Cybersecurity Leaders, CTS Technology Solutions, Infiltrate Rhysida Ransomware Command Center to Uncover Attack Tactics

From Incident Response to Infiltration: CTS Uncovers Rhysida's Inner Workings, Providing Crucial Insights for Industry Protection

CTS Logo

DALLAS, TX, UNITED STATES, April 3, 2025 /EINPresswire.com/ -- Leland, a Sr. Security Operations Engineer at CTS Technology Solutions, has conducted an in-depth investigation into the Rhysida ransomware operation, culminating in unprecedented access to one of their active Command-and-Control (C2) servers. Over the past two months, Leland—who also goes by "c0mmrade"—meticulously tracked the group's activities after a local unmanaged client fell victim to their attack.

> “I saw active sessions with compromised organizations, some in the early stages of infiltration. It became a mission to identify these victims and alert them before it was too late.”
>
> *Leland, Sr. Security Operations Engineer at CTS Technology Solutions*

Emerging in mid-2023, Rhysida has quickly become a significant cyber threat, known for its double-extortion tactics and sophisticated techniques. Leland's investigation began with a standard ransomware recovery effort for a client, but his technical curiosity and persistence led him down a path of threat hunting that yielded remarkable insights into Rhysida's operations.

Through diligent analysis of network traffic, forensic data, and open-source intelligence, Leland identified a previously unknown C2 server used by Rhysida. In a bold move, he accessed this server, providing a rare, real-time view into the ransomware group's active campaigns and victim connections.

"Witnessing these attacks unfold in slow motion was alarming," said Leland. "I saw active sessions with compromised organizations, some in the early stages of infiltration. It became a mission to identify these victims and alert them before it was too late."

Leland's efforts have been instrumental in identifying and notifying numerous organizations under active attack by Rhysida. By leveraging the information gleaned from the C2 server, including victim IP addresses and session details, he was able to contact potential targets, providing critical early warnings that allowed some to mitigate the attacks before significant damage occurred. To date, Leland estimates his efforts have helped disrupt around 14 ongoing Rhysida attacks.

The investigation also shed light on a potential initial access vector exploited by Rhysida. Leland observed a correlation between compromised organizations and the use of unpatched Fortigate firewalls with exposed management interfaces. His analysis suggests Rhysida may be leveraging the recently disclosed `CVE-2024-55591` authentication bypass vulnerability in these devices for initial entry. While emphasizing this as a working theory, Leland successfully replicated the exploit against vulnerable systems.

CTS, a leader in proactive cybersecurity through its Security Operations Center (SOC) and Security Information and Event Management (SIEM) solutions, fully embraced and supported Leland's investigation, demonstrating its deep commitment to understanding and combating emerging threats. The company emphasizes the importance of continuous learning and threat intelligence in safeguarding clients and the broader digital landscape.

"Leland's dedication and ingenuity in uncovering these details about Rhysida are a testament to the caliber of our security team," said Josh, CEO of CTS. "His work has not only helped potential victims avoid significant harm but also provided valuable intelligence to law enforcement."

CTS has been actively collaborating with the Federal Bureau of Investigation (FBI), sharing the findings of Leland's investigation, including details of the C2 server, indicators of compromise (IOCs), and observed attack tactics. The FBI is currently investigating this information further to potentially identify and disrupt the Rhysida ransomware operation.

Leland's experience underscores the critical importance of proactive security measures, including:

- Maintaining up-to-date patching schedules for all network devices and software.
- Implementing robust endpoint detection and response (EDR) solutions.
- Ensuring comprehensive and offsite data backup strategies.
- Limiting exposure of management interfaces to the public internet.
- Partnering with experienced cybersecurity providers for continuous monitoring and threat intelligence.

CTS Technology Solutions' ongoing commitment to providing cutting-edge cybersecurity is clearly demonstrated by Leland's major investigation into the Rhysida ransomware group. This proactive approach, extending beyond standard security protocols, highlights why CTS continues to lead the way in the fight against cybercrime. By protecting its clients and contributing valuable threat intelligence to the broader security community and law enforcement, CTS reinforces its leadership in the ever-evolving cybersecurity landscape.

About CTS:
CTS is the leading provider of Technology Solutions, CMMC & Cybersecurity Consulting, SOC and SIEM, Management Services, Fractional IT, Co-Managed IT, Compliance as a Service and more for businesses nationwide. With unmatched expertise and industry know-how, CTS delivers innovative IT services and best-in class support to help companies maximize efficiency & improve their bottom line. Working closely with clients to deliver tailored solutions to help them stay ahead of the curve in an ever-evolving technology landscape. To learn more, visit www.cts-tex.com

PR
CTS Technology Solutions
email us here
Visit us on social media:
Facebook
X
LinkedIn
YouTube