Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Free Trials of Sticky Notes Installer Trojanized

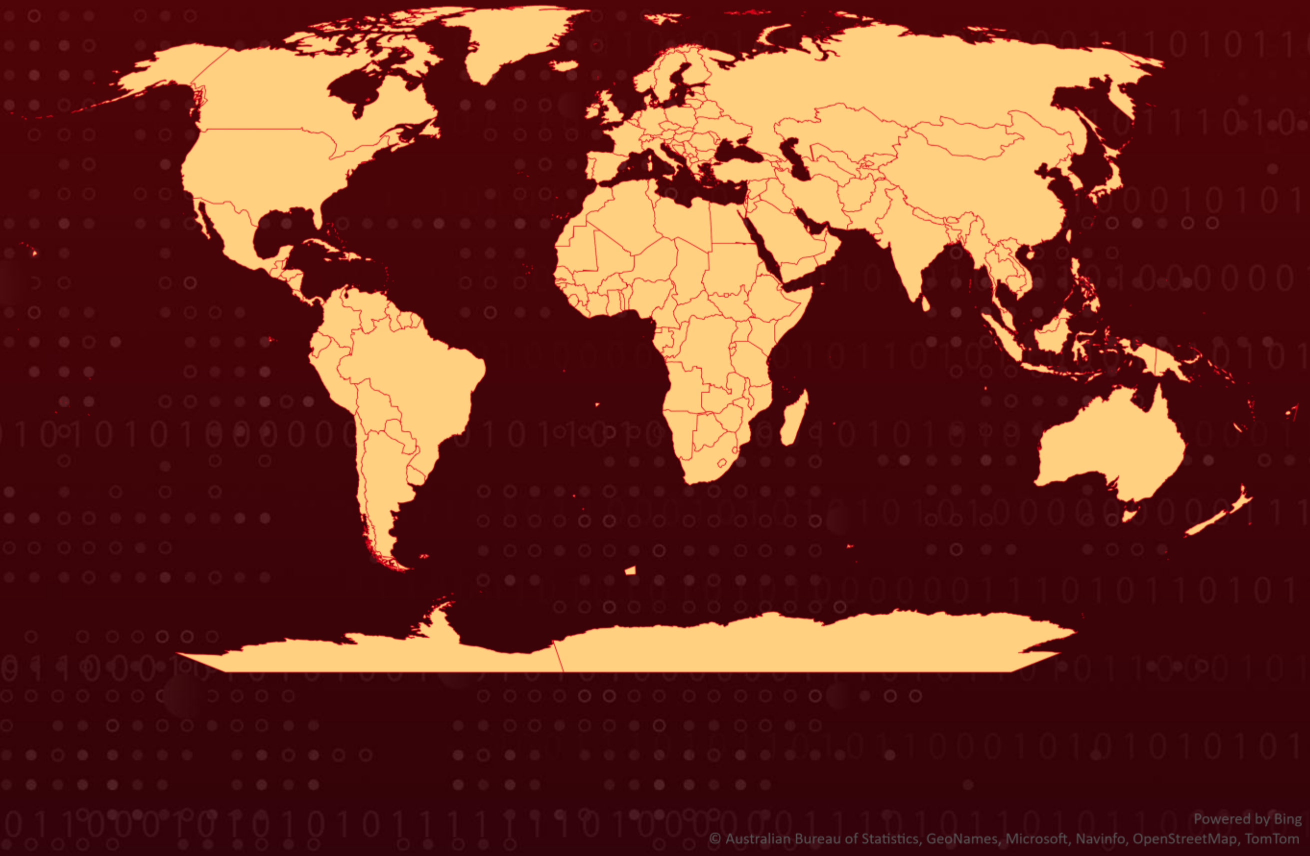
Date of Publication	Admiralty Code	TA Number
July 2, 2024	A1	TA2024252

Summary

Attack Commenced: January 2024
Affected Products: Notezilla, Copywhiz, and RecentX
Affected Browsers: Mozilla Firefox, Google Chrome
Malware: dllFake
Attack Region: Worldwide

Attack: Free trial downloads of software products from the official website of the India-based company have had their installers trojanized to distribute the dllFake information-stealing malware. This malware, which has been circulating since at least January 2024, can steal browser credentials and cryptocurrency wallet information.

