Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

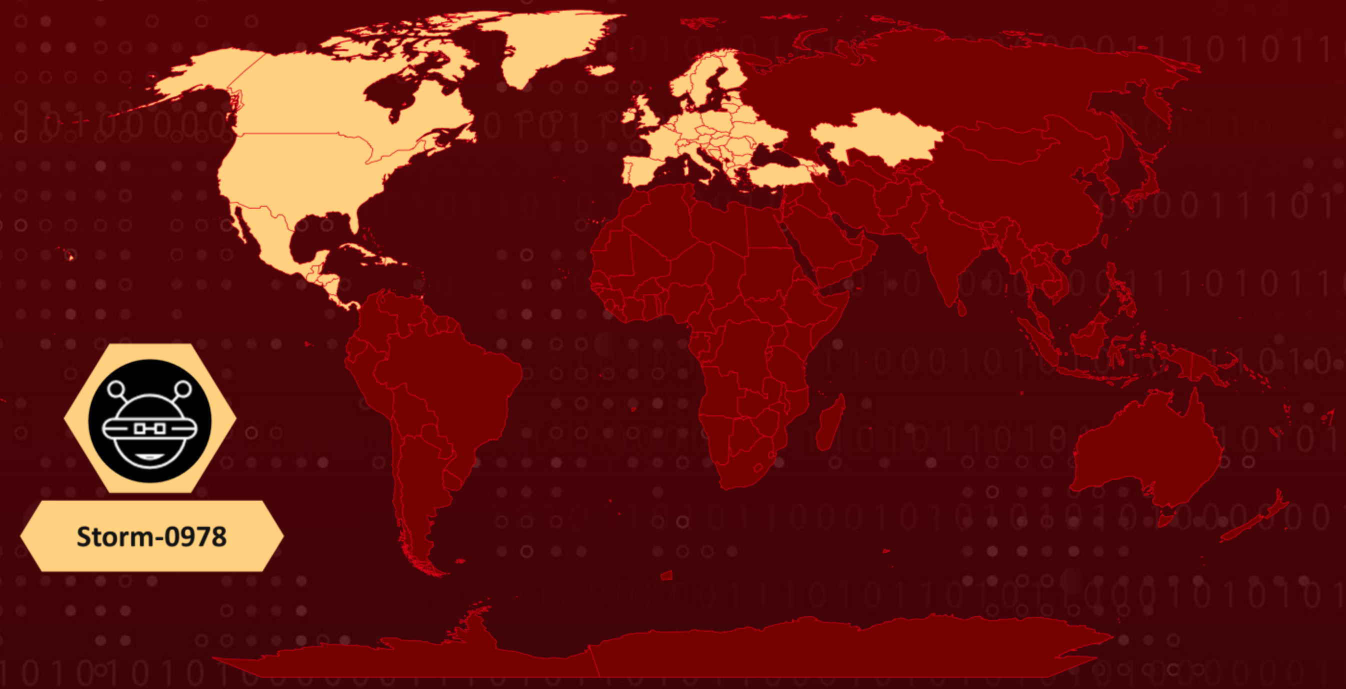
Storm-0978 actively exploited the Office zero-day

Date of Publication	Last Update Date	Admiralty code	TA Number
July 13, 2023	August 29, 2023	A1	TA2023298

Summary

First Appearance: 2022
Actor Name: Storm-0978 (aka DEV-0978, RomCom)
Target Industries: Finance, Telecommunications, Political, Defense, and Government
Target Region: Europe, North America, and Ukraine
Malware: RomCom Backdoor

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-36884	Office and Windows HTML Remote Code Execution Vulnerability	Office and Windows	✓	✓	✓

Actor Details

#1

Starting in 2022, Storm-0978, also known as DEV-0978, is a cybercriminal group originating from Russia that specializes in executing sophisticated phishing campaigns. In June 2023, Storm-0978 was found to be engaged in a new wave of attacks, leveraging the exploitation of CVE-2023-36884 to distribute a backdoor that bears striking similarities to the notorious RomCom malware.

#2

Storm-0978 is actively involved in the development, operation, and dissemination of the RomCom backdoor. Additionally, this group is associated with the deployment of the Underground ransomware, which exhibits close ties to the Industrial Spy ransomware that first emerged in the wild in May 2022.

#3

The most recent campaign Storm-0978, uncovered in June 2023, employed the exploitation of a Zero-day vulnerability CVE-2023-36884. This vulnerability enabled remote code execution and was leveraged through Microsoft Word documents. Additionally, the campaign made use of vulnerabilities that facilitated a security feature bypass. The purpose of these exploits was to distribute a backdoor that exhibits resemblances to the RomCom malware.

#4

The cybercriminal group Storm-0978 adopts a phishing technique wherein they create a deceptive website posing as a reputable and well-known software provider. They cunningly impersonate various popular software products such as Adobe offerings, SolarWinds Network Performance Monitor, SolarWinds Orion, Advanced IP Scanner, KeePass, and Signal. This tactic serves as the initial infection vector employed by Storm-0978.

