Best Practices
AKIRA Precautions

Regular Backups:

Maintain regular and multiple backup copies of all critical data and ensure that these backups are not accessible for modification or deletion from the systems where the data resides.

Update and Patch Systems:

Keep all systems, including network device firmware, operating systems, and software, up to date with the latest security patches to prevent exploitation of known vulnerabilities.

Antivirus and Anti-Malware Solutions:

Use reputable antivirus and anti-malware programs and keep their signatures up to date.

Email Filtering and Scanning:

Implement email gateways that can scan emails for malicious attachments and links..

Network Segmentation:

Divide the network into segments to prevent the spread of ransomware if one segment is compromised and ensure that (Network Access Control) is allowing only necessary network inter-communication between segments.

Access Controls:

Implement the principle of least privilege, ensuring users have the minimum level of access required to perform their duties.

Akira specific IOC
This Trend Micro article on the Akira ransomware approach is a great starting point for understanding Indicators Of Compromise (IOC) for this particular threat.

Security Training and Awareness:

Educate users about the risks of phishing emails, suspicious attachments, and links. Regular training can help prevent accidental clicks on malicious content.

Disable Macro Scripts:

Disable macro scripts from office files transmitted over email and consider using Office Viewer software to open Microsoft Office files transmitted via email..

Remove or Disable Unnecessary Software:

Remove unnecessary software, services, and protocols to reduce potential attack vectors..

Strong Password Policies:

Enforce the use of strong passwords and consider using multi-factor authentication (MFA) wherever possible.

Secure Remote Access:

Use VPNs and ensure that any remote desktop access is secure and limited.

Incident Response Plan:

Have a ransomware incident response plan ready to implement in the event of an attack.

Monitor ingress:

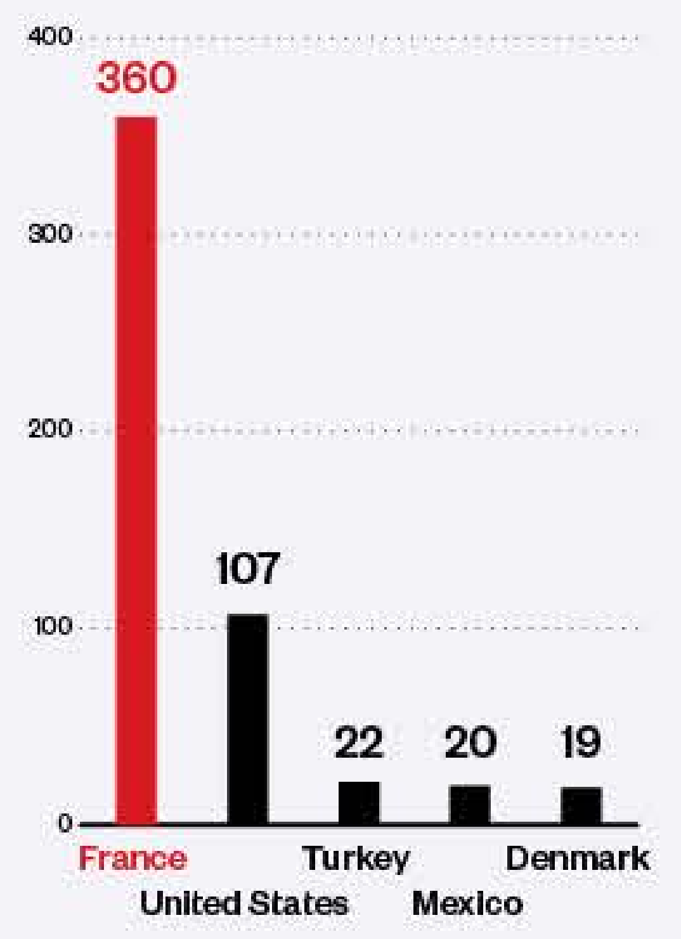
Pay attention to ingress logs and note traffic from unfamiliar addresses for follow-up and analysis.

