TARX

AKIRA

Threat Actor Report

ABR 2024

XG3 UNIT

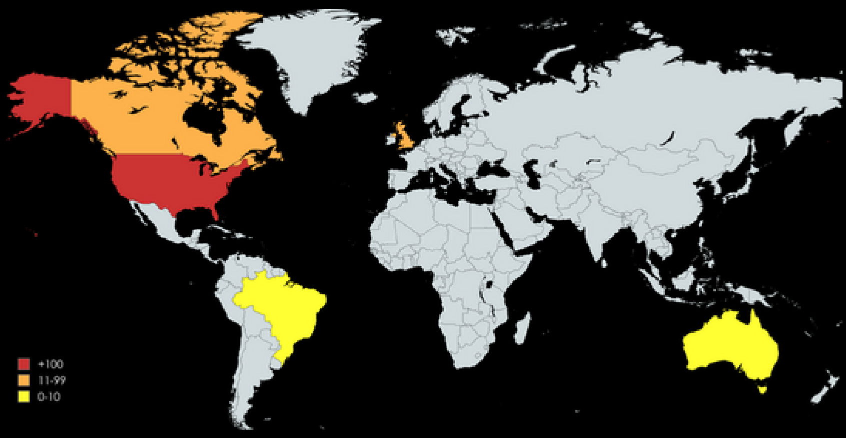
xMDR powered by Cipher

Akira Ransomware

09/04/2024
Last Seen

Ransomware
Type

Risk **Medium**
Risk



Education, Infraestructure, Health, Finance, Construction, Industrial, Transport, Services, Technology
Sectors

Medium
Sofistication

Financial gain
Motivation

10/04/2024
Last Update

MITRE Arsenal Used by Actor: 23.5%

Akira is a relatively new and fast-growing ransomware group that leverages the ransomware-as-a-service (RaaS) business model to deploy Akira ransomware. Akira extracts data before encrypting victims' devices and leverages it for double extortion. A notable peculiarity is that part of its code is based on the leaked source code of another ransomware known as Conti.

Akira Ransomware

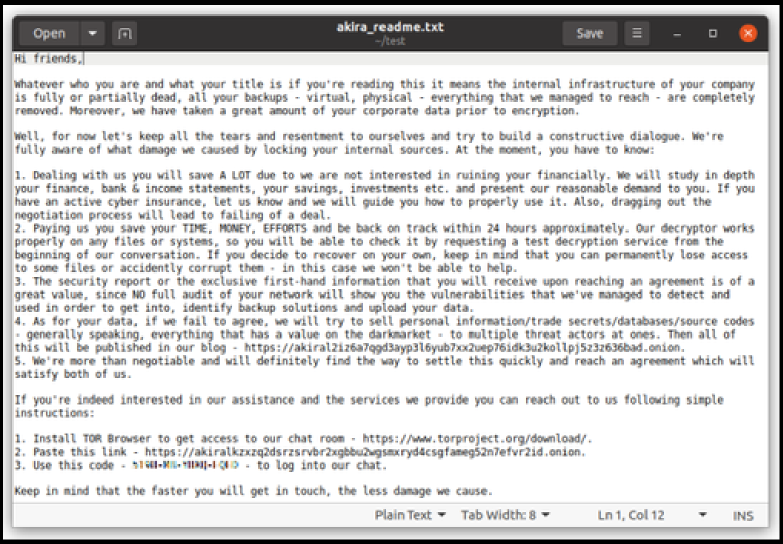
May 2022 saw the end of the ransomware gang known as CONTI. It is common that, when a group exits the market, its affiliates or workers go elsewhere, either by joining existing groups or by founding new ones.

A remarkable peculiarity of Akira is that part of its code is based on the leaked Conti source code. Therefore, the possible origin of the users who are part of Akira was in the previously existing giant.

Akira is a ransomware group first identified in March 2023. The group operating this ransomware has been active since then, running several campaigns that have impacted more than 200 victims, most of them located in the United States. Various industries, including services, education, finance, construction, healthcare, among others, have been affected by these attacks.

This ransomware makes use of double extortion where they not only encrypt data, but also exfiltrate sensitive information, threatening to sell it or leak it publicly on their website on the Tor network if the ransom demand is not met.

According to cybersecurity firm Artic Wolf, the Akira ransomware group deviates from the typical ransom model. Unlike others, they allow victims to choose between paying for decryption assistance or data deletion, rather than demanding both. However, failure to pay the ransom (which can range from $200,000 USD to over $4 million USD based on Artic Wolf's incident response experience) results in the victim's information being leaked on Akira's dedicated data breach website.



```
Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company
is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely
removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're
fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth
your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you
have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the
negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works
properly on any files or systems, so you will be able to check it by requesting a test decryption service from the
beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access
to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a
great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and
used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes
- generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of
this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will
satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple
instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.
3. Use this code - [redacted] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.
```

Akira Ransomware note: akira_readme.txt

Cryptographic process

Akira uses symmetric and asymmetric cryptography to encrypt files on its victims' computers. Specifically, when executed, Akira calculates a random encryption key and initialisation vector for the Chacha20 algorithm.

