Trend Micro Urges Security Teams to Prepare for the Next Era of Ransomware

Latest research details how cybercrime business models might change

DALLAS, Dec. 15, 2022 /PRNewswire/ -- Global cybersecurity leader Trend Micro published a new report today warning that the ransomware industry could be on the verge of a revolution that sees actors expand into other areas of cybercrime or partner with hostile governments and organized crime groups.

To read a full copy of the report, *The Near and Far Future of Today's Ransomware Groups*, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-future-of-ransomware

The report highlights the key building blocks of modern ransomware attacks and predicts where threats may be evolving.

Jon Clay, vice president of threat research at Trend Micro:"Change is the only constant in cybercrime, and sooner or later, economic and geopolitical forces may compel ransomware groups to adapt or die. Amidst this uncertain threat landscape, network defenders need platform-based security to provide visibility and control across all attack surfaces, including hybrid cloud infrastructure. Our latest report will help them prepare for the future."

The report highlights the history of ransomware and the key building blocks of modern attacks before proposing scenarios that show where threats may be evolving.

Threat actors will continue to evolve their attacks in response to corporate defensive strategies, law enforcement successes, and government sanctions. This could include scaling up attacks through increased automation, targeting more IoT and cloud environments, improving professionalism and execution, and more effectively monetizing attacks.

The report also predicts that ransomware actors will eventually be motivated to change their business models due either to the cumulative impact of relatively small changes or by more radical global factors. This could lead to them developing supply chain attacks to cut out reliance on initial access brokers, using stolen data for stock manipulation, selling more services to traditional organized crime syndicates, merging with other criminal groups, or even working with government actors.

There is no silver bullet to solve these challenges. As they emerge, network defenders and governments should tackle changes to cybercrime business models. Trend Micro's report also provides a set of potential actions to prepare for these scenarios, including:

- Hardening internet-facing and internal corporate systems
- Migrating to cloud services
- Focusing defensive efforts on detection and response and initial access vectors
- Strengthening government sanctions on major actors and facilitators
- Regulating cryptocurrency to increase transparency, protect consumers against fraud and make money laundering harder

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911,media_relations@trendmicro.com

---

Additional assets available online: Photos (1)