Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

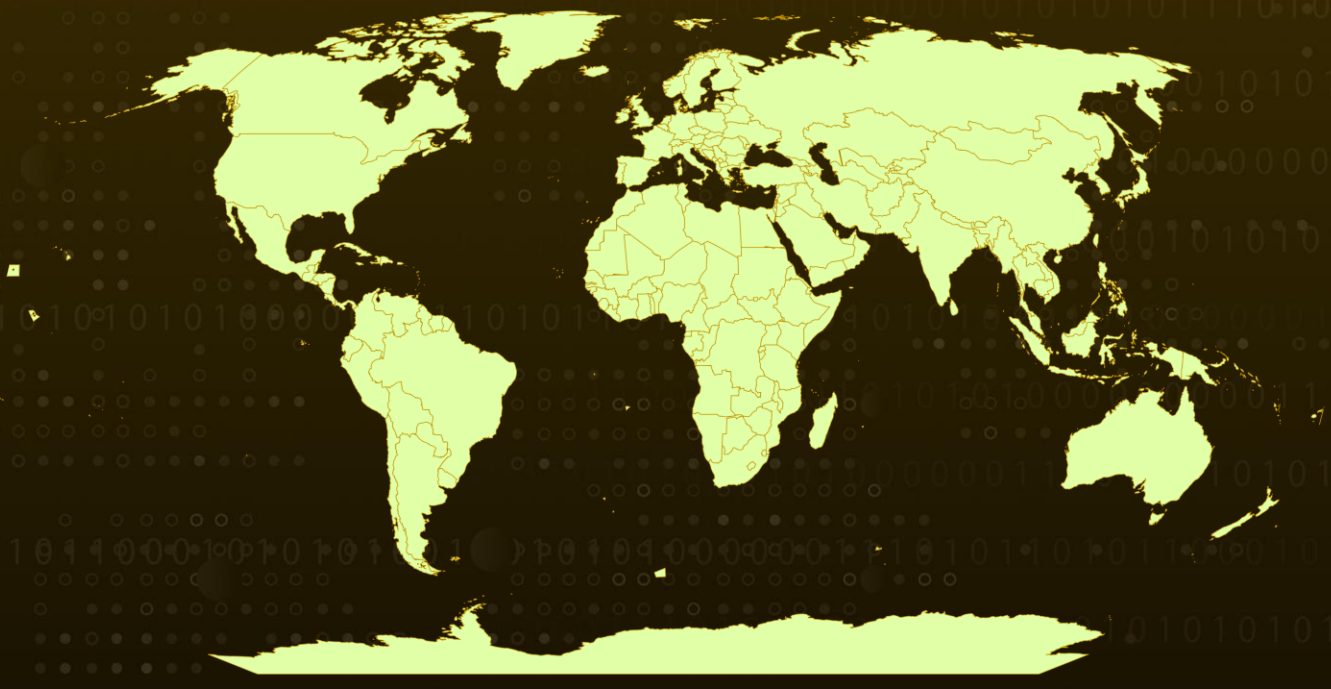
Malware Concealed Within PDFs for Data Theft

Date of Publication	Admiralty Code	TA Number
March 13, 2024	A1	TA2024099

Summary

Attack Began: March 2024
Attack Region: Worldwide
Attack: In a recently observed campaign an infostealer masquerading as the Adobe Reader installer was being distributed. The file is being distributed by the threat actor in PDF format, luring people to download and execute it, collecting sensitive information.

Attack Regions



Attack Details

#1 A recently discovered campaign involves an infostealer disguised as the Adobe Reader installer being circulated. The threat actor distributes the file in PDF format, urging recipients to download and execute it for stealing the sensitive data.

#2 Initially the users receive a PDF which instructs the users to install the Adobe Reader and falsely claims that it is necessary to access a file, the pdf is written in Portuguese, containing malware, and users are unwittingly encouraged to install it.

#3 Users are redirected to a message containing a malware file named "Reader_Install_Setup.exe," which is disguised as an Adobe Reader icon. Upon downloading the file, users are prompted to run it. The execution process of the malware is divided into three phases: file creation, DLL hijacking & UAC bypass, and information leak.

#4 In the initial phase, two malicious files are created by the Reader_Install_Setup.exe, which leverages msdt.exe to run Bluetooth diagnostics and perform DLL hijacking to load malicious dll. The malicious DLL file simply has the DllMain function, which runs the malicious require.exe programme produced by Reader_Install_Setup.exe.