#5

The primary objective of these malicious endeavors was to specifically target individuals within the government and military organizations. By deploying such tactics, Storm-0978 aimed not only to distribute the RomCom malware but also to surreptitiously acquire the credentials of high-value targets operating within these entities.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Storm-0978 (aka DEV-0978, RomCom)	Russia	Europe, North America, and Ukraine	Finance, Telecommunications, Political, Defense, and Government
	MOTIVE		
	Espionage		

Recommendations

CVE-2023-36884 was exploited in the wild. There are mitigation measures that can be implemented to minimize the risk associated with this vulnerability. It is essential to promptly install the security **patches** provided by Microsoft to address critical and high-severity vulnerabilities. Ensure your software remains up to date by regularly checking for and applying the latest security updates and patches from the vendor.

Implement measures to block the execution of executable files. This step helps mitigate the risk associated with running potentially malicious executables, providing an additional layer of protection against harmful software.

Consider implementing a policy that **blocks** all Office applications from creating child processes. By enforcing this restriction, you can further fortify your defenses against potential threats, reduce the attack surface, and enhance your overall security posture.

If organizations are unable to utilize the aforementioned protections, they have the option to set the
FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION
registry key to prevent exploitation. It is recommended to restart the affected applications after adding the registry key. Note that while these registry settings mitigate the issue, they may affect certain regular functionalities related to these applications. Therefore, thorough testing is advised. To disable the mitigation, delete the registry key or set it to "0".

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
T1566 Phishing	T1204 User Execution	T1082 System Information Discovery	T1217 Browser Bookmark Discovery
T1083 File and Directory Discovery	T1070 Indicator Removal	T1534 Internal Spearphishing	T1550 Use Alternate Authentication Material
T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1071 Application Layer Protocol	T1005 Data from Local System

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666, a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f, e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539, d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a, 3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
SHA1	fb4ad5d21f0d8c6755eb4addba0ac288bd2574b6
MD5	059175be5681a633190cd9631e2975f6

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

References

https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

https://blog.cyble.com/2023/07/12/microsoft-zero-day-vulnerability-cve-2023-36884-being-actively-exploited/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-zeroday-exploit

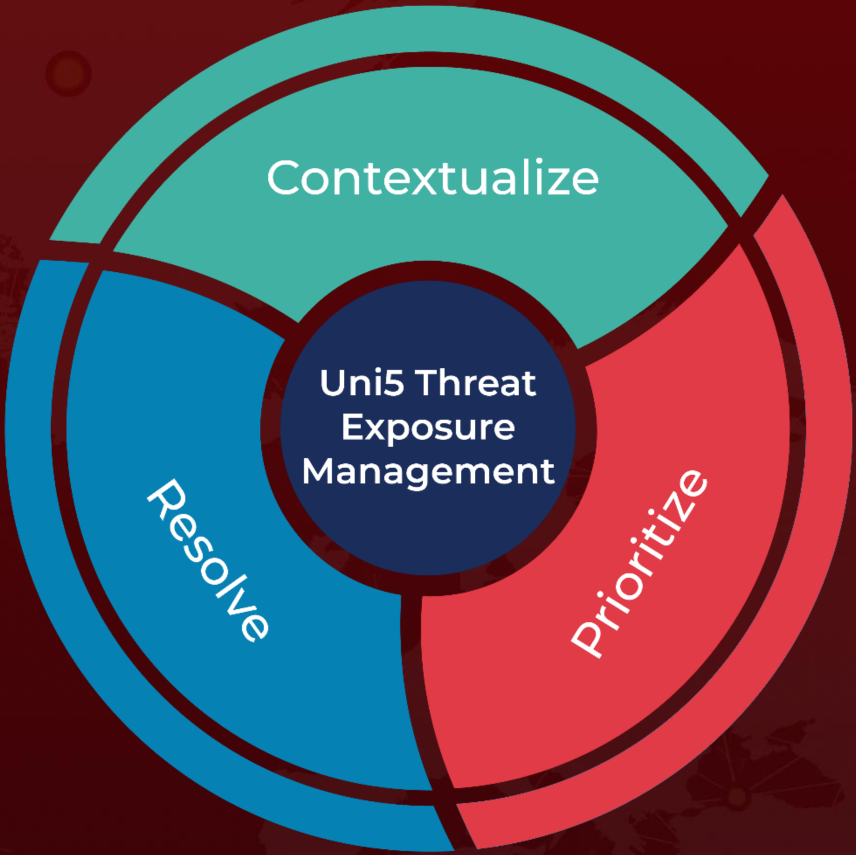
https://www.hivepro.com/industrial-spy-ransomware-trades-stolen-data-on-dark-web-marketplace/

https://www.hivepro.com/microsofts-july-2023-patch-tuesday-addresses-5-zero-day-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

July 13, 2023 • 7:00 AM

More at www.hivepro.com