CYBER THREAT INTELLIGENCE

CRITICALSTART® Security Advisory

TLP AMBER // [CS-SA-26-0305] Security Advisory on Axios NPM Compromise

Executive Summary

On March 31, 2026, the npm package Axios, a widely downloaded used HTTP client with approximately 100M+ weekly downloads, was compromised through a maintainer account hijack. The attacker published two malicious versions injecting a cross-platform Remote Access Trojan (RAT) capable of fully compromising Windows, macOS, and Linux systems.

With high confidence, researchers attribute this incident to BlueNoroff, the financially motivated subgroup of North Korea's state-sponsored Lazarus Group (APT38, DPRK). The attack is the latest in a documented, multi-year campaign pattern targeting the developer supply chain and arrives only days after a separate actor, TeamPCP, conducted a series of structurally similar attacks across multiple open-source ecosystems.

This incident is part of a broader threat: Software Supply Chain Compromise. Notably, Critical Start's H2 2025 Cyber Threat Intelligence Report explicitly identified Software Supply Chain and Developer Ecosystem Compromise as the first of three primary trending cybersecurity concerns for the period. The Axios supply chain compromise on March 31, 2026, is a direct materialization of that risk, confirming that the concern Critical Start flagged in H2 2025 has not diminished. It has intensified. This advisory details the incident, broader software supply chain risks, and prioritized organizational mitigation strategies.

Attack Overview

Attribute	Detail
Compromised package	Axios (versions 1.14.1 and 0.30.4)
Malicious dependency	plain-crypto-js@4.2.1
C2 server	sfrclak.com:8000 (142.11.206.73)
Attribution	BlueNoroff / Lazarus Group (DPRK)

Two newly published versions of Axios: 1.14.1 and 0.30.4 were found to inject `plain-crypto-js@4.2.1` as a fake dependency. The attacker published both versions using the compromised npm credentials of the primary Axios maintainer ('jasonsaayman'), bypassing the project's GitHub Actions CI/CD pipeline.

The attack was not opportunistic. The malicious dependency was staged 18 hours in advance. Three separate payloads were pre-built for three operating systems. Both the 1.x and 0.x release branches were hit within 39 minutes. Every trace was designed to self-destruct. The embedded malware launches via an obfuscated Node.js dropper (setup.js) and branches into one of three attack paths depending on the host operating system:

- macOS: Runs an AppleScript payload to fetch a trojan binary from `sfrclak.com:8000`, saves it as `/Library/Caches/com.apple.act.mond`, makes it executable, and launches it in the background. The AppleScript is then deleted.

- Windows: Locates the PowerShell binary, copies it to `%PROGRAMDATA%\wt.exe` (disguised as Windows Terminal), and drops a VBScript to the temp directory that contacts the same C2 to fetch and execute a PowerShell RAT.
- Linux: Uses Node.js execSync to fetch a Python RAT script from the same C2, saves it to `/tmp/ld.py`, and executes it in the background using nohup.

After launching the main payload, the dropper performs three anti-forensic cleanup steps: removes the postinstall script, deletes the package.json referencing the postinstall hook, and renames a pre-staged clean package.md to package.json - replacing the malicious manifest with a benign-looking one to defeat post-infection inspection.

The payload exhibits distinct capabilities across platforms. On macOS, written in C++ as a Mach-O universal binary and detected as NukeSped, it performs process injection, AppleScript execution, filesystem enumeration, and communicates with a command-and-control server every 60 seconds. On Windows, implemented in PowerShell and detected as Trojan.Boxter, it leverages reflective .NET loading, process hollowing into cmd.exe, and maintains persistence through the registry. On Linux, developed in Python, it carries out credential harvesting, command execution, and confirmed sandbox evasion.

Broader Software Supply Chain Attacks

The Axios compromise is part of a sustained, multi-year pattern of adversaries weaponizing the open-source software supply chain, a threat explicitly highlighted in Critical Start H2 2025 Cyber Threat Landscape Report. This attack should not be viewed in isolation. Since the SolarWinds intrusion in 2020 demonstrated that tampering with trusted software distribution channels could achieve strategic-scale compromise with a single action, threat actors across all motivation profiles, including nation-state, ransomware, and financially opportunistic groups, have steadily expanded into developer ecosystems.

