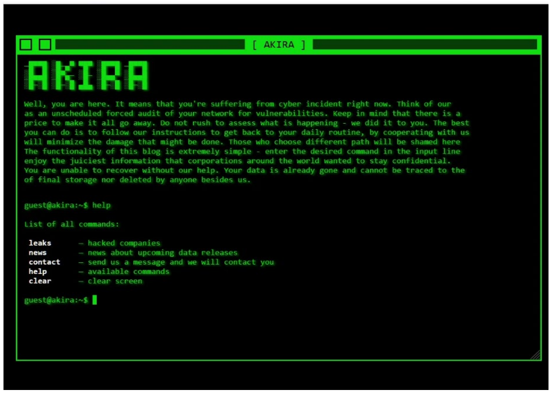
NIGC Tech Alert

AKIRA from Anime to Ransomware

Some may recall Akira, a famous Japanese manga and subsequent anime filmed in 1988 but set in a dystopian 2019. The plot of the film involves an individual who acquires telekinetic abilities after a motorcycle accident. Those abilities later threaten a military complex and spur a rebellion in a futuristic city of Neo Tokyo. At the time it was considered one of the best films made and garnered a massive following. Akira is back, not as a brilliant film but this time as an ominous ransomware attack.

The name Akira is no accident. Thinking about the eighties and technology of the time, green screen consoles were a thing. Now in 2023, the ransomware authors wish to mimic that fictionally created havoc and eighties retro-aesthetic, by physically creating havoc worldwide with ransomware. Akira ransomware has penetrated industries like finance, real estate, and manufacturing to name a few.



```
[ AKIRA ]
AKIRA
Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. The best
you can do is to follow our instructions to get back to your daily routine, by cooperating with us
will minimize the damage that might be done. Those who choose different path will be shamed here
The functionality of this blog is extremely simple - enter the desired command in the input line
enjoy the juiciest information that corporations around the world wanted to stay confidential.
You are unable to recover without our help. Your data is already gone and cannot be traced to the
of final storage nor deleted by anyone besides us.

guest@akira:~$ help

List of all commands:

 leaks      – hacked companies
 news       – news about upcoming data releases
 contact    – send us a message and we will contact you
 help       – available commands
 clear      – clear screen

guest@akira:~$
```

bleeping computer: Akira data leak site

Excerpt from screenshot

Well, you are here. It means that you're suffering from cyber incident right now. Think of our as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a price to make it all go away. Do not rush to assess what is happening – we did it to you. …Your data is already gone and cannot be traced to the of final storage nor deleted by anyone besides us.

The Akira ransomware will encrypt victims' files with an ".akira" extension and demand ransom for decryption. The malicious software can also delete Windows Shadow Volume (backup) copies from devices by running a command to prevent data recovery. The attackers can also disable antivirus software and other security tools on some devices, leaving desktops and/or networks open and extremely vulnerable.

According to experts with the Sophos Incident Response team -- in two identified incidents attackers used sophisticated methods to gain access to victims' networks. The attackers would first exploit a user account that was configured to bypass multi-factor authentication and access the account through an anonymized TOR VPN exit node. Next, the attacker used VPN to access the vulnerable local account with only single-factor authentication. Once inside, tools are used to escalate privileges, move laterally within the network, and exfiltrate data and deploy the Akira ransomware payload.

The significance of these type of attacks to Indian Country centers around the need for extra vigilance in assuring network infrastructures are being properly monitored and maintained. Some common practices for protection against Akira ransomware and similar threats include:

- Enabling MFA for ***all*** remote access (CFR 543.20(h)) accounts and audit any bypass exceptions
- Use of endpoint detection and response (EDR) solutions that can detect and block ransomware in real time
- Educating users about spotting and avoiding phishing emails and malicious attachments
- Keeping systems and applications updated with latest security patches

See Sophos article for additional context:
Akira Ransomware is "bringin' 1988 back" – Sophos News

NIGC Division of Technology:
NIGC Division of Technology | National Indian Gaming Commission

June 2023

Contact Us: ocio@nigc.gov