CVE-2023-36884

Microsoft Office and Windows HTML Remote Code Execution

investigate as Incident Responder

LetsDefend

Table Of Content

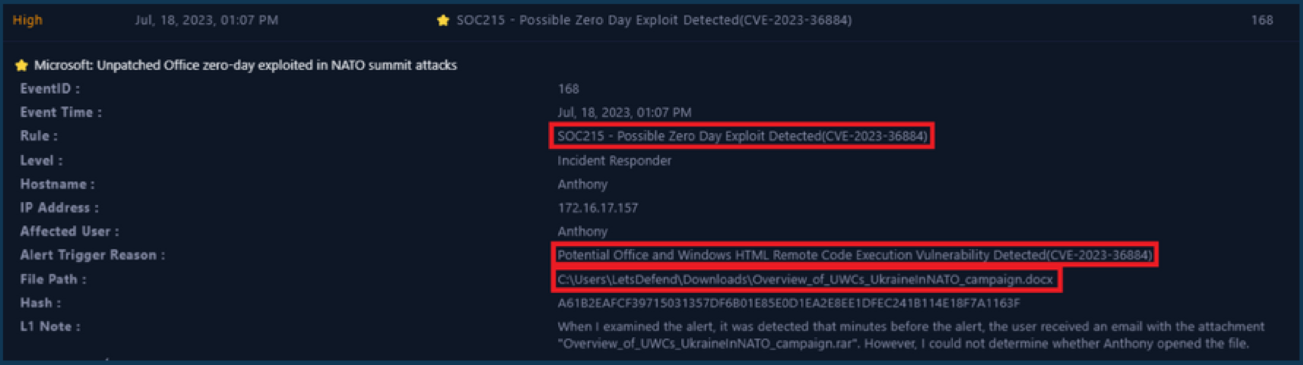
03 Alert
04 Verify
05 Initial Access
09 IP Reputation
17 Containment
18 Lessons Learned

Author: Muhammet Donmez

Alert

Looking at the reason that triggers the Alert, it has been found out that the system is trying to exploit the CVE-2023-36884 vulnerability which is a critical level alarm with RCE (Remote Code Execution).

A file named "Overview_of_UWCs_UkraineInNATO_campaign.docx" is shared under the downloads folder in the alert details. In addition, the L1 analyst investigation noted that the file "Overview_of_UWCs_UkraineInNATO_campaign.rar" was sent to Anthony via e-mail.



High Jul, 18, 2023, 01:07 PM ★ SOC215 - Possible Zero Day Exploit Detected(CVE-2023-36884) 168

★ Microsoft: Unpatched Office zero-day exploited in NATO summit attacks

EventID :	168
Event Time :	Jul, 18, 2023, 01:07 PM
Rule :	SOC215 - Possible Zero Day Exploit Detected(CVE-2023-36884)
Level :	Incident Responder
Hostname :	Anthony
IP Address :	172.16.17.157
Affected User :	Anthony
Alert Trigger Reason :	Potential Office and Windows HTML Remote Code Execution Vulnerability Detected(CVE-2023-36884)
File Path :	C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_campaign.docx
Hash :	A61B2EAFCF39715031357DF6B01E85E0D1EA2E8EE1DFEC241B114E18F7A1163F
L1 Note :	When I examined the alert, it was detected that minutes before the alert, the user received an email with the attachment "Overview_of_UWCs_UkraineInNATO_campaign.rar". However, I could not determine whether Anthony opened the file.

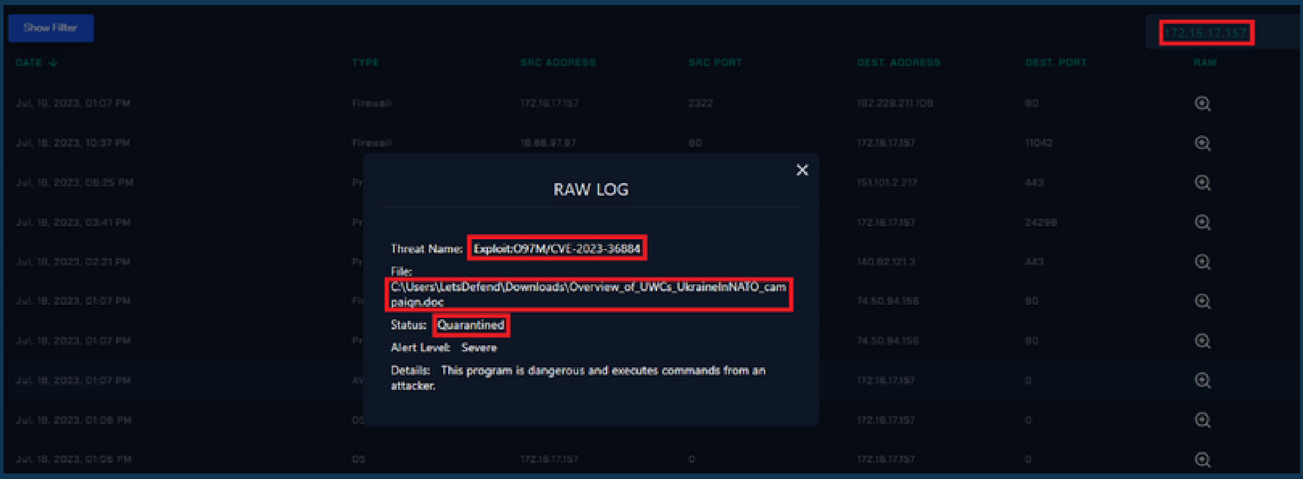
First, this alert should be verified by checking the existing logs, and then it should be determined whether the attack was successful or not.

LetsDefend

Verify

We start investigating the logs by searching the source IP address (172.16.17.157) in the alert in the Log Management. As a result of our searches, we have seen the OS, Proxy, Firewall and AV/EDR logs.

We can check the AV/EDR logs to be able to confirm the alarm. In the details of the relevant log, We see that the file C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_campaign.doc file is paired with "Exploit:O97M/CVE-2023-36884" and the malware was quarantined.



DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul. 19, 2023, 01:07 PM	Firewall	172.16.17.157	2322	192.229.211.108	80	🔍
Jul. 18, 2023, 10:37 PM	Firewall	18.66.97.97	80	172.16.17.157	11042	🔍
Jul. 18, 2023, 08:25 PM	Pr			151.101.2.217	443	🔍
Jul. 18, 2023, 03:41 PM	Pr			172.16.17.157	24298	🔍
Jul. 18, 2023, 02:21 PM	Pr			140.82.121.3	443	🔍
Jul. 18, 2023, 01:07 PM	Fi			74.50.94.156	80	🔍
Jul. 18, 2023, 01:07 PM	Pr			74.50.94.156	80	🔍
Jul. 18, 2023, 01:07 PM	AV			172.16.17.157	0	🔍
Jul. 18, 2023, 01:06 PM	OS			172.16.17.157	0	🔍
Jul. 18, 2023, 01:06 PM	OS	172.16.17.157	0	172.16.17.157	0	🔍

