Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

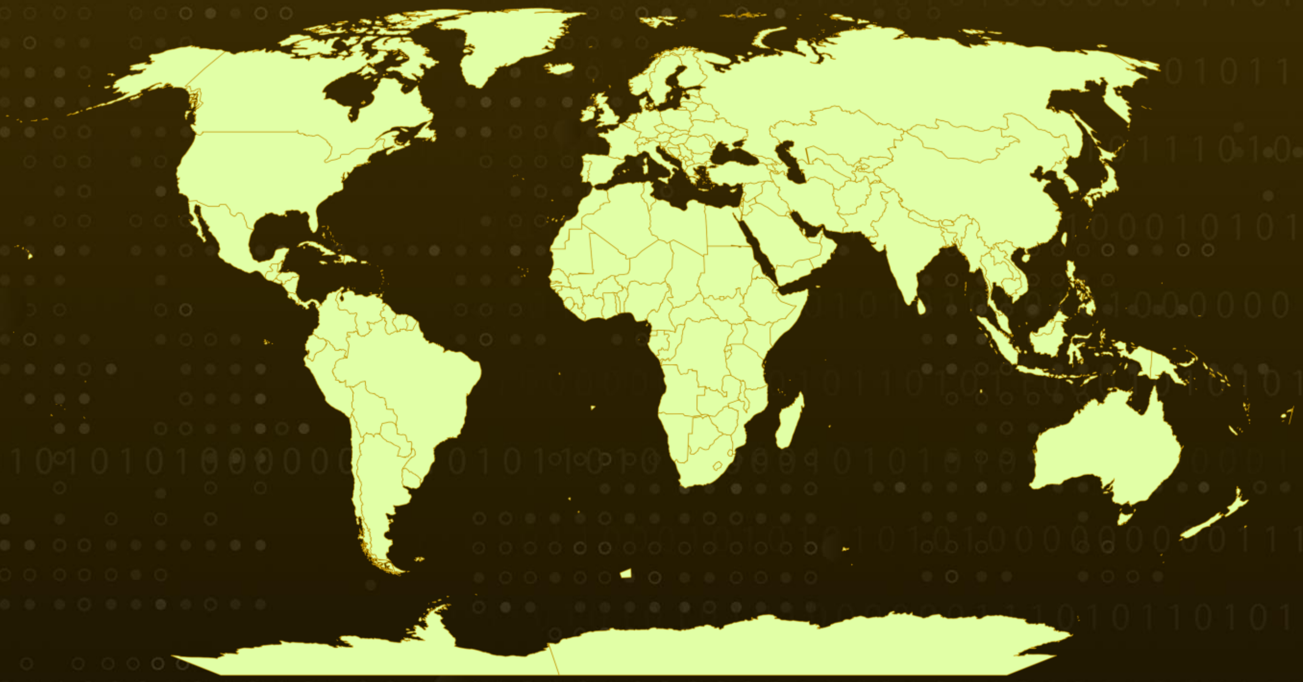
HijackLoader a Deceptive Modular Malware Loader

Date of Publication	Admiralty Code	TA Number
September 11, 2023	A1	TA2023364

Summary

Attack Began: July 2023
Malware: HijackLoader
Attack Region: Worldwide
Attack: A new malware loader, HijackLoader, is swiftly gaining prominence within the cybercriminal sphere, being leveraged to disseminate an array of malicious malware strains, including DanaBot, SystemBC, and RedLine Stealer.

Attack Regions



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

Attack Details

#1 A novel malware loader, named HijackLoader, is rapidly gaining prominence within the cybercriminal underworld, where it is harnessed to deploy various malicious malware families, including DanaBot, SystemBC, and RedLine Stealer. Initially observed in July 2023, HijackLoader employs syscalls to elude detection by security solutions and integrates embedded modules, enabling versatile code injection and execution.

#2 The precise initial access vector employed for infiltrating targets remains undisclosed. Upon execution, HijackLoader initiates by running a modified Windows C Runtime function. Despite its anti-analysis countermeasures, the loader features a central instrumentation module, facilitating adaptable code injection and execution via embedded components. Persistence on the compromised host is achieved by generating a shortcut file (LNK) within the Windows Startup folder, which is directed to a Background Intelligent Transfer Service (BITS) job.

Recommendations

Persistence Monitoring: Regularly monitor Windows Startup folders and other system areas for unusual or unauthorized changes, which could indicate persistent threats like HijackLoader.

Firewalls and Intrusion Detection Systems (IDS): Use firewalls and IDS solutions that can analyze network traffic and syscalls to detect and block malicious activity.

