Emergence of Akira Ransomware Group

Eric Capuano

The Recon SOC recently worked an IR case involving the newly emerged Akira Ransomware Group. News didn't begin to break about this threat actor until May 7, 2023, but our investigation shows evidence this crew began this particular campaign in early-mid April.

When we began the IR, the targets of the ransomware activity were multiple VMware ESXi servers and a single Windows server. We moved quickly to get the environment into a defensible posture to prevent further spread of the ransomware itself.

About Akira

The Akira group surfaced around March of 2023. The group hosts a tor hidden service blog which contains entries for each organization it has hit, and allegedly, serves the files stolen from victims that did not pay the ransom.

Source: https[://]akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion

Additional References

- https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/
- https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

Observed TTPs

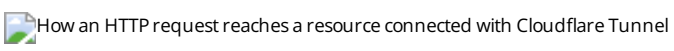
Installation of cloudflared for remote access into target environment

Description taken directly from Cloudflare's website:

> Cloudflare Tunnel provides you with a secure way to connect your resources to Cloudflare without a publicly routable IP address. With Tunnel, you do not send traffic to an external IP — instead, a lightweight daemon in your infrastructure (`cloudflared`) creates outbound-only connections to Cloudflare's global network. Cloudflare Tunnel can connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare. This way, your origins can serve traffic through Cloudflare without being vulnerable to attacks that bypass Cloudflare.

How it works

> Cloudflared establishes outbound connections (tunnels) between your resources and Cloudflare's global network. Tunnels are persistent objects that route traffic to DNS records. Within the same tunnel, you can run as many `cloudflared` processes (connectors) as needed. These processes will establish connections to Cloudflare and send traffic to the nearest Cloudflare data center


How an HTTP request reaches a resource connected with Cloudflare Tunnel

Multiple systems had services aimed at renamed copies of `cloudflared.exe`, a ZeroTrust networking agent, in locations such as

- `C:\ProgramData\VMware\VMware.exe`
- `C:\ProgramData\sun\sun.exe`
- `C:\ProgramData\GenPatch\GenPatch.exe`

Despite the renamed binaries, these executions are easily found by auditing process command line arguments looking for the following pattern

```
<renamed_binary>.exe tunnel run --token <attacker_cloudflare_token>
```

This daemon connects the victim system to an attacker-controlled software-defined network, similar to a VPN. With this tunnel, the attacker could connect directly to this system, even if they lose other footholds into the network.

Generally, cloudflared expects a configuration file, but in these instances, the configuration information was passed directly on the command line which makes even the renamed binaries detectable with the right telemetry. We dissected the token being passed to the binary and learned it consists of the following components

```
{"a":"ACCOUNT_ID","t":"TUNNEL_UUID","s":"TUNNEL_SECRET"}
```

Network enumeration with netscan.exe

The attacker leveraged the free Netscan tool to perform network sweeps and discover open ports on hosts. This tool was also used to directly launch RDP sessions on discovered systems.

This tool has previously been leveraged by other groups as well.

Credential theft via Mimikatz

The attacker leveraged mimikatz to obtain credentials on at least one system.

Credential theft via DonPAPI

Adversary was observed leveraging the open source DonPAPI credential theft toolkit which is capable of "Dumping relevant information on compromised targets without AV detection." This required dropping Python on the victim host as well.

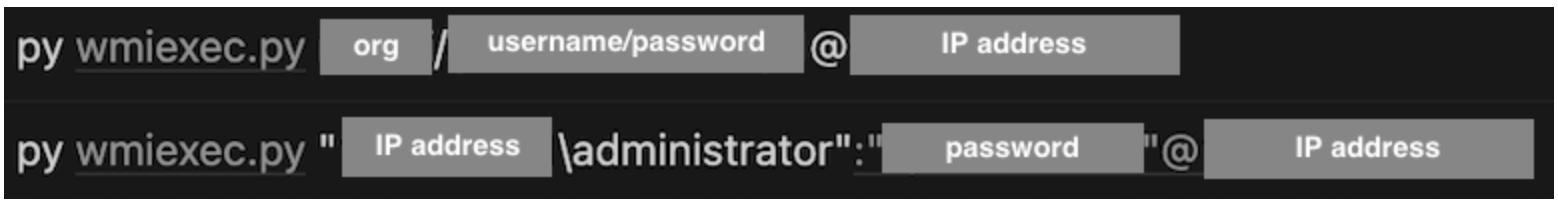
Targeted credentials include:

- Windows credentials (Taskscheduled credentials & a lot more)
- Windows Vaults
- Windows RDP credentials
- AdConnect (still require a manual operation)
- Wifi key
- Internet explorer Credentials
- Chrome cookies & credentials
- Firefox cookies & credentials
- VNC passwords
- mRemoteNG password (with default config)

Lateral movement with Remote Desktop

The attacker was observed using RDP almost exclusively to move around the environment. This was accomplished with multiple compromised administrator accounts due to a combination of credential harvesting and weak passwords.

