New Ransomware Tactic: Adversaries Target ESXi Servers

crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

Eric Loui - Sergei Frankoff February 26, 2021

This is Part 1 of a two-part blog series. Read Part 2 here.

Targeted large-scale ransomware campaigns, referred to as big game hunting (BGH), remained the primary eCrime threat to organizations across all sectors in 2020. The relentless volume and pace of these campaigns mean that some sophisticated BGH actors have not attracted much attention. Two such groups are SPRITE SPIDER, the operators of the *Defray777* ransomware (aka *Defray, Defray 2018, Target777, RansomX, RansomEXX*), and CARBON SPIDER, a group formerly focused on compromising point-of-sale (POS) devices, and that was responsible for introducing the *Darkside* ransomware.

While ransomware for Linux has existed for many years, BGH actors have not historically targeted Linux, much less the ESXi hypervisor specifically. This likely reflects the overwhelming dominance of the Windows operating system in businesses and large organizations. However, in the second half of 2020, SPRITE SPIDER and CARBON SPIDER began deploying Linux versions of *Defray777* and *Darkside*, respectively, designed specifically to affect ESXi.

Affected victims include organizations that have used virtualization to host many of their corporate systems on a few ESXi servers, creating a virtual jackpot for the ransomware. By deploying ransomware on these ESXi hosts, adversaries were able to quickly increase the scope of affected systems within the victim environments, resulting in additional pressure on victims to pay a ransom demand. This is a new BGH tactic CrowdStrike refers to as *Hypervisor Jackpotting*.

What Is ESXi?

ESXi is a Type-1 hypervisor (aka a "bare-metal" hypervisor) developed by VMware. A hypervisor is software that runs and manages virtual machines (VMs). In contrast to Type-2 hypervisors that run on a conventional host operating system, a Type-1 hypervisor runs directly on a dedicated host's hardware. ESXi systems are commonly managed by vCenter, a centralized server administration tool that can control multiple ESXi devices. While ESXi is not a Linux operating system, it is possible to run some Linux-compiled ELF binaries within the ESXi command shell.

According to multiple estimates, VMware holds an overwhelming majority of the worldwide virtual machine market share, well ahead of its nearest competitor. This means that threat actors seeking to encrypt virtual infrastructure may prioritize developing malware that can affect VMware environments.

SPRITE SPIDER and Defray777 Ransomware

SPRITE SPIDER is an eCrime actor that conducts low-volume BGH ransomware campaigns using the *Defray777* ransomware. Other tools used by SPRITE SPIDER include the *Vatet* loader and the *PyXie* remote access tool (RAT). The adversary has established initial access by exploiting vulnerable Citrix Application Delivery Controllers, as well as by using LUNAR SPIDER's *BokBot* trojan. To avoid detection, SPRITE SPIDER often stages payloads on internal servers within a victim network and uses in-memory-only deployments of its later-stage tooling. SPRITE SPIDER uses both *PyXie* and *Cobalt Strike* to move laterally within a victim environment after obtaining initial access.

Like other BGH actors, SPRITE SPIDER first attempts to compromise domain controllers (DCs). After acquiring DC access, SPRITE SPIDER collects and exfiltratrates sensitive victim data, then deploys its *Defray777* ransomware. In November 2020, SPRITE SPIDER launched a dedicated leak site (DLS) on a Tor hidden service domain to publish files from noncompliant ransomware victims.

Leaking stolen data in an effort to pressure victims into paying is part of a broader trend across the BGH ecosystem. Compared to other BGH actors, SPRITE SPIDER was relatively late to adopt this tactic, possibly due to a desire to avoid attention.

In July 2020, SPRITE SPIDER began using a Linux version of its *Defray777* ransomware. The Linux version contains the same file scanning and encryption logic as its Windows counterpart, and is designed to receive a command-line argument with a path to the directory where it will begin its recursive encryption process. Files are encrypted using AES in ECB mode with a 256-bit key that is uniquely generated for each file. The key is then encrypted using an embedded 4096-bit RSA public key and appended to the encrypted file. Each victim is targeted with a unique build of *Defray777* containing a unique RSA public key. If a victim pays the ransom, they receive a decryption tool containing an RSA private key that corresponds to the public encryption key.