RANSOMWARE SPOTLIGHT Akira

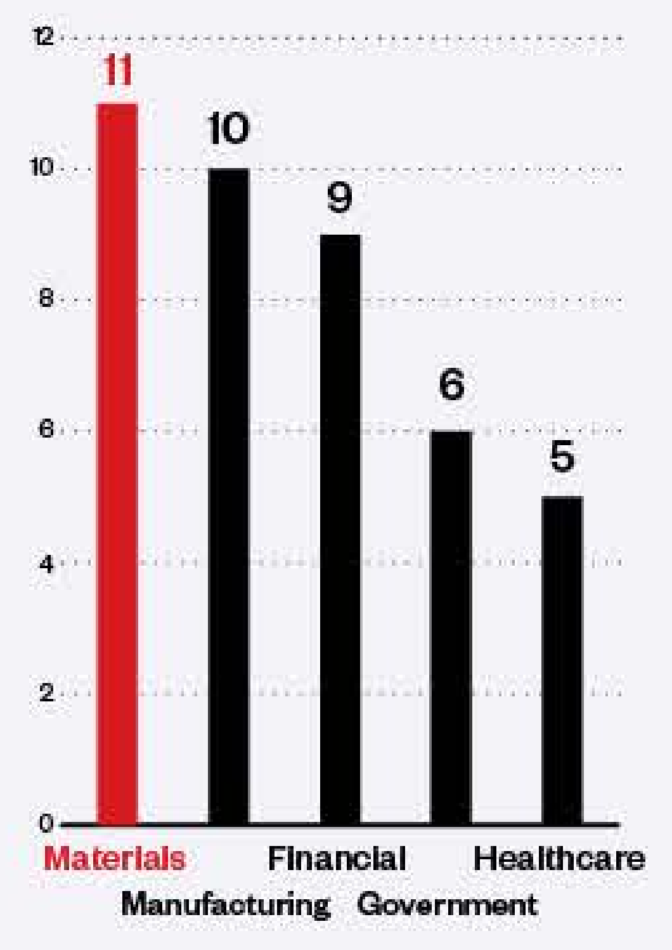
Despite being relatively new after its emergence in March 2023, the Akira ransomware is swiftly becoming one of the fastest-growing ransomware families thanks to its use of double extortion tactics, a ransomware-as-a-service (RaaS) distribution model, and unique payment options. It has been known to target companies based in the US and Canada.

Akira Ransomware Detections

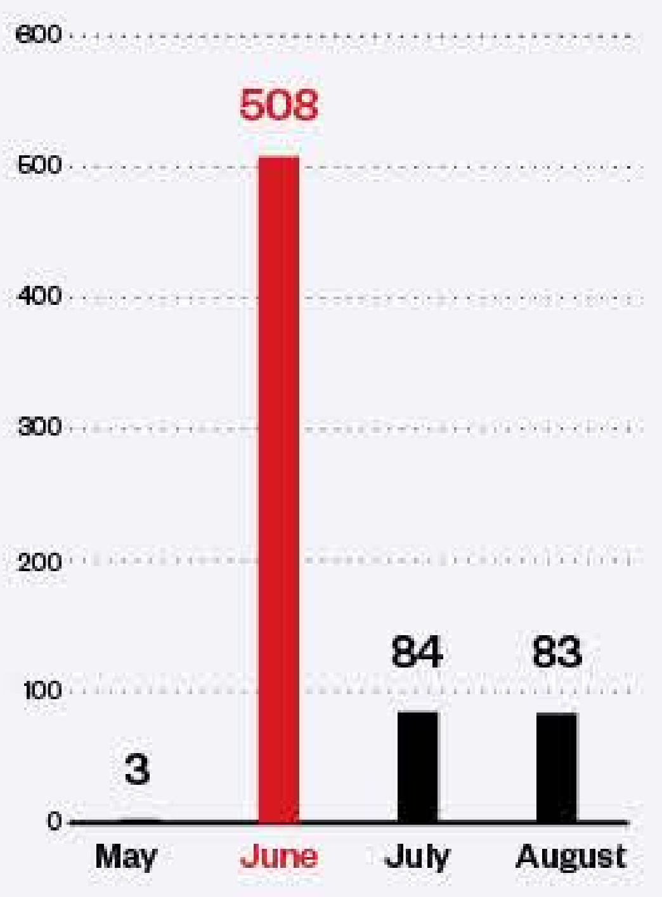
France had the most Akira ransomware attack attempts at 360 detections, followed by the US at 107.*



Materials, manufacturing, and financial businesses are the sectors that had the highest Akira-related detections.*



