Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

UNC4990 Leverage Hosting Platforms in USB Infection Chain

Date of Publication	Admiralty Code	TA Number
February 1, 2024	A1	TA2024041

Summary

Attack Discovered: 2020
Attack Region: Italy
Targeted Industries: Health, Transportation, Construction, and logistics
Actor: UNC4990
Malware: EMPTYSPACE (also known as VETTA Loader and BrokerLoader), QUIETBOARD
Attack: UNC4990, a financially motivated threat actor, has been observed targeting organizations in Italy by utilizing weaponized USB drives as an initial infection vector. Additionally, they are employing trusted websites such as Vimeo, GitHub, and Ars Technica to host encoded payloads disguised within seemingly benign content.

Attack Regions

Attack Details

#1 Weaponized USB drives are being utilized as the initial infection vector by UNC4990, a financially motivated threat actor, to target organizations in Italy. This campaign has been ongoing since at least 2020. The threat actor has shifted from using seemingly harmless encoded text files to hosting payloads on well-known websites like Vimeo, GitHub, Ars Technica, and GitLab.

#2 The attacker's campaign began with abusing the Vimeo platform, hosting malicious payload in video description but after the video's removal, they shifted to leverage Ars Technica. They utilized similar public platforms to host payload, seamlessly integrating the encrypted payload within regular site contents to avoid detection.

#3 The infection begins when a victim double-clicks on a malicious LNK shortcut file found on a USB device. This action triggers the execution of a PowerShell script, which in turn decodes, decrypts, and executes an intermediate payload retrieved from legitimate websites, leading to the deployment of EMPTYSPACE on the compromised system. EMPTYSPACE establishes C2 and downloads a backdoor named 'QUIETBOARD', along with cryptocurrency miners designed to mine Monero, Ethereum, Dogecoin, and Bitcoin.

#4 QUIETBOARD is a sophisticated multi-component backdoor with a range of capabilities. These include executing commands on the compromised system, manipulating clipboard content to facilitate cryptocurrency theft, infecting USB and other removable drives for further propagation, capturing screenshots for information theft, collecting detailed system and network information, and determining the geographical location of the infected system.

#5 The examination of EMPTYSPACE and QUIETBOARD indicates that the threat actors adopted a modular strategy in crafting their toolset. The Python variant of EMPTYSPACE illustrates versioning, employing various programming languages for distinct versions. Notably, the URL changed when a Vimeo video was taken down, showcasing a tendency for experimentation and adaptability in their approach.

Recommendations

Remain Vigilant: Avoid the use of unknown or untrusted USB devices. Be especially cautious when encountering a malicious LNK shortcut file on a USB drive.

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.

USB Device Management: Implement centralized USB device management solutions that allow administrators to monitor and control the use of USB devices across the organization. This can help prevent unauthorized devices from being connected to company systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**T1204** User Execution	**T1204.001** Malicious Link
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1071** Application Layer Protocol	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1566** Phishing	**T1113** Screen Capture	**T1082** System Information Discovery
T1016 System Network Configuration Discovery	**T1614** System Location Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be, 98594dfae6031c9bdf62a4fe2e2d2821730115d46fca61da9a6cc225c6c4a750, d09d1a299c000de6b7986078518fa0defa3278e318c7f69449c02f177d3228f0, 7c793cc33721bae13e200f24e8d9f51251dd017eb799d0172fd647acab039027, 6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c0900886095436114a17443, a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40, 8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d, 060882f97ace7cb6238e714fd48b3448939699e9f085418af351c42b401a1227, 8c25b73245ada24d2002936ea0f3bcc296fdcc9071770d81800a2e76bfca3617, b9ffba378d4165f003f41a619692a8898aed2e819347b25994f7a5e771045217, 84674ae8db63036d1178bb42fa5d1b506c96b3b22ce22a261054ef4d021d2c69, 15d977dae1726c2944b0b4965980a92d8e8616da20e4d47d74120073cbc701b3, 26d93501cb9d85b34f2e14d7d2f3c94501f0aaa518fed97ce2e8d9347990decf, 26e943db620c024b5e87462c147514c990f380a4861d3025cf8fc1d80a74059a, 71c9ce52da89c32ee018722683c3ffbc90e4a44c5fba2bd674d28b573fba1fdc, 539a79f716cf359dceaa290398bc629010b6e02e47eaed2356074bffa072052f
URLs	hxxps://bobsmith.apiworld[.]cf/license.php, hxxps://arstechnica[.]com/civis/members/frncbf22.1062014/about/, hxxps://evinfeoptasw.dedyn[.]io/updater.php, hxxps://wjecpujpanmwm[.]tk/updater.php?from=USB1, hxxps://eldi8.github[.]io/src.txt, hxxps://evh001.gitlab[.]io/src.txt, hxxps://vimeo[.]com/api/v2/video/804838895.json, hxxps[://]monumental[.]ga/wp-admin[.]php, hxxp[://]studiofotografico35mm[.]altervista[.]org/updater[.]php, hxxp[://]ncnskjhrbefwifjhww[.]tk/updater[.]php,

