Linkc Ransomware: The New Cybercriminal Group Targeting Artificial Intelligence Data

redhotcyber.com/en/post/linkc-ransomware-the-new-cybercriminal-group-targeting-artificial-intelligence-data/

20 February 2025

Pietro Melillo : 20 February 2025 18:07

In the DarkLab group's underground analysis activity, we ventured onto an onion site that is apparently a Data Leak Site (DLS) of a new ransomware cyber gang.

This new actor called Linkc, was the author of a recent heist against H2O.ai. Their Data Leak Site-a minimalist page devoid of any further information-leaks only the essentials: a leak of sensitive data and source code belonging to a company specialising in artificial intelligence.

A New Group, Familiar Methods?

Even though Linkc appears to be a brand-new group, their operation follows the well-known **double extortion** model:

1. **Compromising and encrypting** the victim organization’s systems.
2. **Stealing and gradually releasing** sensitive data on a Data Leak Site.

What’s novel in this case is the site’s extreme minimalism, featuring:

- A logo and a brief post
- Details regarding the breach at H2O.ai
- No additional sections (no FAQ, contact page, or “about us”)

This approach could serve operational security purposes (reduced traceability) and create a stronger media impact by showcasing the target and stolen data right away.

The First Alleged Victim: H2O.ai

Linkc’s first reported target is a company specializing in the development of Machine Learning platforms and AI services. According to the leak:

- **Non-anonymized customer datasets** were stolen, intended for AI model training.
- **Complete source code** from Git projects was exfiltrated, including software for autonomous driving and GPT models.

At present, we cannot confirm the accuracy of this information, as the organization has not released any official press statement on its own website regarding the incident. Therefore, this article should be viewed as an “intelligence source.”

Why H2O.ai Specifically?

- **High Visibility**: Targeting a company working in AI garners significant media attention.
- **Data Value**: Proprietary datasets and AI source code are prime assets for unfair competition, industrial espionage, and cybercrime activity.
- **Reputational Pressure**: Tech companies are often scrutinized—and sometimes penalized—for security breaches.

Conclusions

Linkc has made its debut on the cybercrime scene with an intimidating approach and a minimalist web presence. Their choice to target H2O.ai highlights their inclination to go after organizations involved in Artificial Intelligence, potentially to monetize high-value data and technologies. For cybersecurity professionals, it is essential to:

- Maintain strict vigilance over AI platforms and sensitive assets
- Investigate the Indicators of Compromise (IoCs) and TTPs of new groups like Linkc
- Share threat intelligence in real time, pooling resources and expertise to counter ransomware threats

The cybercrime world is constantly evolving, and Linkc is yet another confirmation of that trend. It remains to be seen whether this group will launch more high-profile attacks or focus on selected cases. In the meantime, security experts must further refine their monitoring and defense tools, preparing for new digital extortion tactics.

As is our custom, we extend an invitation to the company involved to provide any updates on the incident. We will be glad to publish those details in a dedicated article to shed more light on the situation.

RHC will continue monitoring the matter to post any significant developments on the blog. Anyone with relevant information who wishes to remain anonymous can use the whistleblower's encrypted email address.

Pietro Melillo
Head of the Dark Lab group. A Computer Engineer specialised in Cyber Security with a deep passion for Hacking and technology, currently CISO of WURTH Italia, he was responsible for Cyber Threat Intelligence & Dark Web analysis services at IBM, carries out research and teaching activities on Cyber Threat Intelligence topics at the University of Sannio, as a Ph.D, author of scientific papers and development of tools to support cybersecurity activities. Leads the CTI Team "RHC DarkLab"