RAW LOG

Threat Name: Exploit:O97M/CVE-2023-36884

File: C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_campaign.doc

Status: Quarantined

Alert Level: Severe

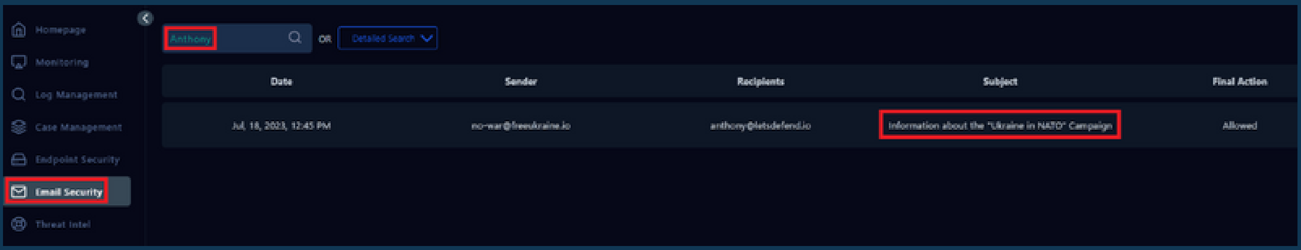
Details: This program is dangerous and executes commands from an attacker.

We were able to verify that the alarm was True Positive within our first examinations.

LetsDefend

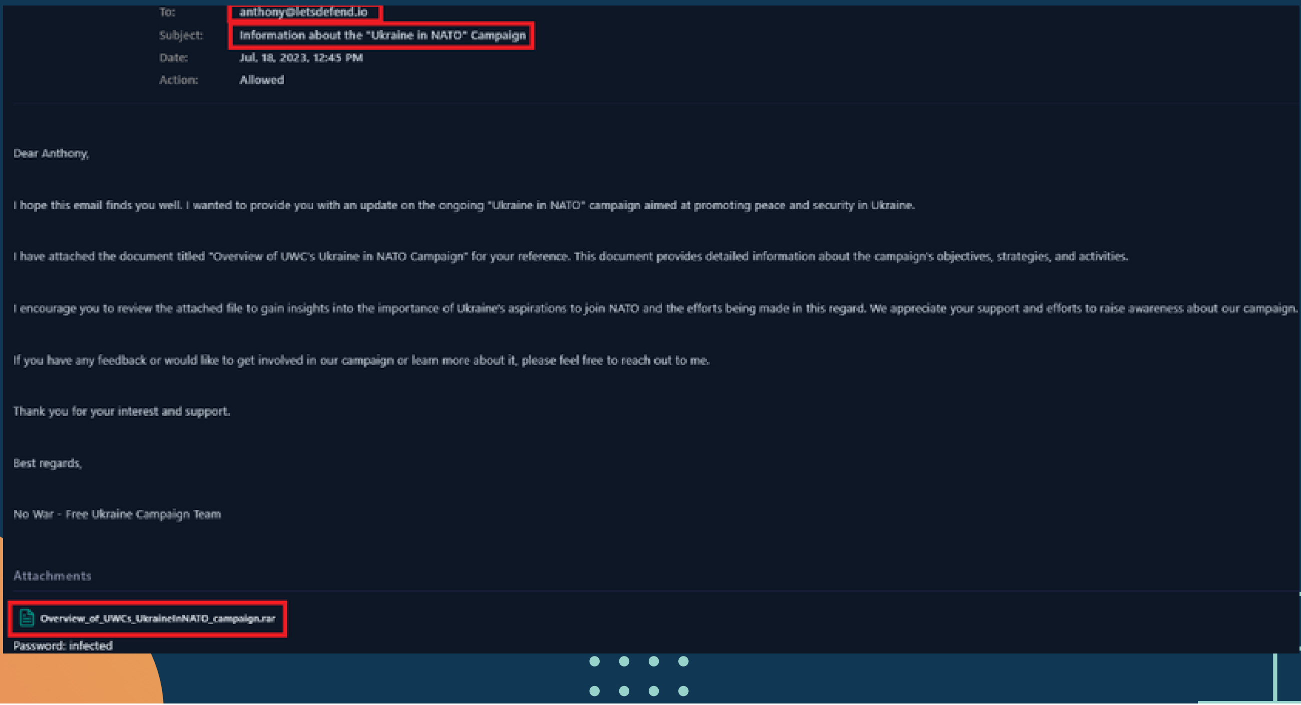
Initial Access

We should check our Email Security tool to confirm the email mentioned in the LI analyst note. Our search comes with at result showing that the relevant user receives an e-mail with the subject “Information about the "Ukraine in NATO" Campaign” from the “no-war@freeukraine.io” sender.



Date	Sender	Recipients	Subject	Final Action
Jul, 18, 2023, 12:45 PM	no-war@freeukraine.io	anthony@letsdefend.io	Information about the "Ukraine in NATO" Campaign	Allowed

We have also detected the “Overview_of_UWCs_UkraineInNATO_campaign.rar” file when we check the emails attachment.



To: anthony@letsdefend.io
Subject: Information about the "Ukraine in NATO" Campaign
Date: Jul. 18, 2023, 12:45 PM
Action: Allowed

Dear Anthony,

I hope this email finds you well. I wanted to provide you with an update on the ongoing "Ukraine in NATO" campaign aimed at promoting peace and security in Ukraine.

I have attached the document titled "Overview of UWC's Ukraine in NATO Campaign" for your reference. This document provides detailed information about the campaign's objectives, strategies, and activities.

I encourage you to review the attached file to gain insights into the importance of Ukraine's aspirations to join NATO and the efforts being made in this regard. We appreciate your support and efforts to raise awareness about our campaign.

If you have any feedback or would like to get involved in our campaign or learn more about it, please feel free to reach out to me.

Thank you for your interest and support.

Best regards,

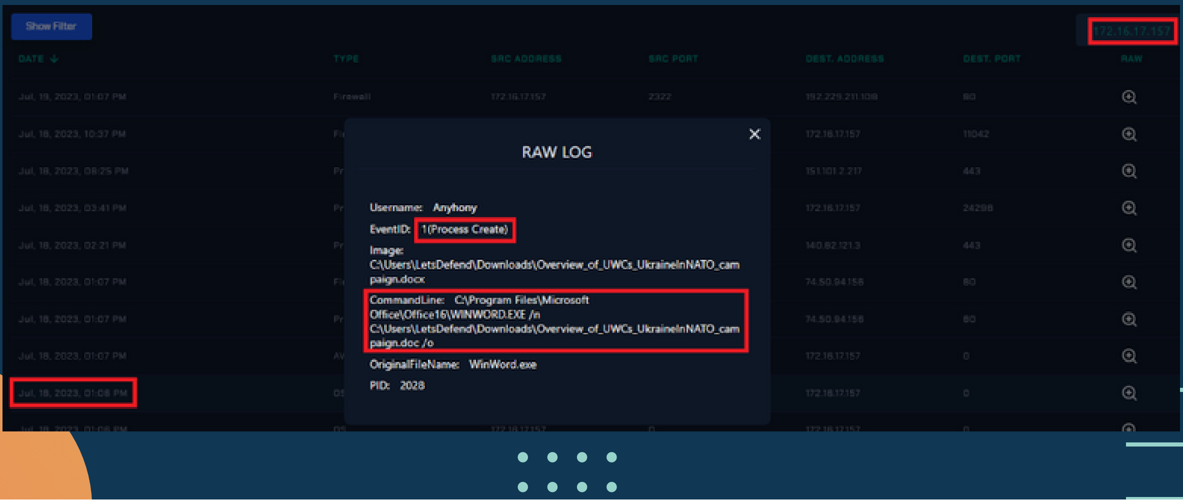
No War - Free Ukraine Campaign Team

Attachments

Overview_of_UWCs_UkraineInNATO_campaign.rar
Password: infected

Now, we need to review 2 critical points here. We first need to confirm whether the file has been downloaded and if it was run on the system. We can go through and investigate the OS logs in detail for 172.16.17.157. As a result of our search, we found out that the following file was created at 01:06 PM: “C:\Users\LetsDefend\Downloads\~$erview_of_UWCs_UkraineInNATO_campaign.doc”.

