Nathan Montierth

valicyber | Threat Intel Lead

- Vali Cyber recently recognized as a Key Startup in Security Software by Gartner
- Graduated with a degree in Computer Science from the US Air Force Academy
- Prior position in cyber operations with the US Air Force

Emerging Tech: Techscape for Startups in Security Software | *Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

HYPERVISOR RANSOMWARE EXPLOSION

3-Fold YoY Increase in ESXi attacks

- **State actor attacks on the rise**
  - **UNC3886 / "Fire Ant"** (China-linked espionage) has been focused on attacking governments since early 2025
  - **ALPHV/BlackCat ransomware gang** (with suspected ties to Russian intelligence) breached the Florida Supreme Court in 2025
  - A **Chinese nation-state adversary** breached MITRE in 2024
- **Ransomware groups are also looking at critical infrastructure**
  - **Scattered Spider** has been targeting the insurance and airline industries, costing more than $1B in damages over the last 4 years
  - **LockBit** has hit various infrastructure targets including U.S. municipal governments, public education systems, healthcare, and emergency services — about 1,700 attacks in the U.S. since 2020

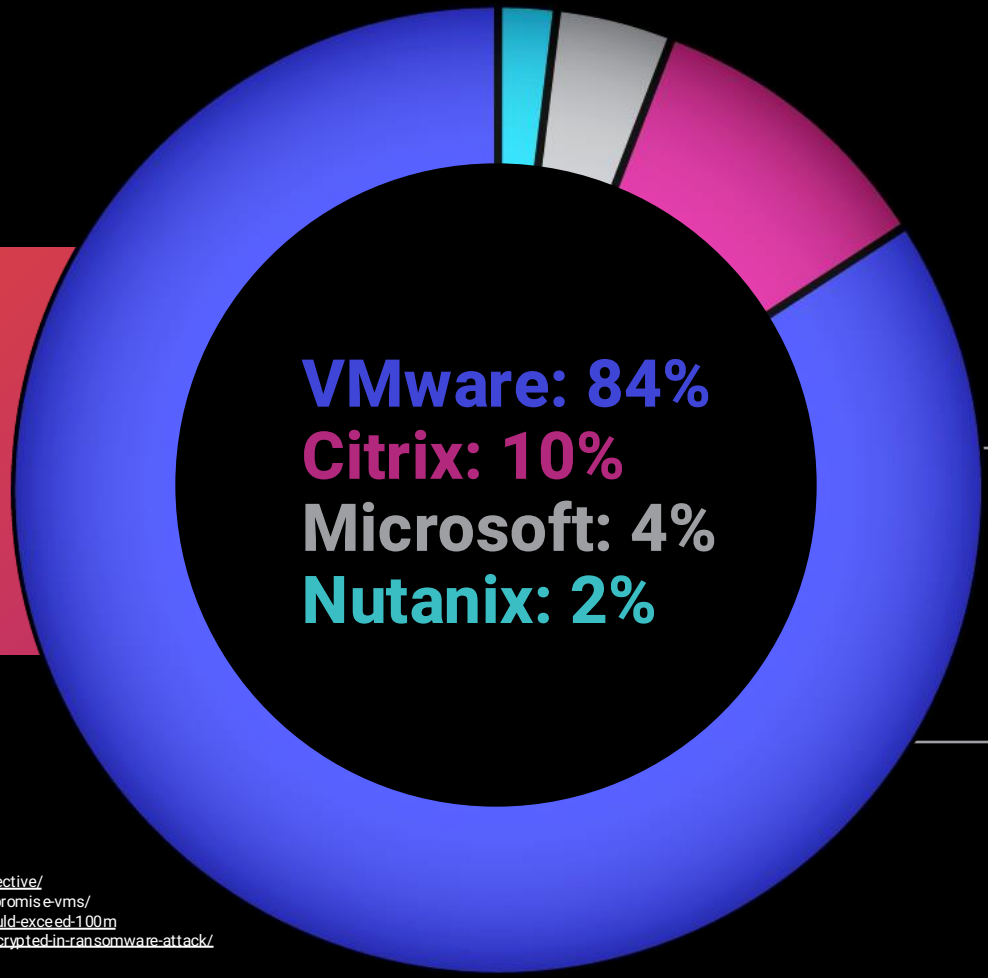
DAF leverages VMware products, making it a possible target for state actor attacks.

https://www.vmware.com/solutions/industry/federal-government-it-solutions

https://www.csoonline.com/article/4029545/chinese-fire-ant-spies-start-to-bite-unpatched-vmware-instances.html
https://www.txone.com/blog/unmasking-unc3886/
https://heimdalsecurity.com/blog/florida-circuit-court-ransomware-attack/
https://thehackernews.com/2024/04/mitre-corporation-breached-by-nation.html
https://www.cybersecuritydive.com/news/what-we-know-about-the-cybercrime-group-scattered-spider/756312/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
https://www.backblaze.com/blog/1700-attacks-in-three-years-how-lockbit-ransomware-wreaks-havoc/
https://www.bleepingcomputer.com/news/security/unc3886-hackers-use-linux-rootkits-to-hide-on-vmware-esxi-vms/

THE STATE OF HYPERVISORS

As the most used virtualization platform, VMware ESXi is the focus of hypervisor attacks.



How breaches typically start on a hypervisor:

Credential Compromise
Stolen, AD Compromise-Lateral Movement, No MFA

Misconfiguration
Secure Boot Disabled, SSH Enabled, Improper Firewall Rules, etc.

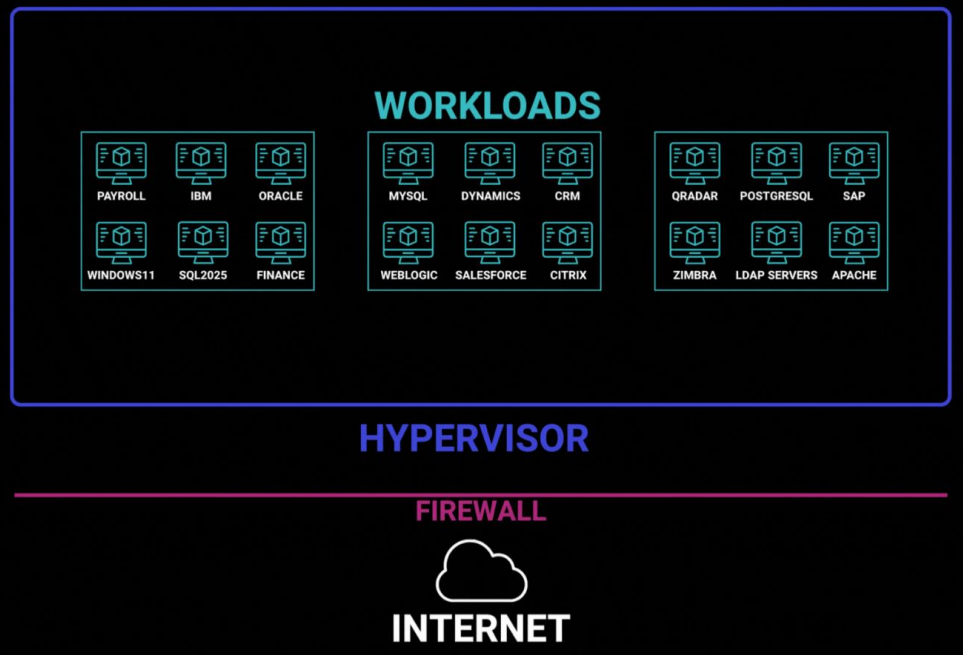
Vulnerability/Exploit
Currently 117 known

https://www.cybersecuritydive.com/news/VMware-ransomware-increase/642576/
https://www.controlup.com/resources/blog/hypervisor-market-share-controlup-perspective/
https://vulnera.com/newswire/chinese-hackers-exploit-VMware-esxi-zero-day-to-compromise-vms/
https://www.securitymagazine.com/articles/99990-mgm-resorts-cyberattack-cost-could-exceed-100m
https://bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/

FIREWALLS AREN'T ENOUGH

No visibility inside trusted connections.

