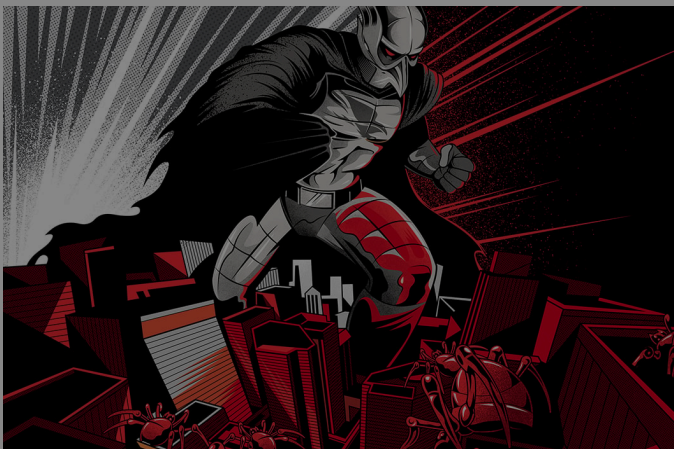**CROWDSTRIKE** | BLOG

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

August 30, 2021 | Michael Dawson | From The Front Lines

This is Part 2 of a three-part blog series. Read Part 1 *and* Part 3.

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE ✕

CROWDSTRIKE | BLOG

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

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

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.

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

shown in Table 2.

Command
`pkill -9 vmx-*`
`esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName"`

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

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

`esxcli --formatter=csv vm process list`	List the running VMs on this sys
`find /vmfs/volumes/ -type f -name "*.vmdk"`	Search for all virtual disk files w
`chmod a+x /tmp/<FILENAME>`	Add execute permission to Rag
`/tmp/<FILENAME> /vmfs/volumes/<UUID>/`	Execute Ragnar Locker against
`ps | grep <FILENAME>`	Ensure Ragnar Locker process

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.

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

- 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

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

strategy, visit the *CROWDSTRIKE FALCON® INTELLIGENCE™ 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.*
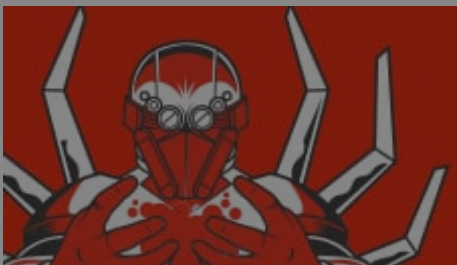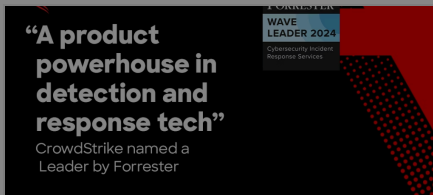
𝕏 Tweet   in Share

Related Content

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

☁ Cloud & Application Security		104
◎ Counter Adversary Operations		184
⊕ Endpoint Security & XDR		306
✕ Engineering & Tech		78
◎ Executive Viewpoint		162
▦ Exposure Management		84
⚠ From The Front Lines		190
◊ Identity Protection		37
◉ Next-Gen SIEM & Log Management		91
▦ Public Sector		37
▦ Small Business		8

CONNECT WITH US

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**
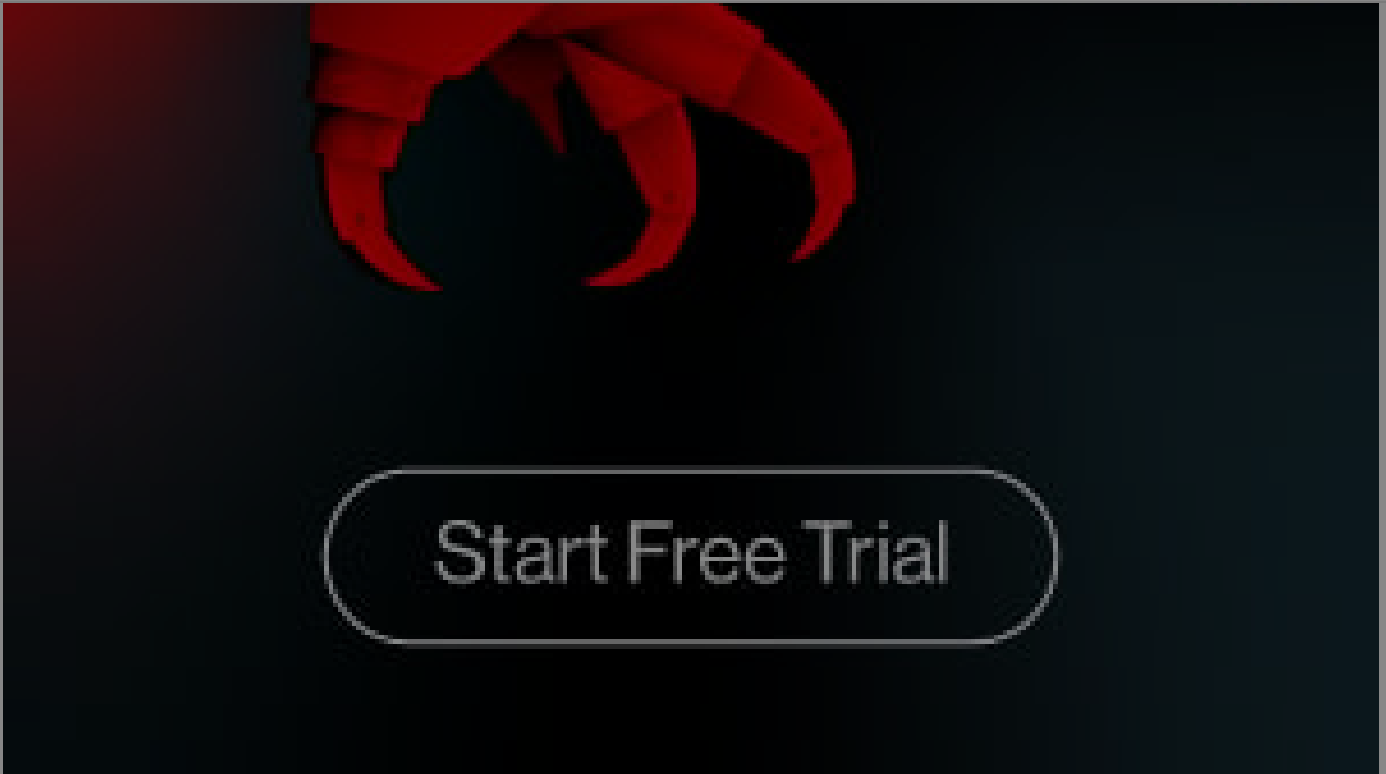
CROWDSTRIKE | BLOG

Start Free Trial

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

Sign Up

Featured

Recent

Video

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**

CROWDSTRIKE | BLOG

ABOUT COOKIES ON THIS SITE

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Cookie Notice**