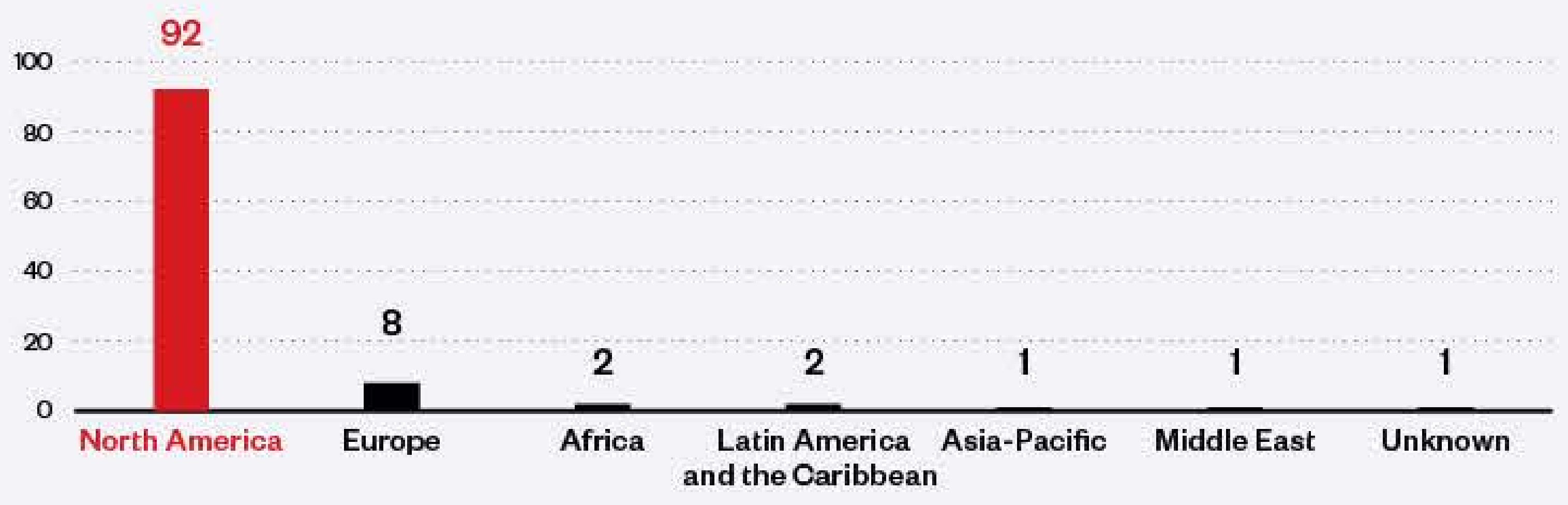
Akira detections surged in June 2023 with 508 attack attempts, a major jump from just three attempts detected in May.*



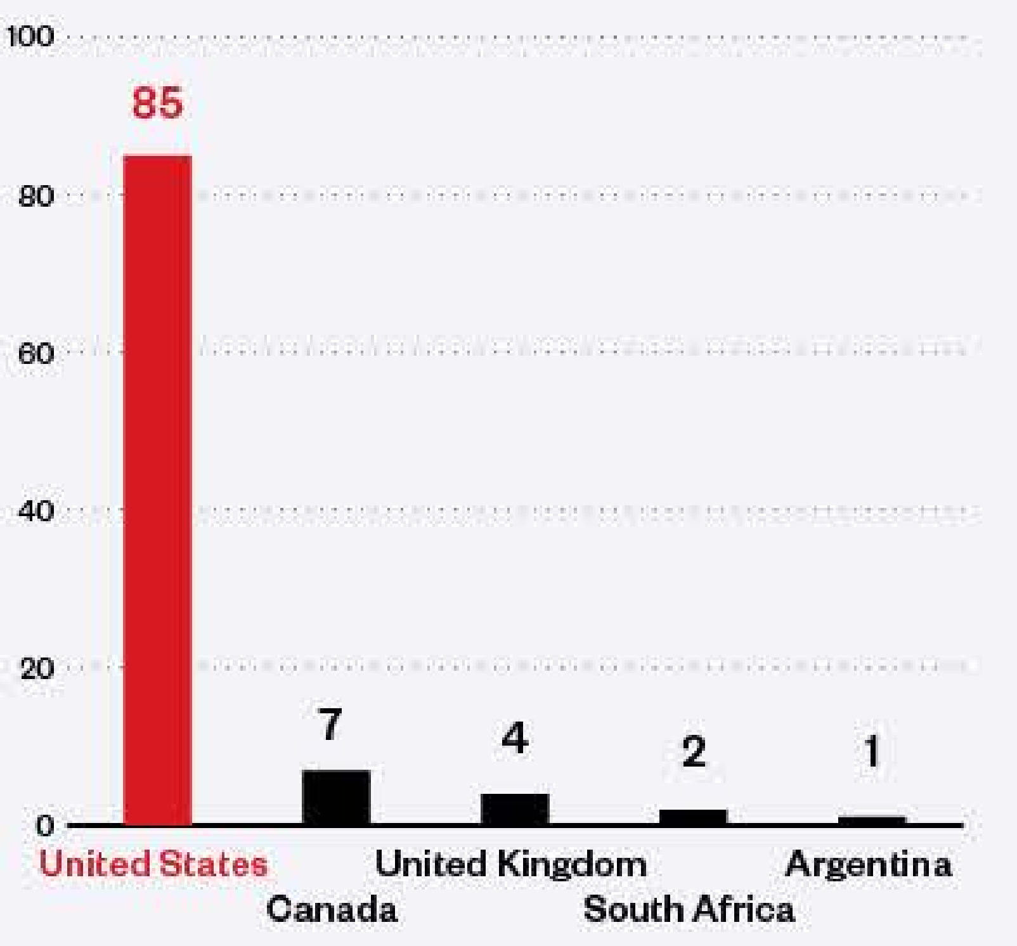
*Based on data gathered through the Trend Micro™ Smart Protection Network™ (SPN) detections per machine from May 1, 2023, to August 31, 2023

