Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

New IDAT Loader Unleashes Infostealers in Fake Browser Update Campaign

Date of Publication

September 5, 2023

Admiralty Code

A1

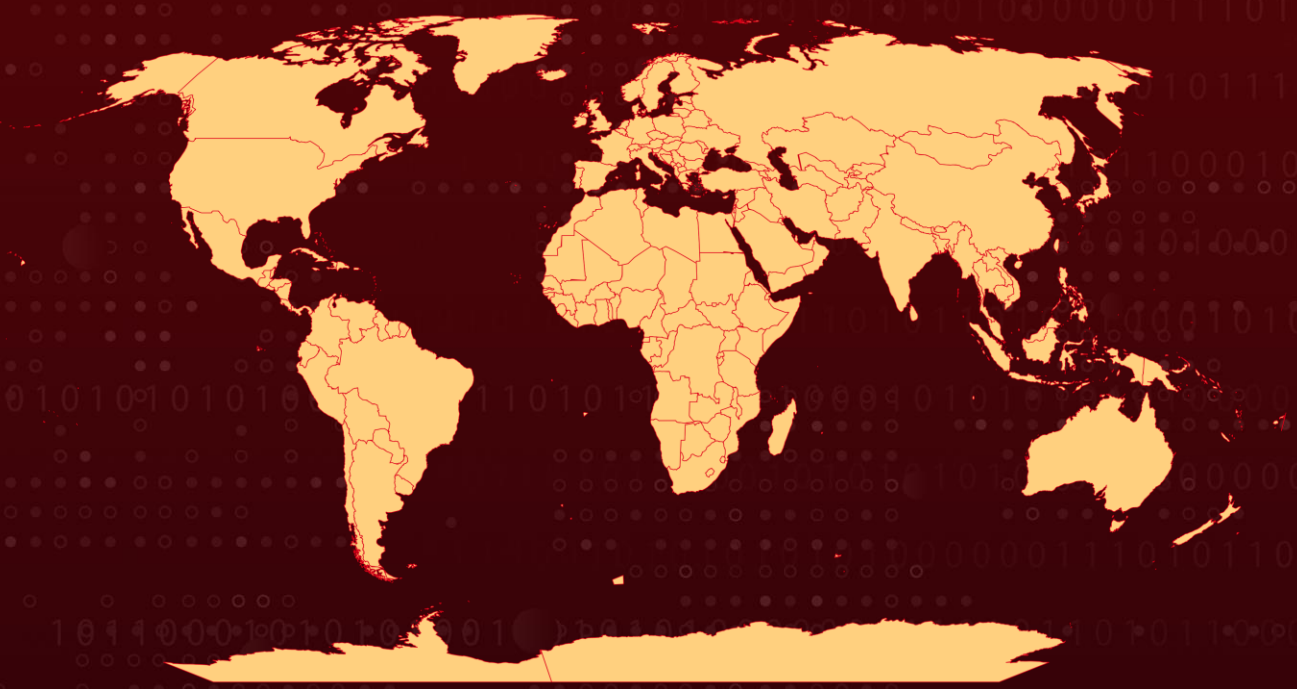
TA Number

TA2023352

Summary

First Appearance: July, 2023
Attack Region: Worldwide
Affected Platform: Windows
Malware: IDAT Loader, StealC, Lumma, and Amadey
Attack: In a recent malware campaign, threat actors utilized a new IDAT Loader to distribute a range of malicious software, including InfoStealers and RATs, employing evasion methods. This loader is packaged within DLLs and discreetly activated by legitimate applications like VMWarehost, Python, and Windows Defender as part of the Fake Update campaign.

Attack Regions



Attack Details

#1

A new malicious campaign involving a Fake Browser Update lure that tricks users into executing harmful binaries. This campaign utilizes a sophisticated loader called IDAT Loader to deploy infostealers like StealC, Lumma, and Amadey on compromised systems. IDAT Loader employs evasion techniques such as Process Doppelgänging, DLL Search Order Hijacking, and Heaven's Gate. It conceals its payload within the IDAT chunk of PNG files.

