Exploitation Of Microsoft Zero Day Vulnerability

Ransomware, RCE, Spyware, RAT

Vairav Advisory Report

19th July 2023

Vairav Technology Security Pvt. Ltd.

Phone: +977 014441540

Mobile: +977-9820105900

Email: mail@vairav.net

Thirbam Sadak 148
Baluwatar, Kathmandu

Executive Summary

The cybercriminal group Storm-0978 performed a sophisticated phishing campaign, and this research emphasizes a crucial and timely identification regarding it. Their main targets are European and North American defense and governmental organizations, concentrating on those active in Ukrainian politics. The exploitation of a zero-day vulnerability, **CVE-2023-36884**, to execute remote code using Word documents, even before Microsoft was aware of the issue, distinguishes this campaign from others. Storm-0978, notorious for its targeted credential-gathering activities and opportunistic ransomware, is using this new strategy to disseminate its RomCom backdoor. Furthermore, their recent use of the Industrial Spy ransomware-related Underground malware raises significant concerns. The most significant takeaway is the use of Storm-0978's extremely risky zero-day vulnerability exploitation tactic. This indicates that they can access and use hidden vulnerabilities to get into systems. This is crucial information to comprehend since it emphasizes the gravity of the threat presented by Storm-0978 and the necessity of acting quickly to protect systems and networks.

Key Points:

- The cybercriminal group Storm-0978 is based in Russia.
- With a focus on organizations active in Ukrainian issues, they have exploited **CVE-2023-36884** to conduct sophisticated phishing efforts against defense and governmental organizations in Europe and North America.
- Their use of a previously unknown vulnerability indicates sophisticated capability and the possibility of covert infiltration. Because of the tremendous security risk this presents, organizations must act right now to protect their systems and networks from this constantly changing danger.

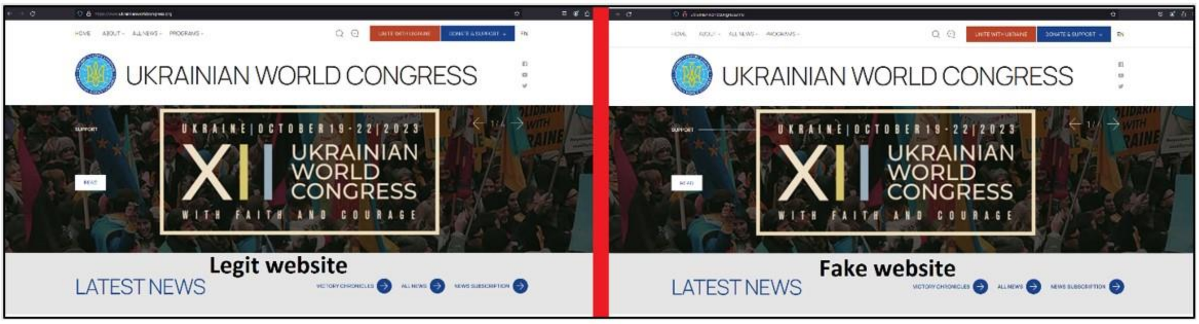
Introduction of Cyber Adversary

A cybercriminal organization called Storm-0978, in Russia, is well-known for its opportunistic ransomware and extortion activities and its targeted credential-gathering initiatives, which are probably carried out in support of intelligence operations. They manage, create, and disseminate the RomCom backdoor and implement the Industrial Spy-related Underground ransomware. They used **CVE-2023-36884** in their most recent campaign, which was discovered in June 2023, to deploy a backdoor that was identical to RomCom. RomCom installs are common after Storm-0978 targets organizations with trojanized versions of well-known software. Their attacks with ransomware have had a big impact on a lot of different businesses, particularly the telecoms and financial sectors.