- Firewall focus on north/south traffic misses lateral (east/west) movement; SSH misuse and credential abuse between hosts go undetected
- Firewalls can be attacked too—breaches can give adversaries wide access
- Relying on a single control point is risky; layered defense is essential
- Advanced threats can mimic legit services like DNS, SMTP, or SFTP



MITRE ATT&CK v17

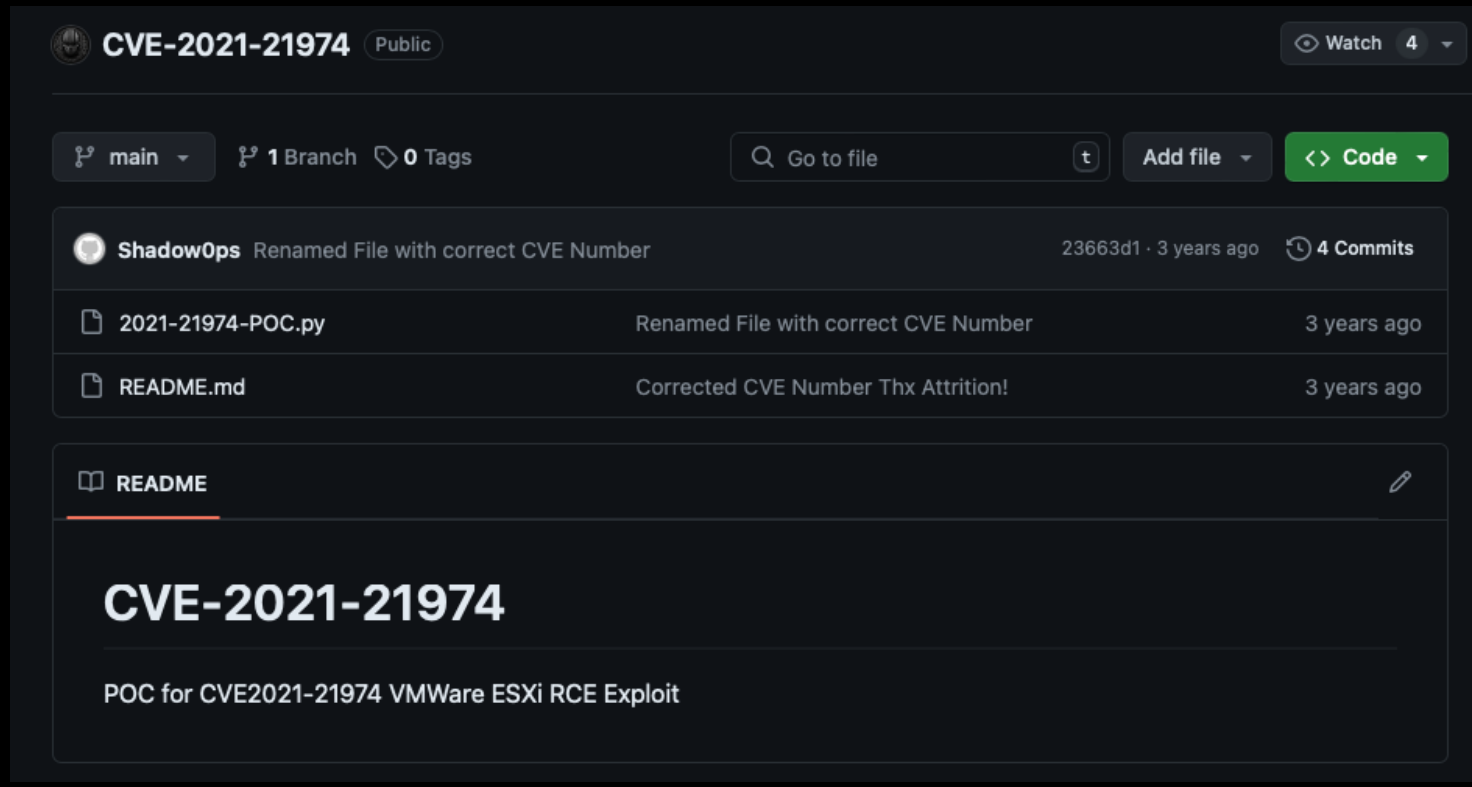
Released 4/22/2025

- For the first time ever, MITRE has included ESXi in their ATT&CK framework, validating the risk many ESXi users have been facing as attacks at the hypervisor level are on the rise.
- The new framework includes 12 categories that focus on the different steps that may be taken during an attack chain
- There are 68 Tactics, Techniques, and Procedures (TTPs) including:
  - 34 techniques adapted to ESXi
  - 4 unique techniques created specifically for ESXi:
    - T1675: ESXi Administration Control
    - T1059.12: Command and Scripting Interpreter: Hypervisor CLI
    - T1505.006: Server Software Component: vSphere Installation Bundles
    - T1673: Virtual Machine Discovery
- This is a landmark move that will have rippling impacts on ESXi security and compliance

EXPLOIT

ESXiArgs

- CVE-2021-21974
- Heap buffer overflow
- 2-step exploit
  - Information leak
  - Memory corruption
- Affects ESXi
  - 7.0 prior to ESXi70U1c-17325551
  - 6.7 prior to ESXi670-202102401-SG
  - 6.5 prior to ESXi650-202102101-SG
- Requires Port 427, TCP or UDP
- T1673: Virtual Machine Discovery
- Exploit POC available on GitHub



https://github.com/Shadow0ps/CVE-2021-21974/tree/main
https://www.keysight.com/blogs/en/tech/nwvs/2023/02/24/remote-code-execution-with-esxi-cve-2021-21974-vmware-esxi-heap-overflow

Navigator
Host
Manage
Monitor
Virtual Machines 3
Gandalf
Monitor
More VMs...
Storage 1
Networking 1

localhost.localdomain

Get vCenter Server | Create/Register VM | Shut down | Reboot | Refresh | Actions

localhost.localdomain

Version: 6.7.0 Update 3 (Build 14320388)
State: Normal (not connected to any vCenter Server)
Uptime: 0 days

CPU — FREE: 11.3 GHz — 3%
USED: 324 MHz — CAPACITY: 11.6 GHz

MEMORY — FREE: 10.72 GB — 11%
USED: 1.27 GB — CAPACITY: 12 GB

STORAGE — FREE: 29.44 GB — 9%
USED: 3.06 GB — CAPACITY: 32.5 GB

Hardware

Manufacturer	VMware, Inc.
Model	VMware20,1
CPU	4 CPUs x Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz
Memory	12 GB
Persistent Memory	0 B
Virtual flash	0 B used, 0 B capacity
Networking	
Hostname	localhost.localdomain
IP addresses	1. vmk0: 192.168.208.152 2. vmk0: fe80::20c:29ff:fe15:b40b
DNS servers	1. 192.168.208.2
Default gateway	192.168.208.2
IPv6 enabled	Yes
Host adapters	1
Networks	Name: VM Network, VMs: 3
Storage	

