Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

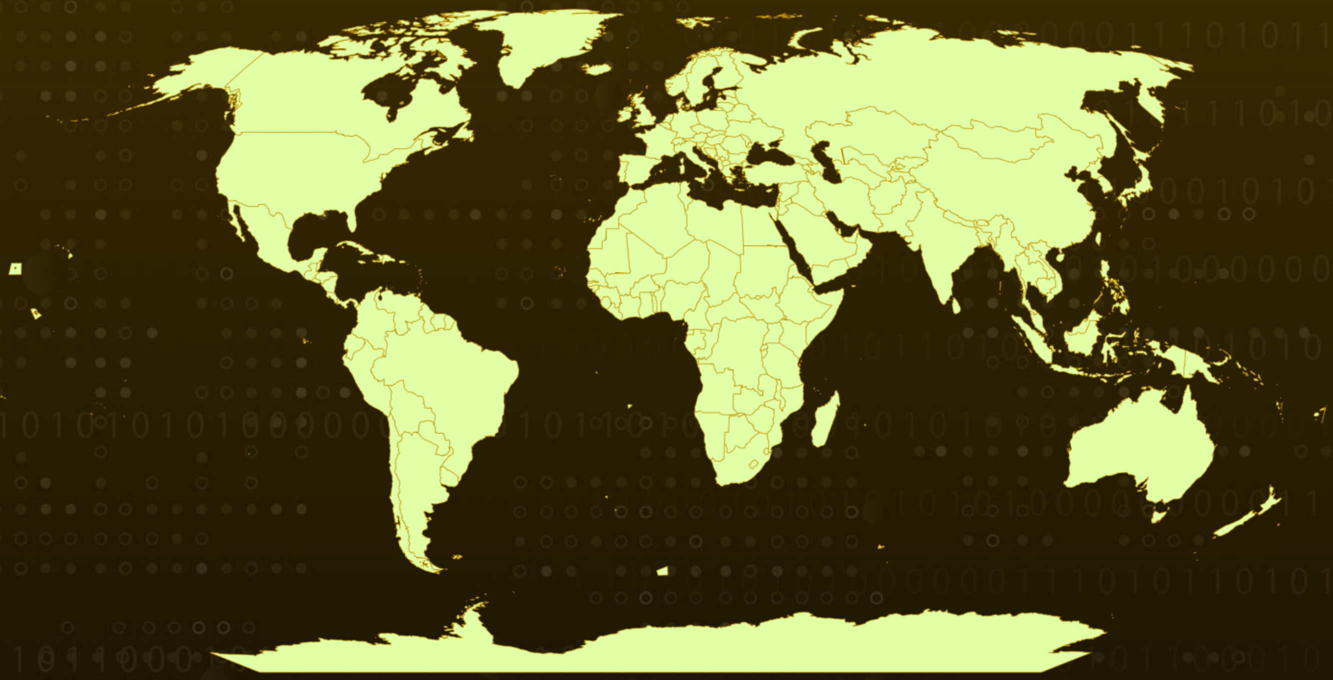
HijackLoader Enhances Its Arsenal with New Evasion Techniques

Date of Publication	Admiralty Code	TA Number
May 8, 2024	A1	TA2024176

Summary

Discovered: 2023
Malware: HijackLoader (aka IDAT Loader)
Attack: HijackLoader, a modular malware loader, has undergone significant evolution through the adoption of novel evasion strategies. New variant of this loader employs a PNG image to disseminate subsequent malware stages. This sophisticated iteration is equipped with multiple modules for injecting and executing code, thereby enhancing its effectiveness and stealth capabilities.

Attack Regions



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

Attack Details

#1

HijackLoader, (aka IDAT Loader), is a potent malware loader equipped with modules designed for code injection and execution. Recently uncovered an updated variant of HijackLoader featuring refined evasion techniques, enhancing its stealth capabilities by including bypass Windows Defender Antivirus, User Account Control (UAC), inline API hooking, and process hollowing. Notably, it employs a PNG image in its attack delivery method. HijackLoader serves as a conduit for deploying multiple malware families.

#2

Initially, the loader undergoes a process of encrypting and decompressing its modules, encompassing the second stage, while dynamically resolving APIs and ensuring internet connectivity. It decrypts embedded shellcode, scans for blocklisted processes, and may delay execution if necessary. The initiation of the second stage may involve loading a copy of itself into memory or downloading a PNG file.

#3

If the PNG is embedded, the loader locates it within its structure; otherwise, it decrypts the URL and utilizes WinHTTP for download. The PNG file contains encrypted blobs, which are meticulously parsed, appended to memory, and decompressed using the LZNT1 algorithm, housing essential modules and configurations for the second stage.

#4

In the second stage, HijackLoader introduces the primary instrumentation module, employing sophisticated anti-analysis techniques. Various malware families distributed by HijackLoader, with Amadey being the most prevalent. Other families include Lumma Stealer, Racoon Stealer v2, Remcos RAT, Meta Stealer, and Rhadamanthys, each targeting different objectives such as data collection, wallet theft, and compromising messaging platforms.