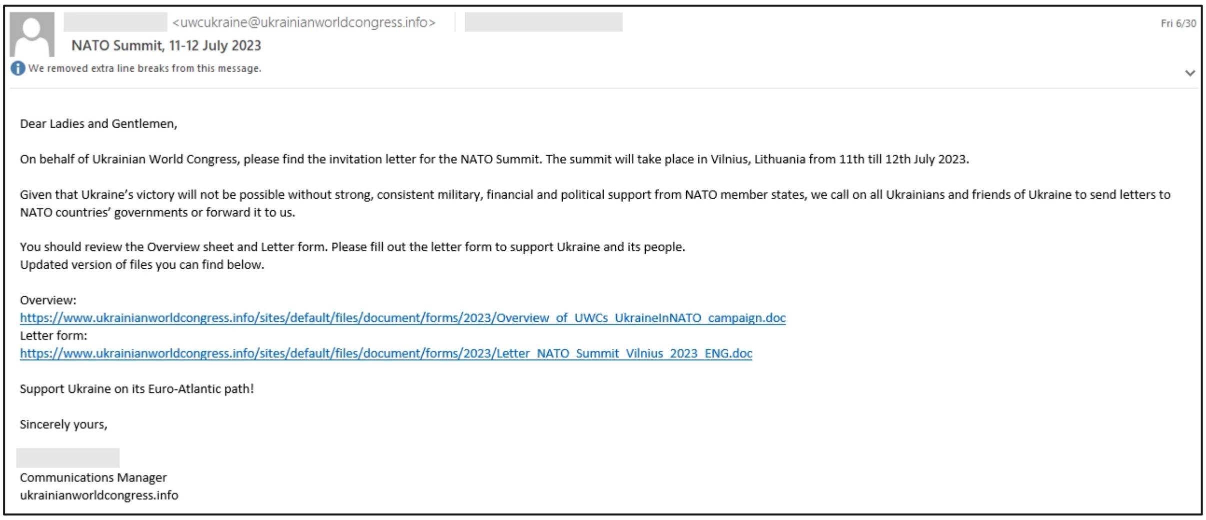
Tactics, Techniques, and Procedure

The Storm-0978 operations, active since late 2022, have been recognized by Microsoft as displaying post-compromise behaviors with possible espionage-related motivations. They started phishing efforts in October and December 2022, focusing on Ukrainian military and government organizations. They performed unauthorized email access to send phishing emails with malicious document attachments to steal sensitive data from victims' computers. They utilized fake websites to propagate the RomCom malware. In June 2023, Storm-0978 allegedly launched a fraudulent phishing attack that targeted European and North American defense and governmental organizations. To spread a backdoor that resembled the RomCom virus, the effort used a phony OneDrive loader.

Real Domain	**Fake Domain**
ukrainianworldcongress[.]org	ukrainianworldcongress[.]info



The fabricated website's source code can be examined to verify that it is a replica of the real.



[redacted] <uwcukraine@ukrainianworldcongress.info> [redacted]

Fri 6/30

NATO Summit, 11-12 July 2023

We removed extra line breaks from this message.

Dear Ladies and Gentlemen,

On behalf of Ukrainian World Congress, please find the invitation letter for the NATO Summit. The summit will take place in Vilnius, Lithuania from 11th till 12th July 2023.

Given that Ukraine's victory will not be possible without strong, consistent military, financial and political support from NATO member states, we call on all Ukrainians and friends of Ukraine to send letters to NATO countries' governments or forward it to us.

You should review the Overview sheet and Letter form. Please fill out the letter form to support Ukraine and its people.
Updated version of files you can find below.

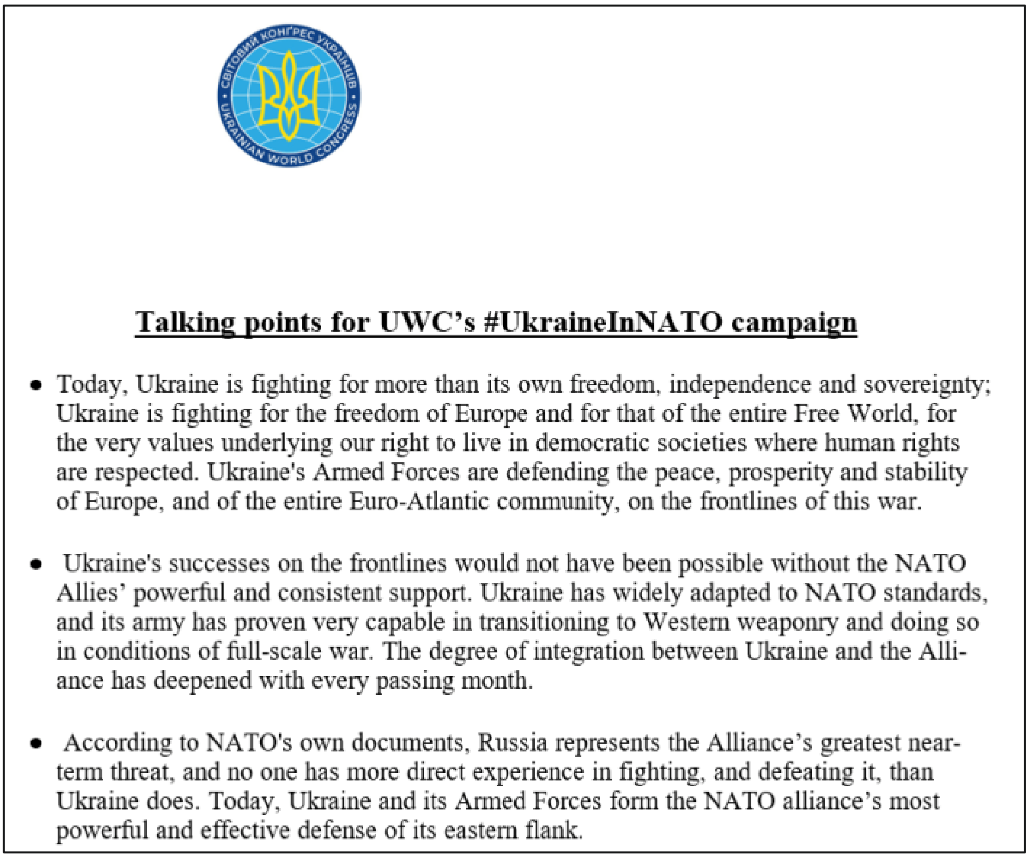
Overview:
https://www.ukrainianworldcongress.info/sites/default/files/document/forms/2023/Overview_of_UWCs_UkraineInNATO_campaign.doc
Letter form:
https://www.ukrainianworldcongress.info/sites/default/files/document/forms/2023/Letter_NATO_Summit_Vilnius_2023_ENG.doc

Support Ukraine on its Euro-Atlantic path!

