JOINT ADVISORY BY THE CYBER SECURITY AGENCY OF SINGAPORE (CSA), SINGAPORE POLICE FORCE AND THE PERSONAL DATA PROTECTION COMMISSION (PDPC) SINGAPORE

JOINT ADVISORY ON AKIRA RANSOMWARE

The Cyber Security Agency of Singapore (CSA), the Singapore Police Force (SPF) and the Personal Data Protection Commission (PDPC) have received several reports from organisations affected by the Akira ransomware variant. This advisory provides information on Akira ransomware variant, observed Tactics, Techniques and Procedures (TTPs) employed by Akira affiliated threat actors to compromise their victims' networks and recommended measures for organisations to mitigate the threats posed. Information from this advisory is drawn from various sources, including but not limited to National CERT publications, open-source information, and threat intelligence reports.

Background of Akira

2 The Akira ransomware variant first emerged in March 2023. The Akira threat group operates as an affiliate-based ransomware[1] threat group, targeting both Windows and Linux systems under a "ransomware-as-a-service" (RaaS) model. The Akira threat group provides its software and infrastructure to cybercriminal groups (affiliates) in return for a percentage of any ransom paid by victim organisations.

3 The Akira threat group has been observed to target businesses and organisations worldwide across a variety of sectors including education, finance, manufacturing, and healthcare, with affiliates observed to be indiscriminate in their targets. Ransom amounts proposed will also be based on their study of the victim organisations' business profile.

Observed Tactics, Techniques and Procedures (TTPs)

<u>Initial Access</u>

4 Akira affiliates have been observed to leverage a range of techniques to gain initial access to a victim organisation's network. These techniques include:

- Exploit known vulnerabilities (e.g. Cisco VPN service without Multi-Factor Authentication (MFA) configured)
- Brute force external-facing services such as Remote Desktop Protocol (RDP)

- Deploy social engineering campaigns to trick victims into downloading malicious software that obtains user credentials or inputting their credentials on phishing websites
- Use compromised credentials that may have been obtained by the affiliate from access brokers

Persistence and Privilege Escalation

5 Akira affiliates have been observed to create a new domain account on the compromised system to establish persistence. Akira affiliates leverage post-exploitation attack techniques, such as Kerberoasting, to extract credentials stored in the process memory of the Local Security Authority Subsystem Service (LSASS). They also use credential scraping tools like Mimikatz and LaZagne to facilitate privilege escalation.

Discovery

6 Akira affiliates have been observed using specific tools to gain knowledge on the victim's system and its connected network, such as PCHunter and SharpHound to gather system information, AdFind alongside the net Windows command and nltest to obtain domain information. Advanced IP Scanner and MASSCAN are used to discover other remote systems for lateral movement.

Defence Evasion and Lateral Movement

7 Akira affiliates have been observed to use tools such as PowerTool or KillAV, that exploits the Zemana AntiMalware driver to terminate antivirus-related processes, as well as utilise Windows Remote Desk Protocol (RDP) to move laterally within the victim's network.

Exfiltration and Impact

8 Akira affiliates employs several methods to exfiltrate sensitive company information prior to encryption. These include the use of legitimate tools such as WinRAR, to split and compress data prior to exfiltration, FileZilla or WinSCP, which are File Transfer Protocol tools, or rclone, an open-source command line cloud storage manager which can be used with filesharing services like Mega.

9 Once data exfiltration is completed, Akira encrypts data using a hybrid encryption algorithm which involves combining a ChaCha20 with an RSA for speed and secure key exchange. Encrypted files are appended with either the .akira or .powerranges extension. Akira's encryptor, w.exe utilises PowerShell commands to delete volume shadow copies (VSS) on Windows systems to inhibit system recovery. Additionally, a ransom note named fn.txt will appear in both the root directory (C:) and users' directory (C:\Users).

10 The Akira ransom note typically includes a code unique to each victim along with instructions to contact the affiliates through a .onion URL. Ransom payments are requested in Bitcoin, which are directed to cryptocurrency wallet addresses specified by the affiliates. The TOR site (.onion) where victims contact the affiliates, contains stolen information and a list of the affected organisations.

Image 1 – Akira TOR site

11 Please refer to Annex A for observed TTPs employed by Akira affiliates mapped to the MITRE ATT&CK framework for Enterprise.

Indicators of Compromise (IOCs)

12 There are several IOCs observed to be associated with Akira. Please refer to Annex B for a list of IOCs and malware characteristics of Akira, which is updated as of April 2024.

Recommended Prevention and Mitigation Measures

13 Organisations are encouraged to implement and regularly monitor the compliance of the following mitigation measures and policies to strengthen their cybersecurity posture and reduce the risks and impact of a ransomware incident.