#2

The attack flow begins with SocGholish malware, initially discovered in 2018 and attributed to TA569. This malware injects malicious JavaScript into compromised websites, primarily targeting Windows OS users from external sources. It presents a fake browser update prompt to victims, leading to the download of a binary called ChromeSetup.exe.

#3

ChromeSetup.exe downloads and runs a Microsoft Software Installer (MSI) package, which employs various switches to avoid detection. The MSI package drops legitimate executables, dependencies, and a malicious Dynamic-Link Library (DLL) file. It also creates an encrypted log file, later decrypted by the malicious DLL.

#4

The malicious DLL, loaded by the legitimate VMWareHostOpen.exe, reads and decrypts the log file, searching for specific hex values. Once found, it copies and decompresses the data, overwriting the mshtml.dll's .text section. This triggers the execution of the decompressed code.

#5

The IDAT Injector, following a similar pattern, creates a new folder under %APPDATA% to copy files from the MSI package. It initiates a second instance of VMWareHostOpen.exe and employs the Heaven's Gate evasion technique, allowing a 32-bit process to run within a 64-bit process.

#6

The IDAT Loader retrieves environment variables and injects code into cmd.exe using code injection techniques. It then proceeds to inject infostealer code into the explorer.exe process using the Process Doppelgänging method. This results in the deployment of the Lumma Stealer. Throughout the attack flow, the malware employs NtDelayExecution to delay execution and evade sandboxes.

Recommendations

Keep software up to date: Regularly update your operating system, applications, and software to the latest versions. Enable automatic updates wherever possible to ensure you're protected against known vulnerabilities.

Use Firewall and Antivirus Software: Enable a firewall on your computer or network to monitor and filter incoming and outgoing network traffic. A firewall adds an additional layer of protection against malicious activity.

Practice Safe Browsing Habits: Exercise caution when visiting websites. Stick to reputable and trusted sites, especially when entering personal information or conducting financial transactions.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0005 Defense Evasion	TA0001 Initial Access	T1059.006 Python
T1189 Drive-by Compromise	T1036 Masquerading	T1059 Command and Scripting Interpreter	T1059.007 JavaScript
T1218.007 Msiexec	T1218 System Binary Proxy Execution	T1204.002 Malicious File	T1204 User Execution
T1574.001 DLL Search Order Hijacking	T1574 Hijack Execution Flow	T1140 Deobfuscate/Decode Files or Information	T1036 Masquerading
T1106 Native API	T1055 Process Injection	T1055.013 Process Doppelgänging	T1497.003 Time Based Evasion
T1497 Virtualization/Sandbox Evasion	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1bcf03b31489b63436d4216249bbf246, e07aa33f0e6aec02240a232e71b7e741, e24bdc9074518cf8e0afd9f017855eee
SHA1	2106fc1e0f83df0f658934129a5a374948cc97a0, afdf930278ae74d600d31463ba31ec2543ceb121, e330e5b7f62ca55cb6e6c97406e0b56878806960
SHA256	3bf4b365d61c1e9807d20e71375627450b8fea1635cb6ddb85f2956e8f6b3ec3, 51cee2de0ebe01e75afdeffe29d48cb4d413d471766420c8b8f9ab08c59977d7, 53c3982f452e570db6599e004d196a8a3b8399c9d484f78cdb481c2703138d47, 5f57537d18adcc1142294d7c469f565f359d5ff148e93a15ccbceb5ca3390dbd, 8ce0901a5cf2d3014aaa89d5b5b68666da0d42d2294a2f2b7e3a275025b35b79, 931d78c733c6287cec991659ed16513862bfc6f5e42b74a8a82e4fa6c8a3fe06, a0319e612de3b7e6fbb4b71aa7398266791e50da0ae373c5870c3dcaa51abccf, b287c0bc239b434b90eef01bcbd00ff48192b7cbeb540e568b8cdcdc26f90959, b3d8bc93a96c992099d768beb42202b48a7fe4c9a1e3b391efbeeb1549ef5039, be8eb5359185baa8e456a554a091ec54c8828bb2499fe332e9ecd65639c9a75b, c9094685ae4851fd5a5b886b73c7b07efd9b47ea0bdae3f823d035cf1b3b9e48, d19c166d0846ddaf1a6d5dbd62c93acb91956627e47e4e3cbd79f3dfb3e0f002
URLs	hxxps://ocmtancmi2c5t[.]xyz/82z2fn2afo/b3/update[.]msi, hxxps://zeltser[.]com/media/docs/malware-analysis-lab[.]pdf
IPv4	94.228.169[.]55