The dependency injection model that enabled the Axios attack has been repeatedly exploited. XZ Utils, backdoored in early 2024 through a years-long social engineering operation against an open-source maintainer, showed that patient adversaries will invest significant time establishing legitimate contributor status before introducing malicious code. The 3CX supply chain attack in 2023, also attributed to Lazarus, confirmed that even compiled desktop applications distributed through official channels can be weaponized, affecting hundreds of thousands of downstream businesses. The codecov breach, the event-stream npm compromise, and polyfill.io's CDN hijacking each followed the same pattern: identify a trusted artifact consumed by millions, inject malicious code, and rely on the distribution network to propagate it at scale.

The current environment differs from these earlier incidents in both tempo and actor diversity. What was once largely the domain of sophisticated nation-state groups has become a widely adopted playbook. Criminal groups like TeamPCP execute regular campaigns across npm, PyPI, and GitHub Actions, while state actors like Lazarus maintain continuous operational presence across registries. The common thread is exploitation of the implicit trust developers, CI/CD systems, and package managers place in recognized registry artifacts. Until this trust model is reinforced with verification, provenance, and behavioral monitoring, the open-source ecosystem remains the highest-leverage initial access vector available to adversaries of any capability level. Both the BlueNoroff-attributed Axios attack and the TeamPCP campaign wave in March 2026 demonstrate that threat actors at every level of sophistication, from state-sponsored APTs to financially motivated criminal groups, are converging on the same high-leverage vector: the trusted open-source ecosystem that underpins modern software development.

Recent NPM Attack Campaigns

Date	Campaign	Method
May 2025	Graphalgo wave 1	Fake recruiter 'Veltrix Capital', LinkedIn/Reddit lures
Sep 2025	npm chalk/debug compromise	18 packages, ~2.6B weekly downloads affected
Dec 2025	BeaverTail new variant	npm is-buffer/eslint/redux mimics, job interview lures
Feb 4, 2026	XPACK ATTACK	HTTP 402 paywall trick, GitHub fingerprinting
Feb 11, 2026	Graphalgo wave 2	bigmathutils v1.1.0 weaponized after 10K+ downloads
Mar 31, 2026	Axios compromise	Maintainer hijack, NukeSped RAT, plain-crypto-js

Threat Actors Overview

Several threat actors are notorious for software supply chain compromise. This advisory highglights BlueNoroff and TeamPCP.

BlueNoroff – BlueNoroff, also tracked as TA444, Sapphire Sleet, COPERNICIUM, STARDUST CHOLLIMA, CageyChameleon, and APT38, is a DPRK-linked subgroup of the Lazarus Group under the Reconnaissance General Bureau. Active since at least 2016, it focuses on financial theft from cryptocurrency and banking, serving as the revenue-generating arm of Lazarus.

Operations begin with social media reconnaissance to create credible personas. Contact occurs over Telegram, impersonating venture capital representatives to deliver malicious ZIPs or GitHub links. In a 2025 Web3 case, a Calendly link redirected to a fake Zoom site, followed weeks later by a staged meeting with deepfake executives that led to installation of a malicious Zoom extension acting as an AppleScript dropper.

Execution on macOS relies on AppleScript via osascript, often disguised as updates. Post-execution activity includes Mach port process injection requiring com.apple.security.cs.debugger. Persistence methods evolve; the Hidden Risk campaign modified zshenv to run across all Zsh sessions without triggering background alerts. Malware is modular and multi-language, including Rust, C++, Python, Go, Swift, Nim, and Objective-C. A 2025 intrusion deployed eight binaries, including a Go backdoor (Root Troy V4), Nim persistence implant (Telegram 2), Objective-C keylogger/screencapture (XScreen/keyboardd), and a Go infostealer targeting 24 cryptocurrency wallets (CryptoBot/airmond).