Sincerely yours,

[redacted]
Communications Manager
ukrainianworldcongress.info

Figure 1: The Ukrainian World Congress and NATO used in the Storm-0978 email.



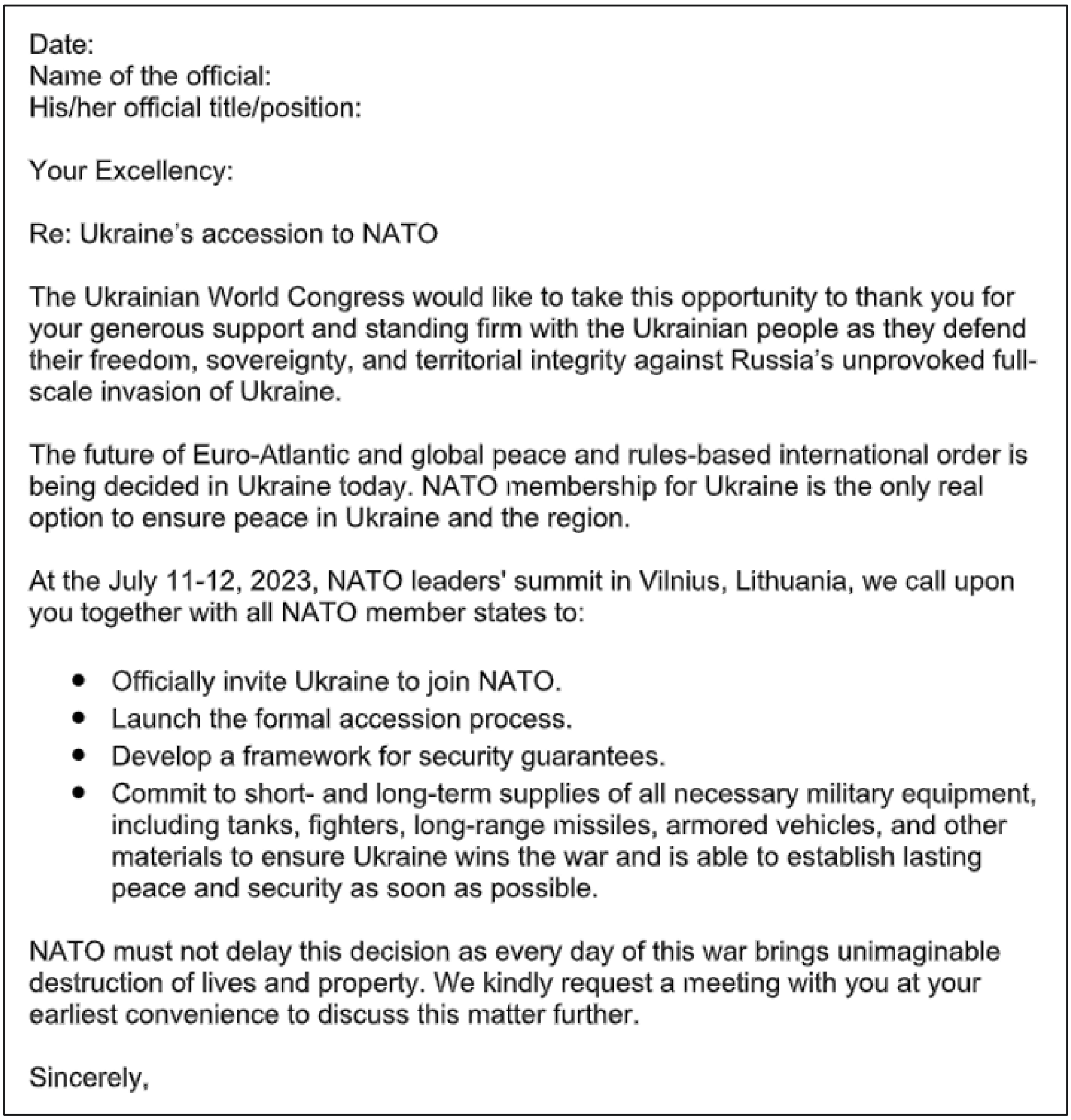
Talking points for UWC's #UkraineInNATO campaign

- Today, Ukraine is fighting for more than its own freedom, independence and sovereignty; Ukraine is fighting for the freedom of Europe and for that of the entire Free World, for the very values underlying our right to live in democratic societies where human rights are respected. Ukraine's Armed Forces are defending the peace, prosperity and stability of Europe, and of the entire Euro-Atlantic community, on the frontlines of this war.

- Ukraine's successes on the frontlines would not have been possible without the NATO Allies' powerful and consistent support. Ukraine has widely adapted to NATO standards, and its army has proven very capable in transitioning to Western weaponry and doing so in conditions of full-scale war. The degree of integration between Ukraine and the Alliance has deepened with every passing month.