Akira Leak Site Data

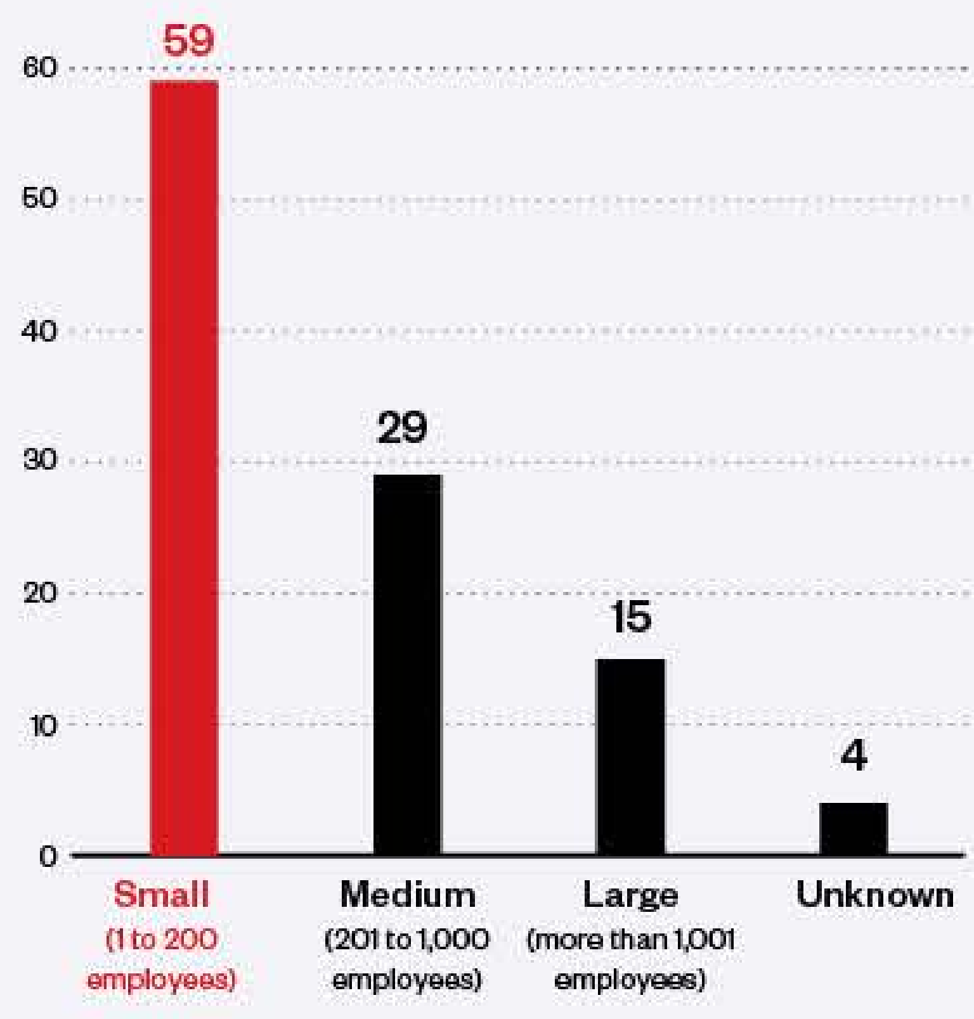
Akira operators compromised a total of 107 organizations between April 1 to August 31, 2023. 85.9% of Akira's victims were organizations based in North America.*



The countries with the most Akira ransomware victims were the US, Canada, and UK, with 79.4%, 6.5%, and 3.7% of victims, respectively.



