureLogs Stealers, PureHVNC, rclone (exfil), QEMU Alpine (proxy)

***Note:** Replica personas, organizations, and documents are AI-generated and randomized for believability. Any resemblance to real-world entities is purely coincidental.*

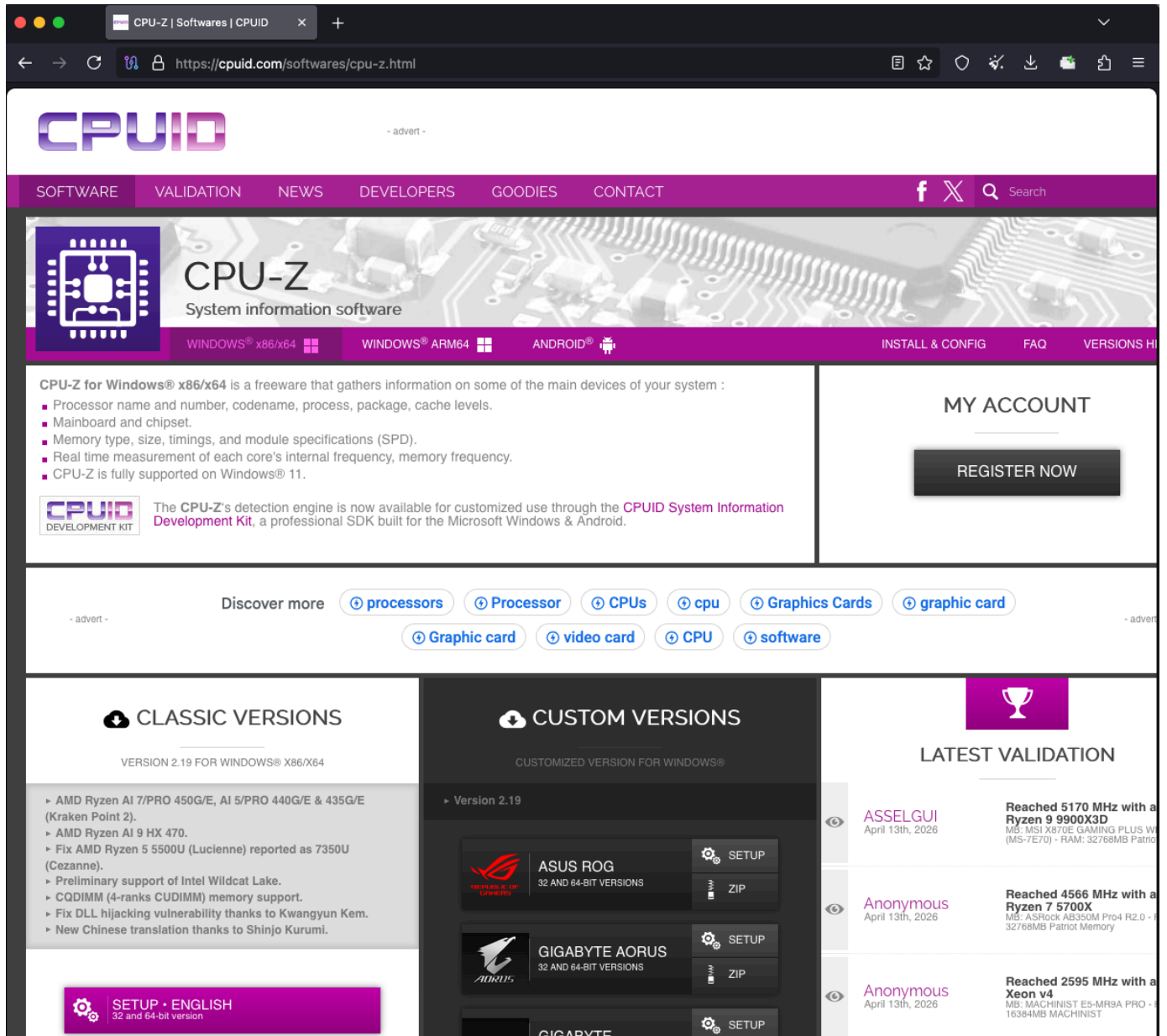


Figure 1: Initial website cpuid[.]com that contained trojanized installer.