Configuration

Image profile	ESXi-6.7.0-20190802001-standard (VMware, Inc.)
vSphere HA state	
vMotion	Supported

System Information

Date/time on host	Tuesday, July 09, 2024, 01:56:05 UTC
Install date	Monday, July 08, 2024, 16:11:30 UTC
Asset tag	No Asset Tag
Serial number	VMware-56 4d c6 86 ca 24 4c 20-68 3f 98 49 a8 15 b4 0b
BIOS version	VMW201.00V.21805430.B64.2305221830
BIOS release date	Sunday, May 21, 2023, 18:00:00 -0600

Performance summary last hour

Recent tasks

Task	Target	Initiator	Queued	Started	Result	Completed
Stop Service	localhost.localdomain	root	07/08/2024 19:55:57	07/08/2024 19:55:57	Completed successfully	07/08/2024 19:55:57
Auto Start Power On	localhost.localdomain	root	07/08/2024 18:16:23	07/08/2024 18:16:23	Completed successfully	07/08/2024 18:16:23
Stop Service	localhost.localdomain	root	07/08/2024 19:56:01	07/08/2024 19:56:01	Completed successfully	07/08/2024 19:56:01

ESXiArgs

- Rapid7 found 18,581 vulnerable ESXi systems on the public internet in February of 2023
- Date of scan is almost 2 years after the release of the patch

Nearly 19,000 ESXi Servers Still Vulnerable to CVE-2021-21974

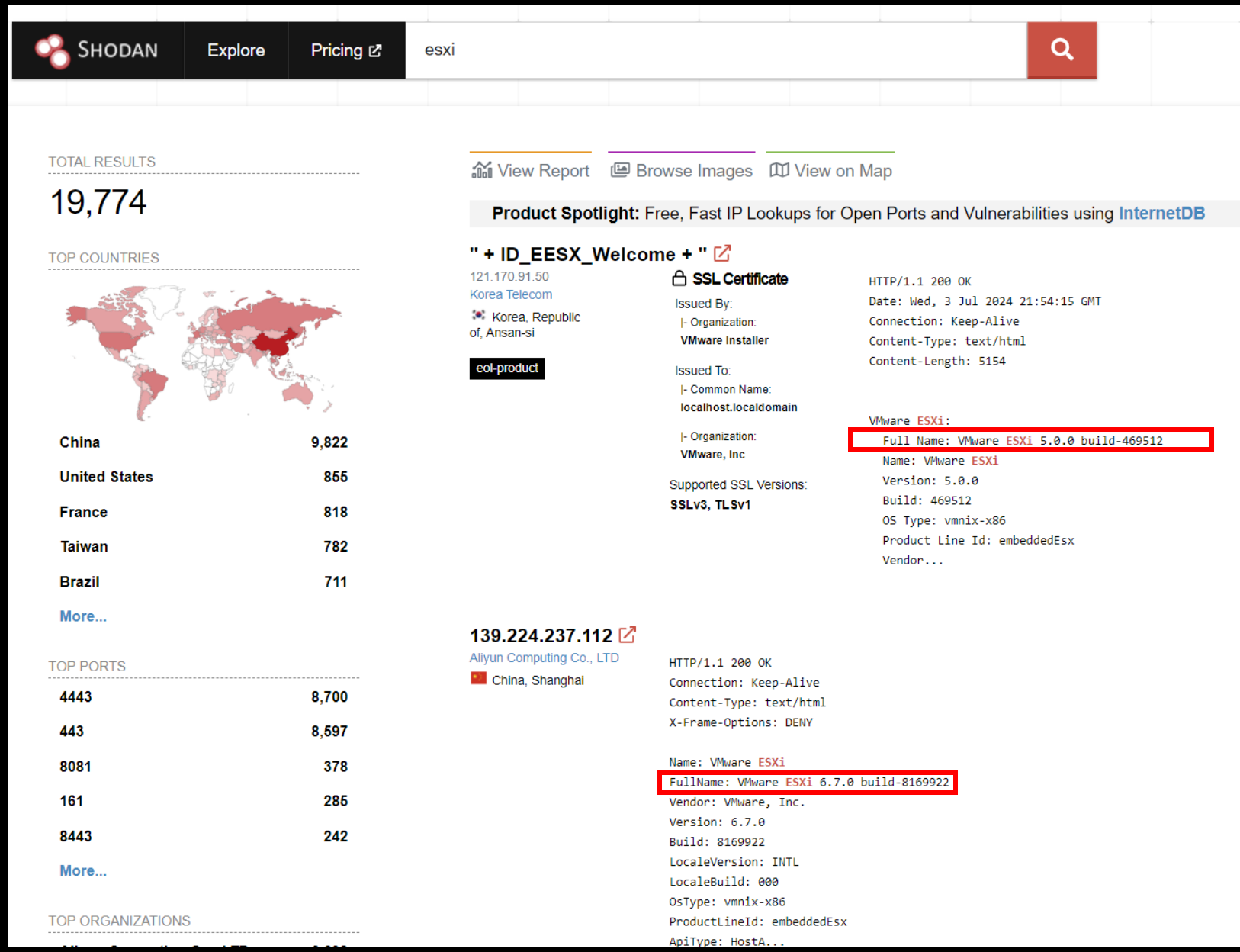
Feb 09, 2023 | 2 min read | Erick Galinkin

Last updated at Fri, 10 Feb 2023 16:55:49 GMT

Last week, multiple organizations issued warnings that a ransomware campaign dubbed "ESXiArgs" was targeting VMware ESXi servers, allegedly by leveraging CVE-2021-21974—a nearly two-year-old heap overflow vulnerability. Two years. And yet, Rapid7 research has found that a significant number of ESXi servers likely remain vulnerable. We believe, with high confidence, that there are at least 18,581 vulnerable internet-facing ESXi servers at the time of this writing.

