Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

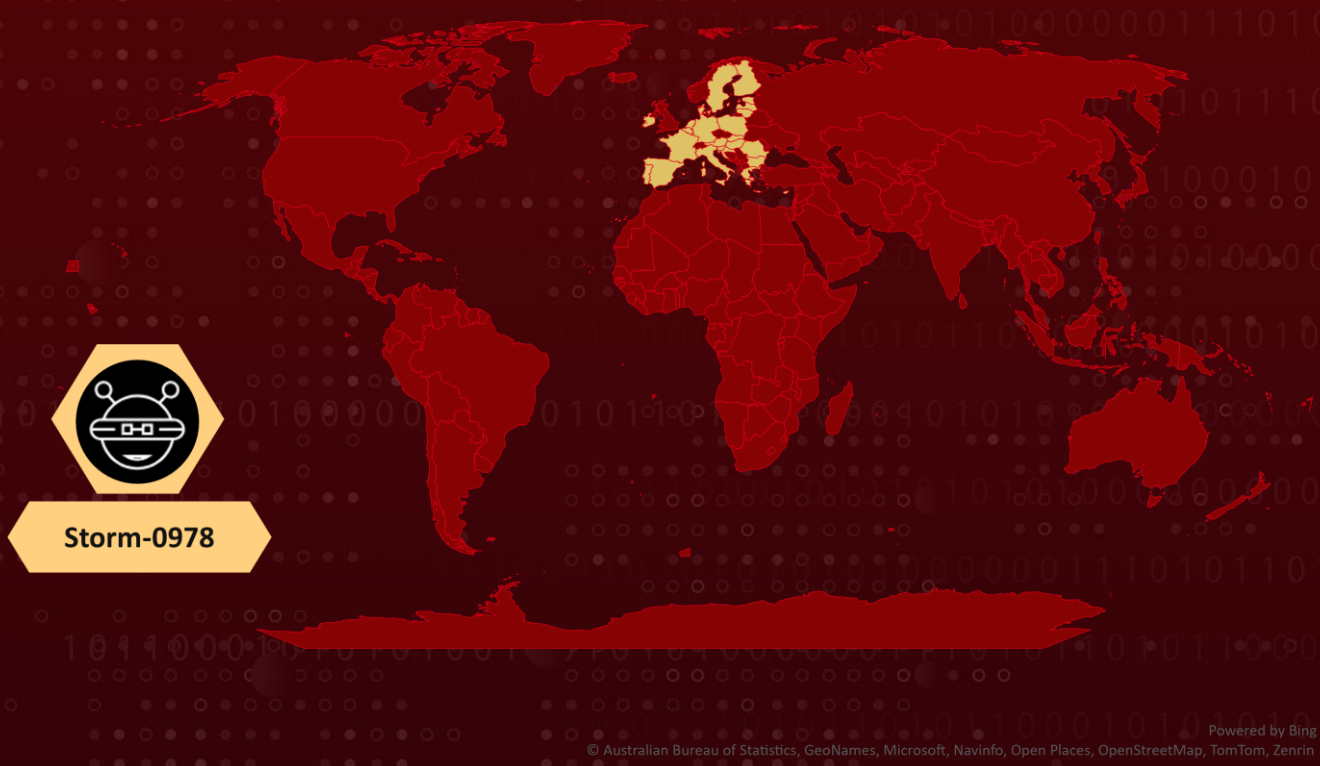
Storm-0978 unleashes PEAPOD to target Women Political Leaders

Date of Publication	Admiralty Code	TA Number
October 16, 2023	A1	TA2023417

Summary

Attack Began: August 8, 2023
Attack Region: European Union
Actor: Storm-0978 (aka Tropical Scorpius, RomCom, Void Rabisu, DEV-0978)
Malware: PEAPOD (aka ROMCOM 4.0)
Attack: Storm-0978, a threat actor group, utilized a new variant of the RomCom backdoor, "ROMCOM 4.0" also referred to as PEAPOD, to target attendees of the Women Political Leaders (WPL) Summit in Brussels. This summit is dedicated to discussions on gender equality and the participation of women in politics. The attackers created a fraudulent website resembling the official WPL portal, tricking individuals into unknowingly deploying the backdoor.

Attack Regions



Attack Details

#1 The threat actor group **Storm-0978** has deployed a new variant of the RomCom backdoor in a recent campaign, targeting European Union military personnel and political leaders engaged in gender equality initiatives. The campaign delivers an updated version of the RomCom RAT, known as PEAPOD.

#2 The actor usually employs targeted spear-phishing emails and deceptive advertisements on popular search engines to distribute RomCom malware. These tactics lure users to websites hosting trojanized versions of genuine applications. The latest version of RomCom, known as PEAPOD, has been simplified to include core features, allowing it to execute commands, manage files, collect system data, and even remove itself from compromised systems.

#3 PEAPOD supports only 10 commands, a significant reduction from the 42 commands supported by its predecessor. This simplification is intended to reduce the malware's digital footprint, making it stealthier and more challenging to detect. Unlike its predecessor, the new variant of RomCom uses an EXE file to fetch XOR-encrypted DLLs, loading all its components directly into memory instead of employing modified MSIs to drop its components onto devices.