- According to NATO's own documents, Russia represents the Alliance's greatest near-term threat, and no one has more direct experience in fighting, and defeating it, than Ukraine does. Today, Ukraine and its Armed Forces form the NATO alliance's most powerful and effective defense of its eastern flank.

They created Word documents with tempting content and sent them to certain participants to gain an advantage from that event. They also discovered another malicious document that was disguised as legitimate from the same threat actor, which they thought was a trap predicated on the approaching NATO Summit supporting Ukraine.



Date:
Name of the official:
His/her official title/position:

Your Excellency:

Re: Ukraine's accession to NATO

The Ukrainian World Congress would like to take this opportunity to thank you for your generous support and standing firm with the Ukrainian people as they defend their freedom, sovereignty, and territorial integrity against Russia's unprovoked full-scale invasion of Ukraine.

The future of Euro-Atlantic and global peace and rules-based international order is being decided in Ukraine today. NATO membership for Ukraine is the only real option to ensure peace in Ukraine and the region.

At the July 11-12, 2023, NATO leaders' summit in Vilnius, Lithuania, we call upon you together with all NATO member states to:

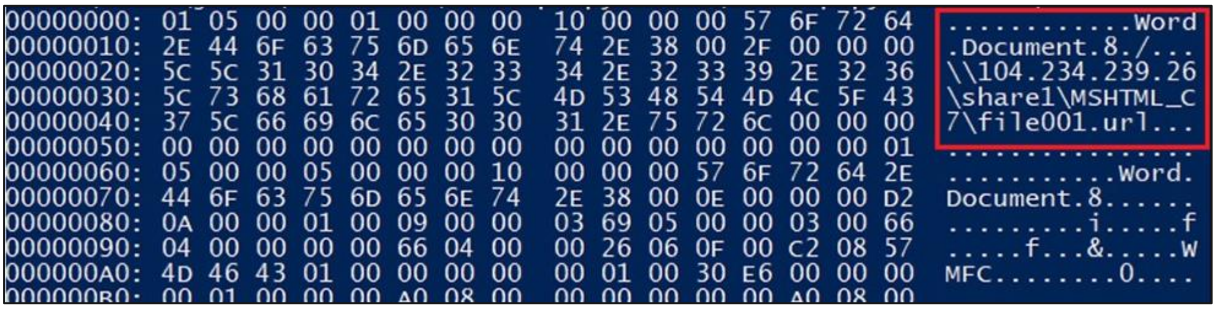
- Officially invite Ukraine to join NATO.
- Launch the formal accession process.
- Develop a framework for security guarantees.
- Commit to short- and long-term supplies of all necessary military equipment, including tanks, fighters, long-range missiles, armored vehicles, and other materials to ensure Ukraine wins the war and is able to establish lasting peace and security as soon as possible.

NATO must not delay this decision as every day of this war brings unimaginable destruction of lives and property. We kindly request a meeting with you at your earliest convenience to discuss this matter further.

Sincerely,

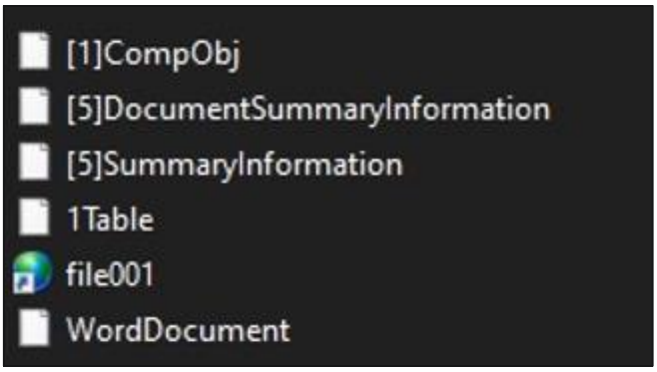
When the victim downloads and opens the infected file, a connection is established to a remote server of the attacker (104[.]234[.]239[.]26), and then the attacker performs the remote code execution vulnerability (**CVE-2023-36884**) to compromise the user's PC.

The document “Overview_of_UWCs_UkraineInNATO_campaign.docx” has an embedded RTF file called afchunk.rtf. Once the Microsoft Word file had been downloaded and executed/opened by the user, an OLE object was loaded from the RTF, which connected to the IP address 104.234.239[.]26, related to VPN/proxies services. The connections were made to ports 80, 139, and 445 (HTTP and SMB services).



```
00000000: 01 05 00 00 01 00 00 00  10 00 00 00 57 6F 72 64  ............Word
00000010: 2E 44 6F 63 75 6D 65 6E  74 2E 38 00 2F 00 00 00  .Document.8./...
00000020: 5C 5C 31 30 34 2E 32 33  34 2E 32 33 39 2E 32 36  \\104.234.239.26
00000030: 5C 73 68 61 72 65 31 5C  4D 53 48 54 4D 4C 5F 43  \share1\MSHTML_C
00000040: 37 5C 66 69 6C 65 30 30  31 2E 75 72 6C 00 00 00  7\file001.url...
00000050: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01  ................
00000060: 05 00 00 05 00 00 00 10  00 00 00 57 6F 72 64 2E  ...........Word.
00000070: 44 6F 63 75 6D 65 6E 74  2E 38 00 0E 00 00 00 D2  Document.8......
00000080: 0A 00 00 01 00 09 00 00  03 69 05 00 00 03 00 66  .........i.....f
00000090: 04 00 00 00 00 66 04 00  00 26 06 0F 00 C2 08 57  .....f...&.....W
000000A0: 4D 46 43 01 00 00 00 00  00 01 00 30 E6 00 00 00  MFC........0....
000000B0: 00 01 00 00 00 A0 08 00  00 00 00 00 00 A0 08 00
```

