RocketCyber
A Kaseya COMPANY

How RocketCyber Stopped Akira Ransomware for ITPartners+

The threat of ransomware will forever continue to be one of the biggest adversaries for businesses everywhere, regardless of size. It has become a preferred means of cyberattack.

RocketCyber, a managed detection and response (MDR) service, demonstrates superior capability in identifying and mitigating advanced threats, including ransomware in all its forms. This whitepaper explores RocketCyber's response to a ransomware attack experienced on a holiday weekend by our MSP partner, ITParters+. The incident involved Akira ransomware, a type of malware that was originally discovered early in 2023. This whitepaper details the attack, response actions and customer experiences.

Understanding Akira ransomware

Akira ransomware, first identified by the Computer Emergency Response Team (CERT-In), employs a sophisticated encryption algorithm to delete volume shadow copies and file-locking techniques to lock a victim's data, demanding a ransom for decryption keys.

It often spreads through phishing emails, exploiting vulnerable Remote Desktop Protocol (RDP) connections and utilizing stolen credentials. Once inside a network, Akira rapidly encrypts data, causing significant operational disruption until the ransom is paid or the data is recovered.

For detailed information on Akira ransomware, refer to the CISA Cybersecurity Advisory.

Incident overview

On Thursday, May 23, 2024, at 4:59 AM, RocketCyber's automated systems detected an initial Indicator of Compromise (IOC) associated with Akira ransomware. The ransomware detection app immediately terminated the malicious process and isolated the affected system to prevent further spread.

Detailed response actions

Upon detection of the ransomware, RocketCyber's SOC team received automated notifications and executed immediate isolation commands across the network. Devices that did not isolate automatically were manually isolated using historical alert data.

The process involved:

Identifying compromised accounts and processes.

Isolating affected devices using RocketCyber and Datto EDR tools.

Preventing the ransomware from accessing shared drives and spreading to other devices.

Our proprietary Ransomware Detection App played a crucial role in identifying and stopping the attack. It utilized real-time detection to kill the malicious process, keeping the threat at bay until further investigation.

A look into the customer's experience

Initial discovery and response

Casey Postma, the Cybersecurity Lead at ITPartners+ describes waking up early that Thursday before the U.S. Memorial Day holiday and discovering the emergency ticket. RocketCyber's quick automated response mitigated the initial threat, isolating the machines and stopping the ransomware's spread.

> ***"I woke up an hour before my alarm and decided to check my email,"*** **said Postma.** ***"I found an emergency ticket from RocketCyber. Their swift action isolated the machines, stopping the ransomware in its tracks."***

Postma highlighted the efficiency of RocketCyber's systems, noting that the response time was within minutes from the initial encryption attempt. This immediate action prevented further damage and allowed for quick containment and remediation.

Detailed customer recovery timeline

Chad McDonald, CTO of ITPartners+, part of the customer's IT team, praised the responsiveness and support provided by RocketCyber during the incident. He emphasized that the collaborative effort and rapid information exchange were crucial in managing and resolving the crisis effectively.

Thursday, May 23, 2024:

- **4:59 AM:** Initial IOC detected by RocketCyber.
- **5:00 - 5:15 AM:** Devices isolated, and an in-depth investigation commenced. RocketCyber created a ticket for the managed security operations center (SOC) communication and to track actions taken for the customer's records.
- **6:03 AM:** The SOC analyst sent an email summarizing initial findings and actions taken to ITPartners+
- **Throughout the day:** Continuous monitoring and additional isolation actions as needed.

Friday, May 24, 2024:

- **All day:** ITPartners+ team continues investigating, securing and verifying all endpoints.
- **Evening:** Preparation for restoring operations from backups.

Saturday, May 25, 2024:

- **Morning:** ITPartners+ team restores critical servers using Datto BCDR.
- **Afternoon:** Verification of data integrity and system functionality.