We also found out that the file was run over WinWord.exe within the same minute: “C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_campaign.doc”. This confirms that the malware infected the system via an e-mail. We should extend our search on the Email Security tool to make sure if it is a phishing or spear phishing attack by searching the sender email address and subject and see if there are any other user who received the same or similar emails.

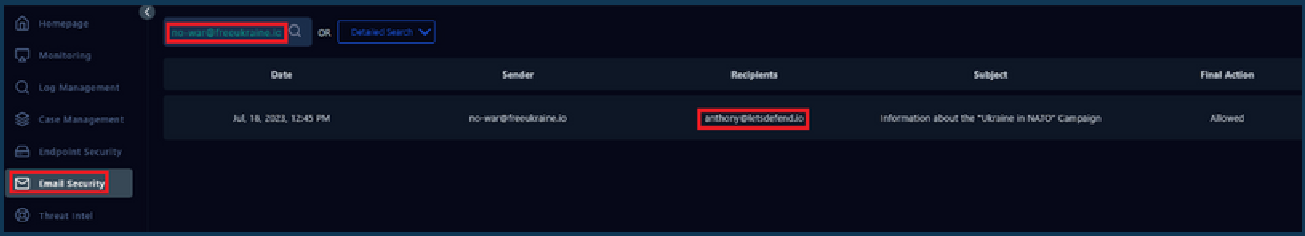


DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jul, 19, 2023, 01:07 PM	Firewall	172.16.17.157	2322	192.229.211.108	80	🔍
Jul, 18, 2023, 10:37 PM	Fi			172.16.17.157	11042	🔍
Jul, 18, 2023, 08:25 PM	Pr			151.101.2.217	443	🔍
Jul, 18, 2023, 03:41 PM	Pr			172.16.17.157	24298	🔍
Jul, 18, 2023, 02:21 PM	Pr			140.82.121.3	443	🔍
Jul, 18, 2023, 01:07 PM	Fi			74.50.94.156	80	🔍
Jul, 18, 2023, 01:07 PM	Pr			74.50.94.156	80	🔍
Jul, 18, 2023, 01:07 PM	AV			172.16.17.157	0	🔍
Jul, 18, 2023, 01:06 PM	OS			172.16.17.157	0	🔍
Jul, 18, 2023, 01:06 PM	OS	172.16.17.157	0	172.16.17.157	0	🔍

RAW LOG

```
Username:   Anyhony
EventID:  1(Process Create)
Image:
C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_cam
paign.docx
CommandLine:   C:\Program Files\Microsoft
Office\Office16\WINWORD.EXE /n
C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_cam
paign.doc /o
OriginalFileName:   WinWord.exe
PID:   2028
```

Our searches on both subject and sender addresses on our Email Security tool showed that the malicious e-mail was only sent to anthony[@]letsdefend.io which we can consider as a “Phishing: Spearphishing Attachment (T1566.001)” for initial access.

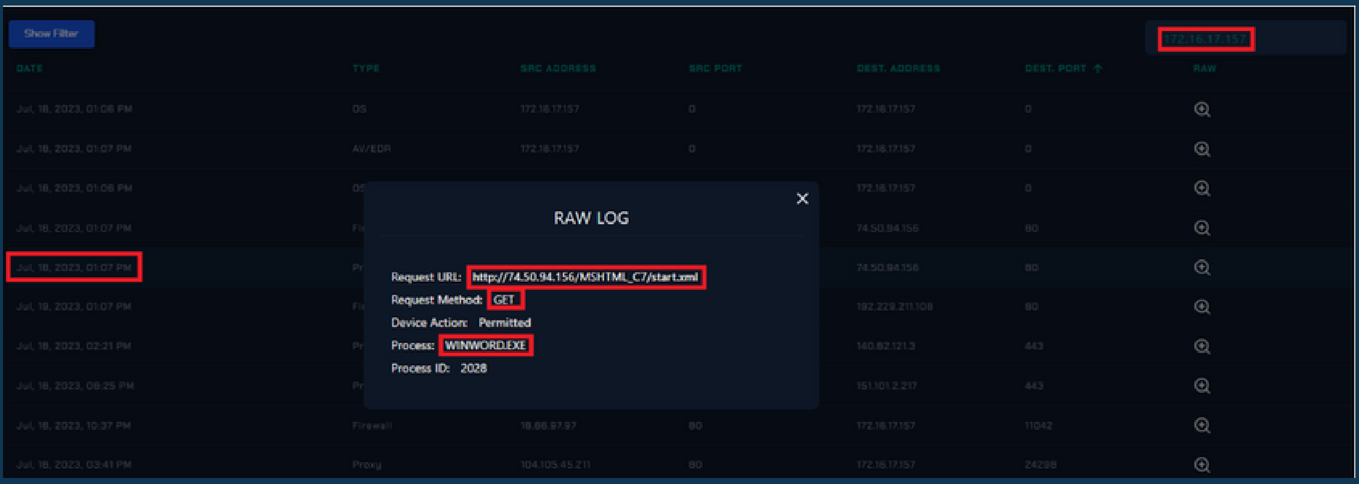


Date	Sender	Recipients	Subject	Final Action
Jul, 18, 2023, 12:45 PM	no-war@freeukraine.io	anthony@letsdefend.io	Information about the "Ukraine in NATO" Campaign	Allowed

We can continue our investigations with other logs remaining on the Log Management. Again, when a search for the 172.16.17.157 IP address, network traffic towards “192.229.211.108” and “74.50.94.156” over port 80 stand out.

We can continue our investigations with other logs remaining on the Log Management. Again, when a search for the 172.16.17.157 IP address, network traffic towards “192.229.211.108” and “74.50.94.156” over port 80 stand out.

