Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

PEAKLIGHT Downloader the Stealthy Malware Living in Memory

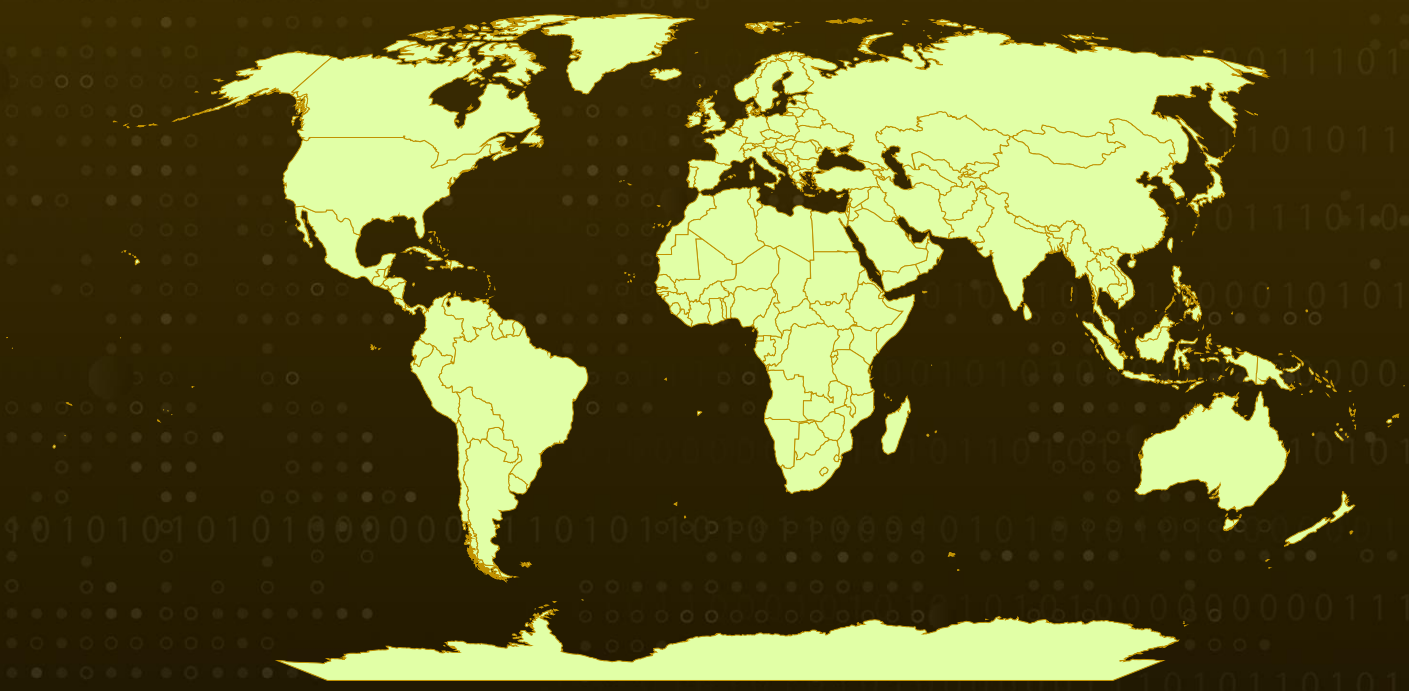
Date of Publication	Admiralty Code	TA Number
August 26, 2024	A1	TA2024328

Summary

Malware: PEAKLIGHT Downloader, Lumma Stealer, SHADOWLADDER (aka Hijack Loader, DOILoader, IDAT Loader), CryptBot
Affected Platform: Windows
Targeted Region: Worldwide

Attack: The PEAKLIGHT Downloader is an advanced and elusive malware designed to operate entirely in memory, making it exceptionally difficult to detect. This heavily obfuscated threat specifically targets Windows systems, intending to deploy information stealers and loaders.

Attack Regions



Attack Details

#1 The PEAKLIGHT Downloader is advanced, stealthy malware engineered to operate exclusively in memory. This PowerShell-based downloader is heavily obfuscated and programmed to search for specific hard-coded filenames on the targeted system, with the ultimate objective of deploying information stealers and loaders on Windows systems.

