Weaponising VMs to bypass EDR – Akira ransomware

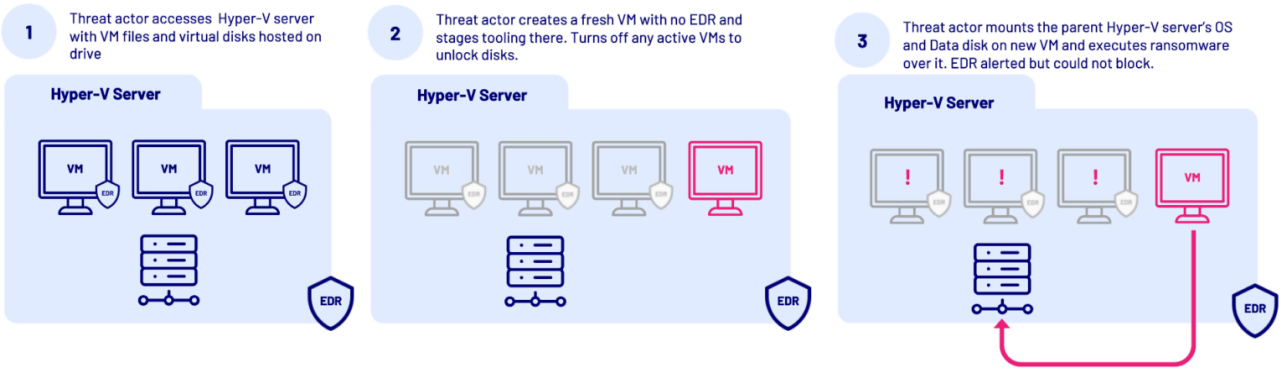
By Lee Davis

Published: 2023-09-15 · Archived: 2026-04-06 00:43:04 UTC

Published by Digital Forensics and Incident Response on 15 September 2023

*The CyberCX DFIR team has been engaged to assist in multiple investigations related to the Akira ransomware group, which has been seen affecting victims since April 2023. One novel technique that we've observed leverages deployment of ransomware onto Windows Hyper-V hypervisor systems, causing major damage to attached virtual machines (**VMs**). Even when Windows-based hypervisor and target virtual machines are running prominent Endpoint Detection & Response (**EDR**) tooling, the threat actor has been observed circumventing this by creating new, unmonitored, VMs on the hypervisor, from which they can navigate directories on the hypervisor and execute their ransomware.*

While Akira leverages many known attack techniques, this article focuses on some standout methods that we've observed.



Initial Access

is aware of several Akira ransomware attacks which leveraged VPN accessmulti-factor authentication (MFA) applied on the initial access point. This was emphasised by Cisco in a recent blog post. In our experience, when conducting a thorough review to ascertain where compromised credentials have been obtained, no obvious locations have been identified. [1] in previous ransomware cases by other threat actors, we believe that Akira typically obtains access through info stealers and credential marketplaces.

Intrusion Activities

CyberCX has observed Akira conducting typical cyber-extortion activity post-initial access which includes but is not limited to:

- Scanning the network using SoftPerfect Network Scanner (netscan.exe)
- Enumeration of data available in the Active Directory through AdFind (AdFind.exe)
- Identifying sensitive information on file shares and servers to exfiltrate by uploading it over SFTP using FileZilla
- Installing SystemBC and creating a scheduled task to remain persistent.

Defence Evasion & Impact

We have observed this threat actor maintain access to compromised environments for several weeks before they achieve their objectives of deploying ransomware. While we expect they intend to encrypt an entire network, we've also observed EDR tooling slowing down their progress to their final objectives. One of our more interesting observations has been the threat actor initially attempting to disable EDR using a vulnerable driver.

Terminator

It was reported by CrowdStrike that in May 2023, a user on a dark web forum, *Spyboy*, promoted a tool they called *Terminator*, that was used to stop actively running EDR tools in an effort to circumvent detection. This tool was for sale for US$3,000 at the time and reverse engineers confirmed that it utilised a signed kernel driver file taken from the *Zemana Anti-Malware* program to perform privileged operations, which is commonly referred to as a Bring Your Own Vulnerable Driver (**BYOVD**) attack.

In early June, a GitHub user *ZeroMemoryEx* created a tool also named *Terminator* with the same functionality and published their source code on GitHub.

Within 3-5 days of the open-source release of *Terminator*, we observed Akira attempt to use this tool (as confirmed with a hash match to the tool on GitHub) to evade detection. We have also seen one prominent EDR agent and Windows Defender detect this program execution as malicious, with no apparent impact to the operation of the EDR agent.

