Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

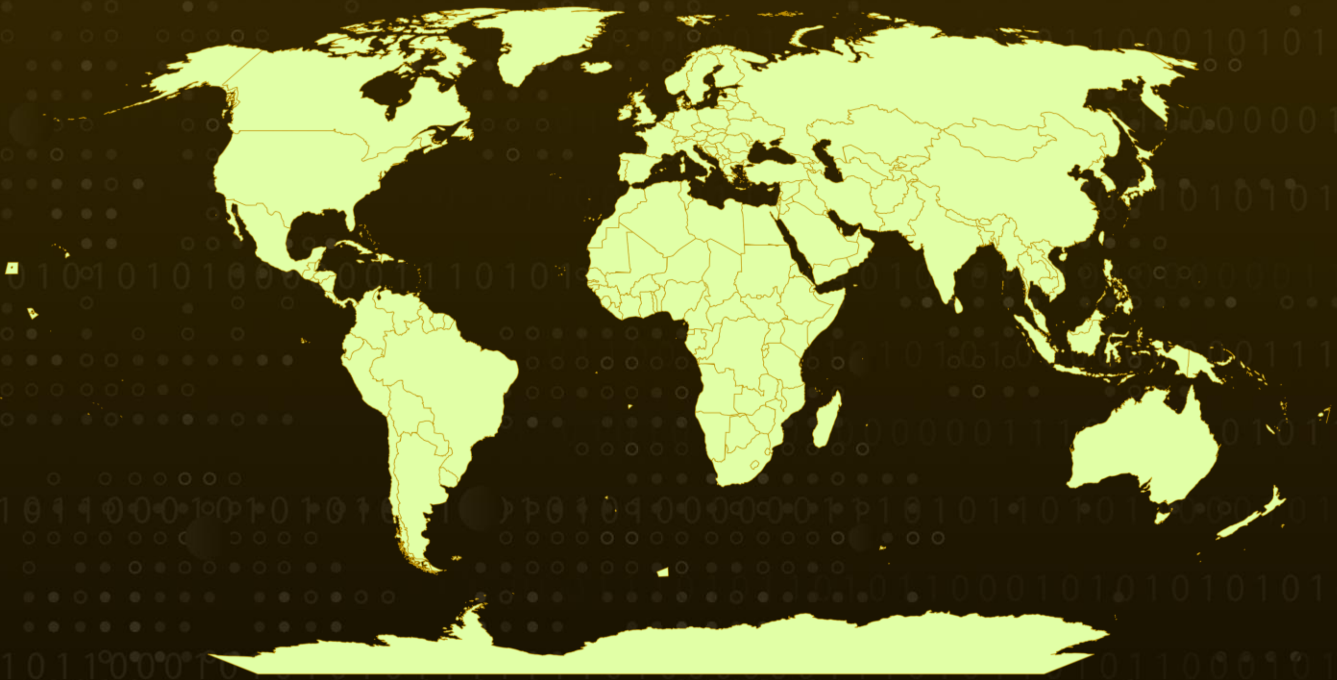
D3F@ck Loader: New Malware Exploits Google Ads and EV Certificates

Date of Publication	Admiralty Code	TA Number
May 22, 2024	A1	TA2024201

Summary

Attack Began: January 2024
Targeted Countries: Worldwide
Malware: D3F@ck Loader
Pricing: $70 per day and $490 for a week
Affected Platform: Windows
Attack: D3F@CK Loader is a new malware loader that leverages Google Ads and EV certificates to bypass security measures. It can download other malware, including Raccoon Stealer and Danabot. It impersonates legitimate applications to trick users into downloading it.

Attack Regions



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

Attack Details

#1

The D3F@ck Loader is a new malware-as-a-service (MaaS) loader that is being spread via Google Ads. First seen in January 2024, this loader can bypass security measures in Google Chrome, Edge, Windows Defender, and SmartScreen. Initially, access to the loader was priced at $70 per day or $490 per week.

#2

The D3F@ck Loader has been used to distribute malware like Raccoon Stealer and Danabot. It is marketed on hacking forums with pricing varying based on the need for an Extended Validation (EV) signature and the payload size. EV certificates are more trusted by security programs, making it easier for malware signed with them to bypass warnings like SmartScreen.

#3

The malware was distributed through fake websites accessed via Google Ads, mimicking legitimate applications like Calendly and Rufus, with installers hosted on MediaFire. The D3F@ck Loader's first stage involves Inno Setup, which subsequently downloads a JPHP executable. JPHP runs on the Java Virtual Machine (JVM) but cannot be compiled by standard Java decompilers, adding an extra layer of obfuscation. Inno Setup, a popular installation system, leverages the Pascal scripting engine for encoding and executing malicious commands.

#4

The loader retrieves and executes commands from a command-and-control (C2) server, deletes itself, and hides its actions. The final payload, retrieved from the C2 server, includes a .NET dropper that injects Raccoon Stealer into the RegAsm.exe process.