Application Whitelisting: Consider implementing application whitelisting to allow only authorized applications to run on systems, reducing the risk of unapproved software like HijackLoader executing.

Zero Trust Model: Adopt a Zero Trust security model, which requires verification from anyone trying to access resources on a network, regardless of location, to minimize the attack surface.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**T1047** Windows Management Instrumentation	**T1053** Scheduled Task/Job	**T1497** Virtualization/Sandbox Evasion
T1059 Command and Scripting Interpreter	**T1129** Shared Modules	**T1543.003** Windows Service	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1012** Query Registry	**T1018** Remote System Discovery
T1057 Process Discovery	**T1082** System Information Discovery	**T1518.001** Security Software Discovery	**T1083** File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7bd39678ac3452bf55359b44c5192b79412ce61a82cd72eef88f91aba5792ee6, 6b1621bded06b082f83c731319c9deb2fdf751a4cec1d1b2b00ab9e75f4c29ca, e67790b394f5238908fcc326a9db940b200d9b50cbb45f0bfa94038db50beeae, 693cace37b4b6fed2ca67906c7a4b1c11273110561a207a222aa4e62fb4a184a, 04c0a4f3b5f787a0c9fa8f6d8ef19e01097185dd1f2ba40ae4bbbeca9c3a1c72
URLs	hxxps://www.4sync[.]com/web/directDownload/KFtZysVO/4jBKM7R0.baa89a7b43a7b73227f22ae561718f7f, hxxps://geupdate-service[.]bond/img/3344379399.png

References

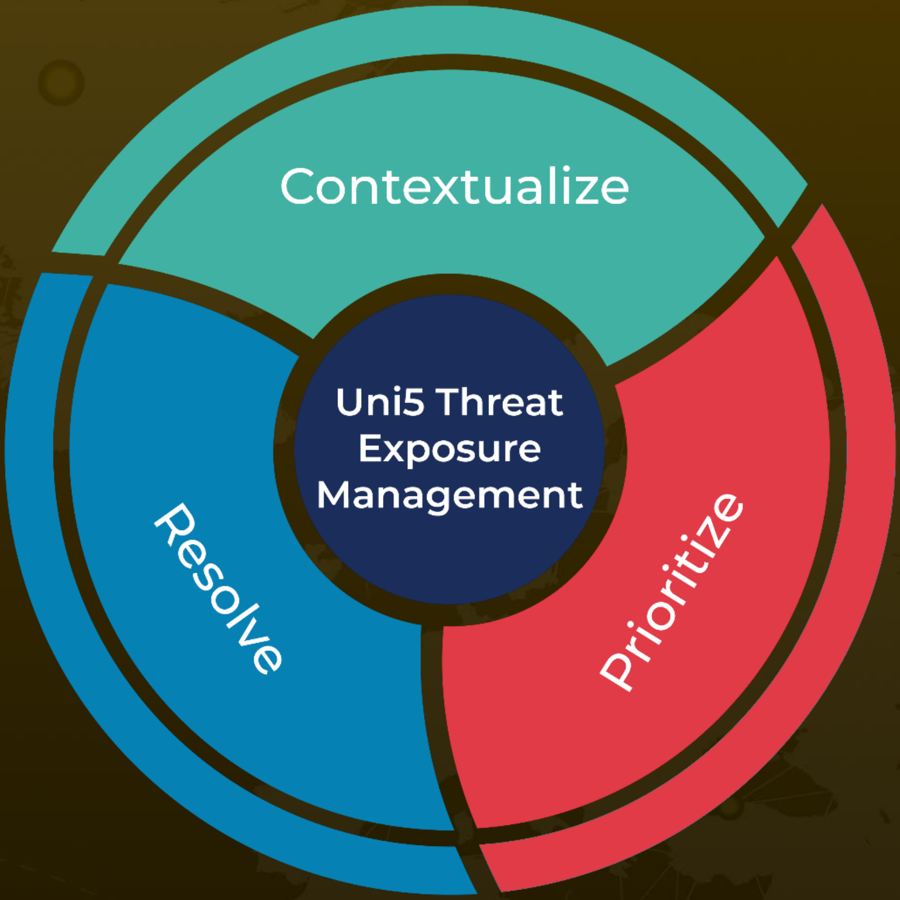
https://www.zscaler.com/blogs/security-research/technical-analysis-hijackloader

https://www.hivepro.com/redline-stealer-used-in-spear-phishing-campaign-targeting-hospitality-industry/

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

September 11, 2023 • 7:00 AM

More at www.hivepro.com