TeamPCP – TeamPCP is a prevalent active non-state supply chain threat actor currently operating. In March 2026 alone, TeamPCP compromised Trivy (a container scanner), KICS (an infrastructure scanning tool), LiteLLM (an AI model routing library), and telnyx (a communications Python SDK). In the telnyx attack, two malicious versions were pushed to PyPI on March 27, 2026, concealing credential harvesting capabilities inside a .WAV audio file using steganography. TeamPCP's target selection focuses on tools with elevated access to automated pipelines - each requires broad read access to credentials, configs, and environment variables by design. This mirrors the Axios attacker's logic of targeting a ubiquitous HTTP library embedded in CI/CD pipelines.

The key distinction between TeamPCP and the Axios attacker is motivation. TeamPCP is financially motivated and credential-focused, harvesting secrets for resale and follow-on ransomware operations, announcing collaborations with LAPSUS$ and the Vect ransomware group. The Axios attacker deployed persistent full-featured RATs, indicating objectives of sustained access and intelligence collection – consistent with BlueNoroff's state-directed mission.

Industry Impact

The impact of software supply chain compromises is concentrated in sectors that rely heavily on modern development practices, cloud-native infrastructure, and third-party software.

Financial Services & Fintech

These organizations face the highest exposure, both as direct targets of state-sponsored actors like BlueNoroff seeking banking and cryptocurrency access, and as heavy consumers of open-source developer tooling. The 3CX supply chain attack in 2023 demonstrated the risk, allowing Lazarus to pivot from a compromised VoIP platform into customer environments across global banks and trading firms.

- Subsector: Cryptocurrency, DeFi, and Web3 – This vertical is precisely targeted due to high-value transactions, reliance on npm and other open-source tooling, and developer-focused attack surfaces. BlueNoroff has maintained continuous operations against blockchain engineers, crypto exchanges, wallet developers, and Web3 applications for years. Combined with social engineering campaigns such as fake job interviews and deepfake meetings, the threat to this subsector is both persistent and multi-dimensional.

Technology Sector

Software companies, SaaS providers, cloud platforms, and managed service providers face disproportionate risk because a single compromised dependency can cascade through products to every downstream customer. Poisoned developer tools and CI/CD pipelines directly affect engineering and security teams, with the blast radius extending across all systems their pipelines touch.

Healthcare & Critical Infrastructure

While not always the direct targets of initial compromises, these organizations are increasingly downstream victims. Cloud-native adoption and reliance on commercial software expose them through dependency chains. Compromised electronic health record systems, operational software, or medical device management platforms can result in operational disruption and patient safety impacts. The Critical Start H2 2025 report highlighted healthcare's sharp rise as the third most targeted industry overall, with supply chain compromise explicitly cited as an initial access vector.

Large Enterprise Organizations Across Industries

Organizations with sizable internal development teams are exposed due to scale. Automated dependency resolution, containerized builds, and continuous integration pipelines against public registries make them susceptible to malicious package uploads. A 2024 Sonatype report estimated over 245,000 malicious package uploads per year, a number growing more than 150% year-over-year, making supply chain compromise an operational norm rather than an exception.

Implications for Organizations

Software supply chain compromises, including malicious npm packages, have far-reaching implications for organizations of all sizes. At a strategic level, they expose enterprises to systemic risk: a single compromised dependency can cascade through internal applications, CI/CD pipelines, and customer-facing products, amplifying the operational and reputational impact. Organizations may face data breaches, intellectual property theft, regulatory violations, and service disruptions, even if the initial compromise targeted a third-party library rather than internal systems directly.

From an operational perspective, these incidents highlight the need for robust dependency governance, continuous monitoring of software supply chains, and verification of package provenance.

Engineering and security teams must implement policies for secure dependency management, code review, and vulnerability scanning, as automated builds and containerized deployments can inadvertently propagate malicious code at scale.

At the workforce level, developers, DevOps teams, and IT staff are directly affected, as their daily workflows intersect with potentially compromised tools. Social engineering campaigns targeting developers, such as phishing, fake job offers, or impersonation, further increase risk, requiring both technical controls and ongoing security awareness training.

For leadership, software supply chain attacks demand a shift from reactive incident response to proactive risk management. This includes integrating supply chain security into enterprise risk assessments, vendor evaluations, and internal software development life cycles. Until organizations adopt verification, provenance tracking, and behavioral monitoring across their software dependencies, open-source ecosystems remain a high-leverage vector that can be exploited by adversaries at any capability level.