The file called file001.url was, in fact, a document in the form of a Microsoft Word file. This file was loaded after the execution of the NATO lure.



```
[1]CompObj
[5]DocumentSummaryInformation
[5]SummaryInformation
1Table
file001
WordDocument
```

Figure 2: Files stored within file001.

The file’s objective was to load the OLE streams into Microsoft Word, triggering the rendering of an iframe tag responsible for executing the next stage of malware. It attempted to retrieve the computer’s IP address, passing it as a parameter “?d=” and constructing a path in /appdata/local/temp/. Additionally, we observed other communications of the main Word payload, where the user’s IP address was passed as a parameter.

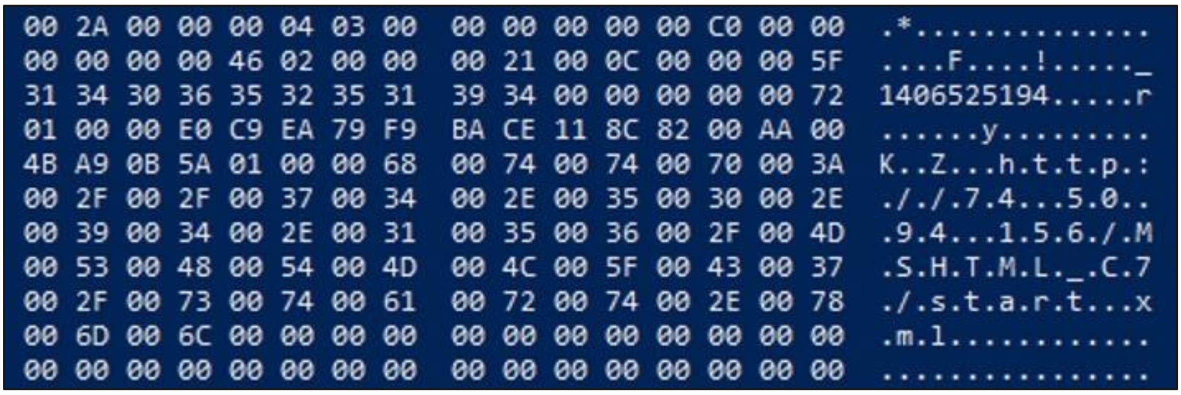
Below are the URLs used for communication:

hxxp://74.50.94[.]156/MSHTML_C7/zip_k.asp?d=34.141.245.25_f68f9_

hxxp://74.50.94[.]156/MSHTML_C7/zip_k2.asp?d=34.141.245.25_f68f9_

hxxp://74.50.94[.]156/MSHTML_C7/zip_k3.asp?d=34.141.245.25_f68f9_

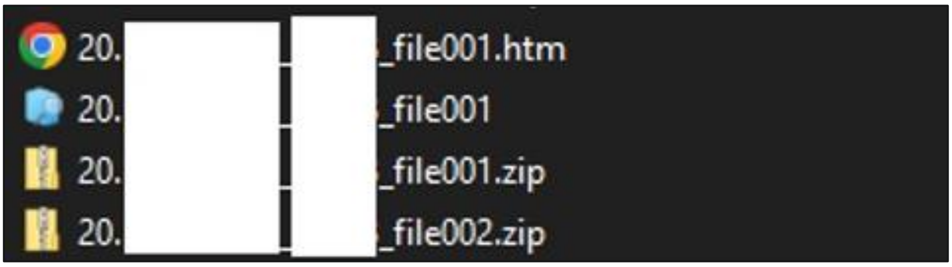
Once the connection to \104.234.239[.]26\share1\MSHTML_C7\file001.url was established, the threat actor made a second connection via HTTP to the same server mentioned in the above three URLs.



```
00 2A 00 00 00 04 03 00  00 00 00 00 00 C0 00 00  .*..............
00 00 00 00 46 02 00 00  00 21 00 0C 00 00 00 5F  ....F....!....._
31 34 30 36 35 32 35 31  39 34 00 00 00 00 00 72  1406525194.....r
01 00 00 E0 C9 EA 79 F9  BA CE 11 8C 82 00 AA 00  ......y.........
4B A9 0B 5A 01 00 00 68  00 74 00 74 00 70 00 3A  K..Z...h.t.t.p.:
00 2F 00 2F 00 37 00 34  00 2E 00 35 00 30 00 2E  ././.7.4...5.0..
00 39 00 34 00 2E 00 31  00 35 00 36 00 2F 00 4D  .9.4...1.5.6./.M
00 53 00 48 00 54 00 4D  00 4C 00 5F 00 43 00 37  .S.H.T.M.L._.C.7
00 2F 00 73 00 74 00 61  00 72 00 74 00 2E 00 78  ./.s.t.a.r.t...x
00 6D 00 6C 00 00 00 00  00 00 00 00 00 00 00 00  .m.l............
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Figure 3: Second connection made by afchunk.rtf.

The URL hxxp://74.50.94[.]156/MSHTML_C7/start.xml contains another iframe HTML tag to load a file named "RFile.asp" from the server path. Moreover, it stores the values "<" and ">" in variables "lt" and "gt", respectively. Each time a user visits the website, the server automatically generates multiple files for use during the intrusion. These files are sent from the URL hxxp://74.50.94[.]156/share1/MSHTML_C7/1/.



20.[redacted] [redacted]_file001.htm
20.[redacted] [redacted]_file001
20.[redacted] [redacted]_file001.zip
20.[redacted] [redacted]_file002.zip

Figure 4: Victim's data captured by the threat actor.

The payload consisted of an executable written in C++. The downloader incorporated several strings essential for its execution. It is noteworthy to mention that a similar string encryption algorithm was identified in the RomCom remote access trojan (RAT) samples encountered a few months ago.

Access to several C2s and numerous victim IPs from a single server was found while researching this campaign. This server accessed well-known RomCom infrastructure in the week before the campaign. It can be said with medium to high confidence that the threat actor behind both infrastructures is the same because of the extensive overlap in access from 143[.]198.18.163 location.

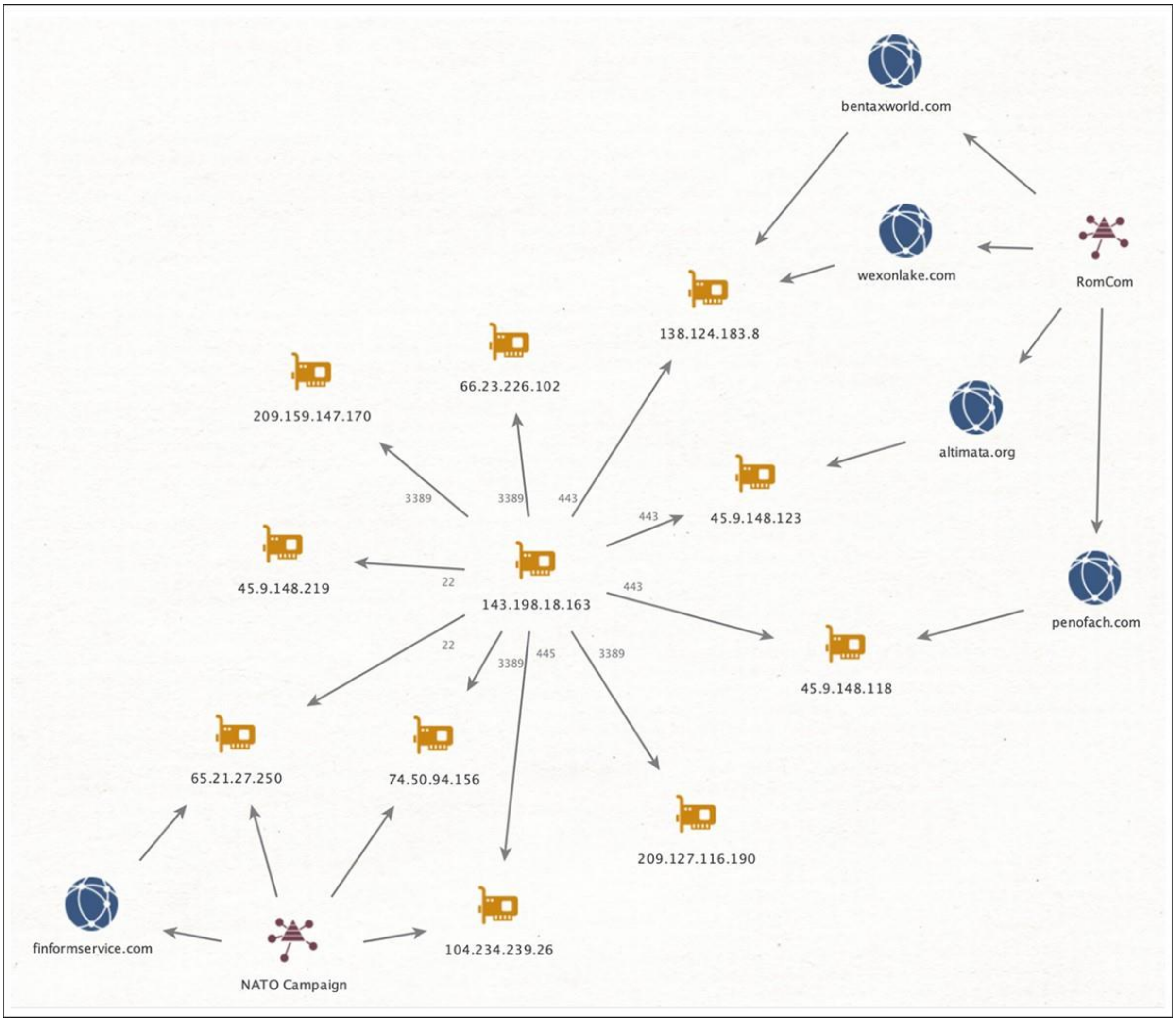


Figure 5: Network infrastructure relationship.

CVE-2023-36884

Critical Remote Code Execution vulnerability has been used as a zero-day in the wild and affects Microsoft Windows and Office. The vulnerability was rated 8.3 by CVSSv3. Microsoft has provided customers with mitigating advice to help stop its exploitation. The backdoor employed in their attacks, Storm-0978, also known as DEV-0978 and RomCom, is blamed by Microsoft researchers for exploiting **CVE-2023-36884**. The threat actor started its exploitation in June 2023, focusing on nations including Ukraine, North America, and Europe. The principal targets of these attacks have been the financial and telecoms sectors.

CVE-2023-36884 specific recommendations

- The usage of the attack surface reduction rule blocks all Office apps from establishing child processes and prevents the vulnerability from being used in existing attack chains.
- Add the following application names to this registry key as values of type REG_DWORD with data 1:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION

- Excel.exe
- Graph.exe
- MSAccess.exe
- MSPub.exe
- Powerpnt.exe
- Visio.exe
- WinProj.exe
- WinWord.exe
- Wordpad.exe