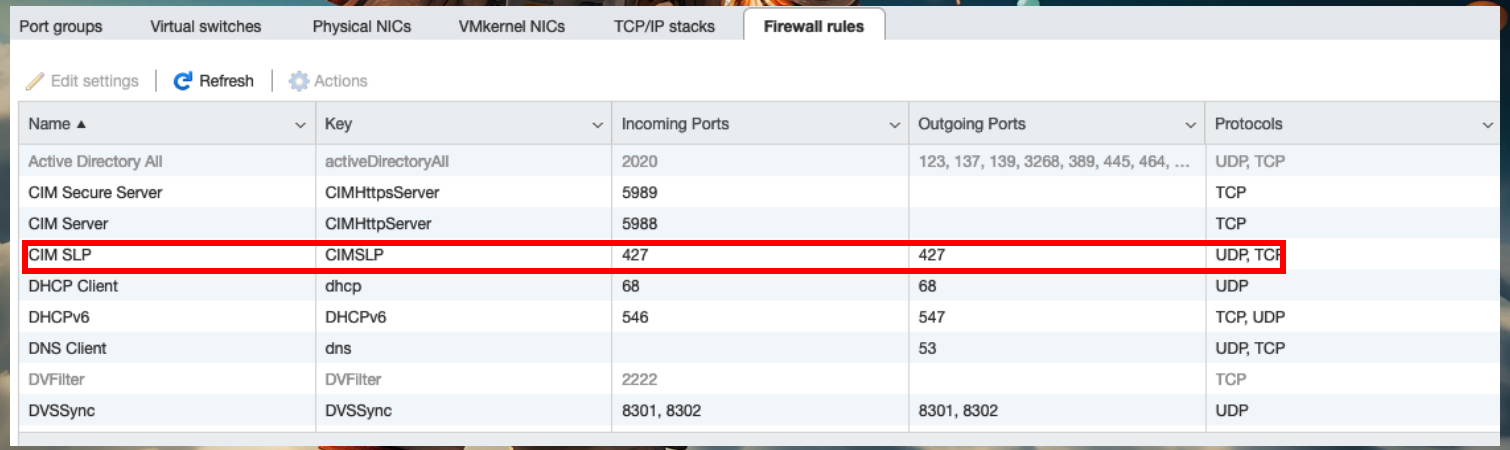
ESXiArgs

- Simple Shodan search
- Almost 20k publicly facing ESXi systems,
- Many have vulnerable ESXi versions.



Exploit: Defending yourself

- Patch
- Network Segmentation
- Disable CIM-SLP firewall rule (CIM-SLP has other CVEs)



Name ▲	Key	Incoming Ports	Outgoing Ports	Protocols
Active Directory All	activeDirectoryAll	2020	123, 137, 139, 3268, 389, 445, 464, ...	UDP, TCP
CIM Secure Server	CIMHttpsServer	5989		TCP
CIM Server	CIMHttpServer	5988		TCP
CIM SLP	CIMSLP	427	427	UDP, TCP
DHCP Client	dhcp	68	68	UDP
DHCPv6	DHCPv6	546	547	TCP, UDP
DNS Client	dns		53	UDP, TCP
DVFilter	DVFilter	2222		TCP
DVSSync	DVSSync	8301, 8302	8301, 8302	UDP

LATERAL COMPROMISE

MGM Resorts

- Breach occurred in October 2023
- $100M Breach
- 100 ESXi hypervisors encrypted
- Multiple lawsuits
- T1059.12: Command and Scripting Interpreter: Hypervisor CLI

The chaotic and cinematic MGM casino hack, explained

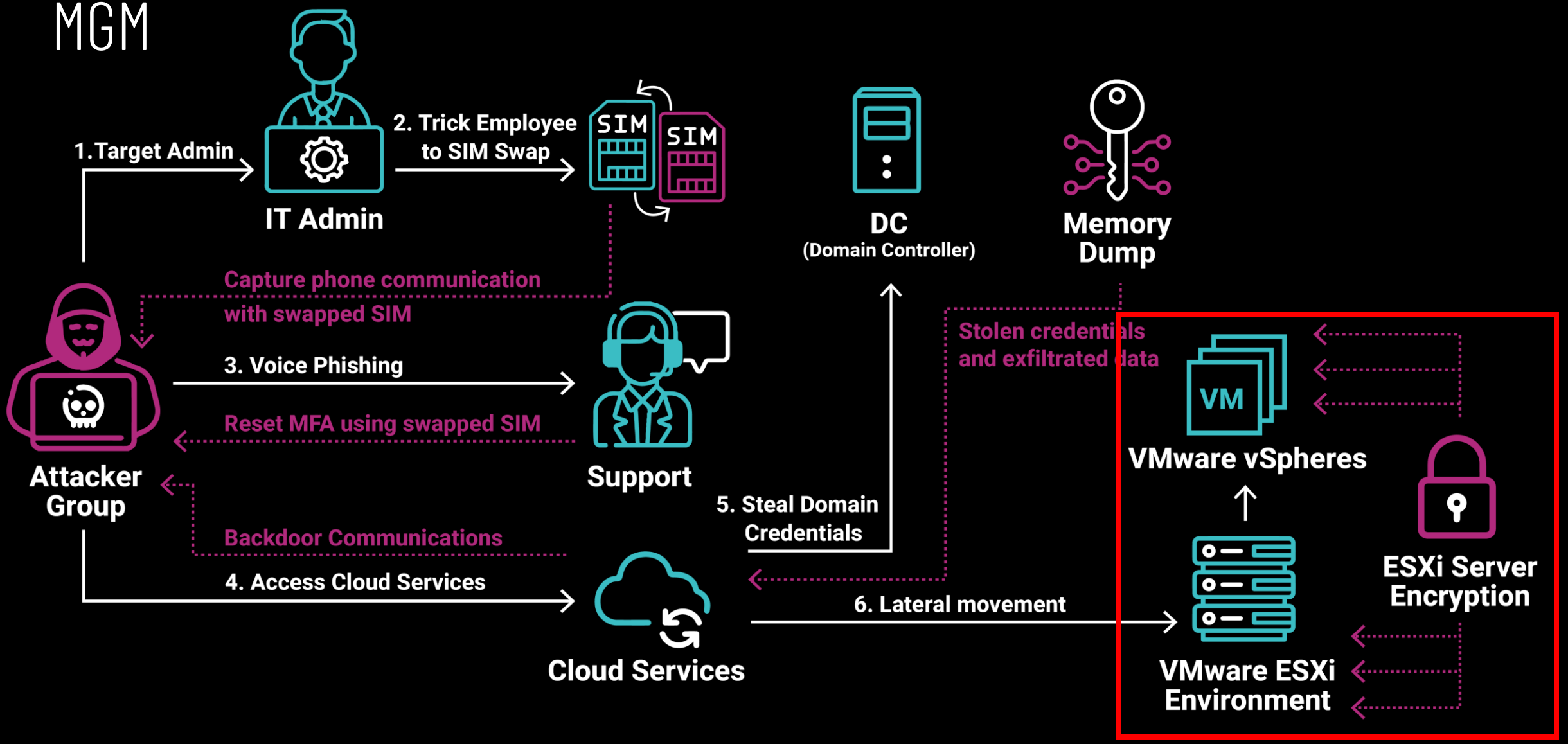
A “limited number” of customers’ Social Security numbers were taken.

by **Sara Morrison**
Oct 6, 2023 at 9:25 AM MDT

People riding an escalator outside the MGM Grand in Las Vegas. Unlike some parts of MGM's business that were affected by the hack, the escalators remained operational. AP/John Locher