What Critical Start is Doing

Critical Start has concluded investigations and notes that there is no evidence of any of our customers being directly exploited as a result of the Axios supply chain compromise. All activity observed to date has been linked to active security alert monitoring within customer environments, demonstrating that our proactive detection and response capabilities are functioning as intended. Critical Start's Cyber Research Unit (CRU) continues to the dark web, and open sources for signs of emerging threats or exploitation.

Prioritized Mitigation Strategies

To mitigate risks associated with the reported Axios npm compromise and related software supply chain attacks, we recommend the following prioritized strategies:

Immediate (< 24 Hours)

- Check all environments and also inspect package-lock.json history via git log. Run `npm list Axios | grep -E '1\.14\.1|0\.30\.4'` and `npm list plain-crypto-js`.
- Rotate ALL credentials, tokens, API keys, and secrets accessible from that environment - including cloud provider credentials, SSH keys, and any secrets stored in environment variables.
- Audit CI/CD pipeline runs during the exposure window: March 31, 00:21–03:15 UTC.
- Block at DNS and perimeter firewall: sfrclak.com, callnrwise.com, nrwise.com, 142.11.206.73.
- Hunt for host artifacts: /Library/Caches/com.apple.act.mond (macOS), C:\ProgramData\system.bat (Windows), /tmp/ld.py (Linux). Note: Endpoint detections are low/inconsistent, and hunting is mandatory for now.

Short-Term (< 2 Weeks)

- Investigate whether any developer in your organization has been contacted by unknown parties offering investment meetings, job opportunities, or requiring download of Zoom or Teams extensions from non-official domains - particularly in crypto, DeFi, or Web3 contexts.
- Audit npm publishing tokens across all projects. Revoke long-lived classic tokens that bypass 2FA and replace with short-lived OIDC tokens scoped to specific GitHub Actions workflows.

- Consider enforcing minimum package release age policies (7 days recommended) via registry configuration or dependency management tooling such as pnpm's minimum-release-age or Aikido Safe Chain.
- For macOS environments in financial/crypto/Web3 sectors: supplement endpoint AV with behavioral detection and memory inspection - the NukeSped RAT evades most traditional AV at time of disclosure.

Conclusion

The Axios supply chain compromise underscores the persistent and evolving risk posed by software supply chain attacks. While no evidence currently indicates direct exploitation of Critical Start customers, the incident highlights the importance of proactive monitoring, dependency governance, and supply chain security practices. Organizations across all industries must remain vigilant, verifying the provenance of open-source dependencies, implementing behavioral monitoring, and integrating supply chain risk into broader cybersecurity strategies. Organizations without a direct axios dependency could still have been exposed through other software/packages/dependencies like `@shadanai/openclaw` or `@qqbrowser/openclaw-qbot`. Critical Start will continue to track developments and provide updates as new intelligence emerges.

For more threat reports, including H2 2025 detailing trending cybersecurity concerns visit Critical Start’s Intel Hub. Should anything new surface, this advisory will be updated. This advisory was written using the best intelligence available at the time and is subject to change as additional information becomes available.

Further Reading

1. N3mes1s - Axios npm Supply Chain Compromise: Verified Threat Intel + Full Payload Reverse Engineering (2026-03-31) https://gist.github.com/N3mes1s/0c0fc7a0c23cdb5e1c8f66b208053ed6
2. The Hacker News - Axios Supply Chain Attack Pushes Cross-Platform RAT via Compromised npm Account (2026-03-31) https://thehackernews.com/2026/03/axios-supply-chain-attack-pushes-cross.html
3. The Hacker News - TeamPCP Pushes Malicious Telnyx Versions to PyPI, Hides Stealer in WAV Files (2026-03-27) https://thehackernews.com/2026/03/teampcp-pushes-malicious-telnyx.html
4. Picus Security - BlueNoroff Group: The Financial Cybercrime Arm of Lazarus (2026-01-20) https://www.picussecurity.com/resource/blog/bluenoroff-group-the-financial-cybercrime-arm-of-lazarus
5. Huntress - Feeling Blue(Noroff): Inside a Sophisticated DPRK Web3 Intrusion (2025-06-18) https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis
6. SentinelOne Labs - BlueNoroff Hidden Risk: Threat Actor Targets Macs with Fake Crypto News and Novel Persistence (2024-11-07) https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/
7. Elastic Security Labs - DPRK Strikes Using a New Variant of RustBucket (2023-07) https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket
8. Jamf - BlueNoroff APT Targets macOS with RustBucket Malware (2023-04) https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware/