When we review If these three logs in detail, we see both proxy and firewall logs towards 74[.]50[.]94.156 IP address. Here in the detail of the proxy log, we see that a GET request was sent to "http[:]//74[.]50[.]94.156/MSHTML_C7/start.xml" and the "WINWORD.EXE" process was the source of this request which could be the reason why we see the traffic on the firewall. No information is shared regarding the traffic towards the 192,229,211.108 IP address in the raw data.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT ↑	RAW
Jul, 18, 2023, 01:08 PM	OS	172.16.17.157	0	172.16.17.157	0	🔍
Jul, 18, 2023, 01:07 PM	AV/EDR	172.16.17.157	0	172.16.17.157	0	🔍
Jul, 18, 2023, 01:08 PM	OS			172.16.17.157	0	🔍
Jul, 18, 2023, 01:07 PM	Fi			74.50.94.156	80	🔍
Jul, 18, 2023, 01:07 PM	Pr			74.50.94.156	80	🔍
Jul, 18, 2023, 01:07 PM	Fi			192.229.211.108	80	🔍
Jul, 18, 2023, 02:21 PM	Pr			140.82.121.3	443	🔍
Jul, 18, 2023, 08:25 PM	Pr			151.101.2.217	443	🔍
Jul, 18, 2023, 10:37 PM	Firewall	18.68.97.97	80	172.16.17.157	11042	🔍
Jul, 18, 2023, 03:41 PM	Proxy	104.105.45.211	80	172.16.17.157	24298	🔍

RAW LOG

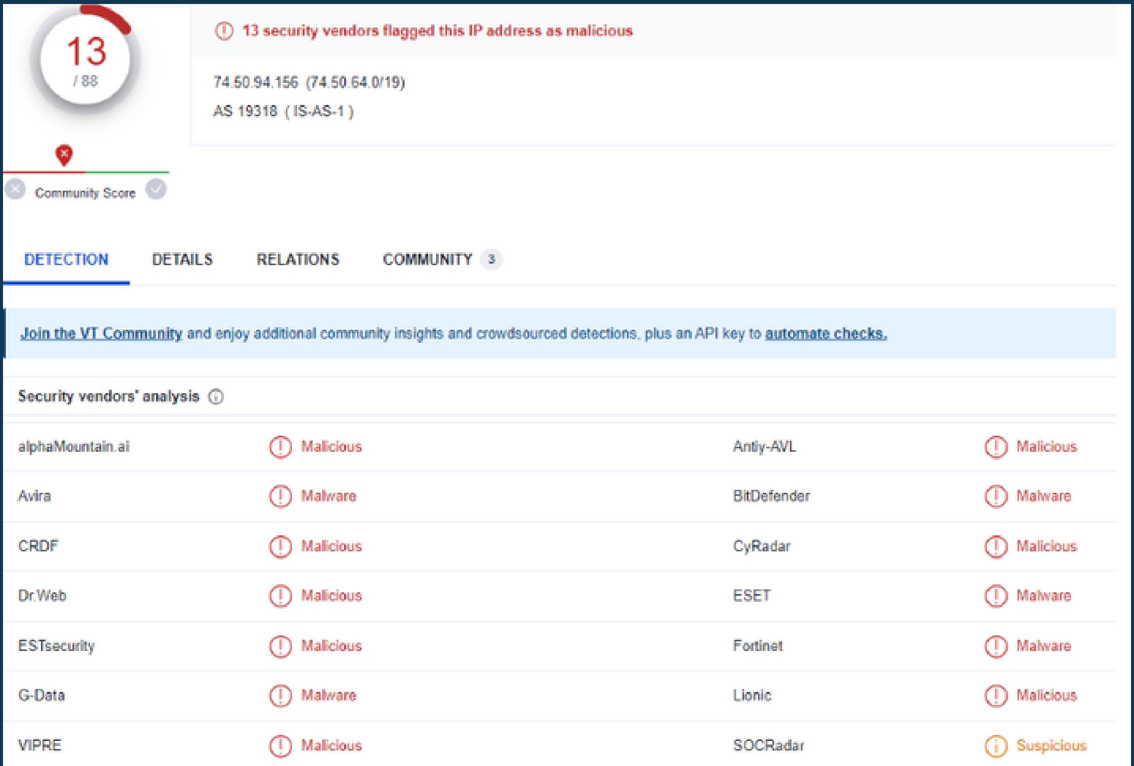
Request URL: http://74.50.94.156/MSHTML_C7/start.xml
Request Method: GET
Device Action: Permitted
Process: WINWORD.EXE
Process ID: 2028

LetsDefend

IP Reputation

We have detected that the malicious file that was run on the system came via an e-mail within our initial examinations. When a conduct a search for "Anthony" on the Log Management tool, we see the mail traffic in the exchange logs that originates from no-war[@]freeukraine.io email address with the source IP of 23.94.78.60.

We should also conduct the IP reputation check for “23.94.78.60” that we detected on the exchange logs as well as the “74.50.94.156” and “192.229.211.108” IP addresses that are queried over port 80.



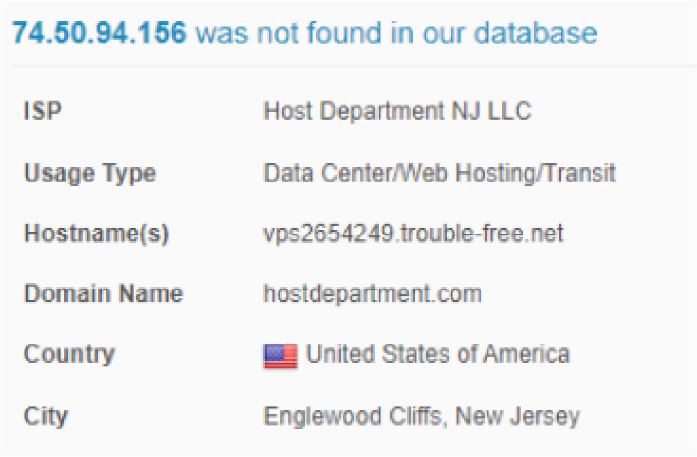
ⓘ 13 security vendors flagged this IP address as malicious

74.50.94.156 (74.50.64.0/19)
AS 19318 (IS-AS-1)

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

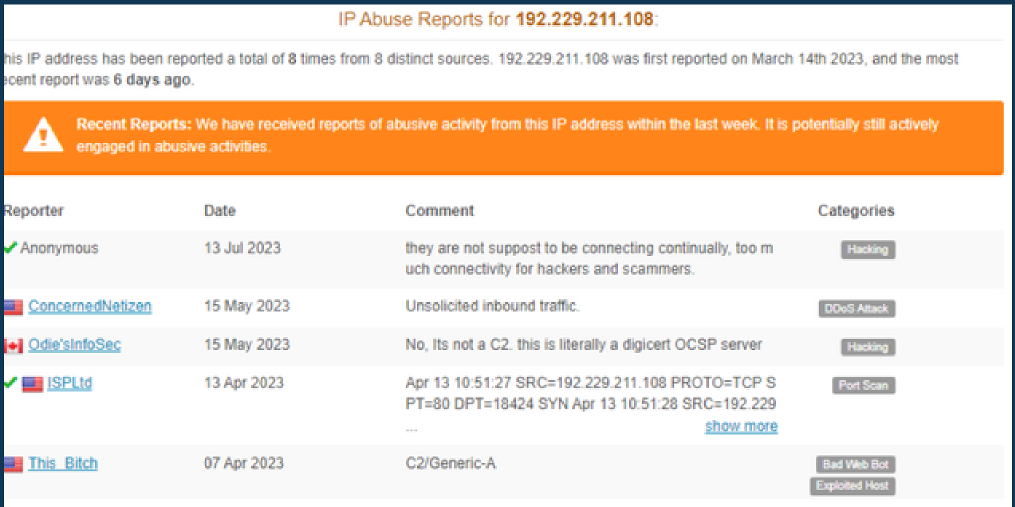
alphaMountain.ai	ⓘ Malicious	Antiy-AVL	ⓘ Malicious
Avira	ⓘ Malware	BitDefender	ⓘ Malware
CRDF	ⓘ Malicious	CyRadar	ⓘ Malicious
Dr.Web	ⓘ Malicious	ESET	ⓘ Malware
ESTsecurity	ⓘ Malicious	Fortinet	ⓘ Malware
G-Data	ⓘ Malware	Lionic	ⓘ Malicious
VIPRE	ⓘ Malicious	SOCRadar	ⓘ Suspicious



