# Aki-RATs – Command and Control Party

By Intrinsec

Published: 2023-11-28 · Archived: 2026-04-05 21:09:49 UTC

[et_pb_section fb_built="1" _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"] [et_pb_row _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"][et_pb_column type="4_4" _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"][et_pb_image src="https://www.intrinsec.com/wp-content/uploads/2023/12/akirat.jpg" alt="AkiRAT" title_text="akirat" _builder_version="4.23.1" _module_preset="default" hover_enabled="0" global_colors_info="{}" sticky_enabled="0"][/et_pb_image][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

## Context

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

During the first half of 2023, CERT Intrinsec handled several incidents involving Akira ransomware group. Companies detected ransomware’s presence, either by reacting to alerts triggered by their security solutions, or, in worst case, by encountering encrypted files on servers.

In all cases involving Akira’s recent operations, CERT Intrinsec’s analysis showed that the attack was divided into 3 phases. During the first phase, Akira affiliates get into the network by leveraging stolen passwords or by exploiting CVE-2023-20269 (Cisco ASA and FTD) vulnerability, allowing them to conduct brute-force attack on local password without being detected. They then perform discovery actions such as network or Active Directory scanning. They establish their persistence in the information system by installing remote access tools or by creating local and domain accounts. At that point, affiliates move laterally, using Remote Desktop Protocol, to different parts of the infrastructure before collecting data, exfiltrating them with WinSCP or Filezilla, and deleting their tracks to avoid detection. The second phase lasts several days: affiliates stay stealthy. They might be studying exfiltrated data or assessing technical data collected from the information system. During the last phase, attackers come back to set up their last persistence points, disable protections, try to destroy backups and delete volume shadow copies before running their encryption binary on targeted servers.

This article presents the intrusion set involved in Akira’s operations handled by CERT Intrinsec, its tactics, techniques and procedures, as well as recommendations to follow in order to avoid facing such an incident.

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## CERT Intrinsec presentation

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

CERT Intrinsec is a French incident response team that performs its operations mainly on France's sector. The team deals with about 50 major incidents per year and works to help its customers to recover from cyber-attacks and strengthen their security. Since 2017, CERT Intrinsec has responded to hundreds of security breaches involving companies and public entities. The majority of those incidents are related to cybercriminality and ransomware attacks with financial objectives, hence, CERT Intrinsec follows those groups activities and generates comprehensive intelligence from the field. ANSSI (French Cybersecurity Agency) granted CERT Intrinsec PRIS (State-Certified Security Incident Response Service Providers) certification. The latter testify that CERT Intrinsec meets specific incident response requirements, using dedicated procedures, qualified people and appropriate infrastructures. Should you need our expertises, Intrinsec provides Incident response & Crisis management services, Threat Intelligence services & datas, IOCs Feeds, Detection services (SOC/MDR/XDR), supported by a large set of other services (pentests & audits, consulting, …) .

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

## Akira Ransomware

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

Akira ransomware is said to have started operating in March 2023 and targeted more than 140 organisations (according to its leak site). Just like many other ransomwares, the Akira's encryption binary deletes volume shadow copies, targets specific file extensions and skip files located in some directories (such as ones containing system files). It seems that the encryption binary also shares obfuscation techniques with Conti ransomware. We can note that Akira appears soon after last operations spotted involving Conti ransom gang. Akira's intrusion set shares also many techniques with other Ransomware-As-A-Service (RaaS) actors: LSASS dumping for credential harvesting, creation of schedule tasks to perform discovery actions, usage of publicly available tools such as PCHunter64 or Advanced IP Scanner. They also heavily rely on RDP protocol with administrator accounts for lateral movement and also manage to disable common defenses such as Windows Defender. Akira recently developed a Linux encryptor to encrypt ESXi virtual machines, but CERT Intrinsec has not observed this encryptor so far.

Akira ransomware gang claimed multiple victims from different countries, especially the United States of America, the United Kingdom of Great Britain and Northern Ireland and Canada. Even if manufacturing, education, construction, retail and consulting are subject to many attacks, Akira compromised information systems from a wide range of sectors and does not seem to target any of them. CERT Intrinsec handled incident responses for which attacks were not claimed. This raises questions about genuine motivations of Akira ransomware gang.