Sunday, May 26, 2024:

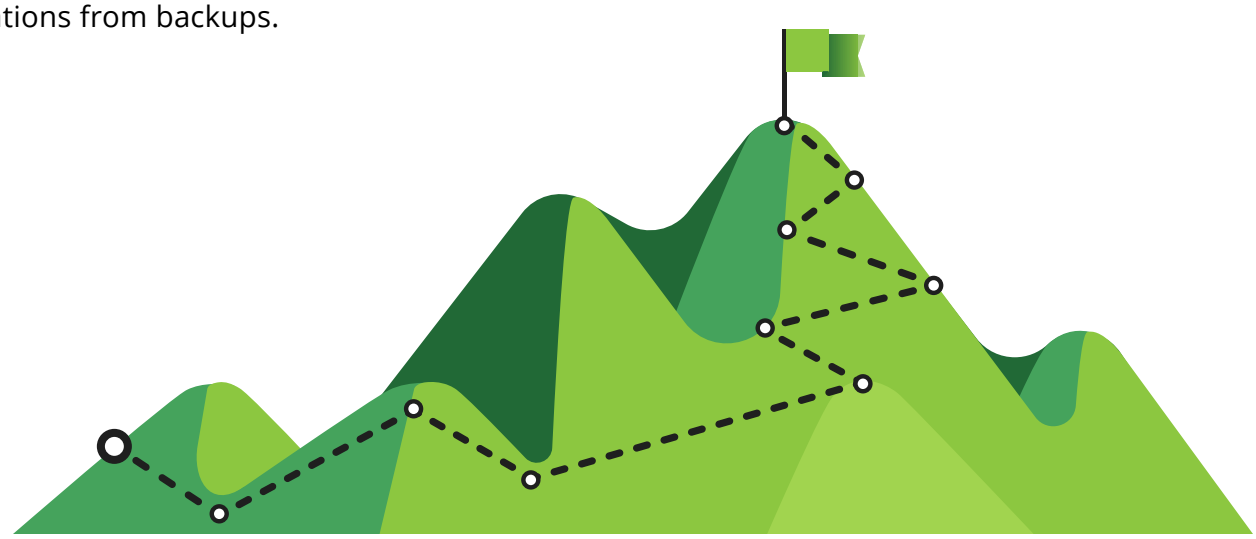
- **All day:** Final checks and testing of restored systems.

Monday, May 27, 2024 (Memorial Day):

- **All day:** Final recovery steps, ensuring all systems are operational and secure.
- **Evening:** Confirmation from their incident response (IR) team that all endpoints are clean and safe to use.

Tuesday, May 28, 2024:

- **Morning:** Business operations resume as usual for ITPartners+ and their customer.



Customer's perspective

McDonald recounts the intense effort over the holiday weekend, stating, *"The timeline of the incident begins Thursday morning. It was actually early in the morning, around 6 AM Eastern. But I think it happened at about 4:58. This is the weekend of Memorial Day. Still, our team worked diligently all weekend."*

Despite the holiday weekend, the customer's IT team, supported by RocketCyber and their comprehensive toolset, managed to restore operations quickly. The proactive measures and responsive support enabled the business to resume normal operations by Tuesday morning.

McDonald further emphasized the critical role of RocketCyber's tools. *"Had we not had all of those pieces — RocketCyber, Datto EDR, Datto BCDR, Datto RMM — we would not have been able to respond and recover as quickly and effectively as we did,"* he said.

Reviewing RocketCyber's powerful MDR capabilities

RocketCyber's handling of the Akira ransomware attack showcases its superior ability to detect, respond and mitigate such advanced threats. RocketCyber and Datto EDR's automated ransomware detection, combined with the dedicated SOC team, ensured minimal disruption and quick recovery for ITPartners+. This incident serves as a testament to the importance of proactive cybersecurity measures and the effectiveness of RocketCyber's MDR services in protecting businesses against ransomware.

GET A DEMO

RocketCyber
A Kaseya COMPANY