Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

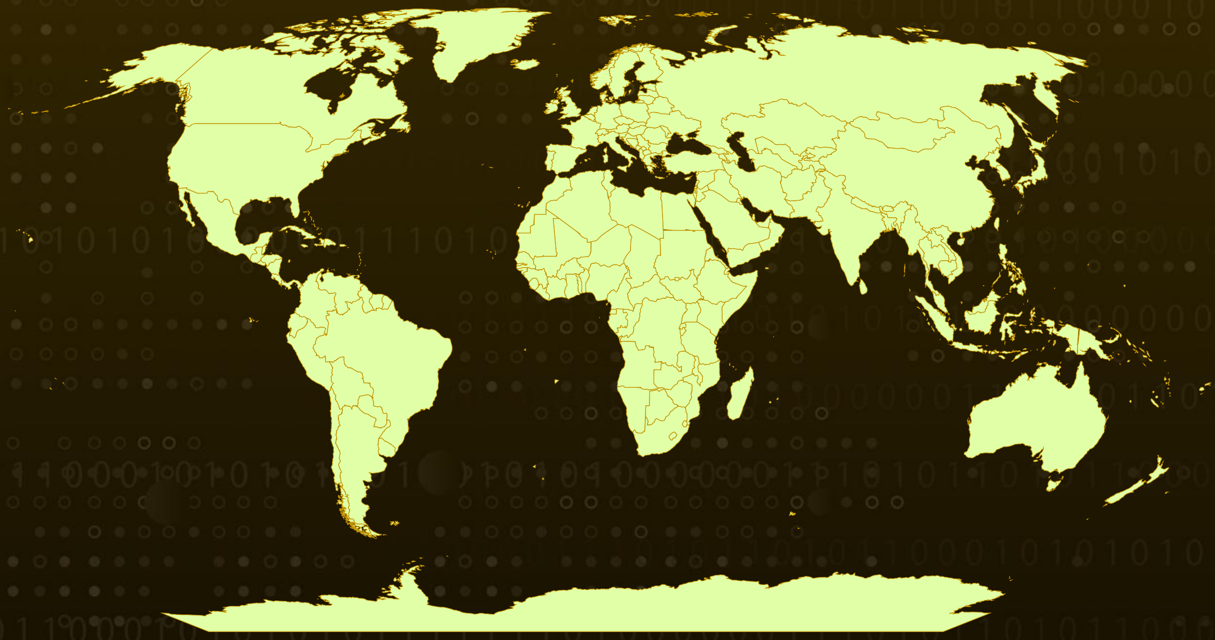
Olymp Loader: Modular Malware Built for Rapid Exploitation

Date of Publication	Admiralty Code	TA Number
October 3, 2025	A1	TA2025303

Summary

Attack Discovered: June 2025
Targeted Countries: Worldwide
Affected Platform: Windows
Malware: Olymp Loader
Attack: In early June 2025, a cybercrime storefront called OLYMPO rolled out Olymp Loader, a slick, assembly-built loader and crypter that quickly turned into a turnkey kit for stealing data and taking over machines. Marketed as Fully UnDetectable, it bundles browser, Telegram and crypto-wallet stealers, ships rapid updates through Telegram, and gets seeded via developer-focused channels (including poisoned GitHub binaries), often acting as a second-stage for commodity RATs like LummaC2 and WebRAT. Its mix of aggressive Defender tampering, customizable shellcode, and easy-to-use modules means even less-skilled actors can mount fast, effective intrusions, so what looks like a single downloader can rapidly become a full-blown data-harvest operation.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 Olymp Loader emerged in early June 2025 as a polished Malware-as-a-Service offering, first advertised on underground forums and a Telegram channel by a developer using the handle OLYMPO. What began as a botnet concept has quickly been retooled into a modular loader and crypter platform: its marketing touts a compact assembly-language core and claims of being Fully Undetectable (FUD). The product now bundles built-in stealers for browsers, Telegram, and cryptocurrency wallets, and its designers have engineered a fast update cadence that lets new features reach paying customers almost immediately, accelerating attack volume and shortening the window between development and abuse.

