Each Payment to Ransomware Attackers Subsidizes Nine Future Attacks

New report from Trend shows how ransomware industry is kept afloat

DALLAS, Feb. 23, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today published a new report warning that although only 10% of ransomware victims pay their extorters, they are enabling attacks on numerous other organizations by doing so.

The research aims to help IT leaders understand their risk and enable policymakers to craft more effective strategies

To read a full copy of the report, *What Decision Makers Need to Know About Ransomware Risk, please visit: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/understanding-ransomware-using-data-science**

Jon Clay, VP of threat intelligence at Trend Micro: "Ransomware is a major cybersecurity threat to enterprises and governments today. It's also continually evolving, which is why we need more accurate, data-driven ways to model ransomware-related risk. This new research aims to help IT decision-makers better understand their risk exposure and provide policymakers with the information they need to craft more effective and impactful strategies."

The report delivers strategic, tactical, operational, and technical threat intelligence and leverages advanced data science to list various threat actor metrics. These metrics can be used to compare ransomware groups, estimate risks, and model threat actor behaviors.

Key findings include:

- The 10% of victims that agree to pay usually do so quickly and are generally being forced to pay more per compromise
- Risk is not homogeneous – it differs across regions, sectors, and organization sizes
- Victims in some sectors and countries pay more often than others, meaning their peers are more likely to be targeted
- Paying a ransom often only results in driving up the overall cost of the incident with few other benefits
- Ransomware monetization activities are at their lowest in January and July-August, making these potentially good times for defenders to rebuild infrastructure and prepare for future threats

The report reveals that by prioritizing protection left of the kill chain, continuing in-depth analysis of the ransomware ecosystems, and focusing global efforts on reducing the percentage of victims paying, industry stakeholders could help drive down ransomware's profitability.

The insights revealed in this report can also enable decision-makers to better assess possible financial risks stemming from Ransomware. This would help:

- IT leaders to justify bigger budgets for ransomware defense
- Governments to budget more accurately for restoration services and law enforcement
- Insurers to price policies more accurately
- International organizations to compare Ransomware more accurately to other global risks

**Jointly produced by Trend Micro and Waratah.io, the report applies data science approaches to information collected from network and host-based telemetry, underground forums, bitcoin, and financial transactions, and chat logs – alongside analysis of criminal business processes – to uncover new trends and choke points of the ransomware ecosystem.*

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;