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

## Akira Victimology

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

Victims analysis shows that majority of compromised companies are located in the USA (73%). United Kingdom and Canada follow with respectively 7% and 5% of referenced victims.

Regarding activity sectors, we have seen following trends:

- 14% of victims belong to manufacturing sector
- 11% in the education
- 9% construction and so on

Basically, all sectors are represented but in lower proportion.

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Key takeaways

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Investigations performed during Akira operations highlight that affiliates will use as many legitimate and living-of-the-land tools as possible, possibly to ensure EDR solutions bypass. For example, in one unique operation, we found at least 4 different command & control solutions such as AnyDesk, Teamviewer, OpenSSH Servers and MobaXterm. Moreover, in the first phase of the adversary’s operations, we notice adversaries efforts to stay relatively stealthy. They managed to tunnel their outgoing traffic through CloudFlare infrastructure, performed common reconnaissance tasks from servers where the EDR solution was not deployed, did not access to critical, and more likely supervised, infrastructure such as domain controllers. They conscientiously explored available file servers and managed to compress then exfiltrate data. They splitted exfiltration into multiple steps, exfiltrating data from a server before moving to another one.

The third part of operations, the encryption one, was marked by faster and “noisy” actions. Indeed, this phase took place in a few hours timeframe, during such they performed a new internal reconnaissance phase, moved laterally mainly on backup and virtualisation servers and finished by executing their encryption binary. Moreover, attackers performed many attempts to exfiltrate Active Directory information, performed multiple network scans with more or less success even from EDR monitored servers and also relied on tools such as Impacket, which can leave lots of characteristic footprints.

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Operation timeline

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

All Akira’s operations share a common characteristic: they took place in 3 different phases, from the start until the end of attacks.

- First days of the intrusion are dedicated to ensure persistance mechanism on a few assets, perform initial internal discovery and manage to escalate privileges. Then we observed a pause in the operations.
- The second phase is dedicated to valuable data identification, gathering and exfiltration. We usually observed a pause of several days before the last phase.
- Last phase, the encryption one, usually takes place during a short timeframe, within a few hours. Attackers manage to ensure their persistence on multiple assets, even if initial ones are already in place. They

perform new network scans, probably to get the list of assets required by the encryption. Affiliates usually tried to delete backups before running the ransomware binary on as many assets as possible.

The following diagram shows these 3 steps:

[/et_pb_text][et_pb_image src="https://www.intrinsec.com/wp-content/uploads/2023/11/attack_path.png" alt="Attack path" title_text="attack_path" _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"][/et_pb_image][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

Akira’s operation timeline

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Tactics, techniques and procedures

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Initial Access

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| External Remote Service | T1133 |
| Valid Account: Domain Accounts | T1078.002 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Adversaries got into the network by leveraging compromised credentials of legitimate accounts and establishing VPN sessions using them. Some of these accounts might have been compromised way before the incident. In two cases, attackers exploited CVE-2023-20269 vulnerability on a Cisco ASA VPN appliance. This vulnerability allows an unauthenticated attacker to conduct a brute-force attack on any local account while bypassing the maximum number of attempts defined.

In order to avoid the use of legitimate accounts as initial access, CERT Intrinsec recommends to:

- Ensure that internet facing solution, such as VPN appliances are patched in priority when security fixes are published by editors
- Enforce Multi-Factor Authentication on VPN solutions
- Apply the principle of least privilege when granting information system access to partners
- Review Active Directory objects to identify old, disabled or useless accounts, on a regular basis
- Enforce a strong password policy
- Raise users’ awareness of phishing emails and password reuse
- Ensure that no account with administrative privileges can connect directly into the VPN solution

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Execution

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Command and Scripting Interpreter: Powershell | T1059.001 |
| Command and Scripting Interpreter: Windows Command Shell | T1059.003 |
| Windows Management Instrumentation | T1047 |
| System Services: Service Execution | T1569.002 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Attackers leveraged PowerShell to execute commands to install Remote Server Administration Tools (RSAT-AD), to list domain users, computers and trusts. To do so, they used Get-ADUser and Get-ADComputer PowerShell cmdlets. They also created a new firewall rule to allow SSH traffic. To perform discovery and persistence actions, attackers leveraged Windows Command Shell as well as WMI via Impacket.