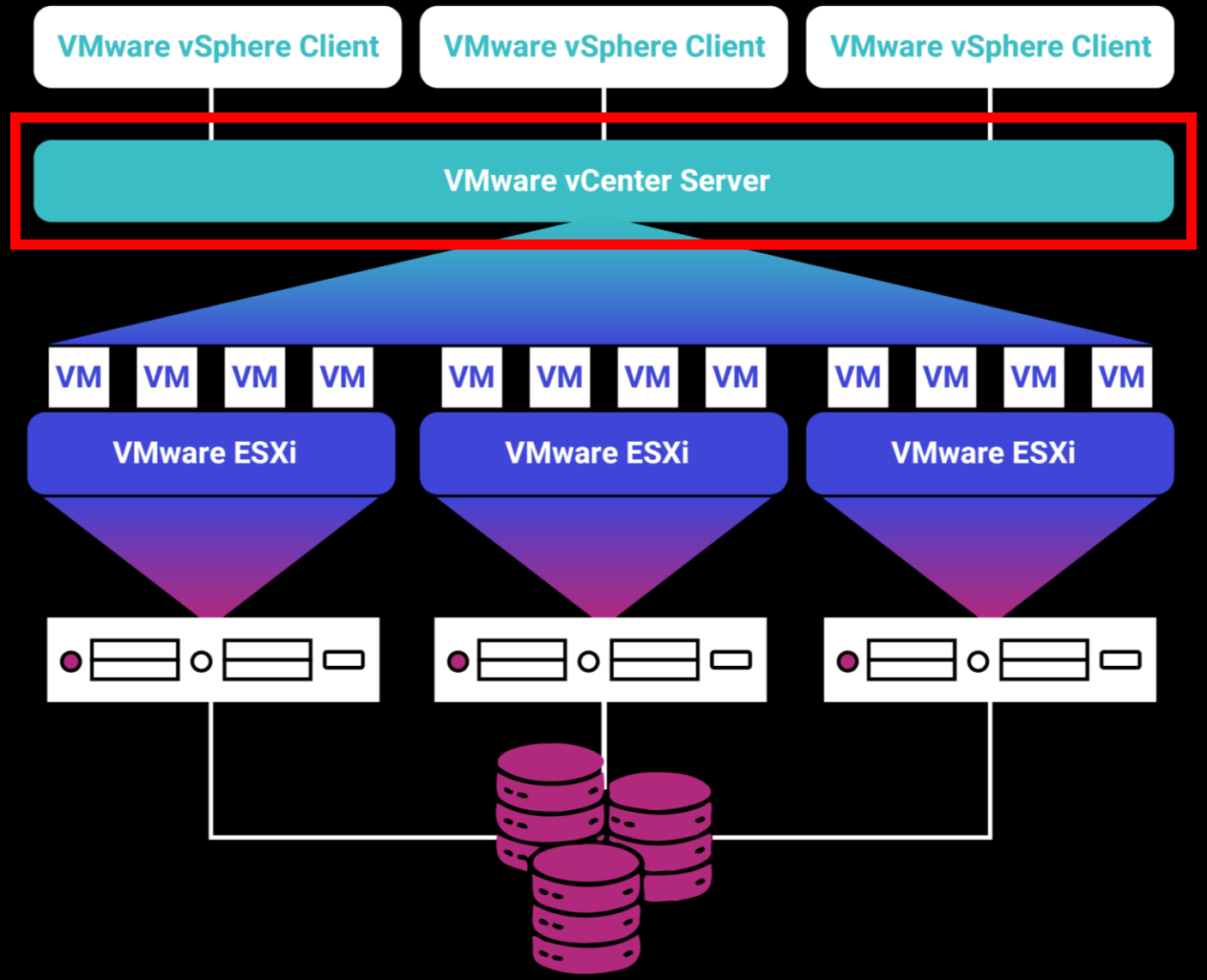
https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