#5 The executable require.exe carries out several tasks, such as gathering data about the computer, corresponding with C2, establishing a path for Windows Defender exclusion, and producing the malicious programme chrome.exe. Using the same icon as the real browser, this file poses as the executable file for the browser. Additionally, it gathers user and system data and sends it to the C2 server.

#6 Users should exercise heightened caution when obtaining files from unofficial sources, particularly when encountering prompts to execute software installations. Malicious actors often exploit such scenarios to distribute malware disguised as legitimate applications.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration
T1566 Phishing	T1140 Deobfuscate/Decode Files or Information	T1036 Masquerading	T1055 Process Injection
T1112 Modify Registry	T1027 Obfuscated Files or Information	T1546 Event Triggered Execution	T1056 Input Capture
T1204 User Execution	T1204.001 Malicious Link	T1574 Hijack Execution Flow	T1574.001 DLL Search Order Hijacking

T1574.007 Path Interception by PATH Environment Variable	**T1041** Exfiltration Over C2 Channel	**T1560** Archive Collected Data	**T1059** Command and Scripting Interpreter
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	84526c50bc14838ddd97657db7c760ca, 0eebfc748bc887a6ef5bade20ef9ca6b, B24441f5249d173015dd0547d1654c6a, 02b96e2079bbc151222bb5bd10a4be9d
Domains	hxxps://blamefade.com[.]br/, hxxps://thinkforce.com[.]br/

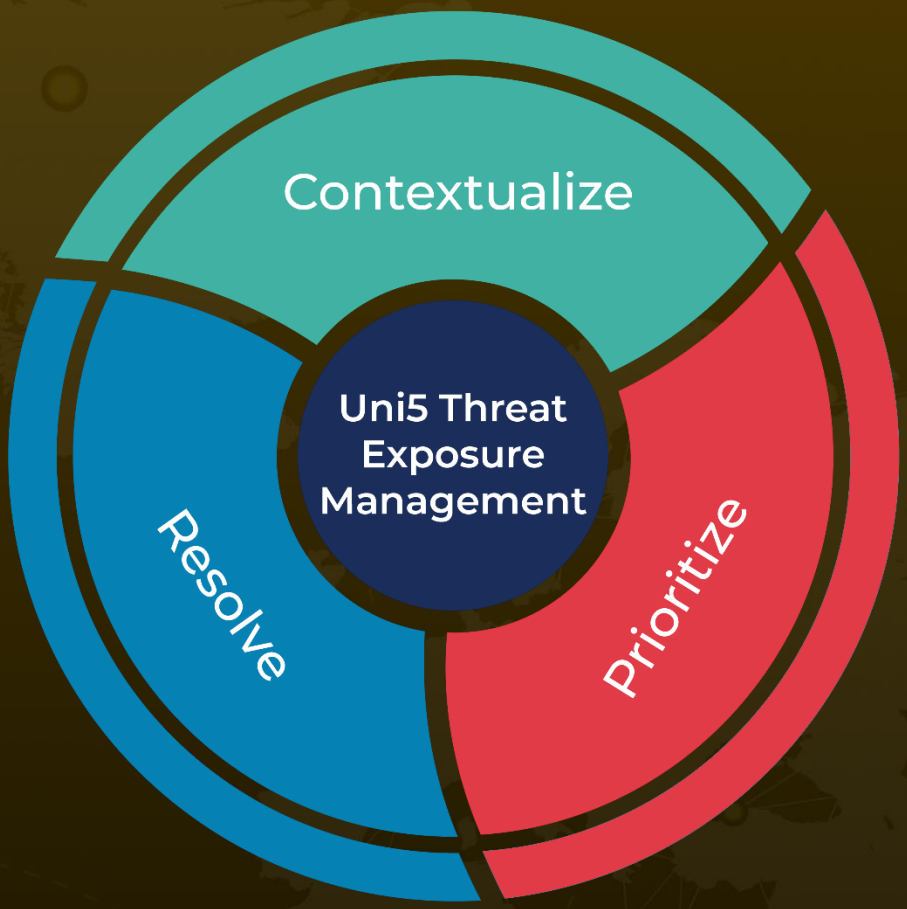
References

https://asec.ahnlab.com/en/62853/

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

March 13, 2024 • 6:30 AM

More at www.hivepro.com