SEQURETEK
SIMPLIFY SECURITY

Cyber Threat Advisory - SQTK/ADV/2024/0032

Akira Ransomware: An Update-IoCs

MALICIOUS FILES AFFILIATED WITH AKIRA RANSOMWARE

File Name	SHA 256 Hash	Description
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Akira ransomware encryptor
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Remote desktop application
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	DLL file that assists with the execution of AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Ngrok tool for persistence
Config.yml	Varies by use	Ngrok configuration file
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Exfiltration tool
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Network file transfer program
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Network file transfer program
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75	Akira_v2 ransomware
	0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc	Akira “Megazord” ransomware
	dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198	
	131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07	
	9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c	
	9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065	
	2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83	
	7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be	
	95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a	
	0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d	

File Name	SHA 256 Hash	Description
	C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Plaintext credential leaking tool
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	PowerShell script for obtaining and decrypting accounts from Veeam servers
PowershellKerberos TicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Kerberos ticket dumping tool from LSA cache
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	OpenSSH Backdoor
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	OpenSSH Backdoor
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Network scanner that scans IP addresses and ports
Win64 Executable	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360	

MITRE ATT&CK TACTICS AND TECHNIQUES

Technique Title	ID	Use
Reconnaissance		
System Information Discovery	T1082	Akira threat actors use tools like PCHunter64 to acquire detailed process and system information.
Remote System Discovery	T1018	Akira threat actors use nltest / dclist to amass a listing of other systems by IP address, hostname, or other logical identifiers on a network.
Resource Development		
Create Account: Domain Account	T1136.002	Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence.
Initial Access		
Create Account: Domain Account	T1136.002	Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence.
External Remote Services	T1133	Akira threat actors have used remote access services, such as RDP/VPN connection to gain initial access.
Phishing: Spearphishing Attachment	T1566.001	Akira threat actors use phishing emails with malicious attachments to gain access to networks.

Technique Title	ID	Use
Execution		
Windows Management Instrumentation	T1047	Akira threat actors create processes via WMI, connect to WMI namespace via WbemLocator, query process information (via WMI, Win32_Process), and delete volume shadow copies.
Impair Defenses: Disable or Modify Tools	T1562.001	Akira threat actors use BYOVD attacks to disable antivirus software.
Persistence		
Inhibit System Recovery	T1490	Akira threat actors delete volume shadow copies on Windows systems.
Privilege Escalation		
Exploitation of Vulnerability	T1210	Akira actors exploit known vulnerabilities in software or systems to gain elevated privileges and escalate their access within the target environment.
Defense Evasion		
Obfuscated Files or Information	T1027	Akira threat actors encode data using Base64, create new keys via CryptAcquireContext, and encrypt or decrypt via WinCrypt to obfuscate files or information.
Credential Access		
OS Credential Dumping	T1003	Akira threat actors use tools like Mimikatz and LaZagne to dump credentials.
OS Credential Dumping: LSASS Memory	T1003.001	Akira threat actors attempt to access credential material stored in the process memory of the LSASS.
Discovery		
Remote System Discovery	T1018	Akira threat actors use nltest /dclist to gather a listing of other systems by IP address, hostname, or other logical identifiers on a network.
Lateral Movement		
Remote Services: SMB/Windows Admin Shares	T1021.002	Akira threat actors may use SMB/Windows Admin Shares to move laterally within a network by accessing shared drives or folders on remote systems.
Collection		
Archive Collected Data: Archive via Utility	T1560.001	Akira threat actors use tools like WinRAR to compress files.
Command and Control		
Remote Access Software	T1219	Akira threat actors use legitimate desktop support software like AnyDesk to obtain remote access to victim systems.