#2 Notable malware strains distributed through this method include Lumma Stealer, SHADOWLADDER (also known as DOILoader, IDAT Loader, or Hijack Loader), and CryptBot, all offered under the malware-as-a-service model. The infection chain typically begins when victims download pirated movies, where LNK files disguised as ZIP archives are embedded.

#3 When the user opens the downloaded archive, expecting to access the movie, they inadvertently execute the LNK file, which connects to a content delivery network (CDN) hosting an obfuscated memory-only JavaScript dropper. This dropper then executes the PEAKLIGHT PowerShell downloader script.

#4 Some variations of the LNK files use asterisks as wildcards to invoke the legitimate mshta.exe binary, covertly running malicious code retrieved from a remote server. The droppers are known to embed both hex-encoded and Base64-encoded PowerShell payloads.

#5 Once active, the PEAKLIGHT Downloader connects to a remote Command and Control (C2) server, the attacker's command hub for issuing instructions and retrieving data. By storing the malware on a CDN and executing it directly in memory, the attack chain avoids leaving significant traces on the system's hard drive, thereby enhancing its ability to evade detection.

Recommendations

Enhance File Download Security: Educate users about the risks of downloading pirated content and the potential for embedded malware. Implement web filtering solutions to block access to known malicious sites and file-sharing platforms.

Strengthen Network Security Measures: Implement network segmentation to limit the spread of malware within the network. Use firewalls and intrusion detection systems (IDS) to monitor and block malicious traffic.

Configure Application Whitelisting: Apply application whitelisting policies to only allow approved applications and executables to run on systems. This can prevent unauthorized scripts or executables from being executed. Regularly review and update the whitelist to accommodate legitimate applications while blocking potentially harmful ones.

Implement Machine Learning-Based Anomaly Detection: Deploy machine learning models that analyze normal system behavior and identify deviations indicative of potential threats. These models can detect unusual patterns in network traffic, file access, and system processes. Continuously train and update the models with new data to improve their accuracy and reduce false positives.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0011 Command and Control	**TA0010** Exfiltration	**T1057** Process Discovery	**T1083** File and Directory Discovery
T1189 Drive-by Compromise	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter	**T1203** Exploitation for Client Execution
T1041 Exfiltration Over C2 Channel	**T1071.001** Web Protocols	**T1105** Ingress Tool Transfer	**T1027** Obfuscated Files or Information
T1574.007 Path Interception by PATH Environment Variable	**T1218** System Binary Proxy Execution	**T1218.005** Mshta	**T1518** Software Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//fatodex[.]b-cdn[.]net/fatodex, hxxps[:]//matodown[.]b-cdn[.]net/matodown, hxxps[:]//potexo[.]b-cdn[.]net/potexo, hxxp[:]//gceight8vt[.]top/upload[.]php, hxxps[:]//brewdogebar[.]com/code[.]vue, hxxp[:]//62[.]133[.]61[.]56/Downloads/Full%20Video%20HD%20(1080p)[.]lnk,

