Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

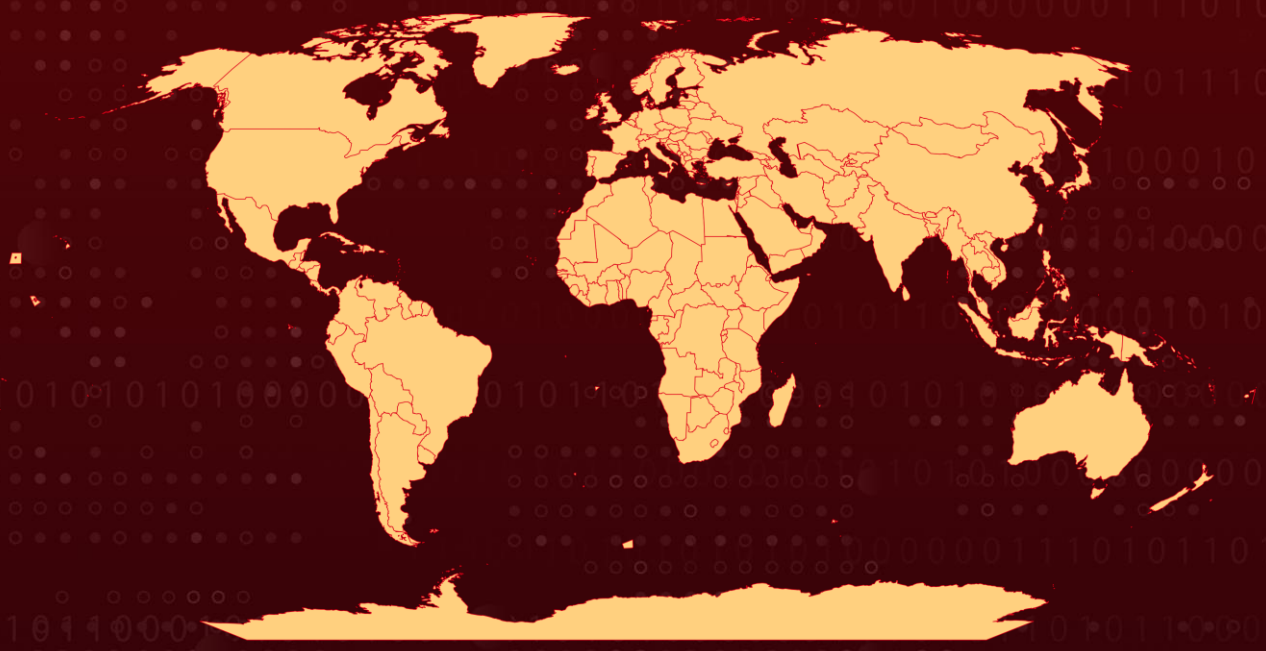
Hackers Utilize MSIX App Packages to Disseminate GHOSTPULSE Malware

Date of Publication	Admiralty Code	TA Number
October 31, 2023	A1	TA2023441

Summary

Attack Discovered: 27 October 2023
Attack Region: Worldwide
Affeted Platform: Windows
Malware: GHOSTPULSE
Attack: A new cyber attack campaign has emerged, involving the use of fake MSIX Windows app packages masquerading as legitimate applications. These deceptive MSIX packages are employed to distribute a new malware loader known as GHOSTPULSE. It operates as a multi-stage loader, decrypting its payload and deploying various types of malware while employing advanced defense evasion techniques.

Attack Regions



Attack Details

#1 A recent cyber campaign has come to light, targeting users by compromising signed MSIX application packages to gain initial access. MSIX is a Windows app package format used by developers to package, distribute, and install applications on Windows systems. The attackers in this campaign utilize a sophisticated loader known as GHOSTPULSE. This loader is designed to decrypt and inject its final payload into the target system.

#2 In a typical attack scenario, users are likely directed to download malicious MSIX packages through compromised websites, search-engine optimization techniques, or malvertising. The attackers often disguise these malicious packages as installers for popular software like Chrome, Brave, Edge, Grammarly, and WebEx. Malicious MSIX packages are designed to mimic legitimate software installation processes to trick users into thinking they are installing a genuine application. In reality, they secretly deliver the malware, which is then decrypted and executed on the compromised system.

#3 The GHOSTPULSE loader is a multi-stage malware that goes through several stages to execute its final payload. In the initial stage, it employs a TAR archive file containing gup.exe (Notepad++ updater) that disguises as different legitimate executable. The TAR archive also contains a file named handoff.wav and a trojanized version of libcurl.dll. This dll is loaded in the next stage of the infection process, taking advantage of the fact that gup.exe is susceptible to DLL side-loading.