Timeline of Operation Activity

2026-04-10 05:04:35 > Deception.Pro operation initialized and baited

2026-04-10 10:04:14 > Infection initiated: *cpu-z_2.19-en.zip* extracted cpuz_x64.exe and executed from Downloads folder

2026-04-10 10:04:14 > CRYPTBASE.dll side-loaded by CPU-Z binary; STXRAT dropper executes; C2 beacon to welcome.supp0v3[.]com

2026-04-10 10:04:17 > Suspicious TLSv1.2 connection from Windows PowerShell to public IP observed; first C2 contact

2026-04-10 10:08:25 > PureLogs Stealer injected into calc.exe; C2: 176.65.144[.]84:8443

2026-04-10 10:08:50 > TLS decrypted PCAP: ET MALWARE zgRAT / PureLogs Stealer CnC ping (SID:2067921); C2 176.65.144[.]84:8443

2026-04-10 10:08:52 > PureLogs Stealer launches headless Chrome and Edge instances with --no-sandbox flags to harvest saved credentials

2026-04-10 10:09:02 > ET MALWARE PureLogs Stealer plugin request (SID:2067922)

2026-04-10 10:26:26 > PowerShell downloads rclone from downloads.rclone[.]org via WindowsPowerShell/5.1 UA; placed in C:\ProgramData\Rclone\

2026-04-10 10:26:27 > PowerShell TLSv1.2 FQDN connection to bitbucket[.]org; QEMU/Alpine ZIP downloads

2026-04-10 10:26:27 > PowerShell: csc.exe compiles ClassLibrary17.dll from %TEMP%; InstallUtil.exe /u launches PureHVNC component; C2: 176.65.144[.]46:65001

2026-04-10 10:27:01 > SSLBL Malicious JA3 RAT to 176.65.144[.]46:65001; TLS1.0 on non-standard port

2026-04-10 10:27:03 > QEMU Alpine VM deployed: qemu-system-x86_64.exe launched; rclone serves C:\ as WebDAV on 127.0.0.1:52800

2026-04-10 10:29:10 > Data exfiltration begins: rclone → 127.0.0.1:52800 → QEMU Alpine VM → 94.156.119[.]71:443 (encrypted tunnel)

2026-04-10 11:04+ > Repeated PowerShell Invoke-Expression chains (non-interactive); dynamic .NET recompilation; multiple STXRAT beacon renewals

2026-04-12 17:00:42 > Data exfiltration to 94.156.119[.]71 ceases; approximately 54 hours of continuous exfil

2026-04-12+ > Continued STXRAT beaconing and PowerShell persistence loops observed through end of operation

2026-04-15 06:04:36 > Operation concluded

Total observed duration: ~ 5 days

Assessment

Threat Actor Profile

This campaign demonstrates a competent, financially motivated threat actor operating with a well-developed toolchain. The cluster of tools observed — STXRAT, PureLogs Stealer, PureHVNC, and rclone-based exfiltration — is consistent with an established crimeware ecosystem, likely offered as a coordinated Malware-as-a-Service (MaaS) stack. Deception.Pro captured the first documented full post-exploitation phase.

Infection Chain Analysis

The initial infection vector was a trojanized CPU-Z 2.19 installer ZIP file containing a malicious CRYPTBASE.dll, a classic DLL side-loading technique that abuses Windows search order to execute attacker code within the context of a trusted, signed binary.

The post-infection chain was highly automated and multi-staged:

- **Stage 1** — STXRAT dropper (CRYPTBASE.dll) established persistence and initiated C2 communication to welcome.sup0v3[.]com.
- **Stage 2** — PureLogs Stealer injected into calc.exe extracted stored credentials from Chrome and Edge profiles using headless browser instances with sandbox-disabled flags, a technique that bypasses many credential-theft detections by abusing legitimate browser binaries.
- **Stage 3** — PureHVNC component deployed via InstallUtil.exe proxy execution (LOLBin abuse), providing the actor with interactive hidden VNC-style access. The JA3 fingerprint of the resulting TLS session matched the SSLBL RAT signature.
- **Stage 4** — rclone and QEMU Alpine VM deployed to enable covert bulk data exfiltration. The use of a locally running VM as a network proxy is a sophisticated sandbox and network monitoring evasion technique, as traffic originates from a guest OS rather than from monitored Windows process contexts.

Exfiltration Assessment

Data exfiltration ran for approximately 54 continuous hours and was routed through an encrypted tunnel (TLS to 94.156.119[.]71:443) originating from within the QEMU Alpine VM — making traditional process-based network attribution difficult. The rclone WebDAV configuration served the entire C:\ drive, meaning credentials, documents, email databases, browser data, and

enterprise configuration files were all in scope. Suricata also detected a single session exceeding 100MB in upload volume to the PureHVNC C2 (176.65.144[.]46:65001), confirming significant data movement.

