Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

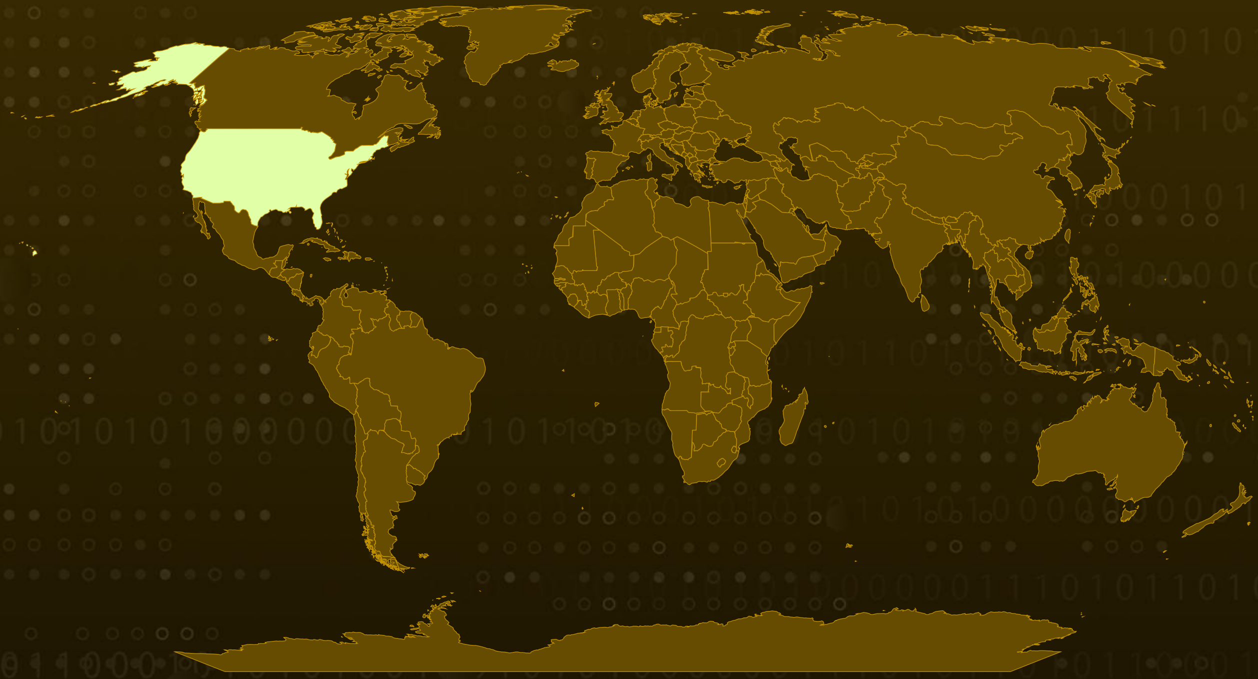
TransferLoader: The Malware That Outsmarts Security

Date of Publication	Admiralty Code	TA Number
May 16, 2025	A1	TA2025153

Summary

Active Since: February 2025
Malware: TransferLoader
Targeted Region: United States
Targeted Industry: Law Firms
Attack: TransferLoader is a sophisticated, modular malware loader equipped with resilient persistence mechanisms. Comprised of a downloader, loader, and backdoor, it employs obfuscation and junk code to evade detection and hinder reverse engineering. Linked to the delivery of Morpheus ransomware and confirmed in attacks against U.S. law firms, TransferLoader is a prime example of the modern, evasive threat.

Attack Regions



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

Attack Details

#1 TransferLoader is a sophisticated malware loader active since February 2025. It follows a modular architecture comprising three core components: a downloader, a backdoor, and a loader for the backdoor. The malware employs advanced evasion techniques, including anti-debugging checks, runtime string decryption, control flow obfuscation, and junk code insertion to evade detection.

#2 The downloader acts as the initial payload, establishing HTTPS communication using crafted HTTP headers to retrieve encrypted payloads. These are decrypted with a decrementing XOR key and executed. To mask its activity, the downloader may open decoy PDF files, either legitimate or junk-laden.

#3 It also resolves function exports dynamically via a custom hashing algorithm and attempts to restart Windows Explorer when necessary. The loader operates within trusted processes such as Explorer or WordPad. It maintains secure communication through encrypted named pipes and achieves persistence via registry modifications and COM hijacking.

#4 Configuration data, including command-and-control (C2) addresses and encryption keys, is stored in the Windows registry. The loader verifies specific file conditions before proceeding with execution. The backdoor functions as the malware's command execution component. It supports arbitrary command execution, file operations, configuration updates, and data exfiltration.

#5 If primary C2 communication fails, it uses the decentralized InterPlanetary File System (IPFS) to retrieve updated C2 addresses. TransferLoader incorporates extensive anti-analysis techniques. It checks its filename for predefined substrings, requires specific command-line arguments, and inspects the Process Environment Block (PEB) for debugging flags.

#6 TransferLoader represents a modern, highly obfuscated malware loader featuring layered persistence mechanisms, resilient fallback communication paths, and multiple embedded payloads. It has been linked to the delivery of Morpheus ransomware, including a confirmed attack against an American law firm.