To spot PowerShell and Windows shell activities, you can implement the following measures:

- Enable PowerShell logging features (Transcript, ScriptBlockText, ConsoleHost_history)
- Enable Sysmon logging on devices
- Monitor equipments to detect execution actions, especially PowerShell and Windows Shell commands
- Improve detection means by building a Security Operations Center (SOC)

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Persistence

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Create or Modify System Process: Windows Service | T1543.003 |
| External Remote Services | T1133 |
| Create Account: Local Account | T1136.001 |
| Create Account: Domain Account | T1136.002 |
| Valid Accounts: Domain Accounts | T1078.002 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

They created multiple local and domain accounts, using the following Impacket commands, to make sure not to lose privileges if one of them is disabled or deleted.

cmd.exe /Q /c net user [ADMIN_USER] ‘[PASSWORD]’ /dom 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

cmd.exe /Q /c net user [ADMIN_USER] ‘[PASSWORD]’ /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

Attackers compromised legitimate accounts as well.

As explained previously, attackers used a lot of legitimate remote administration tools to maintain persistence on information system, they are usually configured as Windows Services. To detect such actions, you can:

- List legitimate remote administration tools, used by your company, to spot easily those used by attackers
- Restrict the use of these tools as much as possible
- Monitor actions performed by administrative accounts
- Monitor suspicious Windows Services creations

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Privilege Escalation

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Valid Accounts: Domain Accounts | T1078.002 |
| Valid Accounts: Local Accounts | T1078.002 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Throughout operations, attackers compromised several accounts, many of them being privileged. They then used them to gain even more privileges. These accounts were:

- Administrator accounts
- Unused administrator account
- Account used on printers
- Service provider account
- Monitoring account
- Accounting account
- Domain administrator account

Several accounts were compromised throughout the operation. It is possible to avoid such actions by implementing the following recommendations:

- Keep an inventory of accounts, especially administrative ones, up-to-date

- Forbid RDP communication between equipments when it is not necessary
- Deploy Windows Credential Guard to protect credentials on systems
- Use dedicated administrative accounts to perform actions related to information system administration only

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Defense Evasion

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Impair Defenses: Disable or Modify System Firewall | T1562.004 |
| Indicator Removal: File Deletion | T1070.004 |
| Modify Registry | T1112 |
| Valid Accounts: Domain Account | T1078.002 |
| Impair Defenses: Disable or Modify Tools | T1562.001 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

During operations, affiliates tried to impair defenses by either deleting evidences or avoiding detection. They actually removed part of their tools as well as the exfiltrated archives containing data.

After creating a malicious account, affiliates modified the following registry key in order to hide this account from the logon screen.

cmd.exe /Q /c reg add

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList

/t REG_DWORD /v [USER] /d 0 /f 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

They created a rule to enable SSH traffic, as explained in the Persistence section, and they edited the SYSTEM hive to enable RestrictedAdmin feature. This latter is a way to connect to a server without sending credentials to it. It prevents administrative credentials from being exposed to an attacker who could leverage them to escalate privileges.

The command used to enable **RestrictedAdmin** is as follows:

cmd.exe /Q /c reg add ‘HKLM\System\CurrentControlSet\Control\Lsa’

/v DisableRestrictedAdmin /t REG_DWORD /d 0 /f

Finally, attackers disabled Windows Defender Real-Time Monitoring feature.

In order to slow down forensic investigations and avoid detection, attackers conducted multiple actions. It is possible to detect those actions and to lower their impacts, by implementing the following measures:

- Collect logs from all equipments, forward them to a central server dedicated to logs storage
- Monitor firewall rules changes

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Discovery

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Account Discovery: Domain Account | T1087.002 |
| Remote System Discovery | T1018 |
| File and Directory Discovery | T1083 |
| Network Service Discovery | T1046 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

As operations were on their way, attackers kept looking for information on targeted systems. They used network scanning tools named *Netscan* and *Advanced IP Scanner* several times. They also browsed file servers, looking for interesting data to exfiltrate. They used Impacket commands and nltest built-in tool to perform some of their actions.

formatenumerationlimit = -1

Install-WindowsFeature RSAT-AD-PowerShell

Get-ADUser -Filter * -Properties * | Select-Object Enabled, CanonicalName, CN, Name,