MGM

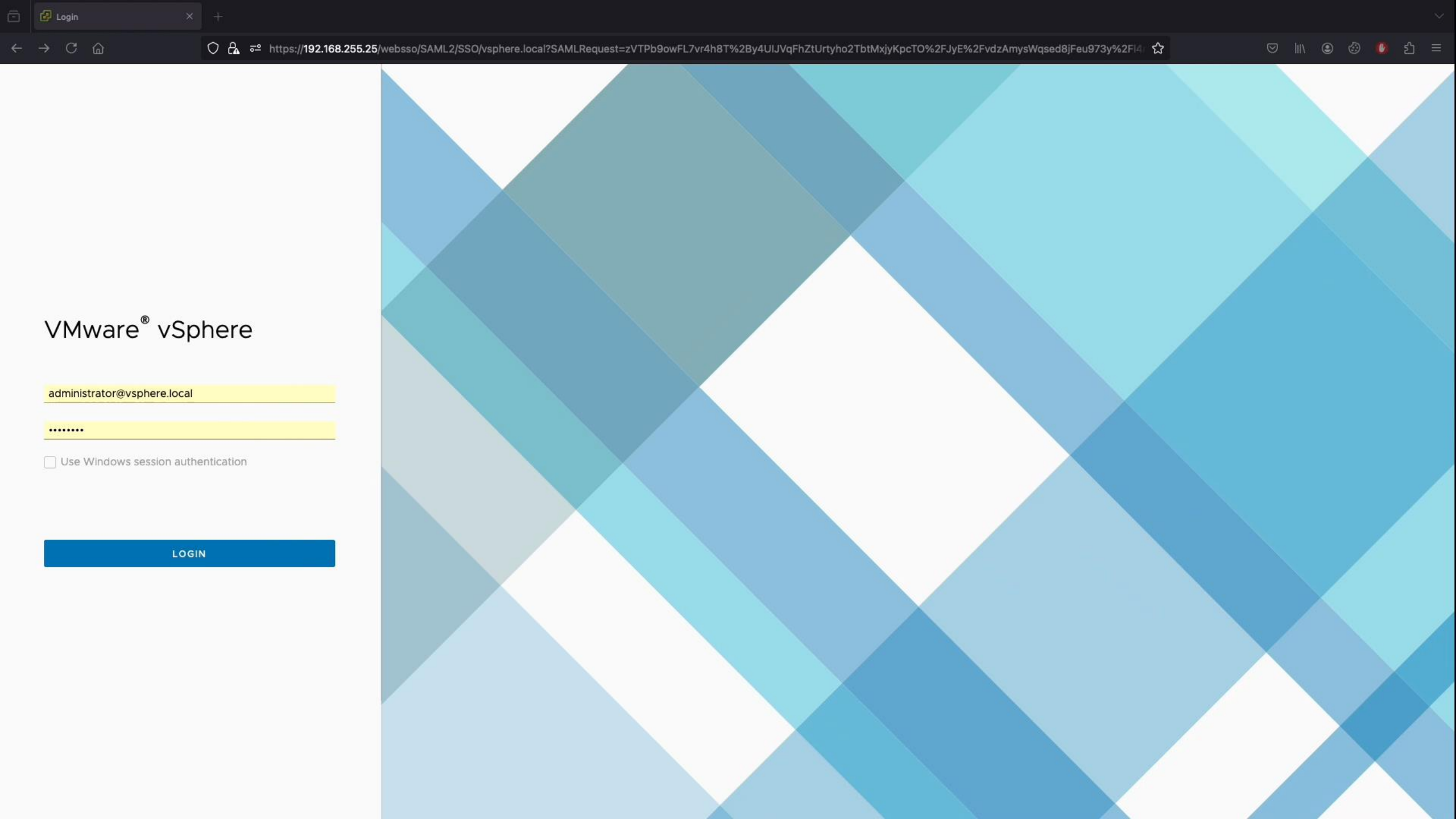


https://blog.morphisec.com/mgm-resorts-alphv-spider-ransomware-attack

MGM



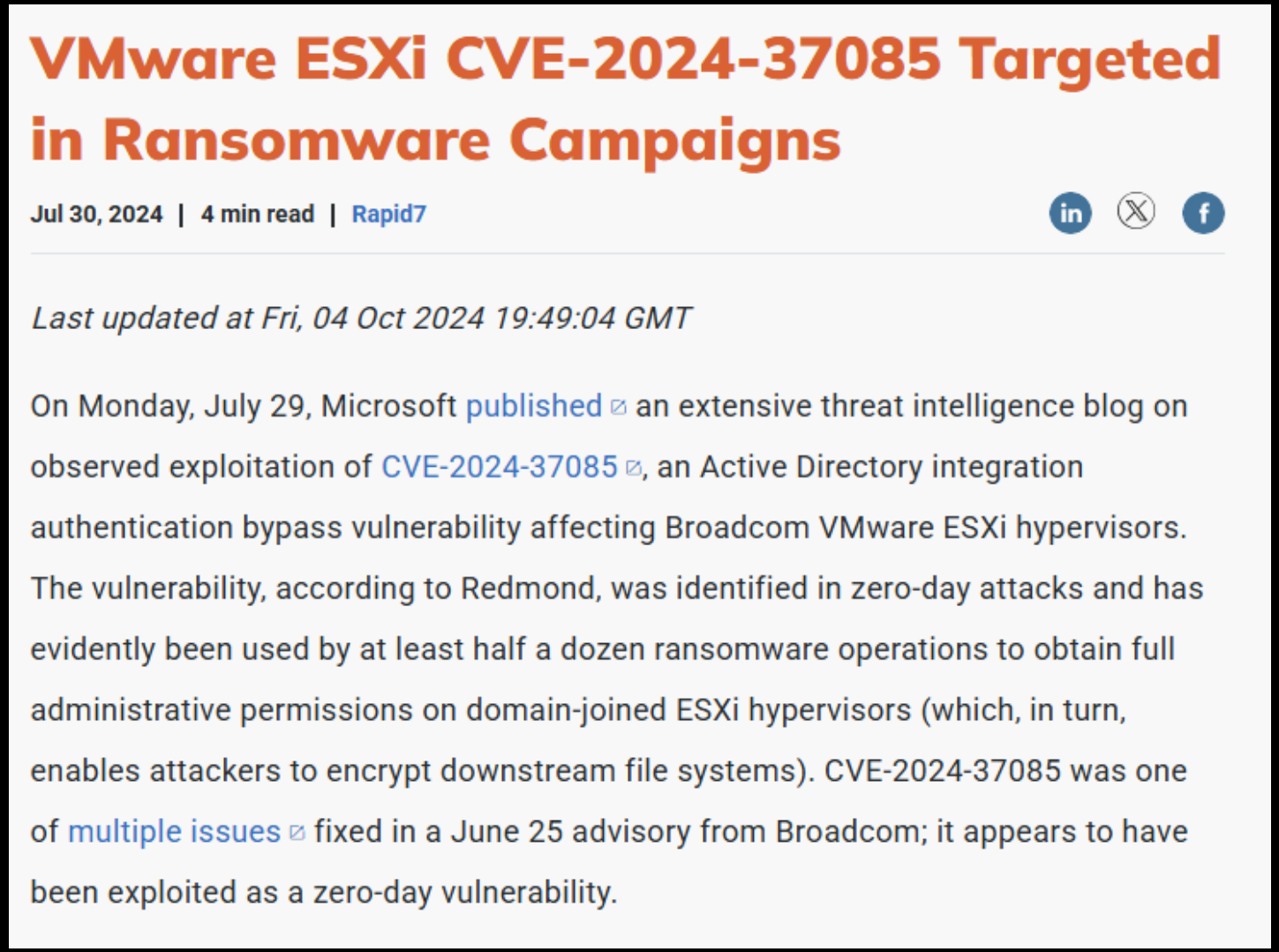
https://www.parkplacetechnologies.com/wp-content/uploads/2022/08/what-is-vmware-vcenter-vs-vsphere-vs-esxi.png


Login
https://192.168.255.25/websso/SAML2/SSO/vsphere.local?SAMLRequest=zVTPb9owFL7vr4h8T%2By4UlJVqFhZtUrtyho2TbtMxjyKpcTO%2FJyE%2FvdzAmysWqsed8jFeu973y%2F
VMware® vSphere
administrator@vsphere.local
Use Windows session authentication
LOGIN

LATERAL COMPROMISE

ESX Admins

- Authentication Bypass Vulnerability
- Requires DC Access
- Group create/modify permissions
- Grants admin level access to ESXi WebUI
- Escalation/persistence through account modification/creation
- VM Manipulation
- Similar to MGM vSphere compromise, but leverages Domain Controller



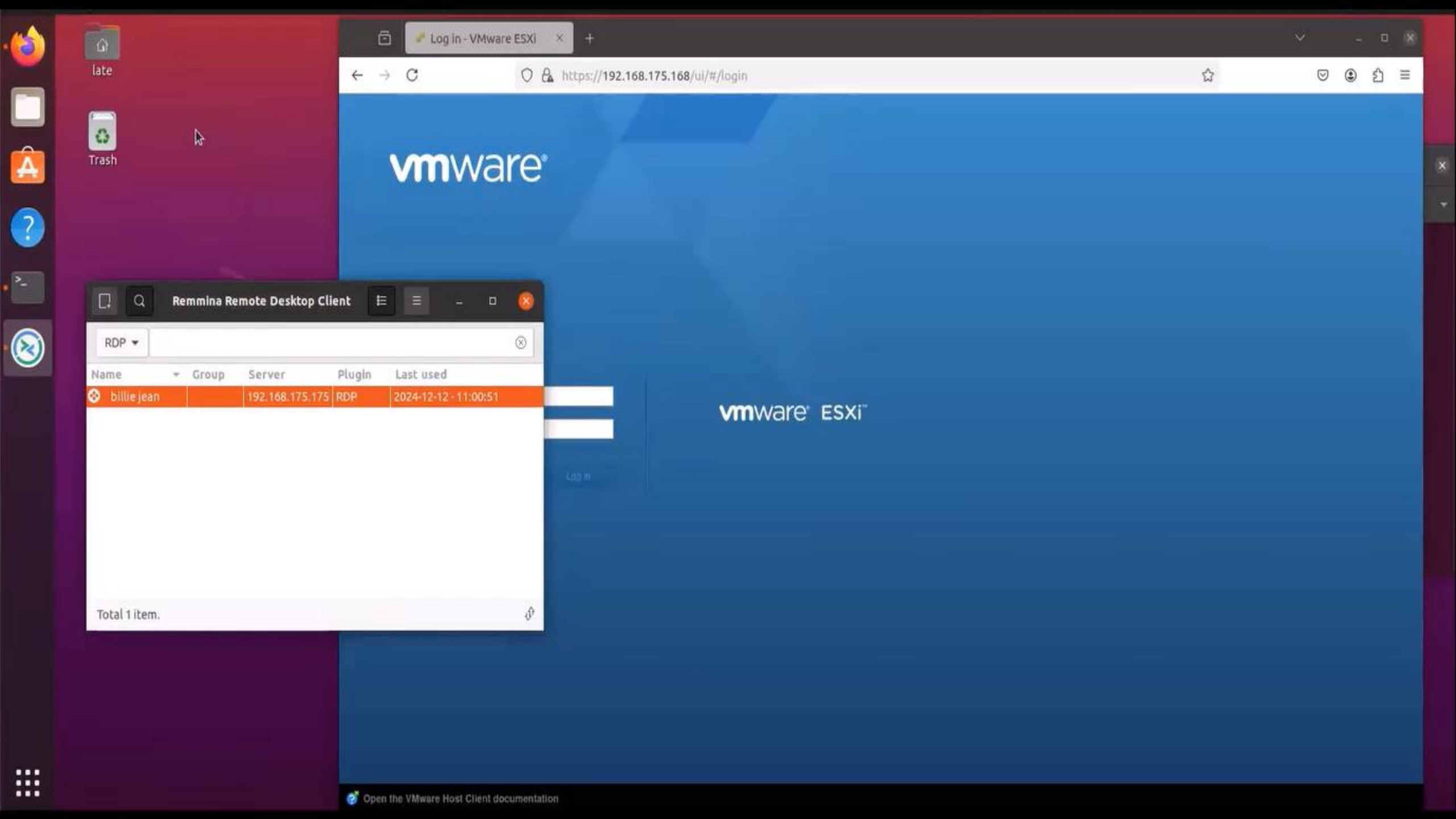
VMware ESXi CVE-2024-37085 Targeted in Ransomware Campaigns

