Microsoft | Microsoft Security

Solutions ⌄   Products ⌄   Services ⌄   Partners | 🔗   All Microsoft ⌄   🔍 Light ◑ Dark

Search the blog

Research **Threat intelligence** **Microsoft Defender** **Ransomware**

9 min read

Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption

By Microsoft Threat Intelligence

July 29, 2024

Microsoft Defender for Endpoint

Microsoft Defender for Identity

Microsoft Defender Threat Intelligence

more ⌄

Microsoft researchers have uncovered a vulnerability in ESXi hypervisors being exploited by several ransomware operators to obtain full administrative permissions on domain-joined ESXi hypervisors. ESXi is a bare-metal hypervisor that is installed directly onto a physical server and provides direct access and control of underlying resources. ESXi hypervisors host virtual machines that may include critical servers in a network. In a ransomware attack, having full administrative permission on an ESXi hypervisor can mean that the threat actor can encrypt the file system, which may affect the ability of the hosted servers to run and function. It also allows the threat actor to access hosted VMs and possibly to exfiltrate data or move laterally within the network.

The vulnerability, identified as CVE-2024-37085, involves a domain group whose members are granted full administrative access to the ESXi hypervisor by default without proper validation. Microsoft disclosed the findings to VMware through Coordinated Vulnerability Disclosure (CVD) via Microsoft Security Vulnerability Research (MSVR), and VMWare released a security update. Microsoft recommends ESXi server administrators to apply the updates released by VMware to protect their servers from related attacks, and to follow the mitigation and protection guidance we provide in this blog post. We thank VMWare for their collaboration in addressing this issue.

PROTECTION INFO

Get mitigation, detection, and hunting guidance ›

This blog post presents analysis of the CVE-2024-37085, as well as details of an attack that was observed by Microsoft to exploit the vulnerability. We're sharing this research to emphasize the importance of collaboration among researchers, vendors, and the security community to continuously advance defenses for the larger ecosystem. As part of Microsoft's commitment to improve security for all, we will continue to share intelligence and work with the security community to help protect users and organizations across platforms.

CVE-2024-37085 vulnerability analysis

Microsoft security researchers identified a new post-compromise technique utilized by ransomware operators like Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest in numerous attacks. In several cases, the use of this technique has led to Akira and Black Basta ransomware deployments. The technique includes running the following commands, which results in the creation of a group named "ESX Admins" in the domain and adding a user to it:

net group "ESX Admins" /domain /add

net group "ESX Admins" username /domain /add

While investigating the attacks and the described behavior, Microsoft researchers discovered that the threat actors' purpose for using this command was to utilize a vulnerability in domain-joined ESXi hypervisors that allows the threat actor to elevate their privileges to full administrative access on the ESXi hypervisor. This finding was reported as part of a vulnerability disclosure to VMware earlier this year.

Further analysis of the vulnerability revealed that VMware ESXi hypervisors joined to an Active Directory domain consider any member of a domain group named "ESX Admins" to have full administrative access by default. This group is not a built-in group in Active Directory and does not exist by default. ESXi hypervisors do not validate that such a group exists when the server is joined to a domain and still treats any members of a group with this name with full administrative access, even if the group did not originally exist. Additionally, the membership in the group is determined by name and not by security identifier (SID).

Microsoft researchers identified three methods for exploiting this vulnerability:

1. **Adding the "ESX Admins" group to the domain and adding a user to it** – This method is actively exploited in the wild by the abovementioned threat actors. In this method, if the "ESX Admins" group doesn't exist, any domain user with the ability to create a group can escalate privileges to full administrative access to domain-joined ESXi hypervisors by creating such a group, and then adding themselves, or other users in their control, to the group.
2. **Renaming any group in the domain to "ESX Admins" and adding a user to the group or use an existing group member** – This method is similar to the first, but in this case the threat actor needs a user that has the capability to rename some arbitrary groups and rename one of them to "ESX Admins". The threat actor can then add a user or use a user that already exists in the group, to escalate privileges to full administrative access. This method was not observed in the wild by Microsoft.
3. **ESXi hypervisor privileges refresh** – Even if the network administrator assigns any other group in the domain to be the management group for the ESXi hypervisor, the full administrative privileges to members of the "ESX Admins" group are not immediately removed and threat actors still could abuse it. This method was not observed in the wild by Microsoft.

Successful exploitation leads to full administrative access to the ESXi hypervisors, allowing threat actors to encrypt the file system of the hypervisor, which could affect the ability of the hosted servers to run and function. It also allows the threat actor to access hosted VMs and possibly to exfiltrate data or move laterally within the network.

