ESXi Ransomware Attacks: Evolution, Impact, and Defense Strategy

By Sygnia

Published: 2024-05-15 · Archived: 2026-04-06 00:51:19 UTC

Understand how ransomware attacks unfold in virtualized environments, and how to defend against these attacks across each phase of the cyber-attack kill chain.

Nital Ruzin, Omer Kidron

15 May 2024

16 min

Executive Summary

In recent years, Sygnia's Incident Response team has seen a steady increase in ransomware attacks targeting virtualized environments, particularly against VMware ESXi infrastructure. Virtualization platforms are a core component of organizational IT infrastructure, yet they often suffer from inherent misconfigurations and vulnerabilities, making them a lucrative and highly effective target for threat actors to abuse.

Sygnia's analysis and investigative activities show that this attack vector is often leveraged by ransomware tools and groups such as LockBit, HelloKitty, BlackMatter, RedAlert (N13V), Scattered Spider, Akira, Cactus, BlackCat and Cheerscrypt.

Through its numerous incident investigations, Sygnia has identified that these attacks follow a typical attack pattern, and has gained a profound understanding of the most effective defense strategies.

This blog post describes how ransomware attacks against virtualized environments unfold across each phase of the attack kill chain, and provides mitigation strategies and specific, actionable tactics for defending against these threats, ensuring the resilience of digital assets in virtualized environments.

Common Virtualization Attack Phases

Sygnia's analysis indicates that ransomware attacks on virtualization environments typically follow a similar pattern:

- **Initial access:** Threat actors gain initial access into the organization using established techniques such as conducting phishing attacks, downloading malicious files, or exploiting known vulnerabilities in internet-facing assets**.**
- **Lateral movement and privilege escalation:** Upon gaining access, threat actors escalate their privileges to obtain credentials for ESXi hosts or vCenter. This escalation can be achieved through various methods,

such as altering domain group memberships for domain-connected VMware, employing brute-force attacks, executing RDP hijacking attempts that target IT personnel.

- **Access validation:** After securing initial access to the virtualization infrastructure, threat actors validate their ability to interface with it. If direct access is denied, attackers use vCenter to enable SSH on all ESXi servers – and might also reset server passwords or execute commands remotely using custom-made vSphere Installation Bundles (VIBs).
- **Virtualized ransomware deployment:** Threat actors then utilize their access to connect to the ESXi, and execute the ransomware on the ESXi hosts.
- **Compromise of backups:** Targeting beyond the virtualized environment, threat actors might try to seize control of backup systems. By encrypting or deleting backup storage and, in some instances, changing the passwords for the backup system, threat actors aim to hinder the recovery of the virtualized environment and thus gain additional leverage over their victims.
- **Data exfiltration:** Threat actors often attempt to enact a double extortion scheme, by exfiltrating data to external locations such as Mega.io, Dropbox, or their own hosting services. This enables threat actors not only to encrypt the existing files, but also to release the exfiltrated data publicly, to cause additional reputational damage.
- **Ransomware execution:** At this point, threat actors shut down all virtual machines and initiate ransomware that encrypts the '/vmfs/volumes' folder of the ESXi filesystem.
- **Additional ransomware deployment:** Threat actors who obtain prior access to deployment mechanisms (such as SCCM or Active Directory) may spread additional ransomware to non-virtualized servers and workstations, amplifying the attack's impact beyond the virtualization realm.