Attacking the Hypervisor Layer

During other investigations we have typically seen threat actors execute their ransomware directly on the hypervisor, which will encrypt all of the files including virtual disk images stored in the various datastores. However, in other situations we believe the threat actor has seen an EDR tool in place, that is clearly capable of preventing their malicious program executions and even their EDR evasion has been successfully stopped. As a result, we've observed them deviating from their standard playbook and using a privileged account to launch a new, clean VM within the hypervisor.

From the threat actor's perspective, the benefit is that the VM they created has all the access needed to the network, and none of the security controls of another typical host on the same network.

After accessing the VM, the threat actor would disable Windows Defender, mount the data storage drives on the hypervisor, stop (shut down) VMs to release locked disk image files, and then execute the ransomware. While EDR tooling can detect that encryption has commenced, it is generally unable to block it as the process is executing on the VM, which would impact VMs in a shutdown state. As the attacker VMs are still running, they are not encrypted, which allowed forensic analysis to piece together the investigation.

The technique of using custom VMs is not new, and CyberCX has seen multiple investigations where a threat actor has built their own VM to conduct their malicious activities. Discussed at the end of this blog, you can find forensic artefacts and detection opportunities that may arise if you are running hypervisors in your environment or investigating a breach across hypervisors.

Analysts across the cybersecurity community have recently confirmed that a vulnerability existed within the Akira ransomware implementation. The decryption vulnerability relates to the use of a stream cipher (ChaCha20) that produces a fixed keystream per execution, which is then used for all files to be encrypted. This allows for the possibility of decryption without paying the ransom, however there are a few limitations. CyberCX confirmed the vulnerability and developed a working capability to decrypt encrypted data under certain circumstances shortly before the public release of the flaw by Avast.

Exploiting the vulnerability requires a file pair before and after encryption (plaintext and ciphertext), however you could only decrypt files smaller than the file pair. The first issue is identifying a valid pair, which can be difficult in cases where all backup data has also been encrypted.

One way to partially navigate this challenge is by identifying a file pair that could be sourced independently. In one case, we used several encrypted ISO files containing default installations of operating systems which were stored on a hypervisor (which is reasonably common in hypervisor datastores). Unencrypted versions of these are

often available from their official sources on the internet and can be used to generate the data needed. This solution has proven adequate for successfully decrypting small files on encrypted servers (specifically smaller than the ISO files). Unfortunately though, it may not be helpful in recovering what is often the most critical files on a hypervisor; large virtual hard disks.

However, as is common in ransomware encryption routines, threat actors rarely encrypt entire disks, each of which could be several hundred gigabytes in size, as this would be too slow. Instead, they often rely on intermittent encryption which only encrypts portions of large files, rendering them unreadable by tools, unable to be mounted cleanly, difficult to recover data from, and practically unusable. Another technique is to target file headers, being metadata stored at the beginning of most files. In these cases, we've seen ransomware actors only encrypting the first few MB of files targeting these file headers, but usually they also intermittently encrypt other portions of the file as well, to make recovery difficult to impossible, depending on the format of the file. SentinelOne produced an excellent article listing intermittent encryption options used by several ransomware variants.

In such cases, relying on available backups is the primary method of data restoration, and carving files and forensic artefacts from the non-encrypted portions of the affected virtual hard disks is the last resort.

"Just because files are encrypted doesn't mean that they're completely unrecoverable!"

CyberCX has significant experience investigating partially encrypted virtual hard disks – in some cases completely recovering the underlying data. Phill Moore recently presented a case study at the on an investigation involving recovering data from an encrypted virtual disk that allowed CyberCX to confirm the initial infection vector during a ransomware attack. Yogesh Khatri wrote an open-source tool – JARP that allows recovery of data from partially encrypted registry hives.

On 29 June 2023, Avast published a decryptor for Akira which utilised the same vulnerability identified above. By releasing the decryptor to the public, it also informed the owners of the ransomware.

An Akira ransomware sample that did not contain the vulnerability was uploaded to VirusTotal on 7 July 2023. The PE metadata recorded that it was compiled on 2 July 2023. This confirmed that within three days, Akira had patched the vulnerability and newer samples did not have the vulnerable code.[2]

As such, we anticipate that any new or recent Akira ransomware attack should be expected to use a newer ransomware variant which is not vulnerable to this weakness. However, any organisation who suffered an Akira ransomware attack prior to around 7 July 2023 and still has their encrypted data, may be able to use this weakness to decrypt their data.

CyberCX has also observed vSphere/ESXi environments being affected by ransomware in a way that would impact recovery. In some cases, threat actors apply different approaches to different ESXi hosts, even within the same network, including encryption through ransomware, changing the root password, or in some cases doing nothing to the hypervisor.

In cases where the threat actor did not (or perhaps could not) shut down the virtual machines, their disks were locked and would not be encrypted, however binaries on the ESXi host would still be encrypted. In these cases,

the remediation team has the opportunity to save the underlying VMs, but forensic analysis of the hypervisor would be impacted.