ESXi Access

In order to compromise ESXi devices, SPRITE SPIDER attempts to harvest credentials that can be used to authenticate to the vCenter web interface. SPRITE SPIDER uses *PyXie*'s LaZagne module to recover vCenter credentials stored in web browsers, and also runs *Mimikatz* to steal credentials from host memory. After authenticating to vCenter, SPRITE SPIDER enables SSH to permit persistent access to ESXi devices. In some cases, the adversary will also change the root account password or the host's SSH keys.

ESXi Encryption

While SPRITE SPIDER uses an in-memory deployment technique for the Windows variant of *Defray777*, on ESXi, the adversary typically writes the Linux version of *Defray777* to `/tmp/`, using a filename attempting to masquerade as a legitimate tool (e.g., svc-new). SPRITE SPIDER enumerates system information and processes on the ESXi host using the `uname`, `df`, and `esxcli vm process list` commands.

Before executing Defray777, SPRITE SPIDER terminates running VMs in order to allow the ransomware to encrypt files associated with the VMs. SPRITE SPIDER may also uninstall VMware Fault Domain Manager (FDM) using a bash script named `VMware-fdm-uninstall.sh`. FDM is a tool that monitors VMs and reboots them when a VM fails.

CARBON SPIDER and Darkside Ransomware

Since 2016, CARBON SPIDER has traditionally targeted companies operating POS devices, with initial access being gained using low-volume phishing campaigns against this sector. CARBON SPIDER has used a variety of backdoors and RATs to enable persistent access. The adversary's signature persistent access tools include the *Sekur* (aka *Anunak*) implant, which has been used since 2016, and the *Harpy* (aka *Griffon*) backdoor, which has been used from 2018 through 2020. CARBON SPIDER extensively uses *Cobalt Strike* for lateral movement, as well as open-source post-exploitation tools like *PowerSploit*.

In April 2020, the adversary abruptly shifted its operational model away from narrow campaigns focused entirely on companies operating POS devices, to broad, opportunistic operations attempting to infect large numbers of victims across almost all sectors. The goal of these campaigns was to deliver the *REvil* ransomware, which CARBON SPIDER obtained from ransomware-as-a-service (RaaS) vendor PINCHY SPIDER. It is likely CARBON SPIDER pivoted to BGH in response to the COVID-19 pandemic, which dramatically reduced in-person retail sales and hospitality business. Similar to SPRITE SPIDER, CARBON SPIDER typically seeks to compromise a DC first before exfiltrating data and deploying ransomware.

CARBON SPIDER deepened its commitment to BGH through 2020 by introducing its own ransomware, *Darkside*. In August 2020, the adversary began deploying *Darkside*, likely in order to avoid sharing profits from BGH campaigns with PINCHY SPIDER, the *REvil* vendor. In November 2020, the adversary took another step into the world of BGH by establishing a RaaS affiliate program for *Darkside*, allowing other actors to use the ransomware while paying CARBON SPIDER a cut. Similar to SPRITE SPIDER and others, CARBON SPIDER operates a DLS for *Darkside*, which has been active since August 2020.

In August 2020, CARBON SPIDER also began using a Linux variant of *Darkside* configured specifically to affect ESXi hosts. The ESXi version of *Darkside* targets files relating to VMware virtual machines, including files with the following file extensions: `vmdk`, `vswp`, `vmem`, `vmsn`, `nvram`, `vmsd`, `vmss`, `vmx`, `vmxf`, `log`. Files are encrypted using the ChaCha20 algorithm with a 32-byte key and 8-byte nonce, uniquely generated per file. The ChaCha20 key and nonce are then encrypted using a 4096-bit RSA public key that is embedded in the ransomware. To speed up the encryption process, *Darkside* also has a configurable encryption size that can be used to control how much of each file is encrypted. In samples recovered by CrowdStrike Intelligence, the encryption size was set to 50MB, which is enough data to prevent the recovery of the virtual machine files. An example of the *Darkside* configuration, as written to its log file, is shown in Figure 1.

```
[CFG] Root Path..............REDACTED
[CFG] Key Size..............548 Bytes
[CFG] Public Key............VALID
[CFG] Part Size.............50mb
[CFG] Search Extension.....vmdk,vswp,vmem,vmsn,nvram,vmsd,vmss,vmx,vmxf,log
[CFG] New Extension.........REDACTED
[CFG] Thread Count..........8
[CFG] ReadMe File...........Dark-ReadMe.TXT
[CFG] ReadMe Size...........REDACTED
```

