Hypervisor Jackpotting, Part 2: eCrime Actors Increase Targeting of ESXi Servers with Ransomware

crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

Michael Dawson August 30, 2021

- CrowdStrike has observed a significant increase in eCrime actors targeting VMware ESXi hypervisors with ransomware since our February 2021 blog post on *Hypervisor Jackpotting*.
- Many of these adversaries share common tradecraft such as gaining interactive access via SSH, listing and terminating running VM processes prior to encryption, and targeting the `vmfs/volumes` datastore path to encrypt disk volumes and snapshots.
- Several defensive controls, listed later in this blog, should be implemented to mitigate the success or impact of hypervisor jackpotting.

In February 2021, CrowdStrike blogged about *Hypervisor Jackpotting*, a technique that involves targeting VMware ESXi hypervisors with ransomware to increase the scope of impact. CrowdStrike noted that two big game hunting (BGH) adversaries, CARBON SPIDER and SPRITE SPIDER, were observed utilizing this technique with their respective ransomware variants, *Darkside* and *Defray777*. Since then, CrowdStrike has observed a significant uptrend in hypervisor jackpotting by other adversaries, including PINCHY SPIDER and VIKING SPIDER. In this blog, we overview each new campaign CrowdStrike has observed targeting ESXi systems and detail defensive controls that can be implemented to protect these critical assets.

Babuk Locker

In March 2021, operators of *Babuk Locker* ransomware offered access to an ESXi variant as part of a sought-out partnership opportunity. In May 2021, CrowdStrike Services observed a victim targeted with this ESXi variant. The ransomware appends the file extension `.babyk_esxi` to files it encrypts, and creates a ransom note named `How To Restore Your Files.txt`. The ransom note contains two URLs: a victim-specific .onion URL for communications, and one for the *Babuk Locker* dedicated leak site (DLS).

FERAL SPIDER and DeathKitty

Since March 2021, FERAL SPIDER, the developers and operators of *DeathKitty* (aka *HelloKitty*) ransomware added functionality to terminate and encrypt virtual machines running on a VMware ESXi hypervisor. If VMware ESXi targeting is enabled (`-e` option), the ransomware will only encrypt file extensions related to disk volumes and snapshots: .`vmdk`, `.vmsd` and `.vmsn`. When executed with the `-k` argument, the ransomware will terminate all running virtual machines using VMware ESXi’s command-line administration utility (`esxcli`) prior to beginning the encryption process.

CYBORG SPIDER and Pysa

Since May 2021, CYBORG SPIDER, the developers and operators of *Pysa* ransomware, have targeted ESXi servers for encryption. After compromising an environment, CYBORG SPIDER operators move laterally to the hypervisors via HTTPS using the native ESXi root account, where they enable SSH for a remote shell. The operators then use PuTTY and WinSCP to copy the ransomware to the `/tmp` directory and execute the commands shown in Table 1.

Command	Description
`python --version`	Check version of Python installed
`cd /tmp/`	Change to /tmp/ directory
`chmod +x <FILENAME>`	Add execute permission to Pysa script
`./<FILENAME> /vmfs/volumes 4096`	Execute Pysa against the VM datastore path

Table 1. *Pysa* commands

CrowdStrike observed multiple cases in which the *Pysa* ransomware script was tailored for the version of Python installed on the ESXi, with *Pysa* filenames `27` and `3` noted as highly likely to correspond with Python v2.7 or v3.x. The ransomware also appends the file extension `.pysa` to files it encrypts, and creates a ransom note named `RECOVER_YOUR_DATA.txt` at the root (`/`) of the volume. The ransom note provides two email addresses, hosted on OnionMail and ProtonMail, for communications and includes *Pysa's* DLS .onion domain.

PINCHY SPIDER and REvix

Since June 2021, PINCHY SPIDER has distributed a Linux ransomware variant named *REvix* to target ESXi systems. The ELF binary uses the same encryption algorithm as PINCHY SPIDER's Windows *REvil* ransomware. The ransomware contains a JSON configuration block that specifies the ransom note filename and encrypted file extension to use. For example, in a sample of *REvix v1.1c*, the ransomware was configured to append the file extension `.rhkrc` to encrypted files, and use the name `rhkrc-readme.txt` as the ransom note. By default, the ransomware will encrypt only the current directory and requires the `--path` option to specify the target folder (e.g., `/vmfs/`), which is then recursively enumerated. Prior to encryption, the ransomware executes the commands shown in Table 2.