We also note that public reporting on a Linux variant of the Akira ransomware has recently been published.

1. Hyper-V Hypervisor Logging and Activities

CyberCX has compiled the following table of hypervisor event logs based on some validation testing that was performed on *Windows Server 2022*. It's worth noting that no logs are generated after creating a "checkpoint (snapshot)" for a VM and when attempting to "connect" to a VM.

Action Performed	Event ID	Channel	Provider
Created VM (Creation started)	18304	Microsoft-Windows-Hyper-V-VMMS-Admin	Microsoft-Windows-Hyper-V-VMMS
Created VM (Successfully Created)	13002	Microsoft-Windows-Hyper-V-VMMS-Admin	Microsoft-Windows-Hyper-V-VMMS
Started VM	12148	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-SynthStor
Started VM	18500	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Saved VM	18510	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Restoring VM	18596	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Exporting VM	18303	Microsoft-Windows-Hyper-V-VMMS-Admin	Microsoft-Windows-Hyper-V-VMMS
Pause VM	18516	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Resume VM	18518	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Turn Off VM	18502	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Reset VM (Using Hyper-V Manager)	18512	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker

Reset VM (Using Guest Operating System)	18514	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Shut Down VM (Using The Shutdown Integration Component)	18504	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Shut Down VM (Using Guest Operating System)	18508	Microsoft-Windows-Hyper-V-Worker-Admin	Microsoft-Windows-Hyper-V-Worker
Moved VM's Storage Location	20927	Microsoft-Windows-Hyper-V-VMMS-Admin	Microsoft-Windows-Hyper-V-VMMS
Deleted VM	13003	Microsoft-Windows-Hyper-V-VMMS-Admin	Microsoft-Windows-Hyper-V-VMMS

2. VMware ESXi / vSphere Logging and Activities

Virtual Machine Audit activity can be reviewed by logging onto the ESXi host utilising an administrator/root account. Activity is recorded in the "hostd.log" file found here:

- /var/log/hostd.log
- /var/run/log/hostd.log

Below is an extract from our test instance demonstrating the creation of a new virtual machine.

```
2023-07-25T07:29:57.870Z info hostd[2098947] [Originator@6876 sub=Vmsvc opID=esxui-46f0-93b4 user=Ev
 /vmfs/volumes/<VOLUME_ID>/MySecretVM/MySecretVM.vmx

2023-07-25T07:29:57.871Z info hostd[2098947] [Originator@6876 sub=Vimsvc.ha-eventmgr opID=esxui-46f0
```

Once the VM was created there was a state change from VM_STATE_INITIALIZING to VM_STATE_OFF.

```
2023-07-25T07:30:00.126Z info hostd[2098947] [Originator@6876 sub=Vmsvc.vm:/vmfs/volumes/<VOLUME_ID>
opID=esxui-46f0-93b4 user=EvilUser] State Transition (VM_STATE_INITIALIZING -> VM_STATE_OFF)

2023-07-25T07:30:00.127Z info hostd[2098947] [Originator@6876 sub=Vmsvc.vm:/vmfs/volumes/<VOLUME_ID>
/vmfs/volumes/<VOLUME_ID>/MySecretVM MySecretVM.vmx
```

When conducting forensics or incident response, you can collect these logs either through direct SSH access to the host or through generating a "support bundle" which includes the necessary logs from */var/log* on the host.

Blue teams should also consider enabling syslog to automatically forward these events to a SIEM or log aggregation platform.

Additional log locations can be found here.

3. Standard or Default Windows Workstation names leaked in Windows authentication logs

When a new Windows endpoint is setup, the hostname, if not manually assigned by the organisation will start with “WIN-“ or “DESKTOP-“ or “PC-“ or “WORKSTATION-“. Most ransomware actors we’ve seen use these defaults, which subsequently end up in event logs. A review of the Security authentication logs on Windows (Event ID 4624/4625) may show attempted or successful accesses. Furthermore, if these authentication attempts have an IP address from your VPN address pool, it may indicate that an unmanaged device is connected.

This may also be observed in Remote Desktop and SMB File share related event logs as well.

4. Audit infrastructure and ensure you have coverage of your security tooling

The CyberCX DFIR team commonly identifies initial access vectors or hives of threat actor activity around unmanaged hosts. Whether it is a test VM in Azure left open to the Internet, or an old “decommissioned” host that is left unpatched, ensuring you have proper visibility of these hosts will enable you to assess your risk.

Authors: Phill Moore and Zach Stanford with contributions from Suyash Tripathi and Yogesh Khatri

CyberCX Security, Testing and Assurance and Managed Security Services

[1] CyberCX assesses with medium confidence these credentials were obtained outside of the affected network.

[2] Akira has also made recent changes to their binary again, now going by “Megazord” – VirusTotal – File – c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