ChaCha20 is a stream cipher algorithm, which indicates that the encryption process is done bit-by-bit on a message or information to be encrypted. Stream cipher algorithms are private key algorithms, so the same key is required for encryption and decryption. These values are encrypted with RSA using a public key that is embedded in the code itself and changed by the actors for each victim. Unlike most ransomware, Akira calculates a single encryption key that is used to encrypt all files. Therefore, if this key is discovered, all files could be decrypted.

Group attack flow

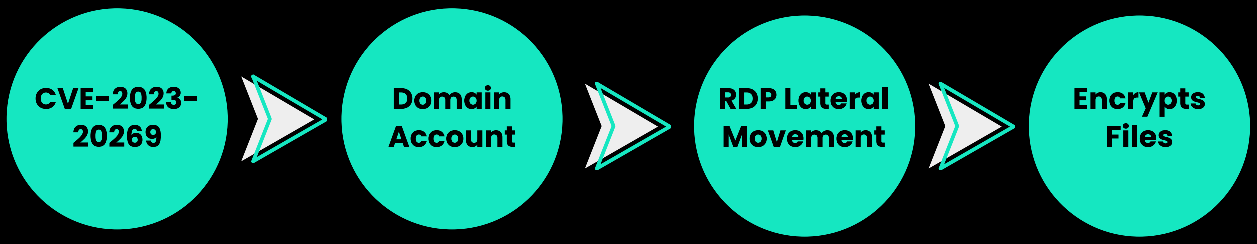
Initial access: gain access to victims' environments using valid credentials. Akira use compromised VPN credentials for initial access. They have also been observed attacking vulnerable Cisco VPNs exploiting CVE-2023-20269.

Persistence: actors create a new domain account on the compromised system.

Discovery: they use tools such as PCHunter and SharpHound, AdFind to gather information about the system.

Lateral movement: actors use Windows RDP as a tool for lateral movement in the victim's network together with the RClone web service, extracting stolen information.

Impact: the ransomware encrypts affected systems using a hybrid encryption algorithm combining Chacha20 and RSA.



CVE-2023-20269 → Domain Account → RDP Lateral Movement → Encrypts Files

APR 2024

Akira Attack Flow

Initial Access

- VPN Credentials
- CVE-2023-20269

Discovery

- PCHunter
- AdFind
- SharpHound
- MASSCAN

Persistence

- Create a new account

Credential Access

- Mimikatz
- LaZagne

Lateral Movement

- Windows RDP

Exfiltration

- Rclone
- FileZilla

Command and Control

- Anydesk
- Moba Xterm
- Cloudflare tunnel
- Radmin

Impact

- Exfiltration of information

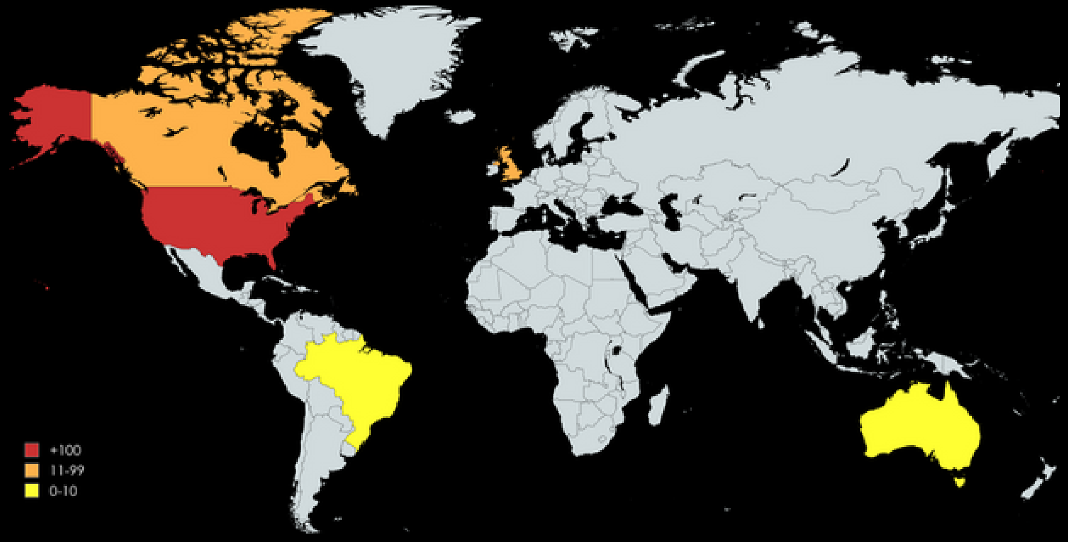
Akira Ransomware

Total Victims

231

Some data

Top Countries	Top Sectors	TOP Victims
USA-**153**	Services - **34%**	Sea Telecom
GBR - **13**	Manufacturing -**24%**	Vita IT
CAN- **12**	Education -**13%**	Brazilian Business Park
	Healthcare - **4,5%**	