74.50.94.156 was not found in our database

ISP	Host Department NJ LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	vps2654249.trouble-free.net
Domain Name	hostdepartment.com
Country	United States of America
City	Englewood Cliffs, New Jersey

https://www.abuseipdb.com/check/74.50.94.156



IP Abuse Reports for **192.229.211.108**:

his IP address has been reported a total of **8** times from **8** distinct sources. 192.229.211.108 was first reported on March 14th 2023, and the most ecent report was **6 days ago**.

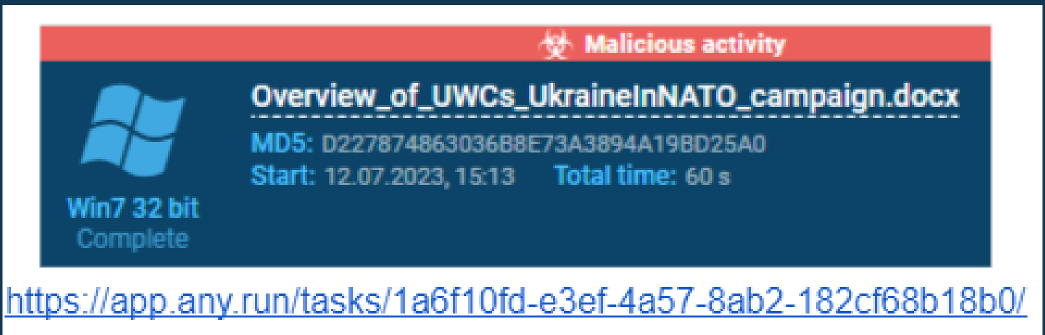
Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	Date	Comment	Categories
✓ Anonymous	13 Jul 2023	they are not suppost to be connecting continually, too m uch connectivity for hackers and scammers.	Hacking
ConcernedNetizen	15 May 2023	Unsolicited inbound traffic.	DDoS Attack
Odie'sInfoSec	15 May 2023	No, Its not a C2. this is literally a digicert OCSP server	Hacking
✓ ISPLtd	13 Apr 2023	Apr 13 10:51:27 SRC=192.229.211.108 PROTO=TCP S PT=80 DPT=18424 SYN Apr 13 10:51:28 SRC=192.229 ... show more	Port Scan
This_Bitch	07 Apr 2023	C2/Generic-A	Bad Web Bot Exploited Host

https://www.abuseipdb.com/check/192.229.211.108

Finally, the risk score of “23.94.78.60” IP address came out clean at the end of our reputation control. Following the IP reputation check, we should also conduct a hash check of the Overview_of_UWCs_UkraineInNATO_campaign.doc file shared in the alarm details.

Hash :
A61B2EAFCF39715031357DF6B01E85E0D1EA2E8EE1DFEC241B114E18F7A1163F



Overview_of_UWCs_UkraineInNATO_campaign.docx

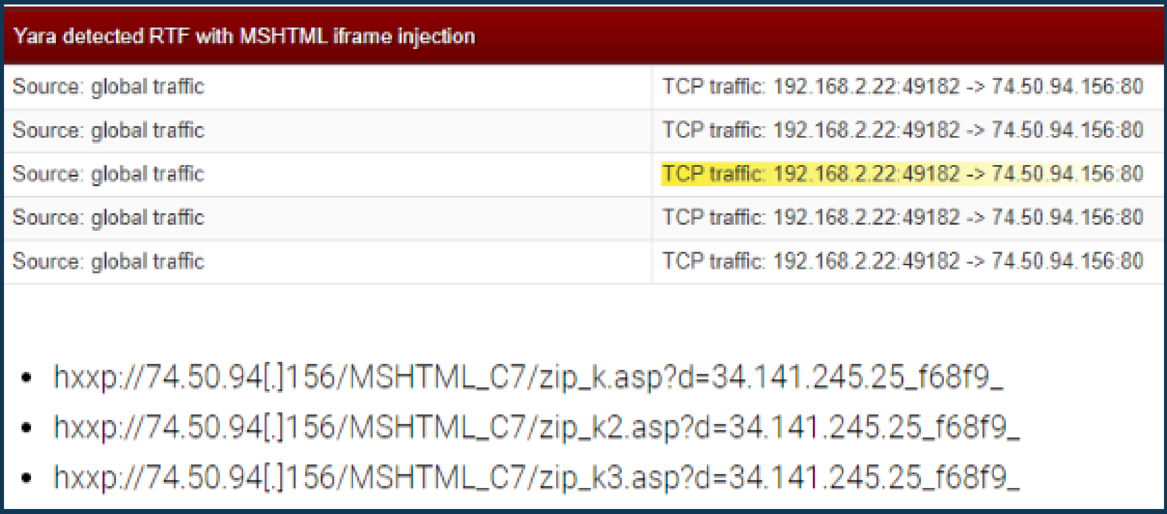
MD5: D227874863036B8E73A3894A19BD25A0

Start: 12.07.2023, 15:13 Total time: 60 s

https://app.any.run/tasks/1a6f10fd-e3ef-4a57-8ab2-182cf68b18b0/

The hash control we performed on multiple sources show that all the sources reported this hash as malicious. VirusTotal also associates it with the "CVE-2023-36884" vulnerability in some sources.

When we search for the details of this vulnerability, we see that the “74.50.94.156” IP address is shared in the IOC lists in all sources.



Yara detected RTF with MSHTML iframe injection

Source: global traffic	TCP traffic: 192.168.2.22:49182 -> 74.50.94.156:80
Source: global traffic	TCP traffic: 192.168.2.22:49182 -> 74.50.94.156:80
Source: global traffic	TCP traffic: 192.168.2.22:49182 -> 74.50.94.156:80
Source: global traffic	TCP traffic: 192.168.2.22:49182 -> 74.50.94.156:80
Source: global traffic	TCP traffic: 192.168.2.22:49182 -> 74.50.94.156:80