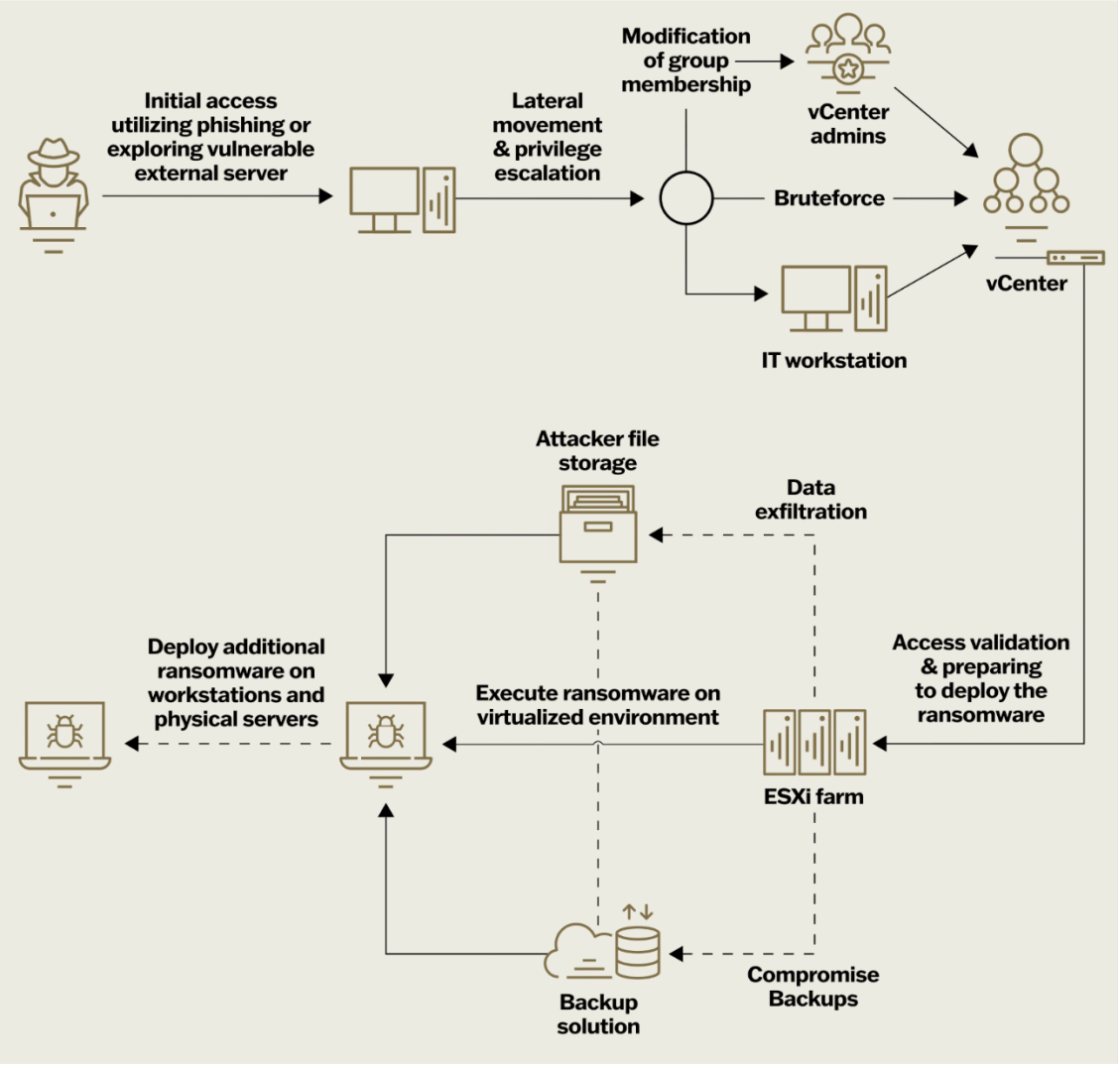

Figure 1: ESXi Ransomware Attack Kill-Chain

The Defender's Perspective

Now that we have a general understanding of the attack flow, let's look at this attack from the defender's perspective. It is usually possible to mitigate – or at the very least, increase the likelihood of recovering from – attacks targeting ESXi infrastructure, by taking the following key elements into consideration:

- **Monitoring** is a cornerstone of detecting, containing, and blocking attacks in the early stages, and can assist in containing an attacker's activities before damage is done.
- **Backups** that are comprehensive and have robust protection are the most reliable way to enable a company to return to operation in a timely manner after a breach.
- **Authentication and authorization** such as Role-Based Access Control (RBAC) helps to restrict attackers' access abilities, inhibiting privilege escalation and containing the attack.
- **Hardening** aids in mitigating attackers' Tactics, Techniques and Procedures (TTPs), and can repel instances of privilege escalation, code execution, data exfiltration and more.
- **Network restrictions** help to limit an attacker's lateral movement.

A Mitigation Strategy

The following recommendations are designed specifically to inhibit ransomware attacks on VMware (versions 6.7 and above) virtualized environments. Nevertheless, similar measures can be adopted to protect any other virtualization environment.

We recommend including the following resources and activities as part of your security hardening, in addition to other security measures and best practices. As always, it is recommended to test the implementation of the following recommendations in a test environment before implementing them in production. The following recommendations are ordered in a way that simplifies implementation, starting with the easiest and quickest solutions.

Monitoring

Monitoring and logging should be in place to ensure that attacks and misuse are detected, and to facilitate forensic examination. Remember that logging and data collection should aim to provide as much information as possible, in preparation for D-Day.