Most of Akira's victims were small-sized businesses, with 1 to 200 employees, at 59 victims.*

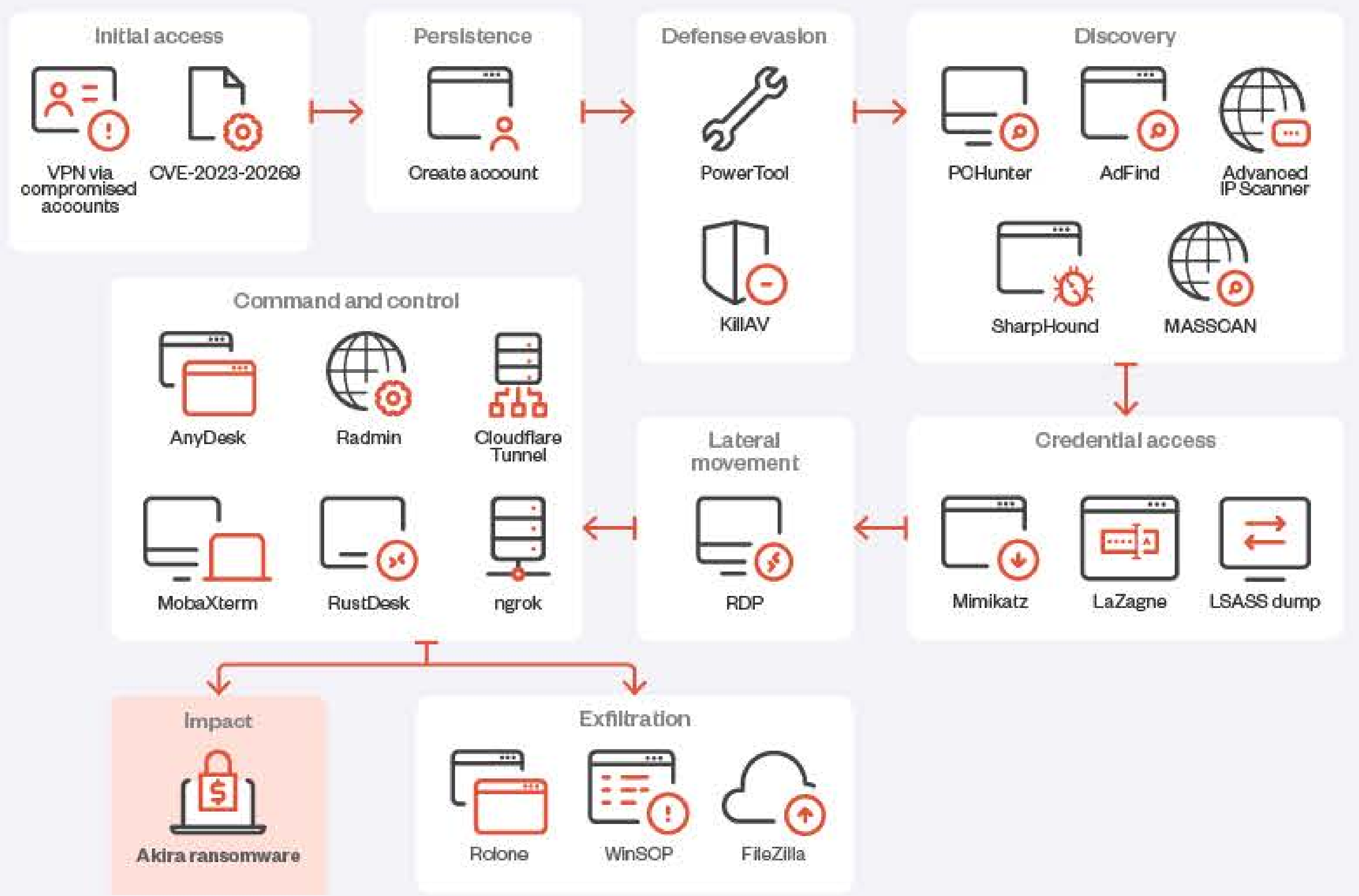


*Based on consolidated data of Trend Micro's open-source intelligence (OSINT) research and investigation of Akira's leak site from April 1, 2023, to August 31, 2023