SamAccountName, MemberOf, Company, Title, Description, Created,

Modified, PasswordLastSet, LastLogonDate, logonCount, Department,

telephoneNumber, MobilePhone, OfficePhone, EmailAddress, mail, HomeDirectory, homeMDB

> C:\ProgramData\AdUsers.txt

Get-ADComputer -Filter * -Property * | Select-Object Enabled, Name, DNSHostName, IPv4Address,

OperatingSystem, Description, CanonicalName,

servicePrincipalName, LastLogonDate, whenChanged, whenCreated > C:\ProgramData\AdComp.txt

nltest /domaintrusts

The above commands perform the following actions:

- Tell PowerShell to display all occurrences when formatting results
- Install Remote Server Administration Tools
- List all Active Directory users, all their properties and select several of them to display
- List all Active Directory computers, all their properties and select several of them to display

As discovery is often the first part of an intrusion set, it is crucial to detect it as early as possible to block subsequent phases of the attack. To do so, you should:

- Monitor security event logs and network connections to spot network scan activities, accounts enumeration, etc
- Monitor systems activities to detect commands executed to remote hosts

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Lateral Movement

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Lateral Tool Transfer | T1570 |
| Remote Services: Remote Desktop Protocol | T1021.001 |
| Remote Services: SMB/Windows Admin Shares | T1021.001 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Attackers used lateral movement techniques to transfer their tools across the network, to connect to devices and to execute commands on remote hosts. They utilised remote administration shares (ADMIN$) to drop files on remote computers and connects via Remote Desktop Protocol to different servers to achieve their malicious actions. Besides, Impacket was used to execute commands on remote systems with Windows Administration Share. Multiple hostnames were found as WorkstationName when attackers tried to authenticate to equipments:

- DESKTOP-3GCJKGQ
- WIN-KFUMVU06ESH
- WIN-OX9CQTDSEIK
- WIN-MV7S8OJTOIK
- HOST14872171171
- DESKTOP-KT76603

Attackers leveraged local accounts as well, adding them to **Administrators** and **Remote Desktop Users** groups, using **net localgroup** command:

net localgroup Administrators [USERNAME] /ADD

net localgroup ‘Remote Desktop Users’ [USERNAME] /add

net localgroup Administrators [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

net localgroup Domain Admins [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

net localgroup Remote Desktop Users [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1

They also used **Enter-PSSession** PowerShell command to start interactive sessions on remote devices and enable Remote Desktop Protocol, as shown below

Enter-PSSession -ComputerName [EQUIPMENT]

netsh advfirewall firewall add rule name=”allow RemoteDesktop” dir=in

protocol=TCP localport=3389 action=allow

During all operations, attackers easily moved from one equipment to another, and from one domain to another, especially leveraging network shares. To avoid such lateral movements, CERT Intrinsec recommends to:

- Monitor information systems to detect suspicious network share accesses (use of Impacket, network shares scan, etc)
- Restrict access to administrative shares as much as possible
- Build efficient isolation procedures to isolate a equipment, a VLAN or even the entire information system

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Collection

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Archive Collected Data: Archive via Utility | T1560.001 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

To reduce the size of data to exfiltrate and to make the process more efficient, affiliates used WinRar utility to create archives containing stolen data.

As ransomware operators often target information about human resources, employees, projects, etc, it is very important to:

- Identify sensitive data and its location, and encrypt it
- Deploy a Data Loss Prevention solution
- Monitor access to sensitive data

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Command and Control

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

| Technique | Technique ID |
|---|---|
| Application Layer Protocol: Web Protocols | T1071.001 |
| Ingress Tool Transfer | T1105 |
| Remote Access Software | T1219 |
| External Remote Services | T1133 |

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

Apart from using AnyDesk, TeamViewer, OpenSSH, MobaXTerm as Remote Administration Tools and Cloudflared to tunnel malicious traffic through the CloudFlare infrastructure, affiliates employed **file.io**, a file sharing service, to download their tools on compromised systems. They also leveraged VPN accesses to conduct their activities on the network.