```
title: Suspicious MS Office Child Process
status: production
description:
 Identifies suspicious child processes of frequently targeted Microsoft Office applications (Word, PowerPoint, Excel).
 These child processes are often launched during exploitation of Office applications or from documents with malicious macros.
author: Elastic
date: "2020-02-18"
logsource:
 category: windows
 product: winlogbeat
detection:
 selection:
  - 'winlog.event_id: 1'   # Windows process start event
  - 'process.parent.name: ["eqnedt32.exe", "excel.exe", "fltldr.exe", "msaccess.exe", "mspub.exe", "powerpnt.exe", "winword.exe", "outlook.exe", “Graph.exe”, “Visio.exe”, “WinProj.exe’]'
  - 'process.name: ["Microsoft.Workflow.Compiler.exe", "arp.exe", "atbroker.exe", "bginfo.exe", "bitsadmin.exe", "cdb.exe", "certutil.exe", "cmd.exe", "cmstp.exe", "control.exe", "cscript.exe", "csi.exe", "dnx.exe", "dsget.exe", "dsquery.exe", "forfiles.exe", "fsi.exe", "ftp.exe", "gpresult.exe", "hostname.exe", "ieexec.exe", "iexpress.exe", "installutil.exe", "ipconfig.exe", "mshta.exe", "msxsl.exe", "nbtstat.exe", "net.exe", "net1.exe", "netsh.exe", "netstat.exe", "nltest.exe", "odbcconf.exe", "ping.exe", "powershell.exe", "pwsh.exe", "qprocess.exe", "quser.exe", "qwinsta.exe", "rcsi.exe", "reg.exe", "regasm.exe", "regsvcs.exe", "regsvr32.exe", "sc.exe", "schtasks.exe", "systeminfo.exe", "tasklist.exe", "tracert.exe", "whoami.exe", "wmic.exe", "wscript.exe", "xwizard.exe", "explorer.exe", "rundll32.exe", "hh.exe", "msdt.exe"]'
 condition: selection
level: medium
```

Table 1: Sigma rule in YAML format.

- Organizations who cannot take advantage of these protections can set the FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION registry key to avoid exploitation. No OS restart is required, but restarting the applications that have had the registry key added for them is recommended in case the value was already queried and is cached. Please note that while these registry settings would mitigate exploitation of this issue, they could affect regular functionality for certain use cases related to these applications. For this reason, we suggest testing. To disable the mitigation, delete the registry key or set it to “0”.

The following QQL query to determine if there are any infections within the ecosystem:

```
file.hash.sha256:["07377209fe68a98e9bca310d9749daa4eb79558e9fc419cf0b02a9e3767
9038d", "1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f",
"3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97",
"a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f",
"e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539"]
```

MITRE ATT&CK techniques

The activities make the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566) • Spearphishing Attachment (T1566.001)
Execution	User Execution (T1204) • Malicious File (T1204.002)
Discovery	System Information Discovery (T1082)
	Browser Information Discovery File and Directory (T1217)
	File and Directory Discovery (T1083)
Defense Evasion	Delete shadow drive data (T1070)
Lateral Movement	Internal Spearphishing (T1534)
	Use Alternate Authentication Material (T1550)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001)
Impact	Data encrypted for impact (T1486)
	Inhibit System Recovery (T1490)

Indicators of Compromise (IOCs)

IOC	Type
74[.]50[.]94[.]156	IP
94[.]232[.]40[.]34	IP
66[.]23[.]226[.]102	IP
104[.]234[.]239[.]26	IP
65[.]21[.]27[.]250	IP
138[.]124[.]183[.]8	IP
45[.]9[.]148[.]118	IP
finformservice[.]com	Domain
altimata[.]org	Domain
penofach[.]com	Domain
bentaxworld[.]com	Domain
wexonlake[.]com	Domain
ukrainianworldcongress[.]info	Domain
hxxp://finformservice[.]com:80/api/v1.5/subscriptiontoken=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTIzNDU2Nzg5LCJuYW1lIjoiSm9zZXBoIn0.OpOSSw7e485LOP5PrzScxHb7SR6sAOMRckfFwi4rp7o	URL
hxxp://65.21.27.250:8080/mds/O------------------------	URL
hxxp://finformservicecom:8080/mds/S------------------------	URL
059175be5681a633190cd9631e2975f6	MD5
a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f	SHA256
e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539	SHA256
3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97	SHA256
48142dc7fe28a5d8a849fff11cb8206912e8382314a2f05e72abad0978b27e90	SHA256
07377209fe68a98e9bca310d9749daa4eb79558e9fc419cf0b02a9e37679038d	SHA256
5f40cb4852ec50ee24f3cd951a172c725d02012d17dd645b6ce22d324aa140ad	SHA256
1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f	SHA256
0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a	SHA256

Threat Summary	
Name	Office and Windows HTML Remote Code Execution Vulnerability
Threat Type	Trojan
Detection Names	CVE-2023-36884, Trojan, Ransomware, RAT, RCE
Symptoms	Possible remote code execution, ransom notes, unauthorized access, the existence of RomCom backdoor activities, and the usage of underground ransomware
Additional Information	Spyware may be installed to steal your credentials or any other personal information.
Distribution methods	Phishing techniques
Damage	Steal sensitive information, encrypts data, downtime, and financial loss.
Sectors	Ukraine, Europe, North America
Malware Removal (Windows)	Use reputable antivirus software to run a full system scan and remove all detected malicious files and objects.

Vairav Recommendations

We strongly advise applying the following complete procedures to properly mitigate and prevent ransomware attacks:

1. Implement Regular Data Backups

Regular data backups are essential because they provide an effective way of restoring the data in the event of a ransomware attack. Backing up vital data regularly ensures that even if the files are encrypted by ransomware, one can restore them from a safe backup source. Offline or isolated network storage methods are advised to keep backups safe during an attack.

2. Develop an Incident Response Plan

It is critical to have a well-defined incident response strategy in place before reacting to a ransomware attack. The strategy should outline specific processes and responsibilities for isolating affected systems, alerting key stakeholders, and beginning the recovery process. Organizations that have an established and rehearsed response strategy can reduce downtime, limit the attack, and swiftly resume operations.

3. Restrict Execution of Files from Untrusted Sources

Ransomware frequently penetrates organizations via malicious email attachments, untrustworthy website downloads, or illegal software. Implementing strict security measures, such as application whitelisting or sandboxing solutions, to prohibit the execution of files from untrusted sources, aids in the prevention of harmful code execution. This gives an extra layer of defense and lowers the risk.

4. Keep Systems and Software Updated

Regularly upgrading operating systems, software programs, and firmware is critical because it helps to fix security weaknesses that ransomware attackers can exploit. Updates and patches are released by software manufacturers to address known vulnerabilities, therefore staying up to date is critical for ensuring a safe computer environment.

5. Implement the Least Privilege Principle

The principle of least privilege guarantees that employees are only provided the access rights and privileges required to carry out their job tasks. Organizations may lower the attack surface for ransomware by restricting access to essential systems and sensitive data. In the case of a successful ransomware outbreak, limiting user rights can reduce the damage and prevent lateral network migration.

6. Use Robust Antivirus and Anti-Malware Solutions:

Using trusted antivirus and anti-malware software adds an extra layer of protection against ransomware. These technologies aid in detecting and preventing harmful files and actions, including known ransomware incidents. Maintaining them ensures that you have the most recent virus definitions to identify and prevent new threats.

7. Implement Multi-factor Authentication (MFA)

Multi-factor authentication strengthens the security of your organization’s systems and accounts. MFA helps prevent unwanted access even if a user’s credentials are compromised by requiring multiple authentication factors, such as a password and a unique verification code. This greatly decreases the possibility of attackers obtaining control of important systems and data.

8. Enable Firewall and Intrusion Detection/Prevention Systems

Firewalls serve as a line of defense between the internal network and external threats. Configuring firewalls to filter incoming and outgoing network traffic aids in the prevention of intrusion and suspicious connections. It monitors network traffic for malicious activity signals and responds quickly to prevent possible ransomware attacks.

9. Engage with cybersecurity professionals.

If your organization lacks the necessary expertise or resources to effectively manage the aftermath of a breach, it is advisable to seek assistance from a trusted cybersecurity firm. Engaging with a reputable cybersecurity professional can provide valuable support in incident response, forensic analysis, and implementing security enhancements.

It is important to remember that the cyber adversaries behind ransomware gangs are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of the Storm-0978 ransomware gang and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar
Kathmandu, Nepal
Phone: +977-01-4441540
Mobile: +977-9820105900
Email: mail@vairav.net
Website: https://vairav.net