- 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_

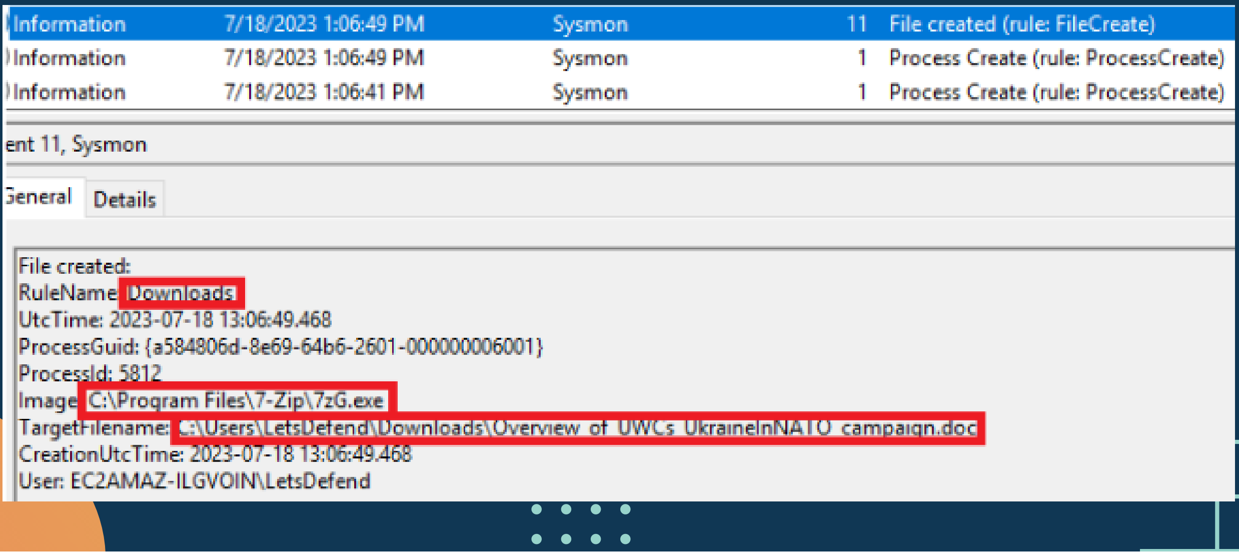
The request that was made to "hxxp://74.50.94.156/MSHTML_C7/start.xml" is an attempt to download a file named "start.xml" to the system.

References: https://www.joesecurity.org/reports/report-d227874863036b8e73a3894a19bd25a0.html
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit

In the investigations made so far, we have found out that a file associated with CVE-2023-36884 was downloaded to the system and requests towards the “74.50.94.156” IP address which is among the shared IOCs for the related vulnerability. You can determine whether the relevant file was run or not by reviewing the logs in the Event Viewer on the system. You can connect to the system through the Endpoint Security tool by pressing the "connect" button.

You should follow the path the below path to open the Sysmon after connecting to the system:
Event Viewer->Application and Services Logs->Microsoft->Windows->Sysmon->Operational

When the related file is searched in the File create logs, we see that the related file was extracted using 7zip at 01:06:49 PM.

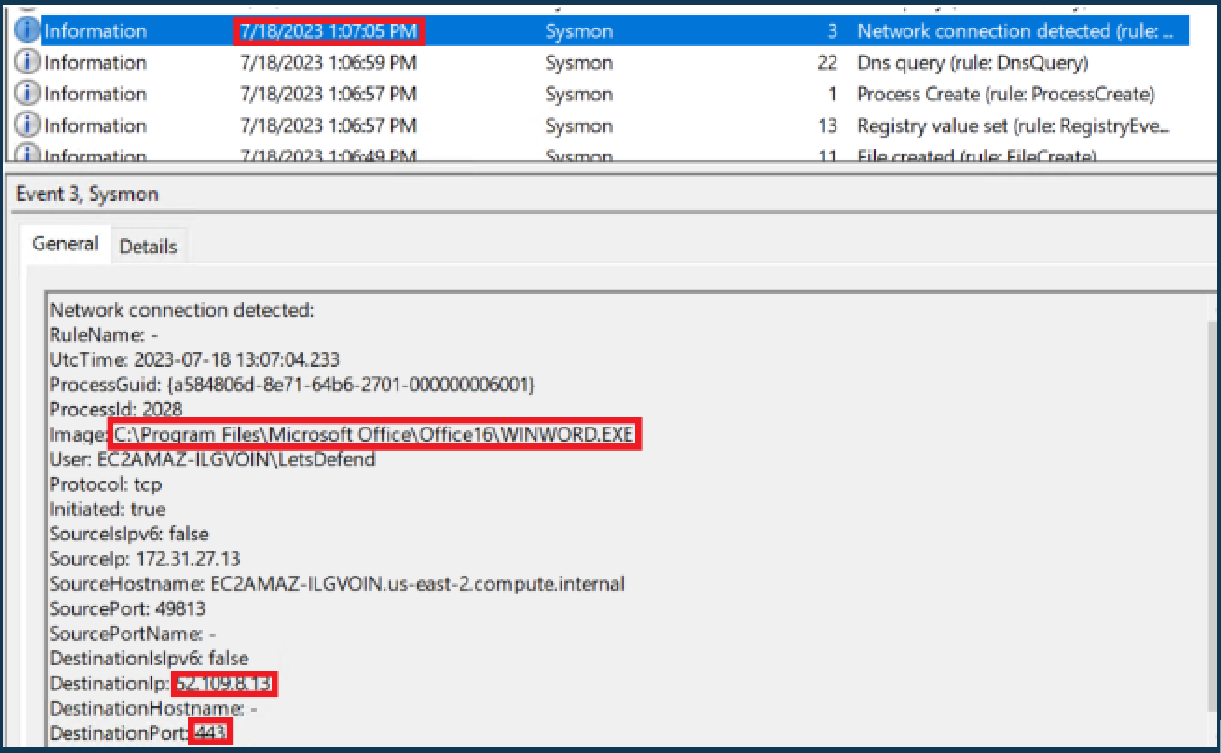


```
Information    7/18/2023 1:06:49 PM    Sysmon    11    File created (rule: FileCreate)
Information    7/18/2023 1:06:49 PM    Sysmon     1    Process Create (rule: ProcessCreate)
Information    7/18/2023 1:06:41 PM    Sysmon     1    Process Create (rule: ProcessCreate)
```

```
File created:
RuleName: Downloads
UtcTime: 2023-07-18 13:06:49.468
ProcessGuid: {a584806d-8e69-64b6-2601-000000006001}
ProcessId: 5812
Image: C:\Program Files\7-Zip\7zG.exe
TargetFilename: C:\Users\LetsDefend\Downloads\Overview_of_UWCs_UkraineInNATO_campaign.doc
CreationUtcTime: 2023-07-18 13:06:49.468
User: EC2AMAZ-ILGVOIN\LetsDefend
```

Then, you can search for “Overview_of_UWCs_UkraineInNATO_campaign.docx” file in the Process Create logs. And, as a result, we see that the file was opened via winword.exe in the relevant log records.

We see that there are a large number of Event ID: 3 (network connections) in a short time after the related process runs. Winword.exe is the process in these logs. Although most of these connections (port 443) are considered to be harmless, traffic over port 80 may worth checking.



