Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

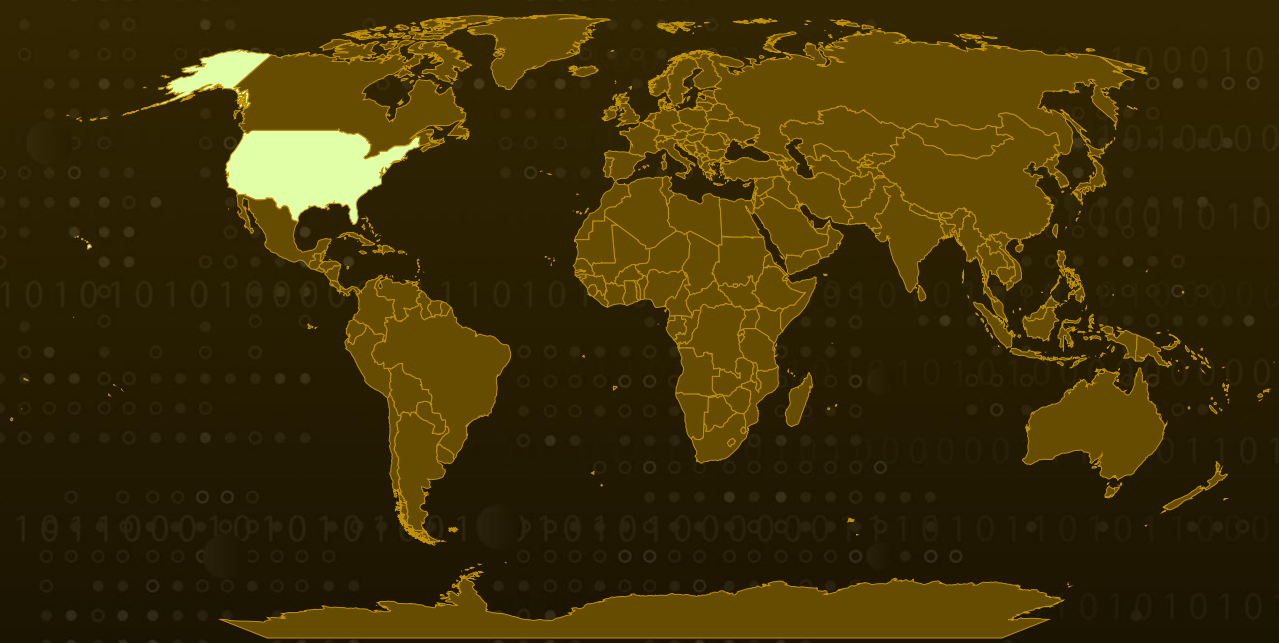
Ghost Crypt Delivers PureRAT in Accounting Firm Attack

Date of Publication	Admiralty Code	TA Number
July 22, 2025	A1	TA2025228

Summary

Attack Discovered: May 2025
Targeted Country: United States
Targeted Industry: Accounting Firm
Targeted Platform: Windows
Malware: PureRAT, Ghost Crypt
Attack: In May 2025, a U.S. accounting firm fell victim to a stealthy cyberattack that used a convincing disguise, a fake new client requesting urgent help through a PDF. Hidden within the file was a ZIP archive containing malware protected by a tool called Ghost Crypt, designed to slip past antivirus defenses. Once opened, the malware quietly installed PureRAT, a remote access trojan capable of stealing sensitive information, including data from crypto wallets and desktop apps. The attackers used clever techniques like sideloading, memory injection, and encrypted communications to stay hidden and maintain control. Highlighting how attackers are combining social engineering with advanced malware to target businesses with valuable data.

Attack Regions



Attack Details

#1 In May 2025, a U.S.based public accounting firm became the target of a stealthy cyberattack involving a newly emerging crypter known as Ghost Crypt. The attackers, posing as a potential new client, sent an email containing a malicious PDF that linked to a ZIP file hosted on Zoho WorkDrive. Inside the ZIP archive were seemingly benign documents, including a license copy and tax forms, cleverly designed to trick the recipient into executing a hidden payload. Once opened, a legitimate executable was abused to sideload a malicious DLL. This DLL was then copied to the victim's Documents folder and used a Windows Registry key to establish persistence on the system.

#2 Ghost Crypt is a commercial crypting service that offers advanced obfuscation and sideloading for EXE and DLL files. It boasts compatibility with x86, .NET, and native binaries, and promises to bypass Windows Defender, cloud-based AV solutions, and even Windows 11 24H2+ security mechanisms. Its marketing claims include full browser-based protection bypass, customizable stub sizes, and a three-day "survival guarantee" offering free re-crypting if detection occurs. Priced at $225, it supports well-known malware strains and **PureRAT** the payload used in this particular attack.

#3 Under the hood, Ghost Crypt employs a modified ChaCha20 encryption scheme to decrypt its payload, which is stored within oledlg.dll. It uses a non-standard setup including a 12-byte null nonce and a null counter and modifies the encryption key mid-stream, making analysis more difficult. The malware leverages a technique dubbed "Process Hypnosis" to decrypt and inject the PureRAT payload. This involves debugging a legitimate process, allocating RWX memory, and writing the malware directly into that memory space using WriteProcessMemory. The final stage resumes execution with the malware fully embedded neatly bypassing modern process injection safeguards, even those on Windows 11.