You can implement the following measures to detect command and control activities:

- Monitor systems and network traffic to identify suspicious file sharing websites or illegitimate cloud services
- Install an Intrusion Prevention Solution to monitor traffic and find unusual remote hosts, flagged C2 domain/IP address/port, etc

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

### AnyDesk

[/et_pb_text][et_pb_text _builder_version="4.23.1" _module_preset="default" global_colors_info="{}"]

The first way to perform command and control activities is the installation of AnyDesk, a remote desktop application. The software was downloaded from **file.io** platform. Several files related to AnyDesk installation were discovered:

- C:\Users\[REDACTED]\Downloads\gcapi.dll
- C:\Users\[REDACTED]\Downloads\AnyDesk.exe
- C:\Windows\Temp\gcapi.dll
- C:\ProgramData\gcapi.dll

A service was also created to make sure that the persistence stays up:

| Service Name | Command |
|---|---|

| | |
|---|---|
| AnyDesk | C:\Program Files (x86)\AnyDesk\AnyDesk.exe –service |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

### SSH Server

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

An SSH server was installed on several servers in order to maintain the access to the information system by tunneling adversaries traffic through an SSH session. OpenSSH was used to create this SSH server and to be able to connect to compromised systems. CERT Intrinsec found evidences of OpenSSH in many directories:

- C:\Users\[REDACTED]\Downloads\OpenSSH.msi\
- C:\Program Files\OpenSSH\sshd.exe\
- C:\Users\[REDACTED]\AppData\Local\Temp\7\[redacted]\bin\ssh.exe\

The service runs **sshd.exe**:

| Service Name | Command |
|---|---|
| SSHD | C:\Program Files\OpenSSH\sshd.exe |

A firewall rule enabling SSH traffic was created as well on servers: its display name is **OpenSSH Server (sshd)**. The rule is enabled and allows the inbound traffic for protocol TCP on port 22.

New-NetFirewallRule -Name sshd -DisplayName ‘OpenSSH Server (sshd)’

-Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

### TeamViewer

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

TeamViewer was installed to allow access remotely to devices (**C:\Program Files (x86)\TeamViewer\TeamViewer.exe**), as well as to ensure persistence to them.

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

### MobaXTerm

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Attackers downloaded MobaXTerm, using an administrator account, on one of the domain controllers (**C:\Users\[REDACTED]\Downloads\MobaXtermInstallerv23.2.zip**).

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

### Cloudflared

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Attackers installed **Cloudflared**, a utility used to create tunnels between compromised hosts and Cloudflare solution. The command line to build a tunnel is as follows:

regid.exe tunnel run –token [TOKEN]

They renamed the cloudflared binary to **regid.exe** to hide in plain sight.

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Exfiltration

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | T1048.002 |
| Application Layer Protocol: File Transfer Protocol | T1071.002 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” hover_enabled=”0″ global_colors_info=”{}” sticky_enabled=”0″]

After creating archives containing collected files, affiliates used different softwares to exfiltrate several gigabytes of data: WinSCP and FileZilla.

FileZilla’s **recentservers.xml** file stores connection information and is very important to identify where data have been sent.

<?xml version=’1.0′ encoding=’UTF-8′?>

<FileZilla3 version=’3.64.0′ platform=’windows’>

<RecentServers>

<Server>

<Host>148[.]72.171.171</Host>

<Port>22</Port>

<Protocol>1</Protocol>

<Type>0</Type>

<User>Administrator</User>

<Logontype>2</Logontype>

<EncodingType>Auto</EncodingType>

<BypassProxy>0</BypassProxy>

</Server>

</RecentServers>

</FileZilla3>

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

For the past few years, adversaries heavily relied on cloud storage provider such as Mega or PCloud to store exfiltrated data. Akira’s operators behave slighly differently by uploading encrypted rar archives directly on their own servers (A Windows workstation with OpenSSH service installed on it). These servers are part of the same Autonomous System (**30083 – AS-30083-GO-DADDY-COM-LLC**), used throughout different operations.

As part of the double extortion strategy, attackers exfiltrate sensitive data from systems and threaten to publish it on their leak sites. Therefore, it is crucial to:

- Monitor outgoing traffic (in terms of volume, IP reputation, time of communication, etc)
- Improve network logging policy to ensure evidences availability in case of an investigation

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Impact

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Technique | Technique ID |
|---|---|
| Data Destruction | T1485 |
| Data Encrypted for Impact | T1486 |
| Inhibit System Recovery | T1490 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

Attackers tried to delete VEEAM backups by connecting to the management console and deleted Volume Shadow Copies using PowerShell commands:

powershell.exe -Command Get-WmiObject Win32_Shadowcopy | Remove-WmiObject

They finally encrypted equipments on the information system, using an Akira encryption binary.