Attack Regions



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

Attack Details

#1 Three different software products developed by the Indian company Conceptworld have had their installers compromised to distribute the dllFake information-stealing malware. This malware can download and execute additional payloads.

#2 The official Conceptworld website offers free trial downloads for each software package, which includes trojanized installers. The dllFake malware appears to belong to an unidentified family of malware that has been circulating since at least January 2024.

#3 Upon initial execution, the installation window for the legitimate installer opens, prompting the user to proceed with the installation of Notezilla. Notezilla, a program for creating sticky notes on a Windows desktop, as well as RecentX and Copywhiz, are among the affected software.

#4 The dllFake malware can steal browser credentials and cryptocurrency wallet information, log clipboard contents and keystrokes, and download and execute additional payloads on infected Windows hosts. It also establishes persistence by creating a scheduled task that executes the main payload every three hours.

Recommendations

Identification of Infection Indicators: If an installer for Notezilla, RecentX, or Copywhiz has been executed on a system within the last month, be vigilant for the following signs of potential infection. The key indicators of infection comprise a concealed scheduled task named Check dllHourly32 and a persistent instance of the Windows Command Prompt, cmd.exe, establishing outbound network connections through curl.exe.

File Integrity Verification: Before installing freely available software like Notezilla, RecentX, or Copywhiz, verify the file integrity by checking the digital signature to ensure the file contains a valid digital signature from the software publisher. Unsigned installers should be treated with caution.

System Inspection and Restoration: Users who installed an installer for Notezilla, RecentX, or Copywhiz in June 2024 are encouraged to thoroughly inspect their systems for signs of compromise. It is advisable to take prompt action, such as restoring affected systems to their original state.

Monitor System Activity: Monitor your system for unusual behavior, such as unexpected pop-ups, sluggish performance, or unauthorized network activity. These could be signs of a malware infection.

Network Segmentation: Utilize network segmentation to isolate critical infrastructure and sensitive data from less secure parts of the network. This can help contain the spread of malware and limit access to valuable assets in case of a breach.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1584.004** Server	**T1195** Supply Chain Compromise
T1195.002 Compromise Software Supply Chain	**T1204** User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1059.006** Python	**T1053.005** Scheduled Task	**T1584** Compromise Infrastructure
T1053 Scheduled Task/Job	**T1555.003** Credentials from Web Browsers	**T1555** Credentials from Password Stores	**T1560.001** Archive via Utility

T1560 Archive Collected Data	T1115 Clipboard Data	T1005 Data from Local System	T1056.001 Keylogging
T1056 Input Capture	T1571 Non-Standard Port	T1048 Exfiltration Over Alternative Protocol	T1496 Resource Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	NotezillaSetup.exe, RecentXSetup.exe, CopywhizSetup.exe, curl.exe, 7z.exe, dllBus.bat, dllBus32.exe, dllCrt.bat, dllCrt.xml, dllCrt32.exe, dll_apps.txt, dll_srv.txt, dll_updt.txt
SHA256	6f49756749d175058f15d5f3c80c8a7d46e80ec3e5eb9fb31f4346abdb72a0e7, 51243990ef8b82865492f0156ebbb23397173647c02a0d83cf3e3dfb4ef8a6bc, 4df9b7da9590990230ed2ab9b4c3d399cf770ed7f6c36a8a10285375fd5a292f, a6ad6492e88bdb833d34ac122c266f1fadd9509ecfe0246e283728e4af49f433, 2eae4f06f2c376c6206c632ac93f4e8c4b3e0e63eca3118e883f8ac479b2f852, fd8d13123218f48c6ab38bf61d94113b4d97095e59fb415e6aa5d9ada012206e, bfa99c41aecc814de5b9eb8397a27e516c8b0a4e31edd9ed1304da6c996b4aaa, 048cae10558cddfb2cf0ade25f1101909bba58d0a448e0d78590cc5e64e95127, ebf2b84ed64629242f8d0abfca7334473620524953947 4e8f57d1d3dbe8ccc41,