Novel Intelligence Value

Industry reporting (Kaspersky, ThreatrayLabs) had previously documented only the initial STXRAT staging phase of this campaign. The Deception.Pro honeynet captured all subsequent stages, including PureLogs credential theft, PureHVNC deployment, and the full QEMU-proxied exfiltration chain to 94.156.119[.]71. This represents unique, operationally obtained intelligence not available through sandbox analysis or threat feeds.

Defender Takeaways

- Hunt for DLL side-loading of CRYPTBASE.dll from non-system paths. Any process loading CRYPTBASE.dll from a user-writable directory (e.g., Downloads, Temp, AppData) should be treated as a high-confidence detection candidate.
- Alert on InstallUtil.exe invoked with /u against DLLs in %TEMP% or %AppData%. This is a well-documented LOLBin execution technique with limited legitimate use.
- Monitor for calc.exe spawning browser processes (chrome.exe, msedge.exe) — especially with --no-sandbox, --disable-gpu, and --user-data-dir flags pointing to Temp directories. This is a hallmark of PureLogs and similar infostealers.
- Flag PowerShell processes using Invoke-Expression with piped stdin ('[Console]::In.ReadToEnd() | Invoke-Expression') — this is the primary STXRAT loader pattern observed across dozens of process instances.
- Detect csc.exe (C# compiler) invocations from non-development directories, particularly from TEMP paths, especially when immediately followed by InstallUtil.exe.
- Alert on rclone.exe deployed to ProgramData with a 'serve webdav' command exposing the full drive root (C:\) to localhost. This is not a legitimate enterprise pattern.
- Monitor for QEMU binaries (qemu-system-x86_64.exe) arriving from downloads (Bitbucket) to ProgramData outside of known IT management tooling. QEMU as a network proxy for exfiltration is an emerging evasion technique.
- Implement JA3/JA3S fingerprinting on TLS traffic. The RAT JA3 hash (SSLBL match) to 176.65.144[.]46:65001 was confirmed by Suricata and should be blocked/alerted at the perimeter.
- Block or alert on outbound TLS to non-standard high ports (e.g., :65001, :8443) from PowerShell and .NET process contexts.

- Consider network-level blocking of rclone[.]org downloads from corporate endpoints unless explicitly whitelisted for IT use.

Indicators of Compromise

Domains & IP Addresses

welcome.sup0v3[.]com - STXRAT C2 (initial DLL beacon)

176.65.144[.]84:8443 - PureLogs Stealer C2

176.65.144[.]46:65001 - PureHVNC

94.156.119[.]71:443 - Data exfiltration destination via rclone → QEMU Alpine proxy

bitbucket[.]org/edge-id/* - Attacker-controlled Bitbucket repo hosting QEMU + Alpine ZIPs

downloads.rclone[.]org - rclone tool download (infrastructure abuse)

95.216.51[.]236:31415 - Additional STXRAT C2

Suricata Alert Signatures

ET MALWARE zgRAT / PureLogs Stealer CnC ping Request

ET MALWARE zgRAT / Purelogs Stealer plugin Request

ET MALWARE zgRAT / PureLogs Stealer userinfo Request

SSLBL: Malicious JA3 SSL-Client Fingerprint detected (RAT)

Suspicious TLSv1.2 from Windows 10 socket / PowerShell / Curl to public IP (possible Meterpreter/CS/PoshC2)

Suspicious TLSv1 connection from Windows PowerShell to public IP

Suspicious SSL/TLS traffic on unusual port

PowerShell (Windows) - TLSv1.2 connection to FQDN

HTTP Connection to Internet from PowerShell (Potential Corporate Privacy Violation)

ET INFO Windows PowerShell User-Agent Usage

ET HUNTING Terse Request for Zip File (GET)

Over 50MB uploaded via TLS to public IP - Possible data exfiltration

File Hashes (SHA-256)

eff5ece65fb30b21a3ebc1ceb738556b774b452d13e119d5a2bfb489459b4a46 cpu-z_2.19-en.zip
(trojanized installer)

49685018878b9a65ced16730a1842281175476ee5c475f608cadf1cdcc2d9524 CRYPTBASE.dll
(STXRAT DLL side-load)

8119f2ea89079ab7394bb4e8ff221a2f369bf236f95d6aa20f83dc7a98933d9a ClassLibrary17.dll
(PureHVNC component)