TYPE	VALUE
URLs	hxxp[://]geraldonsboutique[.]altervista[.]org/updater[.]php, hxxps[://]wjecpujpanmwm[.]tk/updater[.]php, hxxps[://]captcha[.]grouphelp[.]top/updater[.]php, hxxps[://]captcha[.]tgbot[.]it/updater[.]php, hxxps://luke.compeyson.eu[.]org/runservice/api/public.php, hxxps[://]luke[.]compeyson[.]eu[.]org/wp-admin[.]php, hxxps://luke.compeyson.eu[.]org/runservice/api/public_result.php, hxxps://eu1.microtunnel[.]it/c0s1ta/index.php, hxxps[://]davebeerblog[.]eu[.]org/wp-admin[.]php, hxxps://lucaespo.altervista[.]org/updater.php, hxxps://lucaesposito.herokuapp[.]com/c0s1ta/index.php, hxxps://euserv3.herokuapp[.]com/c0s1ta/index.php

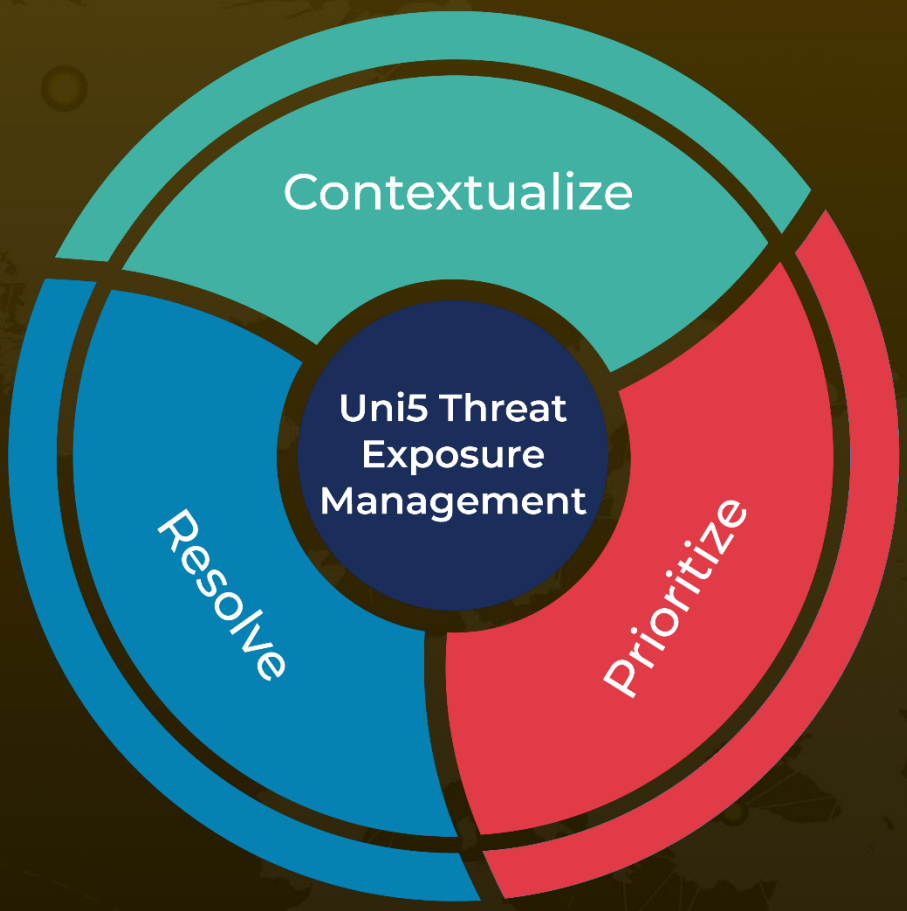
References

https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware

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

February 1, 2024 • 4:30 AM

More at www.hivepro.com