9. SentinelOne - SmoothOperator: Ongoing Campaign Trojanizes 3CX Software in Supply Chain Attack (2023) https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/
10. Kaspersky Securelist - The BlueNoroff Cryptocurrency Hunt Is Still On (2022) https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
11. CISA / FBI / Treasury - Guidance on the North Korean Cyber Threat (AA22-116A) (2022-04-27) https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-116a
12. Snyk - A Post-Mortem of the Malicious event-stream Backdoor (2018) https://snyk.io/blog/a-post-mortem-of-the-malicious-event-stream-backdoor/
13. Codecov - Security Update (2021) https://about.codecov.io/security-update/
14. Sansec - Polyfill Supply Chain Attack (2024) https://sansec.io/research/polyfill-supply-chain-attack
15. openwall / Andres Freund - XZ Utils Backdoor Disclosure (2024-03-29) https://www.openwall.com/lists/oss-security/2024/03/29/4
16. CISA - Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies (SolarWinds/SUNBURST) (2020-12-17) https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
17. FBI / IC3 - North Korea Targeting Employees of DeFi, Cryptocurrency, and Web3 Businesses (PSA240903) (2024-09-03) https://www.ic3.gov/PSA/2024/PSA240903
18. Critical Start - H2 2025 Cyber Threat Intelligence Report (2025) https://security.criticalstart.com/rs/586-OQG-630/images/2025%20H2%20CTI%20Report.pdf?version=0
19. Sonatype - 2024 State of the Software Supply Chain Report https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security
20. StepSecurity – axios Compromised on npm (2026) https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious-versions-drop-remote-access-trojan

Appendices

Appendix A: TTPs Summary Table

The following table summarizes observed BlueNoroff TTPs across documented campaigns including RustBucket, KandyKorn, ObjCShellz, Hidden Risk, GhostCall/GhostHire, and the Axios supply chain attack.

Tactic	Technique ID	Technique Name
Reconnaissance	T1589	Gather Victim Identity Information
Reconnaissance	T1593	Search Open Websites/Domains
Resource Development	T1583.001	Acquire Infrastructure: Domains
Resource Development	T1583.003	Acquire Infrastructure: VPS
Resource Development	T1587.001	Develop Capabilities: Malware
Resource Development	T1588.002	Obtain Capabilities: Tool
Resource Development	T1598.001	Phishing for Info: Spearphishing Service
Initial Access	T1195.002	Supply Chain: Software Dependencies
Initial Access	T1566.001	Phishing: Spearphishing Link
Initial Access	T1566.002	Phishing: Spearphishing Attachment
Initial Access	T1566.003	Phishing: Spearphishing via Service
Execution	T1059.001	PowerShell
Execution	T1059.002	AppleScript (osascript)
Execution	T1059.005	Visual Basic Script
Execution	T1059.006	Python
Execution	T1059.007	JavaScript
Execution	T1204.001	User Execution: Malicious Link
Execution	T1204.002	User Execution: Malicious File
Execution	T1204.004	User Execution: Malicious Copy/Paste (ClickFix)
Persistence	T1543.001	Launch Agent (macOS)
Persistence	T1543.004	Launch Daemon (macOS)
Persistence	T1547.001	Registry Run Keys (Windows)
Persistence	T1176.001	Browser Extensions
Persistence	T1546.004	Unix Shell: .zshenv
Privilege Escalation	T1055	Process Injection
Privilege Escalation	T1548.002	Bypass UAC
Privilege Escalation	T1548.006	TCC Manipulation (macOS)
Defense Evasion	T1027	Obfuscated Files / Information
Defense Evasion	T1027.002	Software Packing (Themida)