#5

This case underscores the threat posed by malware using high-trust mechanisms like EV certificates to evade security solutions, and its strategic distribution through popular platforms like Google Ads to maximize its reach.

Recommendations

Enhanced Ad Security: Use ad blockers and browser extensions that block malicious ads to reduce the risk of encountering harmful advertisements. Organizations should consider using ad verification services to ensure the integrity of ads displayed on their networks.

Regular Software and Security Updates: Keep all software, including operating systems, browsers, and security tools, up to date with the latest patches and updates. Regularly update antivirus and antimalware definitions to recognize and block new threats.

Use of Multi-Layered Security Solutions: Employ a multi-layered security approach that includes firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection platforms (EPP). Implement advanced threat protection solutions that use machine learning and behavior analysis to detect and mitigate unknown threats.

Strict Certificate Management: Monitor and manage digital certificates closely, especially EV certificates. Ensure that certificates are issued from reputable Certificate Authorities (CAs) and verify their legitimacy regularly.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0042** Resource Development	**TA0011** Command and Control	**TA0004** Privilege Escalation
TA0007 Discovery	**TA0003** Persistence	**T1083** File and Directory Discovery	**T1588.001** Malware
T1036 Masquerading	**T1216** System Script Proxy Execution	**T1588** Obtain Capabilities	**T1588.004** Digital Certificates
T1656 Impersonation	**T1059** Command and Scripting Interpreter	**T1132.001** Standard Encoding	**T1132** Data Encoding
T1562 Impair Defenses	**T1562.011** Spoof Security Alerting	**T1055** Process Injection	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	194[.]147[.]35[.]251, 116[.]202[.]188[.]155, 195[.]20[.]16[.]155
MD5	44b14057ff868e25ad444fac098d89f0, 87cb408a03daa827f9cc10698ba69a90, 56f2d534631400ef294d321f8dbdfea, 5cf2e80ac2a7f7fa24f74966d3ec904f, 815b3c88950fd572bb4bfef96d2ca23d, be9989c6c218b0e99671a5bde240341e

References

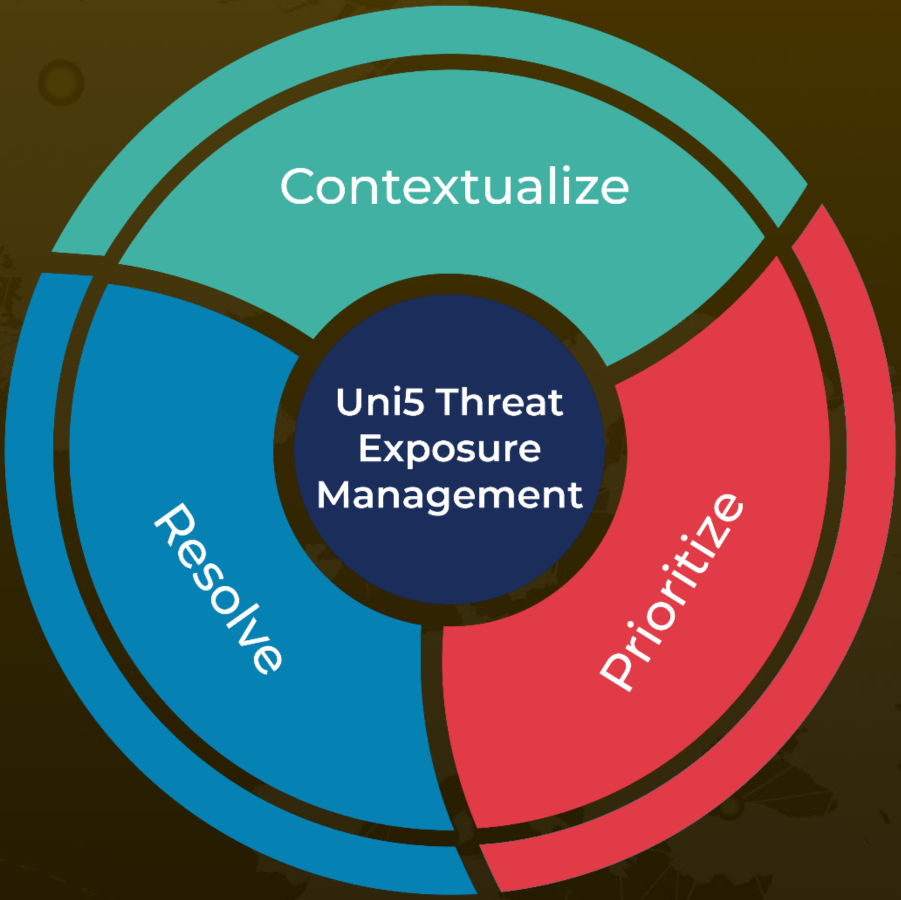
https://www.esentire.com/blog/d3f-ck-loader-the-new-maas-loader

https://www.youtube.com/watch?v=y09ZreJaWE0

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 22, 2024 • 6:30 AM

More at www.hivepro.com