Use Strong Passwords and Multi-factor Authentication (MFA)

14 Organisations should use password policies requiring the use of strong passwords of at least 12 characters with upper and lower case letters, numbers, and special characters, and implement MFA to minimise the risk of unauthorised access to all internet-facing services (e.g. VPNs), and accounts that access critical systems.

Use Anti-Virus/Anti-Malware Software

15 Organisations should install reputable anti-virus/anti-malware software on their computers and networks to detect the presence of Akira or other ransomware variants. This can be done through real-time monitoring of system processes, network traffic, and file activity for IOCs typically associated with the malware. The software can be configured to block the execution of suspicious files, prevent unauthorised remote connections, and restrict access to sensitive files and folders.

Update and Patch Regularly

16 Organisations should periodically scan their systems and networks for vulnerabilities and regularly update all operating systems, applications, and software by applying the latest security patches promptly, especially for functions critical to the business. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented. For applications that have reached end-of-life (EoL), organisations are recommended to migrate to applications that are supported.

Review Settings on Exposed Services and Open Ports

17 Organisations should review exposed services and open ports such as RDP port 3389 and SMB port 445 in their network and restrict connections only to trusted hosts to prevent the spread of ransomware.

Implement Network Segregation or Segmentation

18 Organisations can consider implementing network segmentation that divides a larger network into smaller sub-networks with limited inter-connectivity between them. This will control traffic flow between the sub-networks, prevent lateral movement and limit the spread of ransomware, should one part be compromised. Implementing network segmentation also generates logs for traffic flow between various sub-networks. Organisations should monitor these logs for any suspicious activities and carry out remediation measures, where necessary. Organisations can also consider restricting Internet access (e.g. via blacklisting or whitelisting), using a risk-based approach, especially where there is direct access from endpoints to large amounts of personal or sensitive data. When these endpoints, such as employee laptops, are compromised, there is a higher risk of personal data being exfiltrated.

Maintain Routine Backups of Data

19 Organisations should implement routine backups to create and save copies of important files to external and offline storage devices. The backups should include immutable copies that will allow for system restoration in the event of a cybersecurity incident and minimise data loss. In addition, the backups should be regularly tested to ensure that the backup data can be recovered and restored in time to help the business recover from data corruption or destruction. Organisations are advised to follow the 3-2-1 rule when performing backups:

- 3 copies of backups
- 2 different media formats of backups
- 1 set of backups stored off-site

Develop Incident Response and Business Continuity Plans

20 Organisations should develop an incident response plan and conduct exercises to test the plan before an actual ransomware attack takes place, which will allow organisations to swiftly and decisively implement a plan to mitigate the situation. Organisations should also develop Business Continuity Plans (BCPs) with measures tailored to their needs to minimise the impact on business operations in the event of an attack.

Conduct Security Awareness for Employees

21 Organisations should educate employees and regularly remind them to be alert to phishing and other forms of social engineering tactics. Even with cybersecurity measures in

place, there may be instances of employees' careless actions which provide opportunities for cyber criminals to exploit.

22 Organisations can also conduct periodic security awareness training to help mitigate risks. Simulated phishing exercises are a well-established cybersecurity best practice and are widely considered to be effective as a type of experiential learning. These should complement existing employee education. Organisations should also put in place processes to regularly monitor the awareness and adoption levels of their employees.

Keep Essential Data Only

23 Organisations should only collect, process, store and retain data that are essential for business, operational or legal requirements. By only storing and retaining necessary data, the impact to an organisation due to a data breach can be minimised. Furthermore, additional resources required to protect these unnecessary data can be avoided by simply not collecting them in the first place. Some data minimisation practices include:

- Minimise collection of personal data
- Collect information on personal identifiers (e.g. national identification number) only when absolutely necessary
- Avoid continuous automatic collection of personal data
- Avoid repeatedly collecting the same data at different stages of an interaction
- Be aware of metadata (e.g. EXIF data in image files) embedded within files. Consider not collecting such data or removing them if not needed
- Be aware of caching information in temporary data stores and to regularly clear caches
- Ensure archival data past its retention period are diligently removed

Should you pay the ransom?

24 If your organisation's systems have been compromised with ransomware, we do not recommend paying the ransom and advise you to report the incident immediately to the authorities. Paying the ransom does not guarantee that the data will be decrypted or that threat actors will not publish your data. Furthermore, threat actors may see your organisation as a soft target and strike again in the future. This may also encourage them to continue their criminal activities and target more victims.