To prevent victims from recovering their data, ransomware operators try to locate backups so as to delete them prior to encrypting files. To avoid this impact, CERT Intrinsec recommends to:

- Deploy a backup solution and test restoration process on a regular basis
- Keep at least one version of the backups outside the information system
- Monitor access to backup infrastructure

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## MITRE ATT&CK Matrix

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Tactic | Sub-Techniques | Technique ID |
|---|---|---|
| Initial Access | External Remote Services | T1133 |
| | Valid Account: Domain Accounts | T1078.002 |
| | Exploit Public-Facing Application | T1190 |
| Execution | Command and Scripting Interpreter: Powershell | T1059.001 |
| | Command and Scripting Interpreter: Windows Command Shell | T1059.003 |
| | Windows Management Instrumentation | T1047 |
| | System Services: Service Execution | T1569.002 |
| Persistence | Create or Modify System Process: Windows Service | T1543.003 |
| | External Remote Services | T1133 |
| | Create Account: Local Account | T1136.001 |
| | Create Account: Domain Accounts | T1136.002 |
| | Remote Access Software | T1219 |
| Privilege Escalation | Valid Accounts: Domain Accounts | T1078.002 |
| | Valid Accounts: Local Accounts | T1078.003 |

| | | |
|---|---|---|
| Defense Evasion | Impair Defenses: Disable or Modify System Firewall | T1562.004 |
| | Indicator Removal: File Deletion | T1070.004 |
| | Modify Registry | T1112 |
| | Valid Account: Domain Account | T1078.002 |
| | Impair Defenses: Disable or Modify Tools | T1562.001 |
| Credential Access | Brute Force | T1110 |
| | Unsecured Credentials: Credentials in Files | T1552.001 |
| Discovery | Account Discovery: Domain Account | T1087.002 |
| | Remote System Discovery | T1018 |
| | File and Directory Discovery | T1083 |
| | Network Service Discovery | T1046 |
| Lateral Movement | Lateral Tool Transfer | T1570 |
| | Remote Services: Remote Desktop Protocol | T1021.001 |
| | Remote Services: SMB/Windows Admin Shares | T1021.001 |
| Collection | Archive Collected Data: Archive via Utility | T1560.001 |
| Command and Control | Application Layer Protocol: Web Protocols | T1071.001 |
| | Ingress Tool Transfer | T1105 |
| | Remote Access Software | T1219 |
| | External Remote Services | T1133 |
| Exfiltration | Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | T1048.002 |
| | Application Layer Protocol: File Transfer Protocol | T1071.002 |

| | | |
|---|---|---|
| Impact | Data Destruction | T1485 |
| | Data Encrypted for Impact | T1486 |
| | Inhibit System Recovery | T1490 |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Indicators of Compromise

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Hostname

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Hostname | Comment |
|---|---|
| DESKTOP-3GCJKGQ | Hostname used by attackers to connect to compromised infrastructure |
| WIN-KFUMVU06ESH | Hostname used by attackers to connect to compromised infrastructure |
| WIN-OX9CQTDSEIK | Hostname used by attackers to connect to compromised infrastructure |
| WIN-MV7S8OJTOIK | Hostname used by attackers to connect to compromised infrastructure |
| DESKTOP-KT76603 | Hostname used by attackers to connect to compromised infrastructure |
| HOST14872171171 | Hostname used by attackers to connect to compromised infrastructure |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## IP Addresses

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| IP Address | AS | Location | Comment |
|---|---|---|---|
| 91[.]132.92.60 | 9009 – M247, RO | Danemark | Malicious VPN connections |
| 138[.]124.184.174 | 44477 – STARK-INDUSTRIES | United States | Malicious VPN connections |
| 148[.]72.168.13 | 30083 – AS-30083-GO-DADDY-COM-LLC | U.S.A. | Data exfiltration |

| | | | |
|---|---|---|---|
| 148[.]72.171.171 | 30083 – AS-30083-GO-DADDY-COM-LLC | United States | Malicious VPN connections and data exfiltration |
| 199[.]127.60.236 | 23470 – RELIABLESITE | United States | Malicious VPN connections |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Services