TYPE	VALUE
SHA256	1fa84b696b055f614ccd4640b724d90ccad4afc035358822224a02a9e2c12846, cdc1f2430681e9278b3f738ed74954c4366b8eff52c937f185d760c1bbba2f1d, fdc84cb0845f87a39b29027d6433f4a1bbd8c5b808280235cf867a6b0b7a91eb, a89953915eabe5c4897e414e73f28c300472298a6a8c055fcc956c61c875fd96, 70bce9c228aacbdadaaf18596c0eb308c102382d04632b01b826e9db96210093, ca6ff18ee006e7ab3cb42fc541b08ce4231dadfab0cce57b1c126db3df9f1297, 33e4d5eed3527c269467eec2ac57ae94ae34fd1d0a145505a29c51cf8e83f1b9, 03761d9fd24a2530b386c07bf886350ae497e693440a9319903072b93a30c82d, 6487a0dc9dfbbaa6557af096178a1361e49762a41500aa03f17df5d3b159bf4e, de4e03288071cdebe5c26913888b135fb2424132856cc892baea9792d6c66249
IPv4	212[.]70[.]149[.]210, 5[.]180[.]185[.]42, 50[.]2[.]108[.]102, 50[.]2[.]191[.]154, 104[.]140[.]17[.]242, 104[.]206[.]2[.]18, 104[.]206[.]57[.]117, 104[.]206[.]95[.]146, 104[.]206[.]220[.]113, 170[.]130[.]34[.]114, 185[.]137[.]137[.]74, 212[.]70[.]149[.]210
Domain	conceptworld[.]com

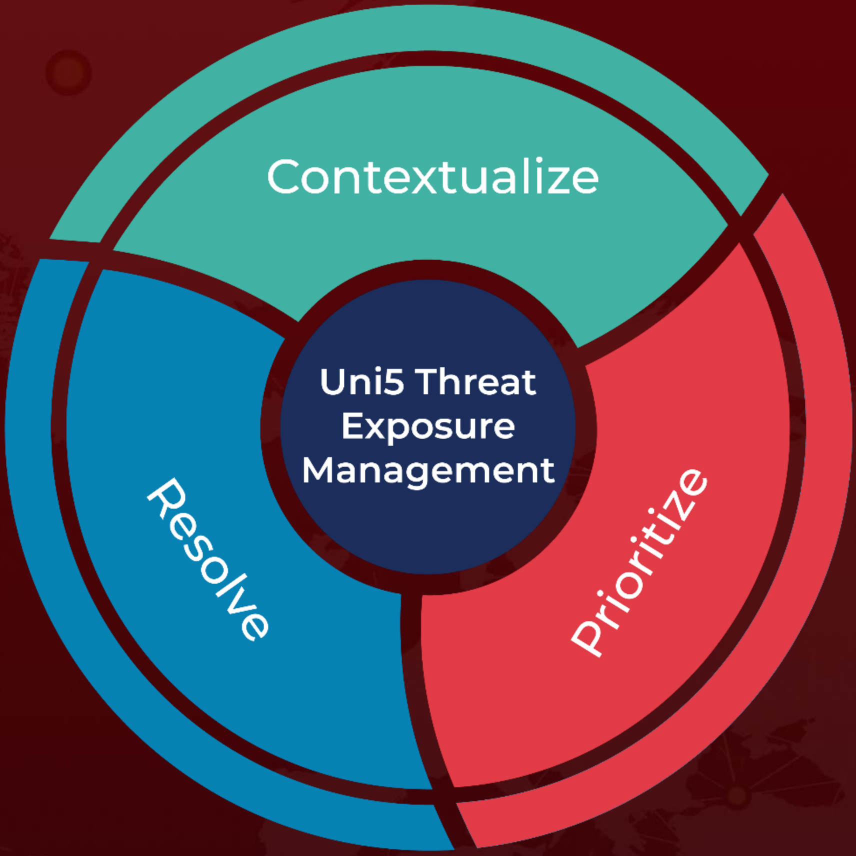
References

https://www.rapid7.com/blog/post/2024/06/27/supply-chain-compromise-leads-to-trojanized-installers-for-notezilla-recentx-copywhiz/

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

July 2, 2024 • 9:00 PM

More at www.hivepro.com