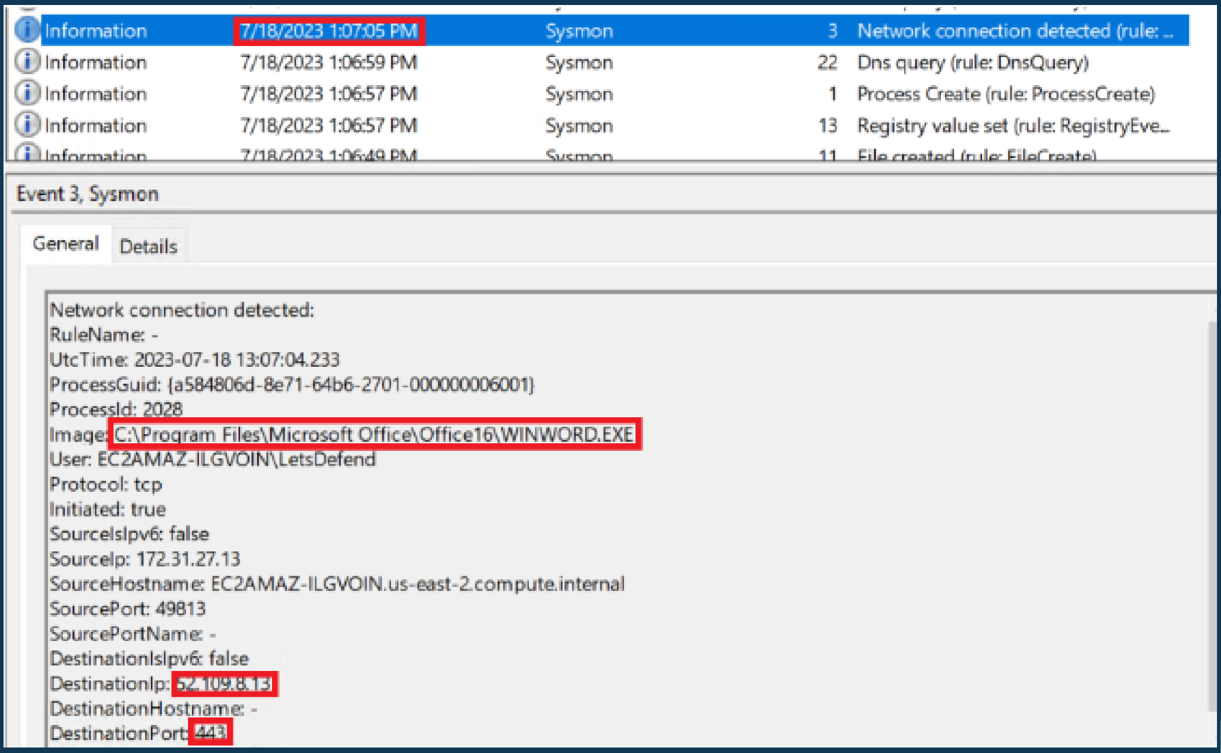
```
Information   7/18/2023 1:07:05 PM   Sysmon    3  Network connection detected (rule: ...
Information   7/18/2023 1:06:59 PM   Sysmon   22  Dns query (rule: DnsQuery)
Information   7/18/2023 1:06:57 PM   Sysmon    1  Process Create (rule: ProcessCreate)
Information   7/18/2023 1:06:57 PM   Sysmon   13  Registry value set (rule: RegistryEve...
Information   7/18/2023 1:06:49 PM   Sysmon   11  File created (rule: FileCreate)
```

Event 3, Sysmon

```
Network connection detected:
RuleName: -
UtcTime: 2023-07-18 13:07:04.233
ProcessGuid: {a584806d-8e71-64b6-2701-000000006001}
ProcessId: 2028
Image: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
User: EC2AMAZ-ILGVOIN\LetsDefend
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.27.13
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 49813
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 52.109.8.13
DestinationHostname: -
DestinationPort: 443
```

Then, you can search for "Overview_of_UWCs_UkraineInNATO_campaign.docx" file in the Process Create logs. And, as a result, we see that the file was opened via winword.exe in the relevant log records.

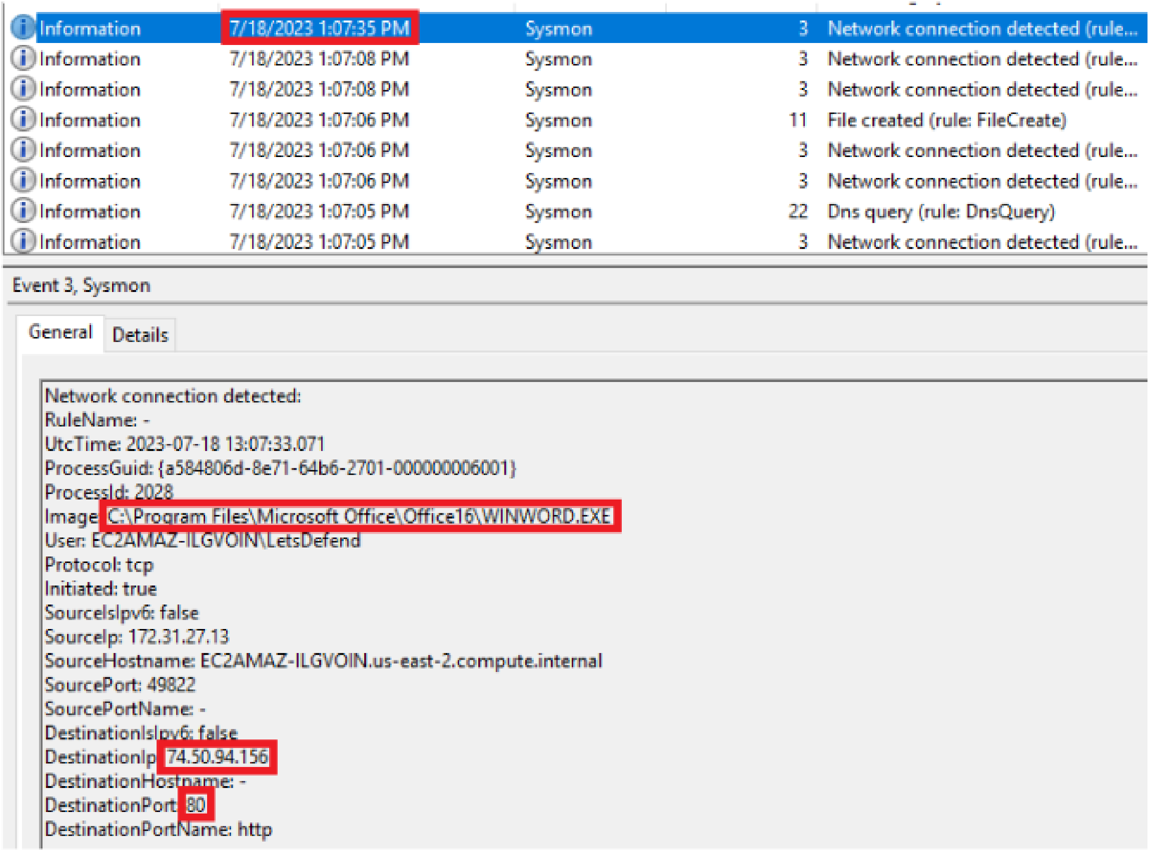
We see that there are a large number of Event ID: 3 (network connections) in a short time after the related process runs. Winword.exe is the process in these logs. Although most of these connections (port 443) are considered to be harmless, traffic over port 80 may worth checking.



```
Information   7/18/2023 1:07:05 PM   Sysmon    3   Network connection detected (rule: ...
Information   7/18/2023 1:06:59 PM   Sysmon   22   Dns query (rule: DnsQuery)
Information   7/18/2023 1:06:57 PM   Sysmon    1   Process Create (rule: ProcessCreate)
Information   7/18/2023 1:06:57 PM   Sysmon   13   Registry value set (rule: RegistryEve...
Information   7/18/2023 1:06:49 PM   Sysmon   11   File created (rule: FileCreate)
```

```
Network connection detected:
RuleName: -
UtcTime: 2023-07-18 13:07:04.233
ProcessGuid: {a584806d-8e71-64b6-2701-000000006001}
ProcessId: 2028
Image: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
User: EC2AMAZ-ILGVOIN\LetsDefend
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.27.13
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 49813
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 52.109.8.13
DestinationHostname: -
DestinationPort: 443
```