#2 As the user base grew, the operators refined functionality, adjusted pricing, and adopted evasion tactics that they advertise aggressively. In early August 2025, they published tiered pricing on Telegram: a "classic" stub at $50 with Defender-bypass guarantees and certificate signing, a $100 option for shellcode customization, and a $200 "unique" stub that pairs custom shellcode with injection into a distinct, legitimate executable.

#3 Olymp Loader is implemented in assembly and can host a wide variety of payload types, with binary sizes that vary according to the legitimate application used for injection. Modules and payloads use deep XOR obfuscation and bespoke algorithms; the authors claim defeat heuristic and ML-based detectors; components are signed, and the platform supports automated persistence, aggressive UAC flooding for privilege elevation, and techniques such as LoadPE/code cave injection.

#4 Attackers have abused developer-focused binaries hosted in public GitHub repositories and have sometimes used Olymp as a second-stage delivered alongside commodity loaders such as Amadey, pointing to possible pay-per-install or reseller chains. Common downstream payloads included LummaC2, WebRAT, QasarRAT, and Raccoon; many samples launched multiple executables from the same stealer family.

#5 Since the launch, the project has been repeatedly reworked: the centralized botnet panel was removed and, after an August 2025 restructure, payloads became embedded and encrypted inside stubs that execute after disabling Defender. New stealing modules for browsers, Telegram, and crypto wallets arrived in late June, and a July API enabled proxy-backed custom modules. Recovered code snippets show practical features, registry reads for Telegram, multi-monitor screenshots, targeted file patterning, and packaged exfiltration, while third-party stealers (BrSteal/BrowserSnatch variants) and a Python/Nuitka toolchain were also observed.

Recommendations

Harden Endpoints: Harden endpoints by blocking execution from folders often abused by malware, such as Downloads, AppData, Temp, and Pictures. Apply least-privilege rules so normal users cannot install or run software that needs administrator rights.

Hunt for the Loader's Behavior Patterns: Hunt for suspicious behaviors like repeated use of cmd.exe with timeout commands, files being copied into AppData or Startup, .bat scripts appearing in startup folders, and PowerShell scripts that establish persistence.

Email Security: Strengthen email and web security with advanced filtering, URL rewriting, and sandboxing. Train users to spot malicious installers and brand impersonation.

Treat Cryptowallet and Telegram Apps as High-risk Assets: Apply strict security controls to machines handling crypto wallets, developer tools, or Telegram apps. Use MFA, hardened workstations, encrypted storage, and limit local storage of private keys.

Monitor for Unusual Certificates and Signed Binaries: Keep an inventory of trusted code-signing certificates and alert on new or unusual certificates. Restrict execution of binaries signed with unknown or suspicious certificates.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1204 User Execution	T1204.002 Malicious File

T1059 Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1059.001** PowerShell	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1036** Masquerading
T1036.005 Match Legitimate Resource Name or Location	**T1055** Process Injection	**T1027** Obfuscated Files or Information	**T1553** Subvert Trust Controls
T1553.002 Code Signing	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1112** Modify Registry
T1016 System Network Configuration Discovery	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1552** Unsecured Credentials
T1552.001 Credentials In Files	**T1113** Screen Capture	**T1005** Data from Local System	**T1567** Exfiltration Over Web Service
T1041 Exfiltration Over C2 Channel	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7bc217f0ee12266d42812af436f494caf599c0705242457a581f64d4eb508904, d36da9c3e5e78aa87bcdcd7fc8d3499d85a60b9dd107bf775d759940fc2f2489, D167a0c6fdba1175b67f10daf4be218b4d8adf2f81280ba5d1510228a4321bca, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23, ff1e159c4c6fcb97c9cb1885796fa4557e1afb92c82ada00f24ae994bffd63e4, 9464a2a1fb53b3a8c783ee4b55bba69cbb74a841f0d06f0cef86a93d607be5ae, 59b143fd884f8450cf5161954ebf38dbd9c951ecdb13de5e1f6aea01a9f92201,