Jul 30, 2024 | 4 min read | Rapid7

Last updated at Fri, 04 Oct 2024 19:49:04 GMT

On Monday, July 29, Microsoft published an extensive threat intelligence blog on observed exploitation of CVE-2024-37085, an Active Directory integration authentication bypass vulnerability affecting Broadcom VMware ESXi hypervisors. The vulnerability, according to Redmond, was identified in zero-day attacks and has evidently been used by at least half a dozen ransomware operations to obtain full administrative permissions on domain-joined ESXi hypervisors (which, in turn, enables attackers to encrypt downstream file systems). CVE-2024-37085 was one of multiple issues fixed in a June 25 advisory from Broadcom; it appears to have been exploited as a zero-day vulnerability.

VMware ESXi CVE-2024-37085 Targeted in Ransomware Campaigns | Rapid7 Blog


late
Trash
Log in - VMware ESXi
https://192.168.175.168/ui/#/login
vmware
vmware ESXi
Log in
Open the VMware Host Client documentation
Remmina Remote Desktop Client
RDP
Name
Group
Server
Plugin
Last used
billie jean
192.168.175.175
RDP
2024-12-12 - 11:00:51
Total 1 item.

Lateral Compromise: Defending yourself

- Patch
- Network Segmentation
- Runtime Protection

MISCONFIGURATION

MITRE

- Breach occurred in May 2024
- Attackers installed a malicious VIB
- VIBs are often used to gain persistence
- Tampered with Acceptance Level
- MITRE T1505.006: Server Software Component: vSphere Installation Bundles

```
a@ubuntu:~/threats/collected-ransomware/ESXi/Akira$
```

```
[root@localhost:/var/log] tail -f ./vmkernel.log
2024-07-09T15:23:58.979Z In(182) vmkernel: cpu2:262166)NMP: nmp_ThrottleLogForDevice:3
863: Cmd 0xa0 (0x4548c18e4540, 0) to dev "mpx.vmhba64:C0:T0:L0" on path "vmhba64:C0:T0
:L0" Failed:
2024-07-09T15:23:58.979Z In(182) vmkernel: cpu2:262166)NMP: nmp_ThrottleLogForDevice:3
868: H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x0 0x0. Act:NONE. cmdId.initiator=0x4538
8409b928 CmdSN 0x0
2024-07-09T15:28:58.979Z In(182) vmkernel: cpu3:262167)NMP: nmp_ThrottleLogForDevice:3
863: Cmd 0xa0 (0x4548c19233c0, 0) to dev "mpx.vmhba64:C0:T0:L0" on path "vmhba64:C0:T0
:L0" Failed:
2024-07-09T15:28:58.979Z In(182) vmkernel: cpu3:262167)NMP: nmp_ThrottleLogForDevice:3
868: H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x0 0x0. Act:NONE. cmdId.initiator=0x4538
8409b928 CmdSN 0x0
2024-07-09T15:33:58.979Z In(182) vmkernel: cpu1:262169)NMP: nmp_ThrottleLogForDevice:3
863: Cmd 0xa0 (0x4548c18f94c0, 0) to dev "mpx.vmhba64:C0:T0:L0" on path "vmhba64:C0:T0
:L0" Failed:
2024-07-09T15:33:58.979Z In(182) vmkernel: cpu1:262169)NMP: nmp_ThrottleLogForDevice:3
868: H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x0 0x0. Act:NONE. cmdId.initiator=0x4538
8409b928 CmdSN 0x0
2024-07-09T15:38:58.978Z In(182) vmkernel: cpu3:262167)NMP: nmp_ThrottleLogForDevice:3
863: Cmd 0xa0 (0x4548c18964c0, 0) to dev "mpx.vmhba64:C0:T0:L0" on path "vmhba64:C0:T0
:L0" Failed:
2024-07-09T15:38:58.978Z In(182) vmkernel: cpu3:262167)NMP: nmp_ThrottleLogForDevice:3
868: H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x0 0x0. Act:NONE. cmdId.initiator=0x4538
8409b928 CmdSN 0x0
2024-07-09T15:43:58.980Z In(182) vmkernel: cpu1:262169)NMP: nmp_ThrottleLogForDevice:3
863: Cmd 0xa0 (0x4548c1880a40, 0) to dev "mpx.vmhba64:C0:T0:L0" on path "vmhba64:C0:T0
:L0" Failed:
2024-07-09T15:43:58.980Z In(182) vmkernel: cpu1:262169)NMP: nmp_ThrottleLogForDevice:3
868: H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x0 0x0. Act:NONE. cmdId.initiator=0x4538
8409b928 CmdSN 0x0
```

MITRE

descriptor.xml

```xml
<?xml version="1.0"?>
<vib version="5.0">
  <type>bootbank</type>
  <name>sampleonesolution</name>
  <version>1.0.0-1OEM.802.0.0.22380479</version>
  <vendor>ZZZ</vendor>
  <summary>Hello World Sample Demon</summary>
  <description>Hello World Sample Demon for VMware ESX</description>
  <release-date>2024-02-22T19:07:13.390123+00:00</release-date>
  <urls/>
  <relationships>
    <depends>
      <constraint name="vmkapi_2_12_0_0"/>
      <constraint name="libvmkuser-8.0.2-1"/>
      <constraint name="uwglibc64-2.12.2-1"/>
      <constraint name="uwvmkcall-8.0.2-1"/>
      <constraint name="nicmgmt" relation="=" version="0.3"/>
      <constraint name="iscsimgmt" relation="=" version="0.0"/>
      <constraint name="srest" relation="=" version="0.3"/>
      <constraint name="esx-version" relation="&gt;=" version="7.0.0"/>
    </depends>
    <conflicts/>
    <replaces/>
    <provides/>
    <compatibleWith/>
  </relationships>
  <software-tags>
    <tag>daemon</tag>
    <tag>sdkname:daemondk</tag>
    <tag>sdkversion:8.0.2-22380479</tag>
    <tag>epkname:esxpackagingkit</tag>
    <tag>epkversion:8.0.2-22380537</tag>
  </software-tags>
  <system-requires>
    <maintenance-mode>false</maintenance-mode>
```

```
a@ubuntu:~/threats/collected-ransomware/ESXi/Akira$ scp malware-3.1.240709162853-x86_64.vib root@192.168.208.153:/scratch
```