#5

A Python script has been created to enhance understanding of HijackLoader's intricacies, enabling the decryption and decompression of the second stage, streamlining the analysis process. The versatility of HijackLoader underscores its profound impact in the threat landscape. Moreover, recent enhancements integrating new modules have bolstered HijackLoader's capabilities, rendering it more resilient against detection and analysis.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0007** Discovery	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1548** Abuse Elevation Control Mechanism	**T1548.001** Setuid and Setgid	**T1548.002** Bypass User Account Control
T1027 Obfuscated Files or Information	**T1027.007** Dynamic API Resolution	**T1140** Deobfuscate/Decode Files or Information	**T1057** Process Discovery
T1055 Process Injection	**T1055.012** Process Hollowing	**T1620** Reflective Code Loading	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7a8db5d75ca30164236d2474a4719046a7814a4411cf703ffb702bf6319939d7, d95e82392d720911f7eb5d8856b8ccd2427e51645975cdf8081560c2f6967ffb, fcadcee5388fa2e6d4061c7621bf268cb3d156cb879314fa2f518d15f5fa2aa2, f37b158b3b3c6ef9f6fe08d0056915fc7e5a220d1dabb6a2b62364ae54dca0f1, e0a4f1c878f20e70143b358ddaa28242bac56be709b5702f3ad656341c54fb76, cf42af2bdcec387df84ba7f8467bbcdad9719df2c524b6c9b7fffa55cfdc8844, c215c0838b1f8081a11ff3050d12fcfe67f14442ed2e18398f0c26c47931df44, 9b15cb2782f953090caf76efe974c4ef8a5f28df3dbb3eff135d44306d80c29c, 56fd2541a36680249ec670d07a5682d2ef5a343d1feccbcf2c3da86bd546af85, 1fbf01b3cb97fda61a065891f03dca7ed9187a4c1d0e8c5f24ef0001884a54da
URL	hxxp://discussiowardder[.]website/api

References

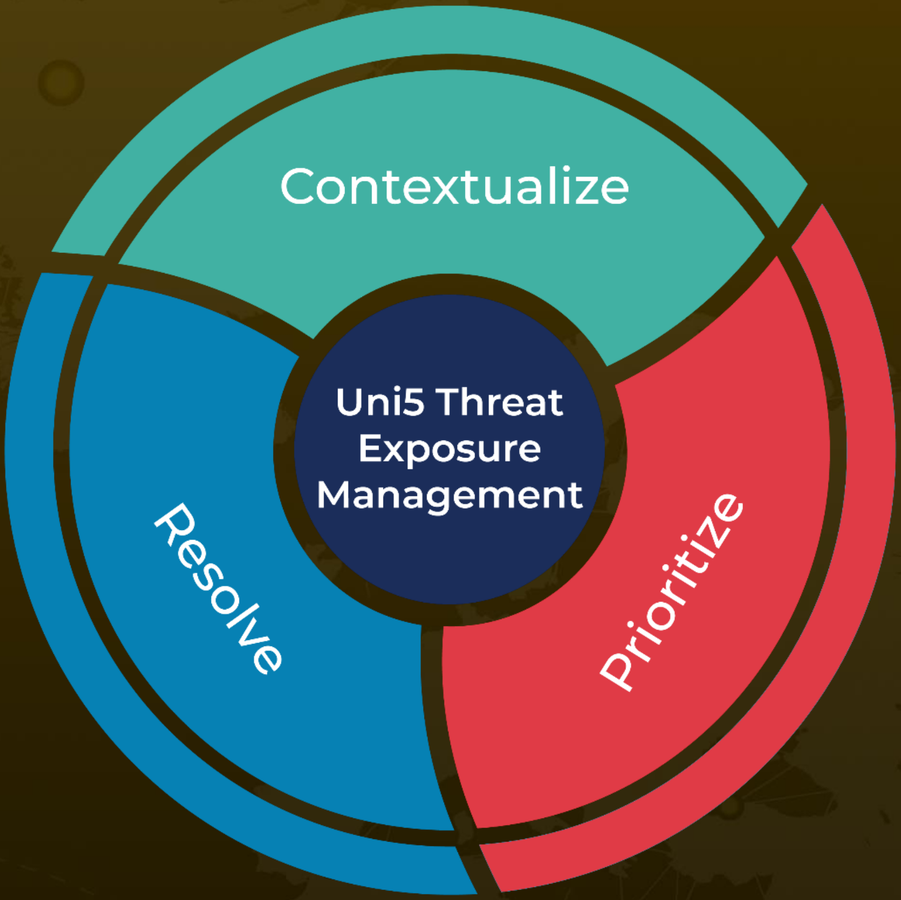
https://www.zscaler.com/blogs/security-research/hijackloader-updates

https://www.hivepro.com/hijackloader-a-deceptive-modular-malware-loader/

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 8, 2024 • 6:30 AM

More at www.hivepro.com