TYPE	VALUE
SHA256	60fec45a29a89c1cb10fd793065e8fc39bdae15daf813e3438e8ff6558fb7e2d, 561809b0c9c67b7d48712ab9e53cf5cc137b94d5a2d8bc65314a2db4c23df99d, 9d5d474791793300a273c5b6e522c7c3acd6fbb26c4da0421d4ef695c82f3fa5, 446c7b9ff49c7c0b8ae02b720054e4f09ef60475c92a5d7f2e2b2bdb4ca5de23, 14e4884288c1740d5a4b67ac83a890000c3b92f945139b2433bf9746acd14f9b, 01562cd36b61d517959fdbe5beaef9e1e9462be292c74a49b36a30057d09bc2c, 60f8b5a6c8621e07124fbec4b9253b913056d1279d6c42fdd99a8b6b14c33e9a, 048701ffc9b7ccfe4228bfaaa0b98a0518f02c6325c7f59365f863eccb65aa6d, c465c1ac750e80ffb4020ec085528ca520b4fca587710ae1a5937bc88e5ad22c, dbe4aaef628f4d392fd25946643424334af4ecb9eb2589884112b465f508ca33, 02eb774341d84b8c83b448186f3de8db139c52bea2376fec0ac88c7112186fd2, Ee1e27a01b884099a614b8eee78cdb1dd02ffecd6ed9f6a54b7b567b9eab979f
URLs	hxxp[:]//fastdownloads[.]live/dl/putty[.]exe, hxxp[:]//jjf[.]life/OpenSSL/build[.]exe, hxxps[:]//jjf[.]life/OpenSSL/ZoomClientSetup[.]exe, hxxps[:]//classic-offensive[.]com/Installer[.]zip

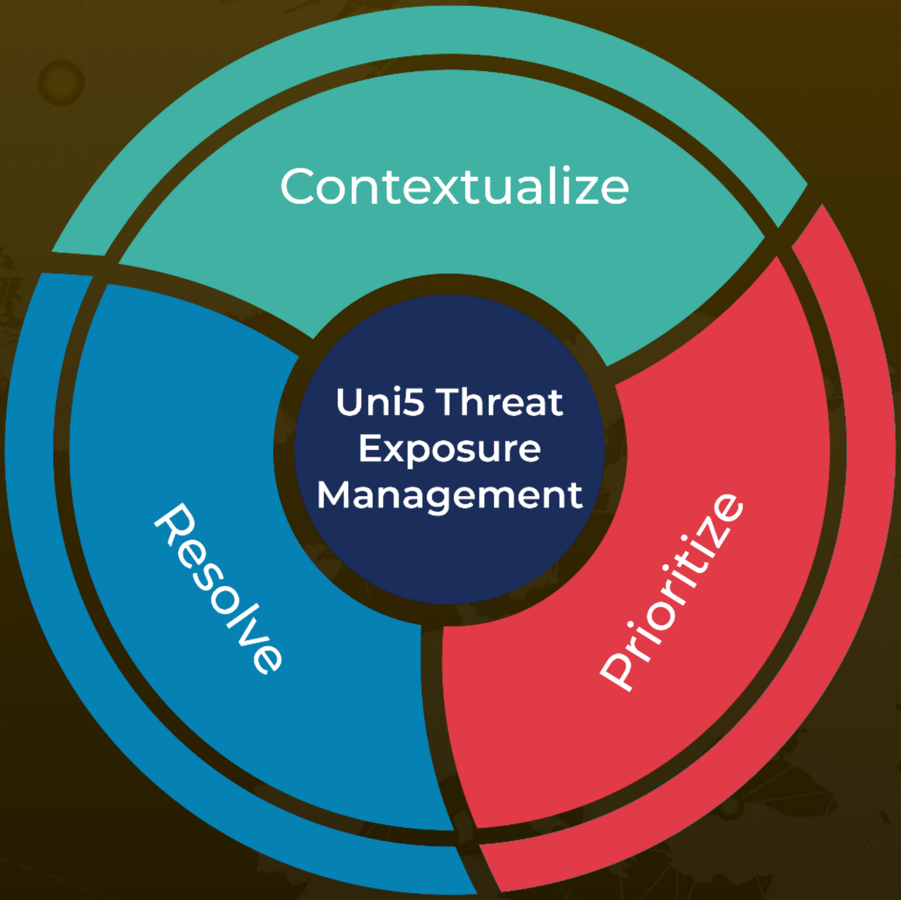
References

https://outpost24.com/blog/olymp-loader-a-new-malware-as-a-service/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 3, 2025 • 8:30 AM

More at www.hivepro.com