Ransomware operators targeting ESXi hypervisors

RANSOMWARE AND EXTORTION

Learn how you can better protect your organization ↗

Over the last year, we have seen ransomware actors targeting ESXi hypervisors to facilitate mass encryption impact in few clicks, demonstrating that ransomware operators are constantly innovating their attack techniques to increase impact on the organizations they target.

ESXi is a popular product in many corporate networks, and in recent years, we have observed ESXi hypervisors become a favored target for threat actors. These hypervisors could be convenient targets if ransomware operators want to stay under the SOC's radar because of the following factors:

1. Many security products have limited visibility and protection for an ESXi hypervisor.
2. Encrypting an ESXi hypervisor file system allows one-click mass encryption, as hosted VMs are impacted. This could provide ransomware operators with more time and complexity in lateral movement and credential theft on each device they access.

Therefore, many ransomware threat actors like Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest, and others support or sell ESXi encryptors like Akira, Black Basta, Babuk, Lockbit, and Kuiper (Figure 1). The number of Microsoft Incident Response (Microsoft IR) engagements that involved the targeting and impacting ESXi hypervisors have more than doubled in the last three years.
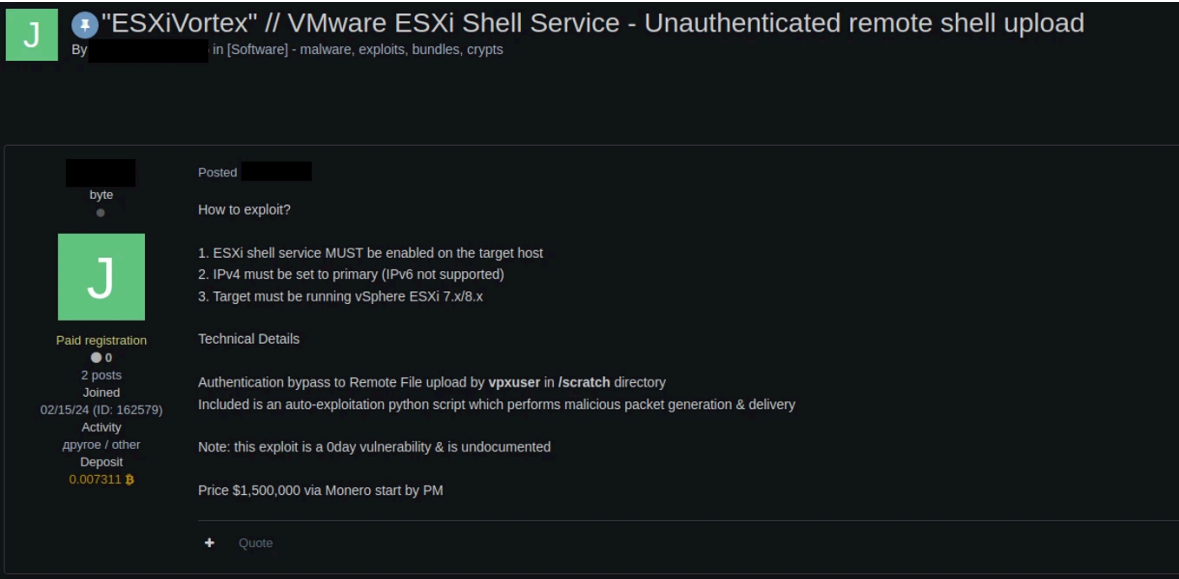

Figure 1. ESXi unauthenticated shell for sale on the dark web

Storm-0506 Black Basta ransomware deployment

Earlier this year, an engineering firm in North America was affected by a Black Basta ransomware deployment by Storm-0506. During this attack, the threat actor used the CVE-2024-37085 vulnerability to gain elevated privileges to the ESXi hypervisors within the organization.

The threat actor gained initial access to the organization via Qakbot infection, followed by the exploitation of a Windows CLFS vulnerability (CVE-2023-28252) to elevate their privileges on affected devices. The threat actor then used Cobalt Strike and Pypykatz (a Python version of Mimikatz) to steal the credentials of two domain administrators and to move laterally to four domain controllers.

On the compromised domain controllers, the threat actor installed persistence mechanisms using custom tools and a SystemBC implant. The actor was also observed attempting to brute force Remote Desktop Protocol (RDP) connections to multiple devices as another method for lateral movement, and then again installing Cobalt Strike and SystemBC. The threat actor then tried to tamper with Microsoft Defender Antivirus using various tools to avoid detection.