Recommendations

Monitor and Block Registry Modifications: TransferLoader frequently alters the Windows registry for persistence. Implement automated registry integrity checks to detect unauthorized changes to the registry, especially in keys related to COM hijacking and C2 configurations.

Signature and Heuristic Analysis: Ensure that the IDPS can analyze not only known malware signatures but also heuristic patterns, including dynamic runtime decryption, to flag potentially malicious behavior in real-time.

File Integrity Monitoring: Employ file integrity monitoring systems to track changes to critical system files and configurations. TransferLoader may attempt to alter or add files to critical directories, and monitoring for unauthorized changes can trigger immediate alerts.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Application Whitelisting: Implement application whitelisting to allow only trusted applications to run on systems. This restricts the execution of unknown binaries like those used by TransferLoader and blocks it from running unauthorized payloads.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0007** Discovery
TA0011 Command and Control	**TA0010** Exfiltration	**T1083** File and Directory Discovery	**T1018** Remote System Discovery
T1059 Command and Scripting Interpreter	**T1106** Native API	**T1055** Process Injection	**T1070.001** Clear Windows Event Logs

T1071.001 Web Protocols	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1070 Indicator Removal
T1070.004 File Deletion	T1127 Trusted Developer Utilities Proxy Execution	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1070.009 Clear Persistence	T1036 Masquerading	T1046 Network Service Discovery	T1036.004 Masquerade Task or Service
T1041 Exfiltration Over C2 Channel	T1027 Obfuscated Files or Information	T1027.001 Binary Padding	T1562 Impair Defenses

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	11d0b292ed6315c3bf47f5df4c7804edccbd0f6018777e530429cc7709ba6207, b8f00bd6cb8f004641ebc562e570685787f1851ecb53cd918bc6d08a1caae750, b55ba0f869f6408674ee9c5229f261e06ad1572c52eaa23f5a10389616d62efe
URLs	hxxps[:]//mainstomp[.]cloud/MDcMkjAxsLKsT, hxxps[:]//baza[.]com/loader[.]bin, hxxps[:]//temptransfer[.]live/SkwkUTIoFTrXYRMd, hxxps[:]//sharemoc[.]space/XdYUmFd2xX, hxxps[:]//ipfs[.]io/ipns/k51qzi5uqu5djqy6wp9nng1igaatx8nxwpye9iz18ce6b8ycihw8nt04khemao

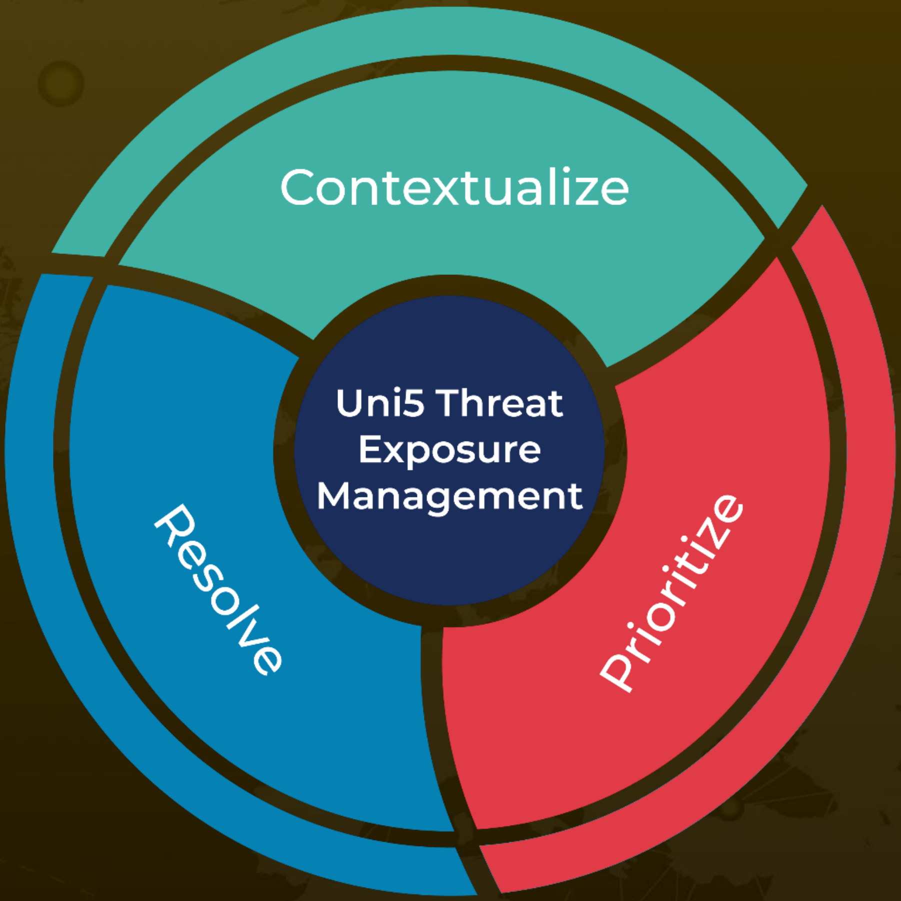
References

https://www.zscaler.com/blogs/security-research/technical-analysis-transferloader

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

May 16, 2025 • 6:30 AM

More at www.hivepro.com