#4 In August 2023, Storm-0978 established a malicious website with the address 'wplsummit[.]com'. This site was designed to closely mimic the legitimate Women Political Leaders (WPL) website. The malicious website included a link to a Microsoft OneDrive folder where an executable file named "Unpublished Pictures 1-20230802T122531-002-sfx.exe" was hosted. This file pretended to be a collection of photos from the Women Political Leaders (WPL) Summit that occurred in June 2023.

#5 The malicious executable was signed using a Elbor LLC certificate and was designed as a self-extracting archive. This executable downloaded a secondary payload, a DLL that was decrypted and loaded into the computer's memory to avoid detection. Once in memory, this DLL initiated communication with the attacker's server and fetched additional components. The DLL file, in its communication with another domain, retrieved the thirdstage PEAPOD artifact.

#6 Given the likelihood of Storm-0978 targeting major conferences related to special interest groups, it's crucial to exercise caution when visiting event websites and to be vigilant against potential spear-phishing attempts or malicious downloads associated with these events.

Recommendations

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.

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.

User Awareness: Regularly train employees on security best practices, emphasizing the risks of phishing attacks and malicious downloads, to minimize the likelihood of falling victim to attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0042 Resource Development	TA0003 Persistence	TA0011 Command and Control
T1566 Phishing	T1566.002 Spearphishing Link	T1608 Stage Capabilities	T1608.001 Upload Malware
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1587 Develop Capabilities	T1587.002 Code Signing Certificates
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1204 User Execution	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hXXps://onedrive.live[.]com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317, hXXps://mctelemetryzone[.]com/favicon[.]ico
SHA256	4f66d6ec70a49aaddb8018af1bf859284a6a4a27eb2615c80a32d5c7c156e476, 4299c16e11a725dd2ac9468c5c0aabf94ea5a90d2232810c19ba13b35b3708f9, 3c014d59cf22acbd062a4e2cab8cb8ede7127b6a69af9db45a7dcefde866369a, 41e995a8554fb6e4160d0e445856221ece2117a2b030012ead9efe76611bdc14, d1ca5349da287dbb13a1ea2a2982d23e6ce34ed822baee7468ce1980a4179d42, 83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c
Filenames	Unpublished Pictures 1-20230802T122531-002-sfx.exe, Security.dll, OneDriveService.dll, pcmf-installer-23.0.5.exe
Domains	netstaticsinformation[.]com, wplsummit[.]com, redditanalytics[.]pm, wirelessvezion[.]com, budgetnews[.]org, pap-cut[.]com, speedymarker[.]com, kayakahead[.]net

References

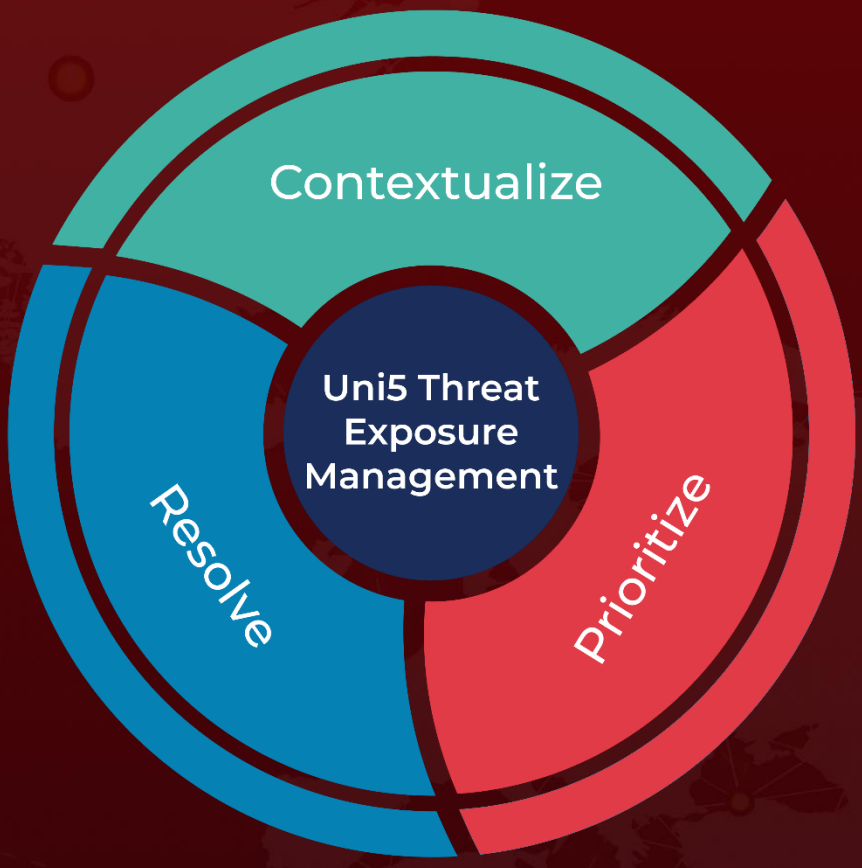
https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html

https://www.hivepro.com/storm-0978-actively-exploited-the-unpatched-office-zero-day/

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 16, 2023 . 4:25 AM

More at www.hivepro.com