TYPE	VALUE
Domains	bgobgogimrihehmxerreg[.]site, buyerbrand[.]xyz, costexcise[.]xyz, doorblu[.]xyz, gapi-node[.]io, lazagrc3cnk[.]xyz, ocmtancmi2c5t[.]xyz, omdowqind[.]site, ooinonqnbdqnjdnqwqkdn[.]space, weomfewnfnu[.]site, winextrabonus[.]life, gstatic-node[.]io

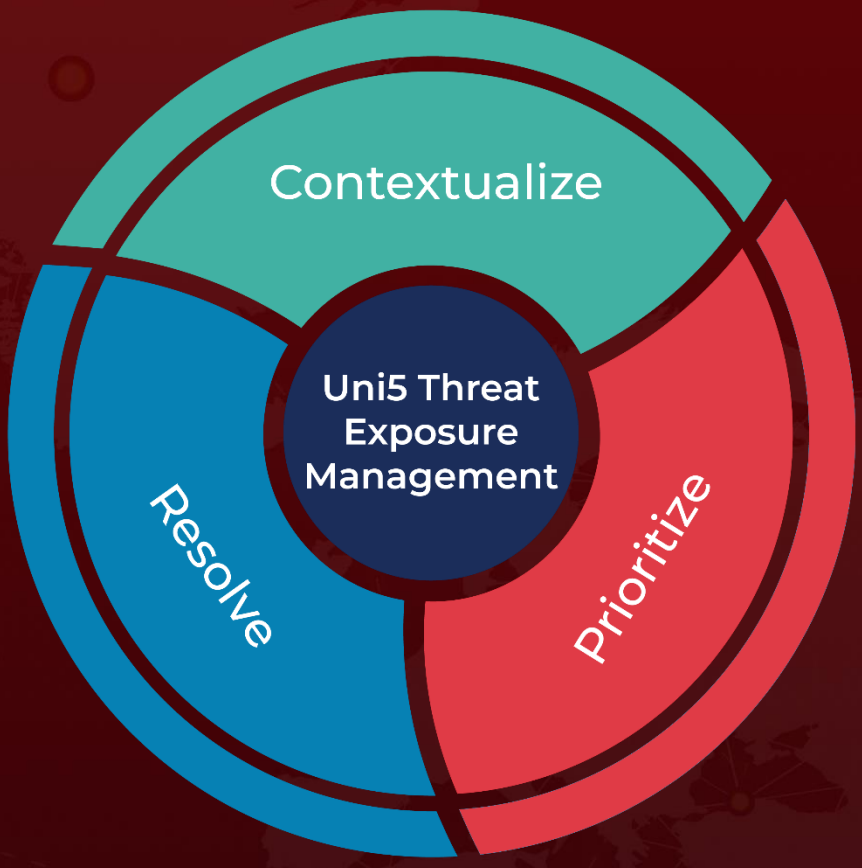
References

https://www.rapid7.com/blog/post/2023/08/31/fake-update-utilizes-new-idat-loader-to-execute-stealc-and-lumma-infostealers/

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 5, 2023 . 4:30 AM

More at www.hivepro.com