1. **Ensure logs are collected:** Make sure that all the components of the virtualization environment – namely ESXi hosts, vCenter, and storage – are sending logs to the Security Information and Events Management (SIEM) solution for retention, correlation, and alerting.
   In some instances, threat actors deliberately encrypt or delete logs to conceal their activities, rendering locally-stored logs unreliable. This highlights the importance of maintaining immutable backups of all logs that are sent to the SIEM – particularly for self-hosted SIEMs. These backups ensure the availability of critical log data for investigation in the event of a total compromise and encryption of the environment.
   - Details on how to configure syslog for ESXi hosts can be found here.
     - Some monitoring solutions look at the log files directly; in such cases, the auth.log file (/var/log/auth.log) holds all authentication attempts to ESXi hosts. Additional information on the ESXi log file can be found here.
     - Examples of authentication and shell logs can be found here.
   - Details on how to configure syslog for vCenter servers can be found here.
2. **Create SIEM alerts:** Configure alerts for suspicious behavior that may indicate that virtualized infrastructure has been compromised. This behavior can range from root password changes to critical configuration changes such as disabling security features, installation of third-party VIBs, and more. These alerts should be custom-fit to the environment to reduce false-positives. Following are some actions that are worth highlighting, as they are mostly unique, and are highly likely to indicate that a ransomware attack is in process:
   - ESXi host shutting down all virtual machines – threat actors have been observed powering off all machines before starting the encryption process. More information about logs related to reasons for virtual machine shutdown can be found here.
   - ESXi host executing command-line commands, including the phrases:
     - *./encryptor*
     - *sudo ./encryptor
     - *encryptor/vmfs/volumes*
   - Look for users' first logins, and logins of abnormal or suspicious user accounts.

- If vCenter is integrated with Active Directory, it is essential to establish alerts for modifications to groups associated with vCenter administrative privileges, such as VMware admins, ESX admins virtualization admins, and storage admins. This proactive measure ensures timely detection and response to unauthorized changes, thereby reinforcing the security posture of the virtualization environment.
    - Event ID for a user being added to an AD group: 4728, 4732, 4756.
    - Event IDs 4728, 4732, and 4756 can also apply when a group (rather than an individual user) is added to another group, depending on the group's scope (global, local, or universal, respectively).
    - Enable "Audit account management" in the Group Policy settings under Computer Configuration → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Management on the domain controllers, to ensure these events are captured.
- Threat actors have been observed using ESXi profiles to perform privilege escalation, by modifying configurations such as running services, Active Directory integration, and even the root password. These modifications can be monitored through specific log files. Key logs to monitor include the vCenter 'vpxd.log' and the ESXi 'hostd.log':
    - Threat actors might alter the configuration of an ESXi host to gain a foothold, by utilizing the built-in feature of ESXi profiles, without having direct access to the ESXi hosts. Trigger alerts on profile changes using the following log entry format: *Profile [profile-name] has been applied to host [host-name]*
    - Unplanned root account password changes can indicate an active threat in the network, gaining elevated privileges on the ESXi. Trigger alerts for root password changes using this log entry: *Applying password change for root user on host [host-name]*
    - Addition of ESXi to Active Directory could suggest that a threat actor is attempting to gain access to the ESXi host using domain credentials. Look for the following entry in the logs: *Host [host-name] has been added to the Active Directory domain [domain-name]*

3. **Set up SIEM redundancy:** Avoid SIEM single point of failure by setting up redundancy – keep in mind that if the SIEM is hosted on a ESX server, a failure of or an attack on the ESX will blind the SIEM.

Backups

Backups are the last resort if all other mitigations have failed. Backups must be secure, robust, and reliable. ***Never test a backup on D-Day for the first time****. Ensure that your backups are working and are hosted in a secure location so that in case of emergency, there are no surprises in your last line of defense. Keep in mind that one of the ways adversaries ensure complete lockdown of the environment is by targeting backup infrastructure – so yours should be well protected.*

1. **Scope:** Backups must be created and retained in alignment with the organization's business impact analysis. These backups should encompass all critical assets of the organization, including the necessary supporting infrastructure. Taking these assets into consideration is crucial for determining which systems must be reinstated to full operation in the event of a crisis, as indicated by the Recovery Time Objective

(RTO). For instance, an ERP system is regarded as a business-critical asset, while Active Directory serves as supporting infrastructure.