#4 Once active, PureRAT decrypts its components using AES-256, decompresses them with GZIP, and proceeds with execution. A separate DLL, protected with .NET Reactor, contains the loader logic. Instead of traditional execution the DLL uses hardcoded class and method names to invoke the payload. Once unpacked, the DLL loads an X.509 certificate and uses SetThreadExecutionState to prevent the system from sleeping, ensuring uninterrupted execution.

#5 After achieving persistence and execution, PureRAT gathers detailed system and user information and exfiltrates it to a remote command-and-control server. Its targets are specifically geared toward financial data, with a focus on Chrome-based crypto wallet extensions and desktop cryptocurrency applications. This operation closely mirrors earlier tactics seen in PureHVNC campaigns. The malware's architecture clearly allows for modular functionality, hinting at further capabilities beyond initial compromise.

Recommendations

- **Be Extra Cautious with Unexpected Emails:** Be skeptical of emails from unknown senders especially those claiming to be new clients or containing links and ZIP files. If an email seems even slightly suspicious, verify it through a separate trusted channel before clicking anything.
- **Use Strong Email Filtering and Attachment Scanning:** Deploy advanced email security tools that can detect and block malicious attachments or links especially embedded ZIP files or PDFs that may contain malware.
- **Block DLL Sideloading:** Monitor and restrict sideloading behavior such as legitimate apps being abused to load harmful DLLs. Limit what DLLs can be loaded from user-writable directories like Documents.
- **Watch for Unusual Persistence:** Regularly audit the Windows Registry and startup folders for suspicious entries. Malware like PureRAT often hides in places where it can quietly restart on boot.
- **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	TA0005 Defense Evasion
TA0007 Discovery	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1204 User Execution	T1204.001 Malicious Link

T1574 Hijack Execution Flow	**T1574.001** DLL	**T1656** Impersonation	**T1041** Exfiltration Over C2 Channel
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1082 System Information Discovery	**T1033** System Owner/User Discovery	**T1071** Application Layer Protocol	**T1083** File and Directory Discovery
T1057 Process Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:Port	196[.]251[.]88[.]111[:]56002, 176[.]65[.]144[.]123[:]56002
Domain	fax-greenry[.]myhome-server[.]de
SHA256	69a40bd2f667845ab95ad8438dae390f2e8b9680f4d30cb20e920c45cda565f9, f3d98823fb6cdc226414bedc49b94e86060fcc511cc50867d63f7c989fe54aed, 1ac0767e5a22839ae581ea31fcfcd693f1d35092a33576cb5269a2f7b415d964
Mutex	6ad742cc0dd3

References

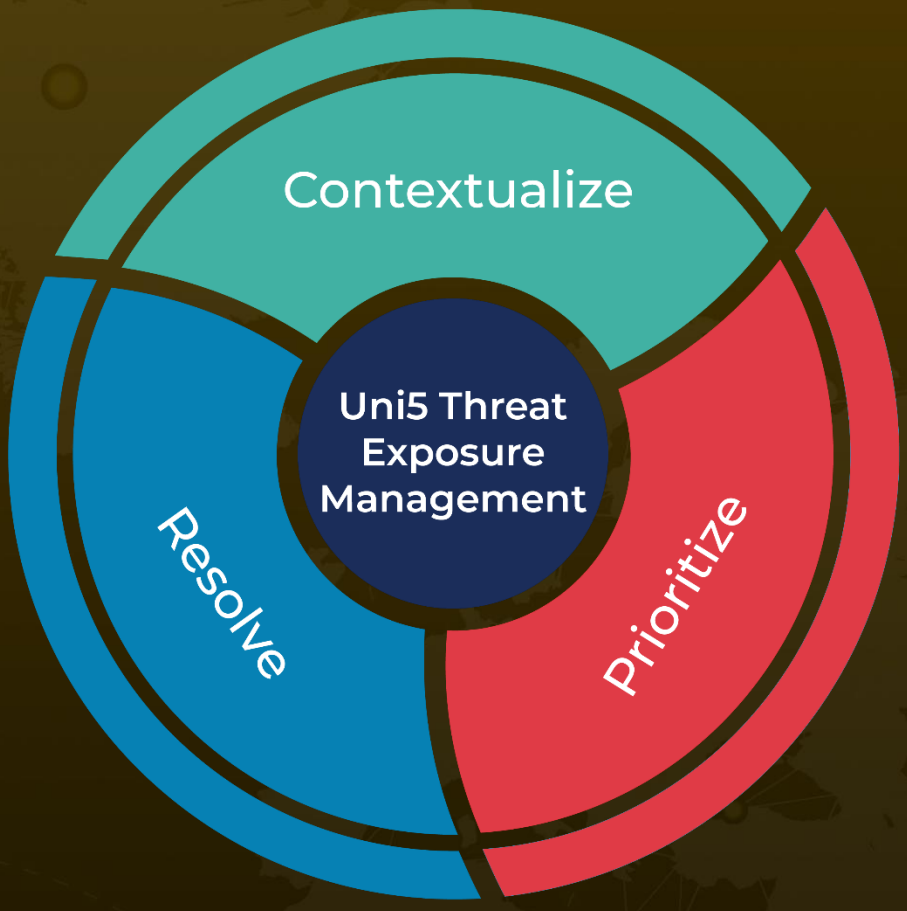
https://www.esentire.com/blog/ghost-crypt-powers-purerat-with-hypnosis

https://hivepro.com/threat-advisory/pure-rats-stealthy-campaign-sweeps-russian-enterprises/

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

July 22, 2025 • 5:30 AM

More at www.hivepro.com