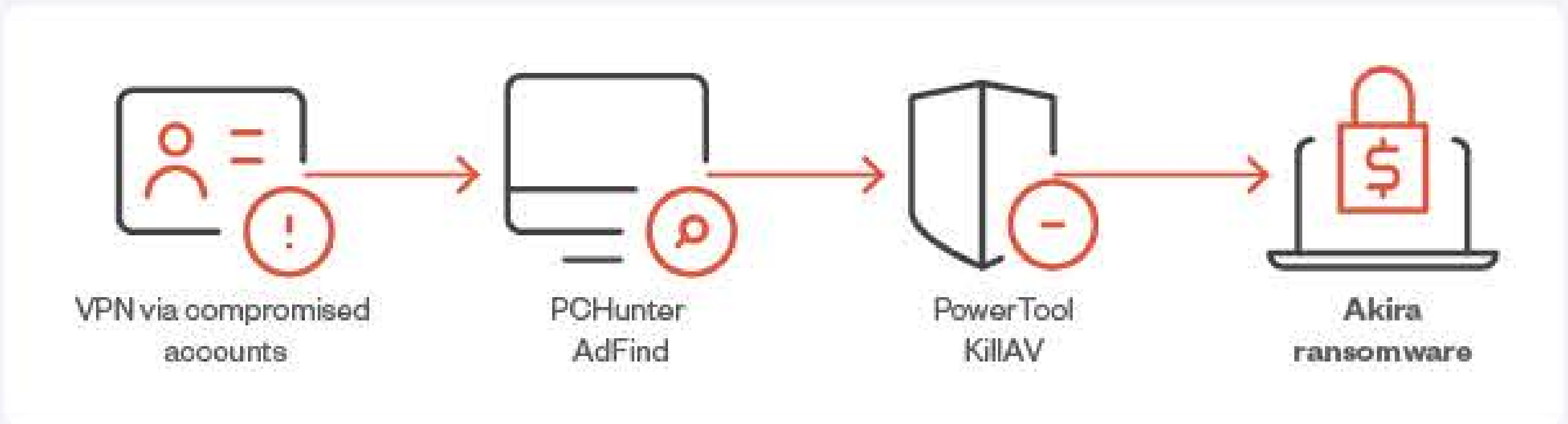
Infection Chain and Techniques

The Akira ransomware typically gains access to victim environments by using valid credentials that were possibly obtained from their affiliates or other attacks.

The typical Akira ransomware infection chain looks like this:



Meanwhile, this is what the infection chain of an Akira ransomware case that we've analyzed looks like:



Initial Access

Akira ransomware actors are known to use compromised VPN credentials to gain initial access. They've also been observed to target vulnerable Cisco VPNs by exploiting CVE-2023-20269, a zero-day vulnerability that affects Cisco ASA and FTD.

Persistence

Akira operators have been observed creating a new domain account on the compromised system to establish persistence.

Defense Evasion

For its defense evasion, Akira ransomware actors have been observed using PowerTool or a KillAV tool that abuses the Zemana AntiMalware driver to terminate AV-related processes.

Discovery

The actors behind the Akira ransomware have been observed using the following to gain knowledge on the victim's system and its connected network:

- PCHunter and SharpHound to gather system information
- AdFind alongside the net Windows command and nltest to obtain domain information
- Advanced IP Scanner and MASSCAN to discover other remote systems

Credential Access

Akira ransomware operators use Mimikatz, LaZagne, or a specific command line to gather credentials.

Lateral Movement

Akira actors use Windows RDP to move laterally within the victim's network.

Command and control

To gain remote access on other targeted systems, malicious actors may use any or a combination of the following tools:

- AnyDesk
- Radmin
- Cloudflare Tunnel
- MobaXterm
- RustDesk
- Ngrok

Exfiltration

Akira ransomware operators have been observed using the third-party tool and web service RClone to exfiltrate stolen information. Moreover, they have also been observed using either FileZilla or WinSCP to exfiltrate stolen information via File Transfer Protocol (FTP).

Impact

Akira ransomware encrypts targeted systems using a hybrid encryption algorithm that combines Chacha20 and RSA. Additionally, the Akira ransomware binary, like most modern ransomware binaries, has a feature that allows it to inhibit system recovery by deleting shadow copies from the affected system.

In addition,

Here is a Excel File with the set of hashes we are using to identify Akira activity:

View File