2. **Method:** At a minimum, it is advised to store backups on a modern, immutable storage and backup platform. This approach guarantees that once a backup has been created, it cannot be erased until the specified retention duration has elapsed.
3. **Testing:** It is essential to verify that backups are functioning as anticipated, and that the data remains recoverable. This verification can be achieved by attempting to restore a service using a backup and ensuring that the data's integrity is preserved. It is important to recognize that certain servers and services necessitate distinct backup protocols. For instance:
    - Microsoft SQL Server backups should be performed through the utilization of the SQL Server Management Studio (SSMS) task schedule, with backups being stored in a secure location. Additional details regarding the creation of full database backups without utilizing backup solutions can be found here.
    - For Active Directory, the built-in 'Windows Server backup utility' can be used. Further information can be found here. Additional information on how to back up and restore Active Directory servers can be found here.
4. **Backup locations:** It is essential to ensure that NAS (Network Attached Storage) and SAN (Storage Area Network) backup locations are completely isolated from the production environment. This can be achieved through dedicated hardware and network segmentation, or by using a dedicated, secure cloud account exclusively for backup purposes. This principle extends to virtual machines and other storage scenarios. For instance, if backups made using snapshots are kept in the same storage location as the machine itself, there is a greater risk that threat actors will encrypt the backups in parallel with the servers. Such scenarios have been observed in several recent ransomware incidents.
5. **Security measures:** It is vital to secure backups against unauthorized access and malicious tampering. When determining suitable security measures for backups in your environment, consider the following critical factors:
    - **Authentication:** Evaluate the authentication method utilized. Enforce multi-factor authentication (MFA) for all access points to the backup and define where you expect sources to connect from; only jump servers or a privileged access management solution should be used for such connections.
    - **Authorization:** Determine the users authorized to access or delete backup data. Specify the conditions under which such actions are allowed – particularly deletions. For example, allow users with deletion capabilities to access the server only from a secure source, such as a Privileged Access Management (PAM) solution, and only during maintenance windows. Consider this access to be equivalent to the use of a break-glass account and configure the appropriate alerts.
    - **Accounting:** Implement comprehensive logging and monitoring mechanisms. Establish protocols for alerting relevant personnel upon detection of potentially destructive actions, such as unauthorized configuration modifications or deletions of backups.
    - **Confidentiality:** Ensure backups are encrypted during transmission and at rest. Ensure that you know which encryption methods are used, the lifecycle of encryption keys, and where they are stored – ideally offline. All of the above should be well documented and referenced in the Incident Response Plan (IRP), to ensure that the relevant information can be retrieved quickly amid the chaos of an attack.

Authentication and Authorization

Strong authentication mechanisms with MFA and strict authorization policies will help reduce the attack surface. Remember: the threat actor will try to take the path of least resistance – so it is crucial to create resistance in your policies, systems, and procedures.

1. **Principle of Least Privilege:** Ensure that only the required personnel have permission (authorization) to access the virtualized environment (e.g., VMware Enterprise vCenter, ESXi hosts), and that each person has their own dedicated personal privileged user account with the minimal permissions required.
    - Implementing a robust separation of duties – and thus permissions – according to system criticality, type, and data will ensure that the attack blast radius is kept to a minimum.
    - Usually only a small and/or dedicated team requires direct access to ESXi hosts – particularly with 'write' permissions – as most deployments utilize vCenter for management, meaning that there is no actual need for continuous ESXi access.
2. **Authentication:** Wherever possible, enforce the use of MFA to access the vCenter – with the exception of the highly-monitored break-glass accounts. This can be achieved using Radius or smart card authentication. Further information about MFA in vCenter can be found here. Ensure that all passwords are complex and unique for each ESXi host and vCenter, as password reuse has been exploited by adversaries to gain access to various systems. If a Privileged Identity Management (PIM) or password vault solution exists in the organization, store the passwords using this solution.
3. **Credential rotation:** If a PIM solution exists in the organization, rotate all Privileged Accounts passwords on a regular basis. Otherwise, ensure periodic rotation of passwords for the dedicated personal users, and once a year change the break-glass account's password.
4. **Break-glass account protection:** It is essential to secure all break-glass accounts (for example, root user accounts) with unique, long passwords. These passwords should be stored offline to guarantee accessibility in emergency situations. Additionally, it is crucial to implement a policy for regular password rotation. If a PIM solution is in place, it should be leveraged to automate this task.

Hardening

The keystone of security is to limit the attack surface to the greatest extent possible, making the adversary's life harder. Hardening is not the be-all and end-all of attack surface reduction, but is a significant aspect of it, and an important tool in the defender's toolkit. For example, a threat actor will not be able to run scripts without resistance if the organization's execution policy is hardened by being set to 'signed only'.

