Cyber Centaurs Details Rare Ransomware Data Recovery Following INC Group Infrastructure Exposure

Independent reporting confirms uncommon incident response outcome impacting twelve U.S. organizations

ORLANDO, FL, UNITED STATES, January 27, 2026 /EINPresswire.com/ -- Cyber Centaurs today released details of a rare ransomware incident response operation that resulted in the recovery of stolen corporate data by accessing attacker-controlled infrastructure used by the INC Ransomware Group. The recovery effort affected twelve U.S. victim organizations across the healthcare, legal, and manufacturing sectors and represents an uncommon outcome in modern ransomware cases. Cyber Centaurs investigation, which has since been independently reported by cybersecurity and enterprise technology media, revealed that INC Ransomware operators relied on a legitimate open-source backup utility to exfiltrate victim data into encrypted cloud storage environments under their control. By identifying attacker configuration artifacts during forensic analysis, Cyber Centaurs investigators were able to trace the exfiltration workflow back to attacker-managed repositories and confirm the presence of stolen data. Rather than treating the incident solely as an extortion event, the response team focused on understanding how the attackers operationalized backup tooling and cloud storage as part of their data theft process. That approach ultimately enabled controlled access to infrastructure used during the attacks and allowed for data validation and recovery. “Most ransomware investigations end once data leaves the victim environment,” said Andrew von Ramin Mapp, Managing Principal of Cyber Centaurs. “In this case, careful forensic analysis revealed an operational trail that led directly to attacker-managed storage. That made recovery possible, something that remains very rare in these situations.”

Abuse of Backup Infrastructure in Modern Ransomware Operations

The case confirms a broader trend observed across recent ransomware activity: the increasing abuse of trusted SMB and enterprise tools to conceal malicious behavior. By leveraging backup utilities and cloud storage platforms commonly used by organizations for legitimate purposes, threat actors are able to blend data exfiltration into normal operational traffic and evade traditional detection mechanisms.

During the investigation, Cyber Centaurs identified indicators linking malicious backup activity to cloud repositories controlled by the attackers. Using the same tooling employed during the exfiltration phase, under strict legal and procedural oversight, investigators were able to reconnect to those repositories and confirm the presence of data stolen during prior incidents. A

detailed technical analysis of the investigative process and findings has been published by Cyber Centaurs to provide additional context for defenders and incident response professionals:

Coordination With Authorities
Cyber Centaurs confirmed that the investigation was conducted in coordination with appropriate law enforcement authorities. Access to attacker infrastructure was limited strictly to validation, recovery, and intelligence purposes. “This was not about disruption or retaliation,” von Ramin Mapp added. “The objective was recovery, accountability, and improving our understanding of how these groups operate so organizations can better defend themselves.”

Implications for Organizations and Defenders
The incident underscores the need for organizations to scrutinize the use of legitimate software within their environments, particularly backup and data transfer tools that may be repurposed by threat actors. As ransomware groups continue to evolve, defenders must assume that familiar technologies can be weaponized and incorporate that reality into monitoring and incident response strategies. Cyber Centaurs continues to analyze artifacts associated with the case to improve detection techniques and response methodologies for future ransomware incidents. The firm provides incident response and data breach investigation services to organizations facing complex cyber intrusions:

About Cyber Centaurs
Cyber Centaurs is a U.S.-based cybersecurity firm specializing in digital forensics, incident response, and threat intelligence investigations. The company supports corporations, law firms, and government entities in responding to data breaches, ransomware incidents, and sophisticated cyber intrusions.
More information is available at:
https://cybercentaurs.com/

Desiree Ward
Cyber Centaurs
+1 407-777-4540
email us here
Visit us on social media:
LinkedIn