827dd3704285eb1c41b42b1594e6568d8bd316298302fd3bcbe46903998af90b alpine.zip (TA
Bitbucket; QEMU Alpine disk image)

22b50a35ab1eb552e0a25feec057e8b47bf56ae15188c0fba80de3fbfdf2d79d qemu.zip (TA
Bitbucket; QEMU binaries)

e5c9df28a017d812bddf80bb0f5ac4c8fa5e0053c9008cd46459f6c20d639829 qemu-system-
x86_64.exe (QEMU binary)

On-Disk Artifacts & Paths

- C:\Users\{REDACTED}\Downloads\cpu-z_2.19-en.zip
- C:\Users\{REDACTED}\Downloads\cpu-z_2.19-en\CRYPTBASE.dll
- C:\Users\{REDACTED}\AppData\Local\Temp\ClassLibrary17.dll
- C:\Users\{REDACTED}\AppData\Local\Temp\mhfy1aqj.rx3\ (Chrome credential temp dir)
- C:\Users\{REDACTED}\AppData\Local\Temp\wq1lah0p.xbc\ (Edge credential temp dir)
- C:\Users\{REDACTED}\AppData\Local\Temp\%TEMP%\siyqqv4x\ (csc.exe compilation staging)
- C:\Users\{REDACTED}\AppData\Local\Temp\%TEMP%\mjrbxuxr\ (csc.exe compilation staging)
- C:\ProgramData\Rclone\rclone.exe
- C:\ProgramData\QemuAlpineVM\qemu-system-x86_64.exe
- C:\ProgramData\QemuAlpineVM\qemu-system-x86_64w.exe
- C:\ProgramData\QemuAlpineVM\alpine.raw

Command-Line Artifacts for Hunting

STXRAT / PowerShell Loader

- powershell.exe -Command "[Console]::In.ReadToEnd() | Invoke-Expression"
- powershell.exe -Command "\$input | Invoke-Expression"

PureHVNC Proxy Execution

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /u  
C:/Users/{REDACTED}/AppData/Local/Temp/ClassLibrary17.dll
```

Rclone Data Exfiltration

```
"C:\ProgramData\Rclone\rclone.exe" serve webdav C:\ --addr 127.0.0.1:52800 --user  
backup --pass localhost --vfs-cache-mode writes
```

QEMU Alpine VM (Network Proxy)

```
"C:\ProgramData\QemuAlpineVM\qemu-system-x86_64w.exe" -m 512 -drive  
file=C:/ProgramData/QemuAlpineVM/alpine.raw,format=raw,if=ide,cache=writeback -nic  
user -accel tcg,thread=multi -smp 2 -nographic -nodefaults -display none -vga none -accel  
whpx
```

PureLogs Stealer Browser Credential Harvest

- "C:\Program Files\Google\Chrome\Application\chrome.exe" --disable-fre --no-default-browser-check --no-first-run --no-sandbox --allow-no-sandbox-job --disable-gpu --mute-audio --disable-audio --user-data-dir="C:\Users\{REDACTED}\AppData\Local\Temp\mhfy1aqj.rx3"
- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --diabile-fre --no-default-browser-check --no-first-run --no-sandbox --allow-no-sandbox-job --disable-gpu --mute-audio --disable-audio --user-data-dir="C:\Users\{REDACTED}\AppData\Local\Temp\wq1lah0p.xbc"

About Deception.Pro

The intelligence in this report was captured exclusively through **Deception.Pro** — a persistent honeynet platform operated by . Deception.Pro runs continuously instrumented Windows Active Directory environments baited to attract real adversaries. Unlike sandboxes or synthetic datasets, every byte of telemetry reflects genuine attacker behavior in a realistic enterprise context: real tooling, real C2 infrastructure, real decision-making.

Our sensor stack captures full-fidelity **LimaCharlie EDR telemetry**, **Suricata EVE JSON** (including decrypted TLS PCAP analysis), **Zeek logs**, and full PCAPs — all MITRE ATT&CK-mapped and available for licensing to AI SOC vendors, security researchers, and threat intelligence teams. The dataset spans hundreds of completed operations and thousands of hours of adversary dwell time, capturing campaigns from commodity crimeware to targeted ransomware precursor activity.

This operation exemplifies what Deception.Pro delivers: intelligence you cannot synthesize, cannot replicate in a sandbox, and cannot find in any public dataset. If your organization trains detection models, builds AI-powered SOC tooling, or requires ground-truth adversary telemetry, **contact us at deception.pro** to discuss dataset access and licensing.