#4 The tampered DLL file then proceeds to parse handoff.wav, which contains an encrypted payload. This encrypted payload is decoded and executed using mshtml.dll, a technique known as module stomping. By minimizing the on-disk footprint of the encrypted malicious code, the threat actor aims to evade file-based antivirus and machine learning scanning methods.

#5 In Last Stage, GHOSTPULSE overwrites the instructions it previously executed with new ones. GHOSTPULSE acts as a loader and uses another method called process doppelgänging to initiate the execution of the final malware. This final payload can include various malicious programs such as SectopRAT, Rhadamanthys, Vidar, Lumma, and NetSupport RAT, which are designed for different malicious purposes.

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.

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.

Download Packages from Official Websites: Always download software packages from the official website of the vendor or developer. Verify the website's URL to make sure it's the correct and official domain.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control	T1608 Stage Capabilities
T1608.001 Upload Malware	T1560 Archive Collected Data	T1056 Input Capture	T1204 User Execution
T1204.002 Malicious File	T1055 Process Injection	T1055.013 Process Doppelgänging	T1106 Native API
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading
T1140 Deobfuscate/Decode Files or Information	T1036 Masquerading	T1102 Web Service	T1129 Shared Modules

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0c01324555494c35c6bbd8babd09527bfc49a2599946f3540bb3380d7bec7a20, ee4c788dd4a173241b60d4830db128206dcfb68e79c68796627c6d6355c1d1b8, 4283563324c083f243cf9335662ecc9f1ae102d619302c79095240f969d9d356, eb2addefd7538cbd6c8eb42b70cafe82ff2a8210e885537cd94d410937681c61, 49e6a11453786ef9e396a9b84aeb8632f395477abc38f1862e44427982e8c7a9
IPv4	78.24.180[.]93
Domain	manojsinghnegi[.]com
URL	manojsinghnegi[.]com/2.tar.gpg
Code Signer	Futurity Designs Ltd, Fodere Titanium Limited, IMPERIOUS TECHNOLOGIES LIMITED

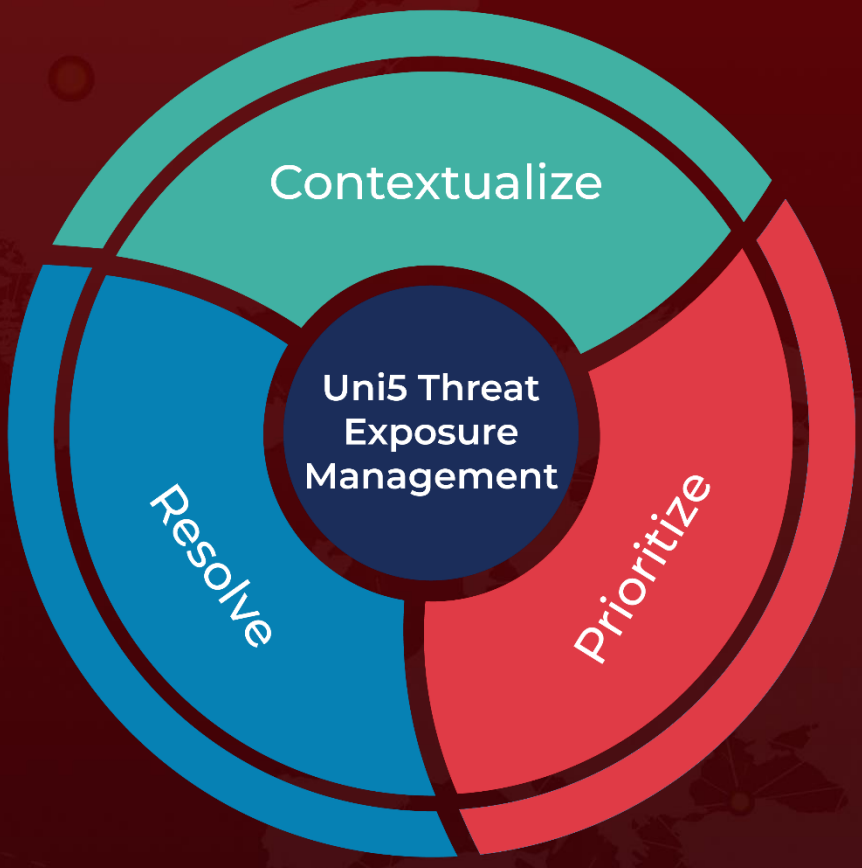
References

https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks

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

October 31, 2023 . 5:30 AM

More at www.hivepro.com