TYPE	VALUE
URLs	hxxps[:]//fatodex[.]b-cdn[.]net/K1[.]zip, hxxps[:]//fatodex[.]b-cdn[.]net/K2[.]zip, hxxps[:]//forikabrof[.]click/flkhfaiouwrqkhfasdrhfsa[.]png, hxxps[:]//matodown[.]b-cdn[.]net/K1[.]zip, hxxps[:]//matodown[.]b-cdn[.]net/K2[.]zip, hxxps[:]//nextomax[.]b-cdn[.]net/L1[.]zip, hxxps[:]//nextomax[.]b-cdn[.]net/L2[.]zip, hxxps[:]//potexo[.]b-cdn[.]net/K1[.]zip, hxxps[:]//potexo[.]b-cdn[.]net/K2[.]zip
Domains	relaxtionflouwerwi[.]shop, deprivedrinkyfaiir[.]shop, detailbaconroollyws[.]shop, messtimetabledkolvk[.]shop, considerrycurrentyws[.]shop, understanndtytonyguw[.]shop, patternapplauderw[.]shop, horsedwollfedrwos[.]shop, tropicalironexpressiw[.]shop
MD5	d6ea5dcdb2f88a65399f87809f43f83c, 307f40ebc6d8a207455c96d34759f1f3, d8e21ac76b228ec144217d1e85df2693, 43939986a671821203bf9b6ba52a51b4, 58c4ba9385139785e9700898cb097538, 95361f5f264e58d6ca4538e7b436ab67, b716a1d24c05c6adee11ca7388b728d3, b15bac961f62448c872e1dc6d3931016, e7c43dc3ec4360374043b872f934ec9e, f98e0d9599d40ed032ff16de242987ca, b6b8164feca728db02e6b636162a2960, bb9641e3035ae8c0ab6117ecc82b65a1, 236c709bbcb92aa30b7e67705ef7f55a, d7aff07e7cd20a5419f2411f6330f530, a6c4d2072961e9a8c98712c46be588f8, 059d94e8944eca4056e92d60f7044f14, dfdc331e575dae6660d6ed3c03d214bd, 47eee41b822d953c47434377006e01fe

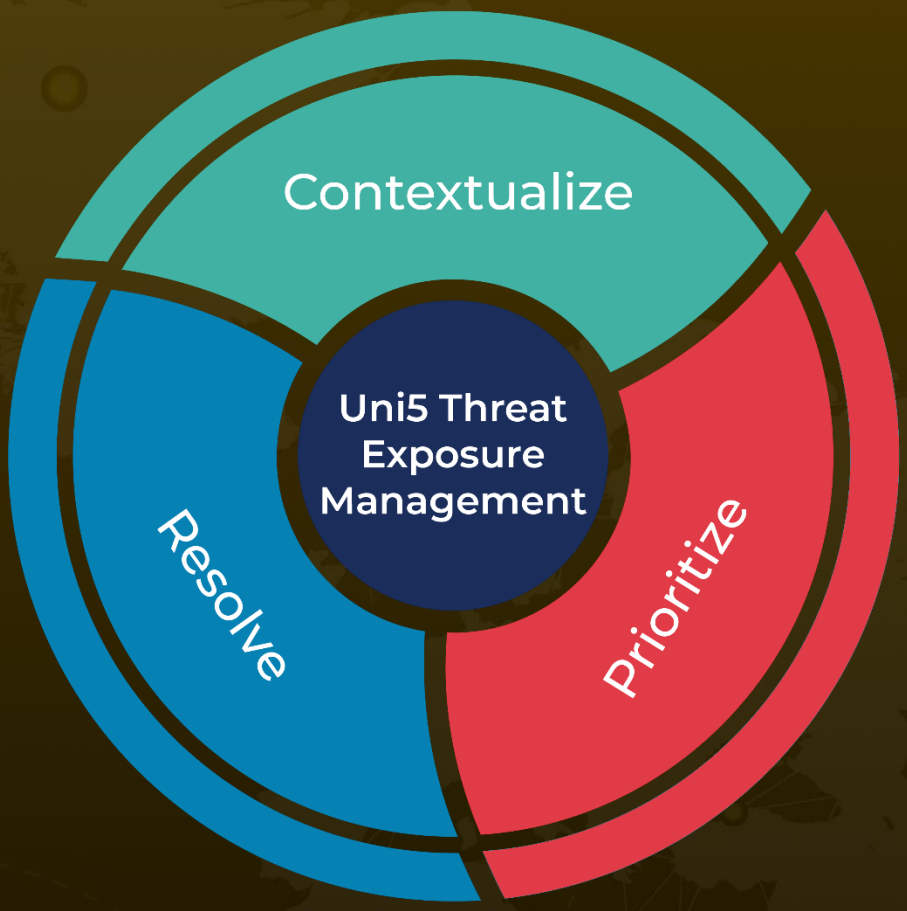
References

https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/

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

August 26, 2024 • 7:30 AM

More at www.hivepro.com