Command	Description
`pkill -9 vmx-*`	Terminate any processes named vmx-*
`esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | awk -F "\"*,\"*" {system("esxcli vm process kill --type=force --world-id=" $1)}`	List the running VMs on this system and force terminate each VM based on the enumerated list of World IDs

Table 2. *REvix* commands

In July 2021, PINCHY SPIDER began distributing *REvix v1.2a*, which added execution of VM termination functionality within a separate thread, and support for additional encryption types. In mid-July 2021, PINCHY SPIDER's DLS infrastructure went offline, leaving in question the future of these operations.

VIKING SPIDER and Ragnar Locker

Since June 2021, VIKING SPIDER has deployed *Ragnar Locker*'s ELF binary to ESXi systems via SSH using the native root account. VIKING SPIDER copies the binary to the `/tmp` directory and issues the commands shown in Table 3.

Command	Description

`uname -a`	Print all system information
`esxcli system version get`	Display the product name, version and build information
`esxcli system hostname get`	Display the fully qualified hostname of the ESXi host
`esxcli system account list`	List local user accounts
`esxcli --formatter=csv vm process list`	List the running VMs on this system
`esxcli vm process kill -w <WID> -t soft`	Perform a “soft” kill (clean shutdown) of the VM associated with the given World ID This command is repeated for each running VM to kill
e`sxcli --formatter=csv vm process list`	List the running VMs on this system (again) to confirm they are all shutdown
`find /vmfs/volumes/ -type f -name "*.vmdk"`	Search for all virtual disk files within the VM datastore path
`chmod a+x /tmp/<FILENAME>`	Add execute permission to Ragnar Locker binary
`/tmp/<FILENAME> /vmfs/volumes/<UUID>/`	Execute Ragnar Locker against the VM datastore path
`ps | grep <FILENAME>`	Ensure Ragnar Locker process is running

Table 3. *Ragnar Locker* commands

The ransomware appends the file extension `.crypted` to files it encrypts, and creates a ransom note per encrypted file using the original filename appended with the extension `.crypted.README_TO_RESTORE`. The ransom note includes a unique victim URL for live chat communications via Tor, as well as VIKING SPIDER’s dedicated leak site (DLS) .onion domain.

How to Protect Your Cluster

Listed below are CrowdStrike’s top five recommendations that organizations should implement to mitigate the success or impact of hypervisor jackpotting.

- **Avoid direct access to ESXi hosts.** Use the vSphere Client to administer ESXi hosts that are managed by a vCenter Server. Do not access managed hosts directly with the VMware Host Client, and do not change managed hosts from the Direct Console User Interface (DCUI). (***Note:*** *This is a VMware-specific recommendation.*)

- **If direct access to an ESXi host is necessary, use a hardened jump server with multifactor authentication.** ESXi DCUI access should be limited to a jump server used for only administrative or privileged purposes with full auditing capabilities and multifactor authentication (MFA) enabled.
- **Ensure vCenter is not exposed to the internet over SSH or HTTP.** CrowdStrike has observed adversaries gaining initial access to vCenter using valid accounts or exploiting remote code execution (RCE) vulnerabilities (e.g., CVE-2021-21985). Although these vulnerabilities have been addressed by VMware, these services should not be exposed to the internet to mitigate risk.
- **Ensure ESXi datastore volumes are regularly backed up.** Specifically, virtual machine disk images and snapshots should be backed up daily (more frequently if possible) to an offsite storage provider.
- **If encryption activity is observed, do not shut down the ESXi hosts.** If encryption activity is observed, system administrators may be tempted to reboot or shutdown VMs. Be aware that 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 actually release the lock and allow the ransomware to encrypt the virtual disk files.

Additional ESXi security recommendations are available from VMware at https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-B39474AF-6778-499A-B8AB-E973BE6D4899.html.

Conclusion

CrowdStrike has observed a significant uptrend in eCrime campaigns targeting VMware ESXi hypervisors with ransomware to maximize encryption impact across a victim environment. This targeting modus operandi is becoming prevalent, with adversaries developing and deploying ESXi ransomware variants, and in some cases seeking partnership opportunities with other operators or access brokers.

CrowdStrike recommends that organizations review their ESXi security posture and implement the specific defensive controls outlined in this blog to protect these critical assets.

Additional Resources

- *To learn more about eCrime adversaries tracked by CrowdStrike Intelligence, visit the CrowdStrike Adversary Universe.*
- *To find out how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*