Microsoft observed that the threat actor created the "ESX Admins" group in the domain and added a new user account to it, following these actions, Microsoft observed that this attack resulted in encrypting of the ESXi file system and losing functionality of the hosted virtual machines on the ESXi hypervisor. The actor was also observed to use PsExec to encrypt devices that are not hosted on the ESXi hypervisor. Microsoft Defender Antivirus and automatic attack disruption in Microsoft Defender for Endpoint were able to stop these encryption attempts in devices that had the unified agent for Defender for Endpoint installed.
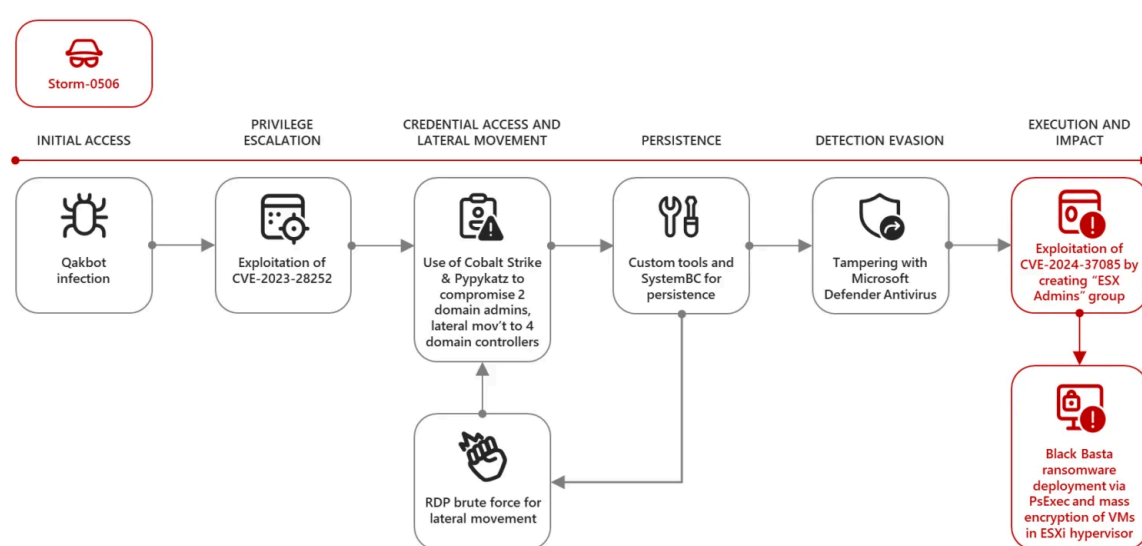
Figure 2. Storm-0506 attack chain

Mitigation and protection guidance

Microsoft recommends organizations that use domain-joined ESXi hypervisors to apply the security update released by VMware to address CVE-2024-37085. The following guidelines will also help organizations protect their network from attacks:

- **Install software updates** – Make sure to install the latest security updates released by VMware on all domain-joined ESXi hypervisors. If installing software updates is not possible, you can use the following recommendations to reduce the risk:
    - Validate the group "ESX Admins" exists in the domain and is hardened.
    - Manually deny access by this group by changing settings in the ESXi hypervisor itself. If full admin access for the Active Directory ESX admins group is not desired, you can disable this behavior using the advanced host setting:
      'Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd'.
    - Change the admin group to a different group in the ESXi hypervisor.
    - Add custom detections in XDR/SIEM for the new group name.
    - Configure sending ESXi logs to a SIEM system and monitor suspicious full administrative access.
- **Credential hygiene** – To utilize the different vulnerability methods, threat actors require control of a highly privileged user in the organization. Therefore, our recommendation is making sure to protect your highly privileged accounts in the organization, especially those that can manage other domain groups:
    - Enforce multifactor authentication (MFA) on all accounts, remove users excluded from MFA, and strictly require MFA from all devices, in all locations, always.
    - Enable passwordless authentication methods (for example, Windows Hello, FIDO keys, or Microsoft Authenticator) for accounts that support passwordless. For accounts that still require passwords, use authenticator apps like Microsoft Authenticator for MFA. Refer to this article for the different authentication methods and features.
    - Isolate privileged accounts from productivity accounts to protect administrative access to the environment. Refer to this article to understand best practices.
- **Improve critical assets posture** – Identify your critical assets in the network, such as ESXi hypervisors and vCenters (a centralized platform for controlling VMware vSphere environments), and make sure to get them protected with latest security updates, proper monitoring procedures and backup and recovery plans. More information can be found in this article.
- **Identify vulnerable assets** – Use Microsoft Defender Vulnerability Management to reduce risk with continuous vulnerability assessment of ESXi hypervisor out of the box.

