CROWDSTRIKE

CROWDSTRIKE SERVICES

ESXi TRIAGE COLLECTION AND CONTAINMENT

QUICK REFERENCE GUIDE

Version 2.0

Dated: October 31, 2022

Overview

CrowdStrike has observed criminal Threat Actor groups targeting ESXi servers hosting virtualized systems, and encrypting the Virtual Machine Disk Files (VMDKs) that contain the virtual hard disks. By leveraging ESXi hosts, these adversaries can increase the scope of affected systems within a target environment.

Threat Actors have been observed accessing ESXi systems themselves to leverage and encrypt client virtualized environments. This Quick Reference Guide (QRG) provides instructions on how to collect relevant investigation data from ESXi hosts as well as common ESXi best practices and containment recommendations.

Data Collection

CrowdStrike has developed a script that collects and consolidates relevant data from an ESXi system for the purpose of forensic triage. This script can be provided by CrowdStrike upon request.

The script collects the common artifacts from an ESXi system and compresses them into a single gzip compressed tar archive. This script was most recently tested on ESXi 6.7.0.

1. To perform the collection, the script must be placed in a location on the datastore volume (i.e., not on the system itself). This can typically be done through vCenter Datastore browser, as shown in Figure 1 below.

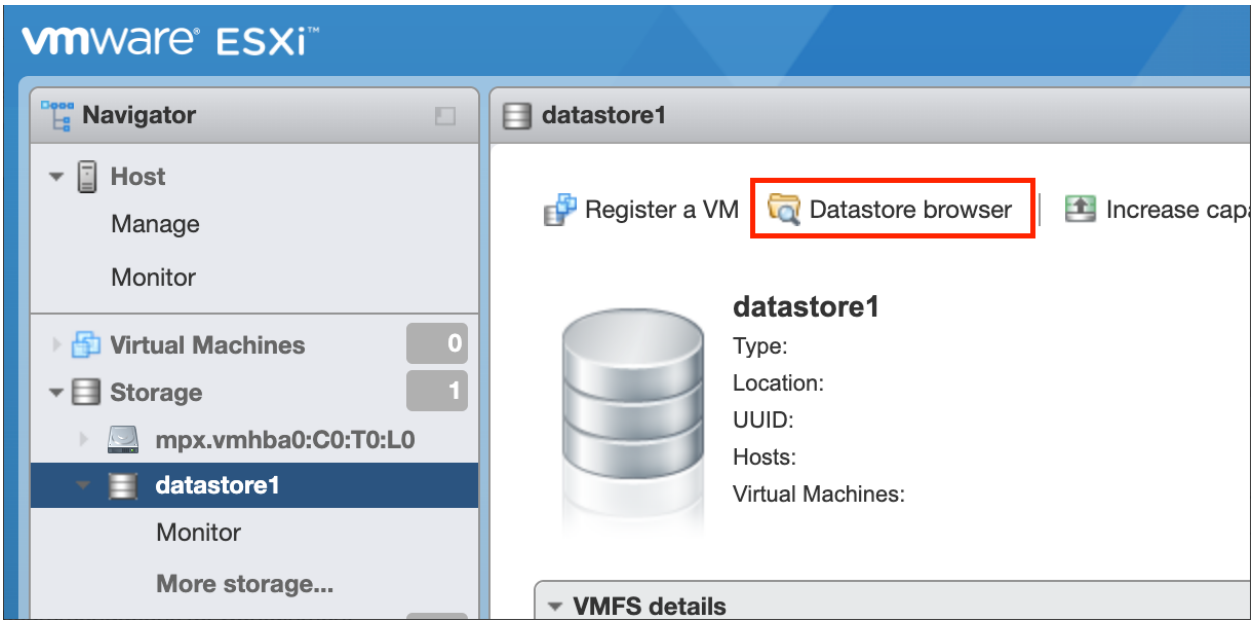

Figure 1: VMware ESXi Datastore Browser

2. Once uploaded, access the ESXi system directly and browse to the location of the script. From this location, give the script execution permissions using the following command:

   ```
   chmod +x <Script Name>.sh
   ```

3. Next, execute the script and allow it to run to completion using the following command:

   ```
   ./<Script Name>.sh
   ```

4. Upon completion, a gzip compressed tar archive will be created that will contain the collected artifacts.

5. Once collection is complete on one ESXi system, repeat these steps to collect from subsequent systems.

Recommendations for Containment

In instances where encryption of the ESXi systems has not yet occurred, or is identified to be in progress, CrowdStrike recommends the following be taken into consideration based on the situation:

- ***Do not immediately reboot or shutdown VMs.*** Ransomware is not able to modify locked files and if a VM is still powered on it will be considered locked. As a result, shutting down or rebooting VMs will release the lock and allow the ransomware to encrypt the file.
- Do not restore virtual machines (VMs) of known compromised ESXi clusters or systems until the malicious processes have been identified and killed.
- When possible, rebuild ESXi hosts from a verified clean image into separate and isolated infrastructure and bring assets back into the isolated cluster.
- Unmount the LUN/datastore (where the VMDKs are stored) from ESXi cluster. This can save any unencrypted VMDKs from being impacted by ransomware. Details can be found in the VMware Knowledge Base article 20046045[1].
- Restrict access to ESXi hosts to a small number of approved systems. Additionally, ensure all systems granted ESXi access have EDR software installed and running.
- Ensure SSH access to the ESXi systems is disabled and/or ensure that access is secured by multifactor authentication.
- Ensure passwords are unique to each ESXi system as well as to the web client. Additionally, ensure passwords are strong and complex using a combination of letters, special characters, and numbers. Avoid using dictionary words and “1337” speak.
- Enable Normal Lockdown Mode to further restrict access. Further guidance can be found in VMware KB article 1008077[2].
- Explore enabling the **`execInstalledOnly`** option, which is designed to prevent binaries being executed on the system that weren’t signed by VMware. This will require a reboot of the system to enable and if using third-party software on the system it could cause issues with said software. However, enabling this option will help prevent non-signed binaries from executing on ESXi systems. Refer to VMware’s article, “Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration”[3].

1 https://kb.vmware.com/s/article/2004605
2 https://kb.vmware.com/s/article/1008077
3 https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9047A43D-BB1F-4878-A971-EEFCAC183C86.html

CROWDSTRIKE SERVICES

If you require additional assistance, please reach out to CrowdStrike's support team at support@crowdstrike.com or contact us via phone:

Americas/Canada	+1 888 512 8906
UK/Ireland	+44(0) 118 453 0400
Australia/New Zealand/APAC	(+61) 1300 245 584
Middle East/Turkey/Africa	+9714 429 5829

If further help is required and you would like to engage CrowdStrike's Incident Response team, please contact Professional Services by completing the form on https://www.crowdstrike.com/experienced-a-breach or contact us via phone:

Americas/Canada	+1 855 276 9347
UK/Ireland	+44 800 0487187
France	+33 801840073
Germany	+49 (0800) 3252669
Australia	+61 1800 290 853
Japan	+81 800 170 5401
India	+91 1800 040 3447
Saudi Arabia	+966 8008803012
UAE	+971 8000320534
Qatar	+974 800101302

Customers with an active CrowdStrike Services retainer should notify the Services team in accordance with the process outlined in your retainer agreement.

CROWDSTRIKE SERVICES

WE STOP BREACHES

QUICK REFERENCE GUIDE