Tactic	Technique ID	Technique Name
Defense Evasion	T1036	Masquerading
Defense Evasion	T1036.001	Invalid Code Signature
Defense Evasion	T1070.004	File Deletion
Defense Evasion	T1140	Deobfuscate / Decode Files
Defense Evasion	T1553.002	Code Signing Subversion
Defense Evasion	T1562.001	Disable / Modify Tools
Defense Evasion	T1564.003	Hidden Window
Credential Access	T1056.002	GUI Input Capture
Credential Access	T1552.001	Credentials in Files
Discovery	T1016	System Network Config Discovery
Discovery	T1033	System Owner / User Discovery
Discovery	T1057	Process Discovery
Discovery	T1082	System Information Discovery
Discovery	T1083	File / Directory Discovery
Discovery	T1497	Sandbox Evasion
Collection	T1005	Data from Local System
Collection	T1056.001	Keylogging
Collection	T1113	Screen Capture
Collection	T1115	Clipboard Data
Command & Control	T1071.001	Web Protocols (HTTP/S)
Command & Control	T1105	Ingress Tool Transfer
Command & Control	T1573.002	Encrypted Channel
Exfiltration	T1041	Exfiltration Over C2
Impact	T1657	Financial Theft

Appendix B: Indicators of Compromise

Network Indicators

Indicator	Type	Description
sfrclak.com	Domain	Primary C2
callnrwise.com	Domain	Secondary C2 (same IP; registered 53 min before primary)
nrwise.com	Domain	Attacker staging domain (same WHOIS registrant as sfrclak.com)
142.11.206.73	IP	C2 server - Hostwinds LLC, Seattle WA (AS54290)
http://sfrclak.com:8000/6202033	URL	Payload endpoint
mozilla/4.0 (compatible; msie 8.0; windows nt 5.1; trident/4.0)	User-Agent	Used across all three RAT platforms
28d28d28d00028d00028d28d28d96d86b34e11c2d3d550 8f7111adf9d91	JARM	C2 TLS fingerprint

Additional Infrastructure (BlueNoroff)

Domain / IP	Campaign
matuaner.com	Hidden Risk
delphidigital.org	Hidden Risk
selinicapital.com (and variants)	Hidden Risk
zoom-client.com	Hidden Risk
23.254.253.75	Hidden Risk C2
us05web-zoom.biz	GhostCall Web3 Intrusion
metamask.awaitingfor.site	GhostCall Web3 Intrusion
productnews.online	GhostCall - CryptoBot C2
firstfromsep.online	GhostCall - Nim implant C2
142.11.209.109	Lazarus infrastructure
23.254.226.90	KandyKorn C2
104.168.214.151	ObjCShellz (swissborg.blog)

File-Based Indicators

File	SHA256
setup.js (dropper)	e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09
macOS NukeSped RAT	92ff08773995ebc8d55ec4b8e1a225d0d1e51efa4ef88b8849d0071230c9645a
Windows PS RAT (Stage 2)	617b67a8e1210e4fc87c92d1d1da45a2f311c08d26e89b12307cf583c900d101
Windows cradle (system.bat)	f7d335205b8d7b20208fb3ef93ee6dc817905dc3ae0c10a0b164f4e7d07121cd
Linux Python RAT (ld.py)	fcb81618bb15edfdedfb638b4c08a2af9cac9ecfa551af135a8402bf980375cf
plain-crypto-js-4.2.1.tgz	58401c195fe0a6204b42f5f90995ece5fab74ce7c69c67a24c61a057325af668
Axios-1.14.1.tgz (compromised)	5bb67e88846096f1f8d42a0f0350c9c46260591567612ff9af46f98d1b7571cd
Axios-0.30.4.tgz (compromised)	59336a964f110c25c112bcc5adca7090296b54ab33fa95c0744b94f8a0d80c0f

Host-Based Indicators

Platform	Path / Registry Key
All	node_modules/plain-crypto-js/setup.js (self-deletes post-execution)
Windows	C:\ProgramData\system.bat
Windows	C:\ProgramData\wt.exe (renamed PowerShell)
Windows	%TEMP%\6202033.vbs / %TEMP%\6202033.ps1
Windows (registry)	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftUpdate
macOS	/Library/Caches/com.apple.act.mond (NOT a legitimate Apple binary)
Linux	/tmp/ld.py