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Name | Command | Comment |
|---|---|---|
| AnyDesk | C:\Program Files (x86)\AnyDesk\AnyDesk.exe –service | AnyDesk Service |
| SSHD | C:\Program Files\OpenSSH\sshd.exe | SSH Server |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Commands

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Command | Comment |
|---|---|
| net user [ADMIN_ACCOUNT] [PASSWORD] /dom | Create an administrator account |
| Enter-PSSession -ComputerName [HOSTNAME] | Starts an interactive session with the remote server [HOSTNAME] |
| netsh advfirewall firewall add rule name=’allow RemoteDesktop’ dir=in protocol=TCP localport=3389 action=allow | Creates a rule enabling remote desktop protocol |
| cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Changes directory command executed by attackers |
| cmd.exe /Q /c net localgroup Administrators [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Adds USERNAME user to Administrators group |

| | |
|---|---|
| cmd.exe /Q /c net localgroup Domain Admins [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Adds USERNAME user to Domain Admins group |
| cmd.exe /Q /c net localgroup Remote Desktop Users [USERNAME] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Adds USERNAME user to Remote Desktop Users group |
| cmd.exe /Q /c net user [USERNAME] [PASSWORD] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Creates USERNAME user with password [PASSWORD] |
| cmd.exe /Q /c net user [USERNAME] [PASSWORD] /add 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Creates USERNAME user with password [PASSWORD] |
| cmd.exe /Q /c reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList /t REG_DWORD /v [USERNAME] /d 0 /f 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Hides USERNAME user from logon screen |
| powershell.exe -Command Get-WmiObject Win32_Shadowcopy \| Remove-WmiObject | Removes Volume Shadow Copies |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Registry Keys

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| Key | Value | Data | Comment |
|---|---|---|---|
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList | [USERNAME] | 0 | Key used to hide USERNAME user from logon screen |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Files

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

| IOC | Value | Comment |
|---|---|---|
| FileName | win.exe | Encryption Binary |

| | | |
|---|---|---|
| FileName | akira_readme.txt | Akira ransom note |
| FileName | WizTree.exe | WizTree (Disk Space Analyzer) |
| FileName | wiztree_4_14_portable.zip | WizTree (Disk Space Analyzer) |
| FileName | regid.exe | Cloudflare tunneling client |
| FileName | cloudflared.exe | Cloudflare tunneling client |
| FileName | Advanced_IP_Scanner.exe | Advanced IP Scanner (Network Scanner) |
| FileName | advanced_ip_scanner_console.exe | Advanced IP Scanner (Network Scanner) |
| FileName | Advanced_IP_Scanner_2.5.4594.1.exe | Advanced IP Scanner (Network Scanner) |
| FileName | advanced_ip_scanner.exe | Advanced IP Scanner (Network Scanner) |
| FileName | AdvancedPortScanner_2.5.3869.exe | Advanced Port Scanner (Network Scanner) |
| FileName | netscan.zip | Netscan (Network Scanner) |
| FileName | netscan.exe | Netscan (Network Scanner) |
| FileName | XWinMobaX1.16.3.exe | MobaXTerm (Remote Administration Tool) |
| FileName | AnyDesk.exe | Anydesk (Remote Desktop Software) |
| FileName | TeamViewer.exe | TeamViewer (Remote Access Software) |
| FileName | OpenSSH.msi | OpenSSH installer |
| FileName | sshd.exe | OpenSSH server |
| FileName | filezilla_3.64.0_win64_sponsored-setup.exe | FileZilla (FTP client) |
| FileName | WinSCP.exe | WinSCP (SFTP client) |
| FileName | WinSCP-5.21.8-Portable.zip | WinSCP (SFTP client) |
| FileName | winrar-x64-621.exe | Compression and archiving tool |

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

## Sources

[/et_pb_text][et_pb_text _builder_version=”4.23.1″ _module_preset=”default” global_colors_info=”{}”]

- https://twitter.com/MalGamy12/status/1651972583615602694
- https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

- https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/
- https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/
- https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/

[/et_pb_text][/et_pb_column][/et_pb_row][/et_pb_section]

---

Source: https://www.intrinsec.com/akira_ransomware/