Additional Resources

One-Stop Ransomware Portal:
https://go.gov.sg/rwportal

SingCERT Ransomware Advisory:
https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/singcertadvisory-protect-your-systems-and-data-from-ransomware-attacks.pdf

SingCERT Ransomware Response Checklist:
https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/ransomwareresponse-checklist.pdf

PDPC Guides to Protect Against Data Breaches:
https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/howto-guard-against-common-types-of-data-breaches-handbook.pdf

https://www.pdpc.gov.sg/Help-and-Resources/2021/08/Data-Protection-Practicesfor-ICT-Systems

https://www.pdpc.gov.sg//-/media/Files/PDPC/PDF-Files/Other-Guides/Cloud-DataBreach-infographic-pdf.pdf?la=en

No More Ransom Initiative:
https://www.nomoreransom.org

MITRE ATT&CK Framework:
https://attack.mitre.org/matrices/enterprise

Other References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira
https://cyberint.com/blog/research/akira-ransomware-what-soc-teams-need-to-know/

Annex A - MITRE ATT&CK Techniques

The table below illustrates Akira's observed tactics and techniques mapped to the MITRE ATT&CK framework for Enterprise.

Technique	ID	Description
Initial Access		
Valid Accounts	T1078	Obtains credentials for valid accounts and abuses the credentials to gain initial access to victim networks.
Exploit Public Facing Application	T1190	Exploits vulnerabilities in internet-facing systems to gain access to victims' systems
External Remote Services	T1133	Exploits VPN/RDP to gain access to victim networks
Phishing	T1566	Uses phishing and spear phishing to gain access to victims' networks
Persistence		
Create Account: Domain Account	T1136.002	Establish persistence by creating new domain accounts
Privilege Escalation		
Exploitation for Privilege Escalation	T1068	noPac exploit was performed to escalate privileges
Defence Evasion		
Impair Defenses: Disable or Modify Tools	T1562.001	Use PowerTool or KillAV to disable antivirus software and/or disable Windows Defender
Credential Access		
OS Credential Dumping	T1003	Use tools like Mimikatz and LaZagne to dump credentials.
OS Credential Dumping: LSASS Memory	T1003.001	Attempt to access the contents of LSASS.exe
Discovery		
System Network Configuration Discovery	T1016	Use tools to scan systems and identify services running on remote hosts and local network infrastructure
System Information Discovery	T1082	Use tools like PCHunter64 to acquire detailed process and system information

File and Directory Discovery	T1083	Perform file and directory discovery
Domain Trust Discovery	T1482	Use the net Windows command to enumerate domain information
Process Discovery	T1057	Use the tasklist utility to obtain details on running processes via PowerShell
Permission Groups Discovery	T1069	Use the net localgroup /dom and/or net group /domain to find groups and permission settings
Remote System Discovery	T1018	Use nltest/dclist to list other systems by IP address, hostname, or other logical identifiers on a network
Network Service Discovery	T1046	Uses Netcat to listen on ports 443 and 902. Use to enumerate available machines on the hypervisor
Lateral Movement		
Remote Services: Remote Desktop Protocol	T1021.001	Uses remote-desktop software to facilitate lateral movement
Command and Control		
Remote Access Software	T1219	Uses AnyDesk to gain remote access to victim systems
Application Layer Protocol: File Transfer Protocols	T1071.002	Uses FileZilla for C2
Exfiltration		
Exfiltration Over C2 Channel	T1041	Use file transfer tools to transfer data over C2 channels
Exfiltration Over Alternative Protocol	T1048	Use file transfer tools to transfer data over unencrypted non-C2 protocol
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Uses RClone to sync files with cloud storage services to exfiltrate data.
Impact		
Data Encrypted for Impact	T1486	Encrypts data on target systems to interrupt the availability to system and network resources
Inhibit System Recovery	T1490	Deletes volume shadow copies residing on disk

Annex B - Indicators of Compromise (IOCs)

Akira Command Line Parameters

Parameters	Description
nltest /dclist	Remote system discovery
nltest /DOMAIN_TRUSTS	Domain trust discovery
net group “Domain admins” /dom	Group permission discovery (domain)
net localgroup “Administrators” /dom	Group permission discovery (local)
tasklist	Process discovery
rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full	Dumping credential from LSASS
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"	Remove volume shadow copies

Files Affiliated with Akira (SHA-256)

File Name	Hash (SHA-256)
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75

Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88
PowershellKerberosTicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0

Files Affiliated with Akira (MD5)

File Name	**Hash (MD5)**
w.exe	931a3fed5ca77da4648b55b97ff1610d
winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c

Akira Ransom Note (example)

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://akira[removed].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://akira[removed].onion.

3. Use this code - [removed] - to log into our chat.

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