FOR IMMEDIATE RELEASE
Contact: IT-ISAC@nahigianstrategies.com

IT-ISAC's New Report Shows Ransomware Economy is Evolving, Becoming More Accessible

Critical Manufacturing, Commercial Facilities, Financial Services, Healthcare and IT Technology were the most targeted sectors in 2023

WASHINGTON (April 12, 2024) — The **Information Technology - Information Sharing and Analysis Center** (IT-ISAC), unveiled its first annual report on the 2023 ransomware landscape and what it could mean for 2024. The **Exploring the Depths** report details insights from over 2,905 ransomware attacks globally, allowing the ISAC to identify the leading threat actors, the most targeted industries, and the latest tactics used by cybercriminals.

"The evolving ransomware landscape presents a persistent threat to critical sectors of our economy and the threat won't be going away any time soon," said **Scott C. Algeier, Executive Director of the IT-ISAC**. "As long as the likelihood of a payday is high, and the risk of getting caught is low, ransomware will continue to be an evolving threat. We thank our members and partners for their collaboration to help get a wider perspective on this aspect of the cyber threat landscape."

In 2023, the top ransomware gangs included LockBit 3.0, which was responsible for 23.5% of the total attacks, ALPHV/Blackcat (12.5%), Cl0p (10.9%), Play (6.9%) and 8Base (5.4%). To help counteract these and other actors, the IT-ISAC and its members have collaboratively developed over 175 adversary attack playbooks to prepare members, both large and small, to defend against these threats.

The IT-ISAC found the Top 5 Most Targeted Sectors in 2023 were:

- Critical Manufacturing - [468 Attacks] - [15.5%]
- Commercial Facilities - [398 Attacks] - [13.1%]
- Financial Services - [375 Attacks] - [12.4%]
- Healthcare and Public Health - [299 Attacks] - [9.9%]
- Information Technology Sector - [283 Attacks] - [9.3%]

While the top five critical infrastructure sectors comprised over 60% of all ransomware attacks, there were also significant targets among organizations operating in Education, Food and Agriculture, Government Facilities, and Transportation Systems.

Looking to the rest of 2024, the IT-ISAC anticipates ransomware will continue to be prevalent in the greater cyber threat landscape. Analysts predict that hackers will exploit Artificial Intelligence (AI) to craft tailored phishing emails and even generate malicious code. As the technology matures, threat actors will likely continue to use these tools to assist in their campaigns.

Additional trends and takeaways from the IT-ISAC's report include:

- Ransomware-as-a-Service (RaaS) has significantly reduced the barriers to entry for individuals and groups seeking to carry out ransomware attacks
- Threat Actors are abusing remote management tools and legitimate software to gain initial access and evade detection
- Attackers are increasingly using Zero Day vulnerabilities and employing custom tooling
- Ransomware operators continue to target third-party vendors to gain access to mission-critical systems and data
- Threat actors are skipping the encryption process altogether and instead using the data to blackmail companies
- Attackers are using alternative programming languages like Rust to expand their targets

The IT-ISAC collected its data from open-source sites, the dark web, ISAC member input, and information shared by partners in the National Council of ISACs.

A link to the report and its recommendations on how companies can mitigate potential attacks can be found **here**.

###

About IT-ISAC: Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform and a trusted forum to engage with senior analysts from peer companies.

For more information about IT-ISAC, please visit www.it-isac.org. X: www.twitter.com/ITISAC LinkedIn: www.linkedin.com/company/it-isac