Recent Victims

- **Ransom Victim:** Radiant Canada || Sector: Transportation || Country: Canada
- **Ransom Victim:** Control Technology || Sector: Manufacturing || Country: USA
- **Ransom Victim:** Lakes Precision || Sector: Manufacturing || Country: USA
- **Ransom Victim:** Santa Cruz Seaside || Sector: Tourism || Country: USA
- **Ransom Victim:** Mermet || Sector: Manufacturing || Country: USA
- **Ransom Victim:** Tanis Brush || Sector: Manufacturing || Country: USA
- **Ransom Victim:** Koi Design || Sector: Manufacturing || Country: USA
- **Ransom Victim:** European Centre for Compensation || Sector: Legal || Country: Poland
- **Ransom Victim:** Vita IT || Sector: Technology || Country: Brazil
- **Ransom Victim:** Calida || Sector: Real Estate || Country: Australia

Break the Rules

Detection rules are the culmination of research conducted by the more blue-team oriented segment of the **x63Unit**, focused on **preventing and detecting** malicious behaviors observed in actors, tools, campaigns, or vulnerabilities. This proactive approach is a testament to the unit's commitment to maintaining the highest standards of cybersecurity, constantly evolving to address the dynamic nature of cyber threats.

Detection Rules = 21

Rule Title | ARR | Tactics | Techniques | Severity

Main rules:

- Mimikatz detection by command line parameters | **80.0** | Credential Access, Defense Evasion, Lateral Movement | Credentials from Password Stores, OS Credential Dumping, Steal or Forge Kerberos Tickets, Use Alternate Authentication Material, Unsecured Credentials | Critical
- Deletion of shadow copies | **72.5** | Impact | Inhibit System Recovery | Critical
- File transfer over WinRM via Powershell | 68.0 | Lateral Movement | Exploitation of Remote Services | High
- Rclone utility detection by name or params | 62.5 | Exfiltration | Exfiltration Over Web Service | High

TOP Mitre TTP Covered:

- OS Credential Dumping
- Inhibit System Recovery
- Exploitation of Remote Services
- Account Discovery
- Credentials from Password Stores

🟥	90-100	*Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores*
🟧	70-90	*Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores*
🟨	50-70	*Rules with all or some of these features: Medium attack techniques, risky adversaries (or not related to any), trending (or not) Mitre TTPs, medium CVE scores*
🟩	0-50	*Rules with all or some of these features: Low attack techniques, not related to any adversaries, trending (or not) Mitre TTPs, low CVE scores*

Conclusion

Key Points:

- **Successor to Conti?** Akira ransomware, identified in March 2023, appears to have ties to the defunct Conti group. Parts of Akira's code share similarities with leaked Conti source code, suggesting potential involvement of former Conti affiliates.
- **Technical Breakdown:** Akira utilizes a hybrid encryption approach, combining ChaCha20 for stream encryption and RSA for public key encryption. Notably, a single encryption key is used, making decryption possible if discovered.
- **Initial Access and Movement:** They gain access through compromised VPN credentials and exploit vulnerabilities in Cisco VPNs (CVE-2023-20269). Once inside, they create domain accounts, use PCHunter and SharpHound for reconnaissance, and leverage Windows RDP and RClone for lateral movement and data exfiltration.

Upcoming:

- Can a decryption key be found? The use of a single key offers a glimmer of hope for future decryption efforts.
- Will law enforcement crack the code? Investigating Akira's origins and potential links to Conti could be crucial in disrupting their operations.

Overall:

The appearance of groups such as Akira confirms that member parts of groups that are disbanded simply find or found new working groups, so we must focus on individual actors.

Threat actor data available in xMDR Platform

TTP'S 46

Top 3 Most Relevant

- User Execution: Malicious File
- Phishing for Information: Spearphishing Attachment
- Boot or Logon Autostart Execution: Registry Run Keys /Startup Forlde

Rules 21

Top 3 Most Relevant

- Mimikatz detection by command line parameters
- Deletion of shadow copies
- File transfer over WinRM via Powershell

CVE's 1

- CVE-2020-3259 **(7.5)**

Tools Used 14

Top 3 Most Used By Actor

- Mimikatz
- Anydesk
- FileZilla

xMDR

ADVERSARIALLY

Threat Actor Report

APR 2024

cipher

a Prosegur company

LEGAL NOTICE: PROHIBITION OF DISTRIBUTION, USE OR SHARING WITHOUT AUTHORIZATION This document (hereinafter, “the Document”) is the exclusive property of Prosegur Ciberseguridad S.L. (hereinafter, “the Owner”). The Owner possesses all intellectual property rights associated with the Document, including, among others, copyright and property rights. Access to this Document is granted only to parties authorized by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorized use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior and express written authorization of the Owner is strictly prohibited. Any unauthorized use of the Document will constitute a violation of the Owner’s intellectual property rights and may result in legal action. Access and use of this Document are subject to the terms and conditions established by the Owner. Any authorized party that receives the Document must comply with the restrictions and obligations established by the Owner.
Any questions or requests for authorization for distribution, reproduction or use of the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.