MITRE

```python
@staticmethod
def _getHostAcceptance():
   # If there is an error or the configured value does not make sense,
   # we return a default.
   try:
      _, out = runcommand([ADVCFG, '-U', 'host-acceptance-level', '-G'],
                          timeout=30.0)
   except RunCommandError as e:
      msg = 'Unable to execute %s: %s' % (os.path.basename(ADVCFG), str(e))
      log.error(msg)
      raise Errors.AcceptanceGetError(msg)

   hostaccept = byteToStr(out).strip()
   if hostaccept in Vib.ArFileVib.ACCEPTANCE_LEVELS:
      return hostaccept
   elif hostaccept:
      log.error("Illegal acceptance level '%s' obtained from "
                "configuration" % (hostaccept))
      return hostaccept
   else:
      log.error("No host acceptance level is configured")
      return ""
```

```python
@staticmethod
def _setHostAcceptance(acceptance):
   if acceptance not in Vib.ArFileVib.ACCEPTANCE_LEVELS:
      msg = "Cannot set acceptance level: unknown level '%s'." % acceptance
      log.error(msg)
      raise Errors.AcceptanceConfigError(msg)

   try:
      res, out = runcommand([ADVCFG, '-U', 'host-acceptance-level',
                             '-S', acceptance])
   except RunCommandError as e:
      msg = 'Unable to execute %s: %s' % (os.path.basename(ADVCFG), str(e))
      log.error(msg)
      raise Errors.AcceptanceConfigError(msg)

   if res != 0:
      msg = ('%s exited with non-zero status %d, output: %s'
             % (os.path.basename(ADVCFG), res, out))
      log.error(msg)
      raise Errors.AcceptanceConfigError(msg)
```

/lib64/python3.8/site-packages/vmware/esximage/HostImage.py

```
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e] esxcli software vib install -v /scratch/malware-3.1.240709162853-x86_64.vib

 [AcceptanceConfigError]
 VIB ValiCyber_bootbank_zerolock_3.0.240709172755-0.0.1's acceptance level is community, which is not compliant with the ImageProfile acceptance level partner
 To change the host acceptance level, use the 'esxcli software acceptance set' command.
 Please refer to the log file for more details.
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e]
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e] esxcli software vib install -f -v /scratch/malware-3.1.240709162853-x86_64.vib

 [AcceptanceConfigError]
 VIB ValiCyber_bootbank_zerolock_3.0.240709172755-0.0.1's acceptance level is community, which is not compliant with the ImageProfile acceptance level partner
 To change the host acceptance level, use the 'esxcli software acceptance set' command.
 Please refer to the log file for more details.
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e]
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e] esxcli software acceptance set --level=CommunitySupported

 [AcceptanceConfigError]
 Secure Boot enabled: Cannot change acceptance level to community.
 Please refer to the log file for more details.
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e]
[root@localhost:/vmfs/volumes/668d457e-333eeac3-b961-000c296e1a2e] esxcli software acceptance get
```

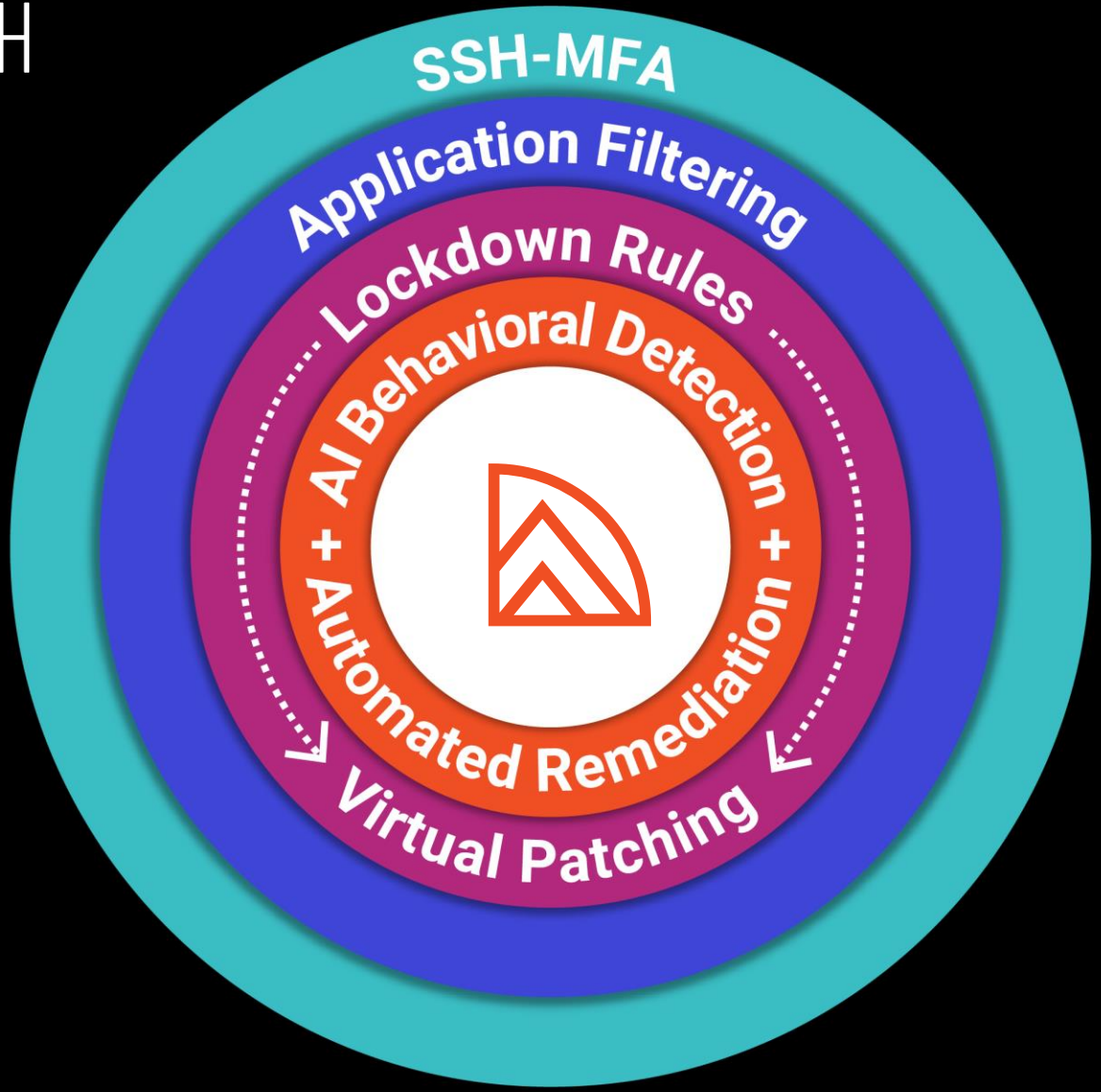
SECURE WITH A DEFENSE IN-DEPTH APPROACH FOR HYPERVISOR

Improve hypervisor resilience

- Maintain a regular patch schedule
- Virtual patching—no downtime required to deploy
- AI-Detection and automated remediation against zero-day attacks—systems are back online within minutes

Reduce risk at the hypervisor level

- Follow best practices for Network Segmentation
- SSH Multi Factor Authentication—prevents outside and inside threats
- Virtual patching—solves known vulnerabilities
- Anti-Tampering—prevents unauthorized change



CHECK IF YOUR PORT IS OPEN USING SHODAN

If you're on here, hackers can see it too!

vCenter

vSphere

ESXi

valicyber™

Questions?

nathan.montierth@valicyber.com

vmware PARTNER TECHNOLOGY ALLIANCE