Lateral movement with wmiexec.py



Sleeper account created on Domain Controller

The attacker created an account on a compromised domain controller that followed a naming convention very similar to the domain name to likely make it blend in. For instance, if the domain name was `abdef.com`, the account was named `abcdfe`.

Network shares enumerated via net use

The actor quickly identified network shares in the environment and mounted them via CLI using stolen credentials. Once shares were mounted, they were accessed via Explorer and many files were copied to a staging location on the system actively in-use by the actor.

Targeted files included many related to insurance, income statements, and various other business-related documents.

Multiple compression tools introduced to file staging system

The attacker dropped several compression utilities onto the desktop of the compromised system, likely via the RDP session. Tools include 7zip, WinRAR, etc.

SSH utilized to access ESXi to encrypt VMFS stores

Leveraging a combination of stolen or weak passwords, the attacker was able to SSH onto multiple ESXi servers to encrypt the underlying file system which housed all virtual systems.

Disabling Microsoft Defender with Defender Control

Actor was observed tampering with MS Defender with Defender Control.

Deletion of Volume Shadows

The win_locker executable deletes volume shadows with the following command

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

This is observable in process command line auditing. Any deletion of VSCs should trigger an alert in most well monitored environments.

Ransomware of Windows system using win_locker executable

The naming convention of the encryptor on the Windows system followed this pattern: `win_locker_1234-ab-cdef-ghij.exe` -- the actual numbers and letters following `win_locker_` have been obscured in this post because they correspond to the unique ID assigned to this victim that is also used in the negotiation steps with the adversary.

Here is a VirusTotal report on the sample, including IOCs. As of the time of this post, it was only detected by **31 of 69 antivirus engines**.

The encryption routine drops `akira_readme.txt` in nearly every directory on the system. Contents of the readme below

Other tools dropped by threat actor

- google-chrome-portable-112-0-5615-87.exe
- WinSCP
- Python

Defense Guidance

- **Properly segment networks**
  - This actor was able to move effortlessly across multiple corporate sites due to lack of network access controls or segmentation.
- **Retire weak or shared passwords**
  - The environment had a well-known, and insecure password shared across many systems and stored insecurely in multiple locations.
  - Deploy LAPS in legacy environments, or leverage the newly integrated LAPS in modern environments.
- **Implement auditing of privileged accounts** to detect unauthorized activities, such as limited-scope contractors accessing out-of-scope machines during non-working hours.
- **Enable Microsoft best practices for Audit Policies** to enable critical telemetry for detection and investigating a breach.
  - Just as important -- ensure you are centralizing these logs somewhere secure so they are available for detection & response efforts.
- **Ensure that Volume Shadow Service is enabled and running** on all critical systems, and ensure that it has a reasonable amount of room to grow. VSS provides a file restoration feature which could be critical in a ransomware recovery, however this is why it is almost always an attacker TTP to delete them prior to encryption. Therefore, you must also:
  - Protect volume shadows by auditing for anomalies around VSC tampering or deletion. For inspiration, see the Yara rule that powers Raccine.
  - Most modern EDR solutions can be configured to detect this activity and terminate the offending process which could be a last-ditch effort to stop an otherwise undetected ransomware execution in progress. This capability is deployed by default across all of our MDR customer systems.
- **Implement blocking of unauthorized tunneling/remote access tools** such as Cloudflare ZeroTrust, ZeroTier, TailScale, and others. These tools are likely to gain popularity by threat actors for gaining covert access to compromised networks.

Want to be Secure with Confidence?

If you are looking to bring new levels of confidence to your enterprise security, consider partnering with Recon and leveraging our Managed Detection & Response offering. You will gain full access to our team of analysts for consistent advisory services in addition to our phenomenal SOC-as-a-Service capabilities.

Incident Response, Intel Sharing, ransomware

Read On

An Encounter with Ransomeware-as-a-Service: MEGAsync Analysis

Analysis of Exploitation: CVE-2019-3396

The Recon incident response team recently worked an intrusion case

Analysis Of Exploitation: CVE-2020-10189

The Recon incident response team recently worked an intrusion case

Recon's SOC recently responded to an attempted ransomware and extortion attack. It had all the...

involving a Confluence web...

involving a ManageEngine Desktop...