1. **Disable unused protocols:** Ensure that SSH is disabled on all ESXi hosts. Emergency access can be achieved by utilizing out-of-band management protocols such as iLO, DRAC, or by temporarily enabling SSH and immediately closing the service again after the activity. Additionally, ensure that other unnecessary management services, such as HTTPS (port 443), vSphere Client for console (902 TCP/UDP), and vMotion (TCP 8000), are properly restricted to minimal required usage, if any.
2. **Up-to-date security patches:** Ensure that vCenter and ESXi hosts receive periodic updates, at least once every year. Additionally, you should follow threat intel feeds and bulletins to stay informed about critical vulnerabilities, such as the Log4Shell vulnerability on vCenter. It is also recommended to use vulnerability scanners on a regular basis, to identify and address vulnerabilities within the platform.

3. **Lockdown mode:** VMware environments can be configured to allow management only via vCenter, and thus to prevent any direct access to ESXi hosts.
    - When using the 'Normal lockdown mode' configuration, the ESXi hosts are accessible only through vCenter and direct console UI.
    - When using 'Strict lockdown mode', direct console is disabled, and only vCenter can change configuration in the ESXi hosts.
    - The emergency break-glass, third-party solution, and external application accounts must be exempted from lockdown mode in order to be able to communicate directly with the ESXi. More information about how to configure the exception list can be found here.
    - Further information about lockdown mode can be found here.
4. **Restrict unsigned scripts:** Disable the ability to execute unsigned scripts on ESXi hosts, to prevent malicious executables such as the encryptor from running on the hosts. As a prerequisite to this configuration, ensure that the infrastructure supports UEFI Secure boot, and that Trusted Platform Module (TPM) is enabled on the hosts.
    - Enable UEFI Secure boot and TPM.
    - Enable the 'execInstalledOnly' flag on all ESXi hosts in the environment. This feature will block any unsigned code from running on the ESXi. Refer to this article for details on how to restrict the execution of the unsigned script.
5. **Segregate hosts containing sensitive systems:** Although not the most cost-effective strategy for safeguarding critical infrastructure, it is highly recommended to segregate ESXi hosts and storage for critical assets from other servers. Such assets include Domain Controllers and Public Key Infrastructure (PKI) systems. The rationale behind this is to mitigate the risk that a compromise, even at the virtualization layer, could provide a threat actor with overarching access privileges, metaphorically handing them the 'keys to the kingdom'. For instance, if an Active Directory virtual machine's storage is not encrypted, a threat actor might extract the NTDS.dit file directly from the virtualization platform. This action could enable the attacker to execute a KRBTGT golden ticket attack, which would severely compromise the environment's security.
6. **Follow best practices:** Ensure that security best practices are followed for VMware.
   Further information on the ESXi host can be found here and here, and CIS recommendations can be found here. Additional information about VMware environment security can be found here.

Network Restrictions

Strict network policies will hinder the lateral movement of an adversary. It is vital to ensure that only the required access is allowed.

1. **Access policy:** Implement a restrictive network access policy for all virtualization components, including storage, ESXi, and vCenter. Access should be restricted solely to essential entities, such as internal components, secure workstations, jump servers, out-of-band machines, and the Privileged Access Management (PAM) solution, if one is deployed.
2. **Restrict administrative access:** Network access to ESXi hosts and administrative interfaces must be strictly controlled. Ensure that such access is granted only after establishing that the source complies with the principle of least privilege, and is one of the entities mentioned above – meaning: personal IT

workstations should not be allowed to have access directly, but relevant jump servers are allowed, with the restriction that the server is denied access to the internet. This can be achieved by utilizing robust firewall policies, or through identity-aware network restrictions.

3. **Outbound traffic:** Deny the ability to initiate outbound traffic to the internet and other non-trusted networks from all virtualization components – or limit the ability to the greatest extent possible. Such components include vCenter, ESXi hosts, and storage components. This approach will mitigate the risk of data exfiltration and other external threats.
4. **Out of band:** For environments that require additional security, restrict access to ESXi hosts and storage to a dedicated administrative out-of-band network. This measure ensures an additional layer of security by segregating administrative traffic from the operational network.

Conclusion

In the modern digital era, virtualized environments are crucial to organizational IT infrastructure, yet they also represent significant ransomware risks. This article highlights how attackers exploit vulnerabilities within hypervisors, transforming operational benefits into severe security risks. Nonetheless, by adopting a proactive security posture – encompassing regular monitoring, stringent network restrictions, robust authentication, timely security patches, and segregation of critical systems – organizations can significantly mitigate these threats. The creation and regular testing of secure, reliable backups is also essential, providing a vital safety net against breaches. Despite the evolving cyber threat landscape, with informed strategies and diligent best practices, businesses can strengthen their defenses against ransomware, ensuring the integrity and resilience of digital infrastructures.
