Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Unveiling Novel Malware Waves by APT28

Date of Publication	Admiralty Code	TA Number
January 02, 2023	A1	TA2024001

Summary

Attack Discovered: December 2023
Attack Region: Ukraine, Poland
Targeted Industries: Ukrainian government entities and Polish organizations
Actor: APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)
Malware: OCEANMAP, MASEPIE, and STEELHOOK
Attack: A recent phishing campaign attributed to the Russia-linked APT28 group has been identified targeting Ukrainian government entities and Polish organizations with email messages urging recipients to click on a link to view a document. The goal is to deploy previously undocumented malware, including OCEANMAP, MASEPIE, and STEELHOOK, to gather sensitive information.

Attack Regions

Attack Details

#1 Between December 15-25, 2023, multiple instances of email distribution were identified targeting state organizations attributed to the Russia-linked APT28 group. These emails contained links to supposed "documents," and visiting these links resulted of previously undocumented malware. The aim of the attack was to gather sensitive information, utilizing malware such as OCEANMAP, MASEPIE, and STEELHOOK.

#2 The initial access in this campaign was achieved through phishing. The provided links redirected victims to a web resource. Utilizing JavaScript and the application protocol "search," a shortcut file was downloaded. Opening this shortcut file triggered a PowerShell command, responsible for downloading a decoy document from a remote (SMB) resource. Additionally, the command initiated the download and execution of the Python interpreter along with the Client.py file, identified as MASEPIE.

#3 MASEPIE is a Python-based tool designed to facilitate the download of files and execution of commands through an encrypted channel using the TCP protocol. This versatile tool can be employed for various purposes, including building tunnels, extracting data from web browsers, and deploying backdoors.

#4 The attacks also facilitate the introduction of two additional malware, including a PowerShell script named STEELHOOK and OCEANMAP. The PowerShell script is proficient in extracting web browser data and transmitting it to a server controlled by the threat actor, encoding the information in Base64 format.

#5 OCEANMAP is coded in C# that leverages cmd.exe for command execution, utilizing the IMAP protocol for communication. It hides its commands within drafts of email mailboxes, holding details about the victim's computer, user, and operating system versions. Additionally, it establishes persistence by creating a .URL file in the autorun directory.

#6 The APT28 group's tactics, techniques, and tools indicate a sophisticated and well-coordinated effort. The approach of compromising individual computers as part of a larger plan underscores the potential risk to the entire organization's information and communication system.

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.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1095 Non-Application Layer Protocol	T1567 Exfiltration Over Web Service	T1021 Remote Services	T1566 Phishing
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1204 User Execution	T1204.001 Malicious Link
T1204.002 Malicious File	T1003 OS Credential Dumping	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1005 Data from Local System	T1071 Application Layer Protocol	T1071.003 Mail Protocols	T1132 Data Encoding
T1132.001 Standard Encoding	T1572 Protocol Tunneling		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	9724cecaa8ca38041ee9f2a42cc5a297, 5f126b2279648d849e622e4be910b96c, 47f4b4d8f95a7e842691120c66309d5b, 8d1b91e8fb68e227f1933cfab99218a4, 6fdd416a768d04a1af1f28ecaa29191b, 5db75e816b4cef5cc457f0c9e3fc4100, 6128d9bf34978d2dc7c0a2d463d1bcdd, 825a12e2377dd694bbb667f862d60c43, acd9fc44001da67f1a3592850ec09cb7
SHA256	4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6, 6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9, 18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6, 6d44532b1157ddc2e1f41df178ea9cbc896c19f79e78b3014073af2d8d9504fe, fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23, 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04, 19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc, 593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4, c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d
IP	173[.]239.196.66, 194[.]126.178.8, 88[.]209.251.6, 74[.]124.219.71, 88[.]209.251.6:80
Domains	czyrqdnvpujmmjkfhhvs4knf1av02demj.oast[.]fun, czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast[.]fun, czyrqdnvpujmmjkfhhvsgapqr3hclnhhj.oast[.]fun, czyrqdnvpujmmjkfhhvsvlaax17vd5r6v.oast[.]fun

TYPE	VALUE
URLs	hXXp://194[.]126.178.8/webdav/wody[.]pdf, hXXp://194[.]126.178.8/webdav/wody[.]zip, hXXp://194.126.178.8/webdav/StrategyUa.pdf, hXXp://194[.]126.178.8/webdav/231130N581[.]pdf, hXXp://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast[.]fun, hXXp://czyrqdnvpujmmjkfhhvsgapqr3hclnhhj.oast[.]fun, hXXp://czyrqdnvpujmmjkfhhvsvlaax17vd5r6v.oast[.]fun, hXXp://czyrqdnvpujmmjkfhhvs4knf1av02demj.oast[.]fun, hXXps://nas-files.firstcloudit[.]com/, hXXps://ua-calendar.firstcloudit[.]com/, hXXps://e-nas.firstcloudit[.]com/, jrb@bahouholdings[.]com, nas-files.firstcloudit[.]com, e-nas.firstcloudit[.]com, ua-calendar.firstcloudit[.]com, qasim.m@facadesolutionsuae[.]com, webmail.facadesolutionsuae[.]com

References

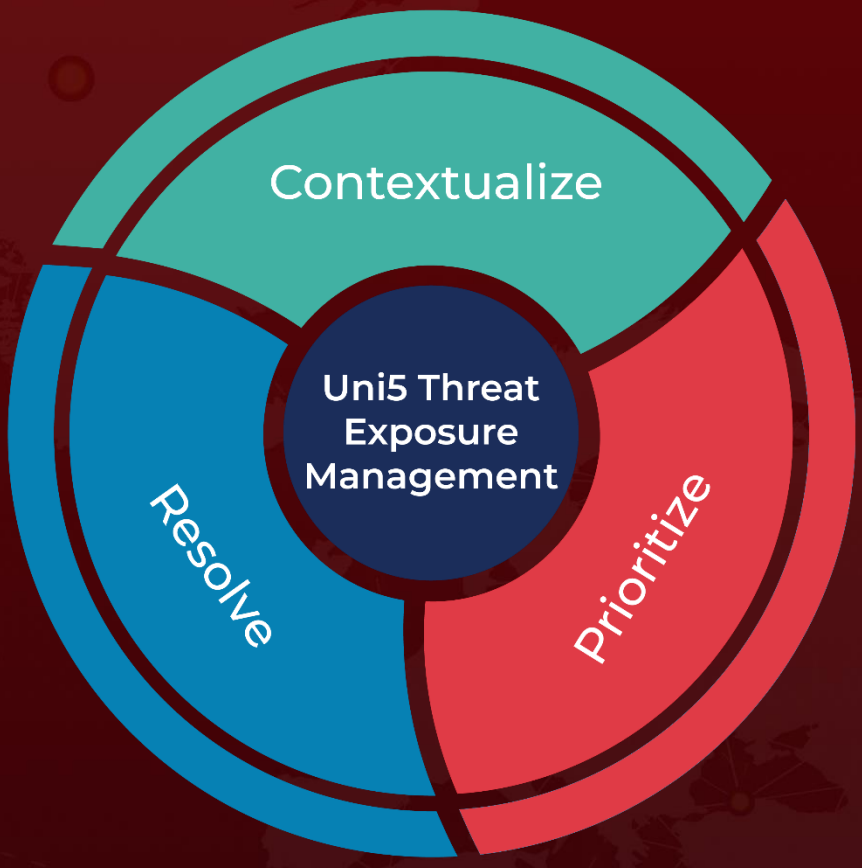
https://cert.gov.ua/article/6276894

https://www.hivepro.com/threat-advisory/apt28s-tactical-exploitation-of-critical-vulnerabilities/

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

January 02, 2024 . 5:30 AM

More at www.hivepro.com