IP Reputation



Information	7/18/2023 1:07:35 PM	Sysmon	3	Network connection detected (rule...
Information	7/18/2023 1:07:08 PM	Sysmon	3	Network connection detected (rule...
Information	7/18/2023 1:07:08 PM	Sysmon	3	Network connection detected (rule...
Information	7/18/2023 1:07:06 PM	Sysmon	11	File created (rule: FileCreate)
Information	7/18/2023 1:07:06 PM	Sysmon	3	Network connection detected (rule...
Information	7/18/2023 1:07:06 PM	Sysmon	3	Network connection detected (rule...
Information	7/18/2023 1:07:05 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	7/18/2023 1:07:05 PM	Sysmon	3	Network connection detected (rule...

Event 3, Sysmon

```
Network connection detected:
RuleName: -
UtcTime: 2023-07-18 13:07:33.071
ProcessGuid: {a584806d-8e71-64b6-2701-000000006001}
ProcessId: 2028
Image: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
User: EC2AMAZ-ILGVOIN\LetsDefend
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.27.13
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 49822
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 74.50.94.156
DestinationHostname: -
DestinationPort: 80
DestinationPortName: http
```

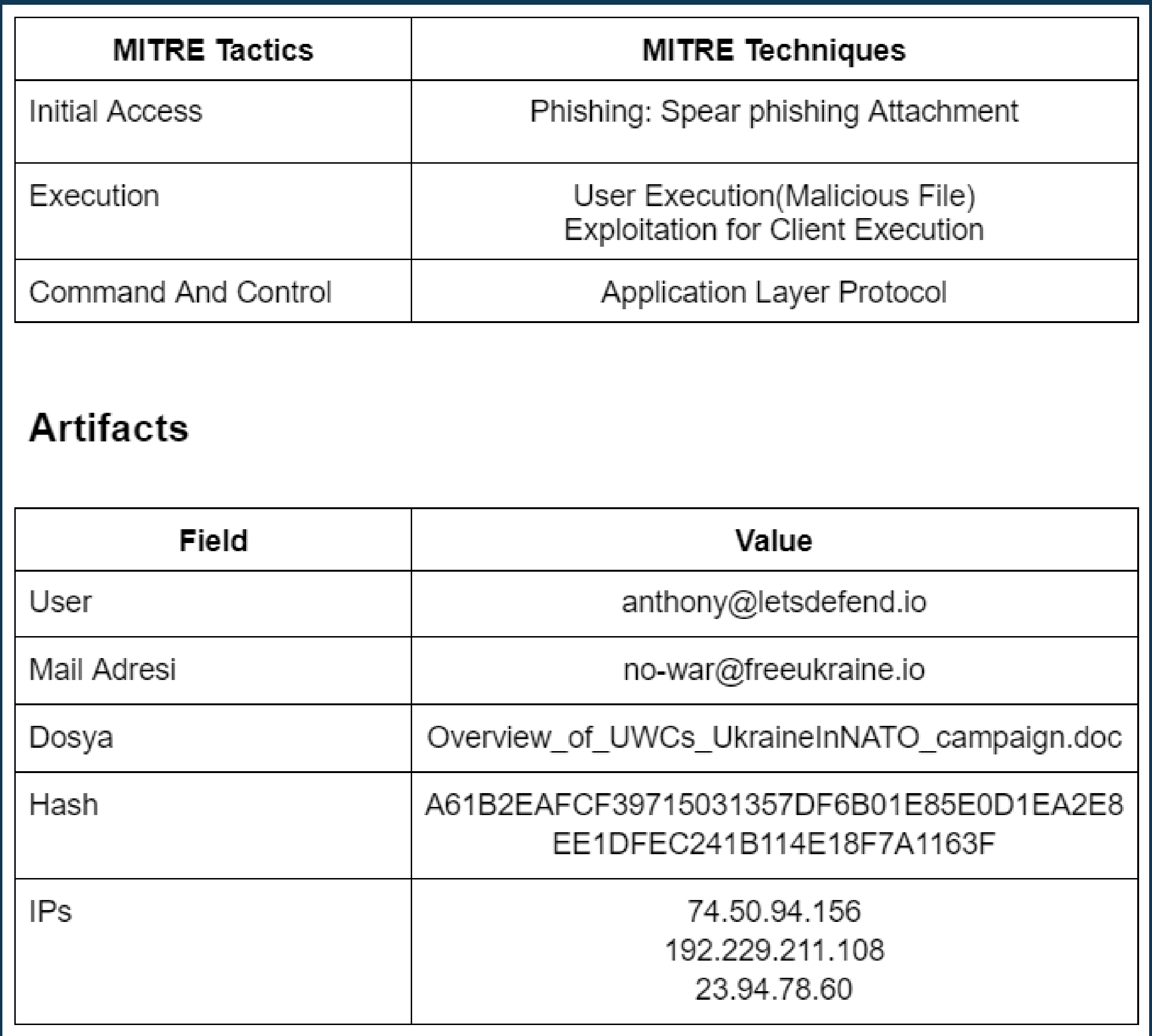
Now, we need to check the Defender AV to see whether it detected these activities or not. For this we can open Virus & Threat Protection > Threat History and see the alarm that was quarantined.

Containment

So far, we have found out that Anthony downloaded a malicious file that was sent through an email. We have confirmed through the logs that he opened that malicious file after downloading it to the system. We have also detected network traffic towards malicious IP address “74.50.94.156”. We see that the malicious file was reported with reported with CVE-2023-36884 when we review its reputation record which is why the system should be isolated from the network.

Lessons Learned

- Vulnerable products should not be used in servers/clients,
- We should increase the users' awareness of information security with routine trainings and phishing tests,
- AV/EDR products on the systems must be active at and their signatures must be up to date at all times.



MITRE Tactics	MITRE Techniques
Initial Access	Phishing: Spear phishing Attachment
Execution	User Execution(Malicious File) Exploitation for Client Execution
Command And Control	Application Layer Protocol

Artifacts

Field	Value
User	anthony@letsdefend.io
Mail Adresi	no-war@freeukraine.io
Dosya	Overview_of_UWCs_UkraineInNATO_campaign.doc
Hash	A61B2EAFCF39715031357DF6B01E85E0D1EA2E8EE1DFEC241B114E18F7A1163F
IPs	74.50.94.156 192.229.211.108 23.94.78.60