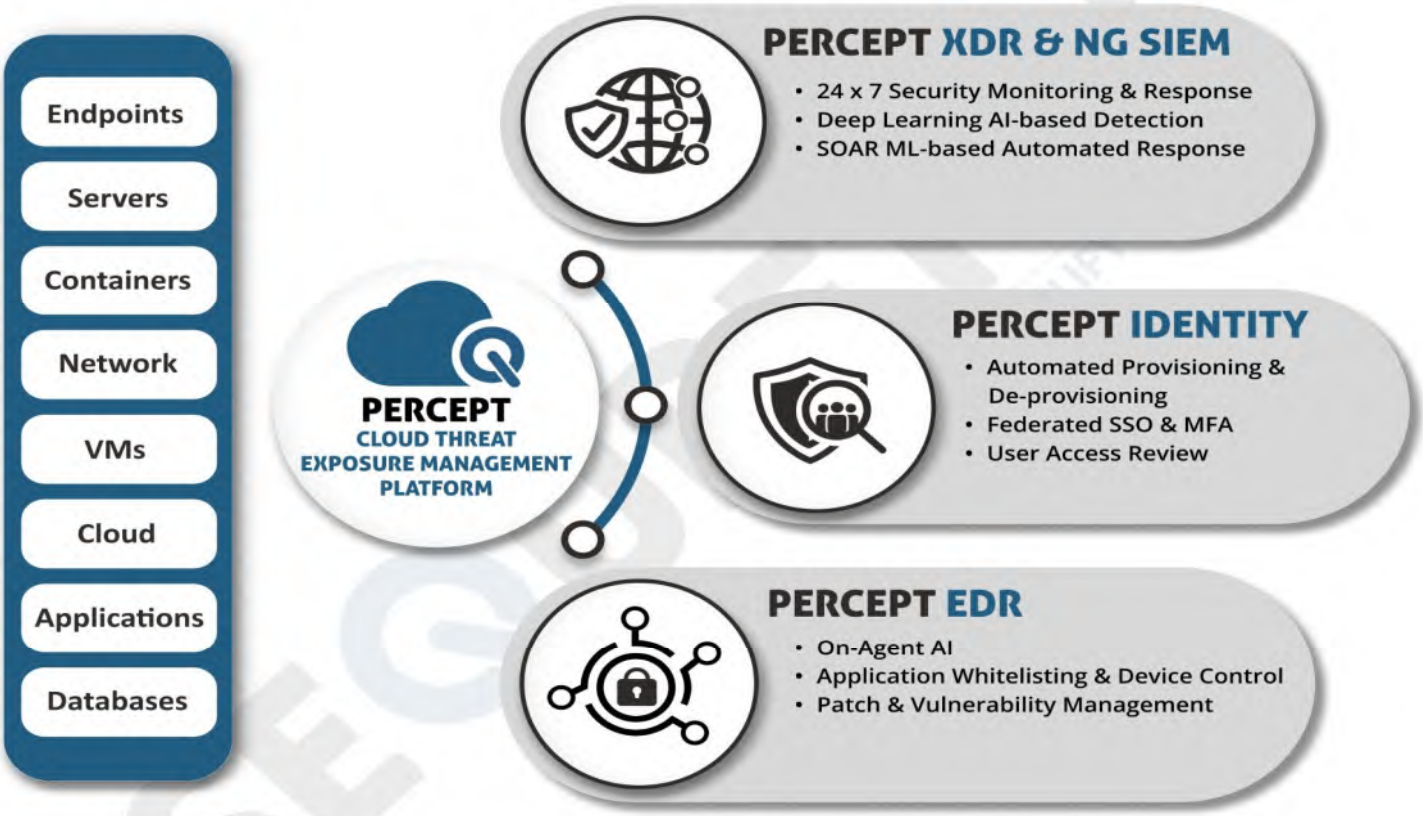
Technique Title	ID	Use
Proxy	T1090	Akira threat actors utilized Ngrok to create a secure tunnel to servers that aided in exfiltration of data.
Exfiltration		
Transfer Data to Cloud Account	T1537	Akira threat actors use tools like CloudZilla to exfiltrate data to a cloud account and connect to exfil servers they control.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Akira threat actors leveraged RClone to sync files with cloud storage services to exfiltrate data.
Impact		
Data Encrypted for Impact	T1486	Akira threat actors encrypt data on target systems and write a notice file (html or txt) to demand a ransom, impacting availability to system and network resources.

10 YEARS | SEQURETEK
SIMPLIFY SECURITY

Trusted by Global Customers, Investors, and Partners

About Sequretek

Sequretek is a global cybersecurity company that offers end-to-end security in the areas of enterprise threat monitoring, incident response, device security, identity & access governance through our own AI powered Percept Cloud Threat Exposure Management Platform.



Take Control of Your Enterprise Security

- Enterprise scale, easy to use, and cloud native
- AI-driven threat detection, protection, remediation, and response
- Quick implementation and integration capabilities
- End-to-End ownership and management of Sequretek products
- Reduced Total Cost of Ownership (TCO) while simplifying security
- Out-of-the-box reporting for compliance and audit purposes

Feel free to reach out to us at info@sequretek[.]com to know more about our products, or schedule a demo at https[:]//sequretek[.]com/request-a-demo/