Figure 1. Darkside configuration from log file

ESXi Access

Similar to SPRITE SPIDER, CARBON SPIDER has gained access to ESXi servers using valid credentials. The adversary has typically accessed these systems via the vCenter web interface, using legitimate credentials, but has also logged in over SSH using the Plink utility to drop *Darkside*.

ESXi Encryption

CARBON SPIDER writes *Darkside* to `/tmp/` on ESXi hosts with a generic filename. The adversary typically does not do the same amount of host reconnaissance that SPRITE SPIDER does. CARBON SPIDER has used built-in VMware Tools scripts to shut down guest VMs in order to make sure these VMs are encrypted by *Darkside*.

Conclusion

By deploying ransomware on ESXi, SPRITE SPIDER and CARBON SPIDER likely intend to impose greater harm on victims than could be achieved by their respective Windows ransomware families alone. Encrypting one ESXi server inflicts the same amount of damage as individually deploying ransomware on each VM hosted on a given server. Consequently, targeting ESXi hosts can also improve the speed of BGH operations.

If these ransomware attacks on ESXi servers continue to be successful, it is likely that more adversaries will begin to target virtualization infrastructure in the medium term.

MITRE ATT&CK® TTP Comparison

The following table provides an overview of SPRITE SPIDER and CARBON SPIDER's tactics, techniques and procedures (TTPs) specific to ESXi ransomware attacks.

Tactic	Technique	SPRITE SPIDER	CARBON SPIDER	Summary
Initial Access	T1078 – Valid Accounts	Y	Y	Both SPRITE SPIDER and CARBON SPIDER authenticate to vCenter using valid credentials
Execution	T1059.004 – Command and Scripting Interpreter: Unix Shell	Y	Y	The adversaries use the ESXi command shell to transfer and execute the ransomware

Persistence	T1078 – Valid Accounts	Y	Y	Previously compromised credentials enable persistent access
Persistence	T-1098.004 – SSH Authorized Keys	Y		SPRITE SPIDER has changed root SSH keys for ESXi hosts
Defense Evasion	T1222.002 – File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	Y	Y	Both adversaries mark their respective ransomware binaries as executable using `chmod`
Defense Evasion	T1036.005 – Masquerading: Match Legitimate Name or Location	Y	Y	*Defray777* and *Darkside* use filenames that appear to be innocuous or legitimate
Defense Evasion	T1070.004 – Indicator Removal on Host: File Deletion	Y		SPRITE SPIDER may delete the *Defray777* binary after execution
Discovery	T1082 – System Information Discovery	Y		SPRITE SPIDER performs basic reconnaissance (e.g., `uname`, `df`)
Discovery	T1057 – Process Discovery	Y		SPRITE SPIDER performs basic reconnaissance (e.g., `esxcli vm process list`)
Impact	T1489 – Service Stop	Y	Y	Both adversaries may attempt to terminate running VMs
Impact	T1486 – Data Encrypted for Impact	Y	Y	*Defray777* and *Darkside* encrypt victim systems

Indicators of Compromise

Example SHA256 hashes of *Darkside* and *Defray777* Linux variants:

Description	SHA256 hash
Darkside Linux Binary	`da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5`
Defray777 Linux Binary	`cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849`

Additional Resources

- *Read Part 2 of this two-part blog series, Hypervisor Jackpotting (Part 2): eCrime Actors Increase Targeting of ESXi Servers with Ransomware.*
- *Read more about big game hunting adversaries tracked by CrowdStrike Intelligence in 2020 in the new CrowdStrike 2021 Global Threat Report.*
- *Check out the Global Threat Report resource hub to learn more about today's adversaries.*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Learn more about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*