Microsoft Defender XDR detections

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Suspicious modifications to ESX Admins group

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- New group added suspiciously
- Suspicious Windows account manipulation
- Compromised account conducting hands-on-keyboard attack

Microsoft Defender for Identity

The following Microsoft Defender for Identity alerts can indicate associated threat activity:

- Suspicious creation of ESX group

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft Defender Threat Intelligence to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments:

- Storm-0506
- Storm-1175
- Octo Tempest
- Manatee Tempest
- Akira
- Black Basta

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR customers can run the following queries to find related activity in their networks

This query identifies ESXi hypervisors in the organization:

```
DeviceInfo
| where OSDistribution =~ "ESXi"
| summarize arg_max(Timestamp, *) by DeviceId
```

This query identifies ESX Admins group changes in the Active directory:

```
1  IdentityDirectoryEvents
2  | where Timestamp >= ago(30d)
3  | where AdditionalFields has ('esx admins')
```

The following queries are for assessing the already discovered ESXi with the Microsoft Defender Vulnerability Management information:

```
DeviceInfo
| where OSDistribution =~ "ESXi"
| summarize arg_max(Timestamp, *) by DeviceId
| join kind=inner (DeviceTvmSoftwareVulnerabilities) on DeviceId
DeviceInfo
| where OSDistribution =~ "ESXi"
| summarize arg_max(Timestamp, *) by DeviceId
| join kind=inner (DeviceTvmSecureConfigurationAssessment) on De
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the [Microsoft Sentinel Content Hub](#) to have the analytics rule deployed in their Sentinel workspace.

Microsoft Sentinel also has a range of hunting queries available in Sentinel GitHub repo or as part of Sentinel solutions that customers can use to detect the activity detailed in this blog in addition to Microsoft Defender detections. These hunting queries include the following:

Qakbot:

- [Qakbot hunting queries](#)

Cobalt Strike:

- [Cobalt Strike DNS Beaconing](#)
- [Potential ransomware activity related to Cobalt Strike](#)
- [Suspicious named pipes](#)
- [Cobalt Strike Invocation using WMI](#)

References

- https://knowledge.broadcom.com/external/article?legacyId=1025569
- https://core.vmware.com/vmware-vsphere-8-security-configuration-guide
- https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html
- https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html
- [https://www.sygnia.co/blog/esxi-ransomware-attacks/?blaid=6088911https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/](https://www.sygnia.co/blog/esxi-ransomware-attacks/)
- https://www.darkreading.com/cloud-security/agenda-ransomware-vmware-esxi-servers
- https://blog.checkpoint.com/2023/02/06/massive-ransomware-attack-targets-vmware-esxi-servers/amp/
- https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/amp/

Danielle Kuznets Nohi, Edan Zwick, Meitar Pinto, Charles-Edouard Bettan, Vaibhav Deshmukh

Microsoft Threat Intelligence Community

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.

Related Posts

Research Threat intelligence Ransomware ·

May 9, 2022 · 37 min read

Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself ›

Microsoft coined the term "human-operated ransomware" to clearly define a class of attack driven by expert human intelligence at every step of the attack chain and culminate in intentional business disruption and extortion. In this blog, we explain the ransomware as a service (RaaS) affiliate model and disambiguate between the attacker tools and the various threat actors at play during a security incident.

Research Threat intelligence Microsoft Incident Response

Threat actors

Oct 25, 2023 · 17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction ›

Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for many organizations across multiple industries.

Research Threat intelligence Microsoft Defender

Social engineering / phishing

Dec 28, 2023 · 10 min read

Financially motivated threat actors misusing App Installer ›

Since mid-November 2023, Microsoft Threat Intelligence has observed threat actors, including financially motivated actors like Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674, utilizing the ms-appinstaller URI scheme (App Installer) to distribute malware.

Research Threat intelligence Microsoft Defender

Social engineering / phishing

May 15 · 10 min read

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware ›

Microsoft Threat Intelligence has observed Storm-1811 misusing the client management tool Quick Assist to target users in social engineering attacks that lead to malware like Qakbot followed by Black Basta ransomware deployment.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy