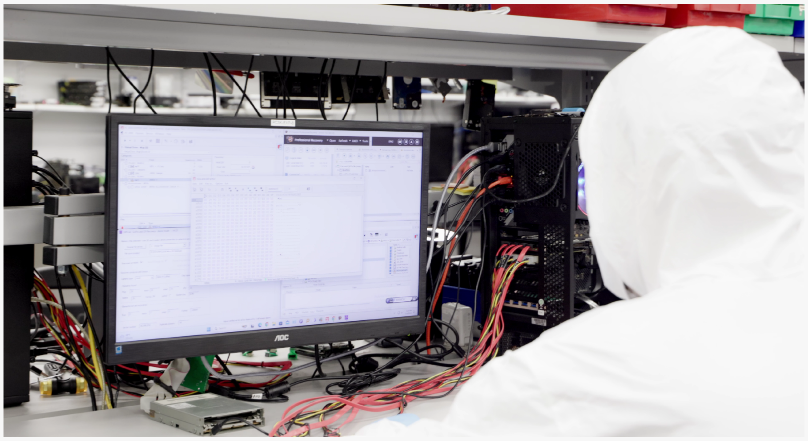
EINPRESSWIRE

Proven Data Announces Advisory Amid Rising Akira Ransomware Threats

Cybersecurity firm outlines steps to protect vulnerable industries from escalating cyberattacks



Proven Data's data recovery lab

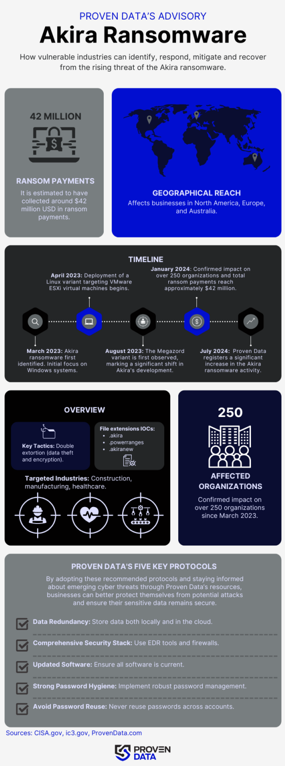
CLEVELAND, OH, UNITED STATES, October 16, 2024 /EINPresswire.com/ -- Proven Data, a leader in incident response services, ransomware recovery, and digital forensics, has released guidelines to help businesses protect themselves from Akira ransomware attacks. Based on internal data and third-party sources, Proven Data experts have observed a rise in Akira-related incidents since July 2024. The most vulnerable industries include construction, manufacturing, and healthcare.

> “
> Large companies, or those handling personally identifiable or health information, are particularly at risk and frequently face network penetration attempts.”
>
> *Chris Morrissey, account manager at Proven Data*

Akira, a ransomware variant first identified in March 2023, is known for its double extortion tactics. Attackers steal sensitive data before encrypting it, then demand a ransom not only to prevent the release of the stolen data but also to provide a decryption key to restore access to files.

“Our data is largely based on U.S. trends, but a review of Akira ransomware reports indicates increasing activity in both the United States and Europe,” says Chris Morrissey, account manager at Proven Data. “Large companies, or those handling personally identifiable or health information, are particularly at risk and frequently face network penetration attempts.”

According to CISA.gov, since March 2023, Akira ransomware has impacted a range of businesses and critical infrastructure across North America, Europe, and Australia. In April 2023, the group behind Akira expanded its attacks by launching a Linux variant that targets VMware ESXi virtual machines. The group has affected over 250 organizations and is estimated to have collected around $42 million (USD) in ransom payments. However, as of October 7, 2024, Akira's payment negotiation site has been offline, leaving victims unable to even attempt to pay the ransom to retrieve their data.



PROVEN DATA'S ADVISORY

Akira Ransomware

How vulnerable industries can identify, respond, mitigate and recover from the rising threat of the Akira ransomware.

42 MILLION

RANSOM PAYMENTS

It is estimated to have collected around $42 million USD in ransom payments.

GEOGRAPHICAL REACH

Affects businesses in North America, Europe, and Australia.

TIMELINE

March 2023: Akira ransomware first identified. Initial focus on Windows systems.

April 2023: Deployment of a Linux variant targeting VMware ESXi virtual machines begins.

August 2023: The Megazord variant is first observed, marking a significant shift in Akira's development.

January 2024: Confirmed impact on over 250 organizations and total ransom payments reach approximately $42 million.

July 2024: Proven Data registers a significant increase in the Akira ransomware activity.

OVERVIEW

Key Tactics: Double extortion (data theft and encryption).

File extensions IOCs:
- .akira
- .powerranges
- .akiranew

Targeted Industries: Construction, manufacturing, healthcare.

250

AFFECTED ORGANIZATIONS

Confirmed impact on over 250 organizations since March 2023.

PROVEN DATA'S FIVE KEY PROTOCOLS

By adopting these recommended protocols and staying informed about emerging cyber threats through Proven Data's resources, businesses can better protect themselves from potential attacks and ensure their sensitive data remains secure.

☑ **Data Redundancy:** Store data both locally and in the cloud.

☑ **Comprehensive Security Stack:** Use EDR tools and firewalls.

☑ **Updated Software:** Ensure all software is current.

☑ **Strong Password Hygiene:** Implement robust password management.

☑ **Avoid Password Reuse:** Never reuse passwords across accounts.

Sources: CISA.gov, ic3.gov, ProvenData.com

PROVEN DATA

Proven Data Advisory Against Akira Ransomware

In response to the growing threat, Proven Data's cybersecurity team has outlined five key protocols to help businesses defend against Akira ransomware:

1) Data redundancy: Ensure data is stored both locally and in the cloud. Even systems with strong endpoint monitoring can be compromised.

2) Comprehensive security stack: Implement a full suite of Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) tools, alongside a well-maintained firewall.

3) Updated software: Use supported and up-to-date software (e.g., Windows Server 2016 will receive security updates until January 12, 2027).

4) Strong password hygiene: Focus on robust password management, especially for Active Directory/Domain Controllers.

5) Avoid password reuse: Never reuse passwords across multiple accounts.

For more information on emerging cyber threats and prevention strategies, visit Proven Data's blog.

ABOUT PROVEN DATA
Proven Data is a leading provider of comprehensive incident response (DFIR) services, data recovery, and digital forensics. Founded in 2011, the company has consistently evolved to meet its clients' growing needs in the face of increasingly sophisticated cyber threats. The Ohio-based service provider's expert cybersecurity team offers comprehensive protection, damage mitigation, and investigative services for ransomware, data breaches, and employee misconduct. Acquired by Porthas Inc. in 2023 and under new leadership, Proven Data leverages enhanced resources and technology while delivering expert solutions and maintaining strict privacy policies. To learn more, visit https://provendata.com/.

Nicole Blake-Baxter
The Blake Agency
+1 678-957-7675
nicole@blakepragency.com
Visit us on social media:

Facebook
LinkedIn