What Decision-Makers Need to Know About Ransomware Risk: Data Science Applied to Ransomware Ecosystem Analysis

To better understand the complexities of today's ransomware landscape, researchers at Trend Micro and Waratah Analytics conducted **data-science experiments** to investigate various aspects of ransomware groups' processes and criminal business practices.

Key Findings

- Of the 120 unique CVEs that were used by ransomware groups under this research, 55 were for Microsoft products. Collectively, the top five most active ransomware groups – Conti, Cuba, Egregor, LockBit, and REvil – were able to compromise 30 unpatched products across 15 vendors.
- Several analyzed data sources suggest that ransomware incidents were lowest in January and July to August over the last two years. Therefore, these months are potentially the best time for defenders to rebuild infrastructure or schedule breaks.
- The initial ransom demand for targeted attacks is mostly based on a target company's revenue, but the minimum negotiable ransom that attackers will settle for depends on the industry of the company, its available funds, and its financial information observed by attackers when they gain access.
- Most organizations that do pay, pay fast. If a company's revenue relies on systems affected by the attack, time for restoration is a key motivator and it's likely that the ransom will be paid quickly.

Insights and Conclusions

- Every victim who does pay subsidizes attacks on another six to 10 victims, because ransomware payments cover the costs of criminal business operations for attacks on victims who do not pay.
- The recovery costs from a breach – including business interruption and incident response costs – amount to more than what a ransomware attacker demands, so paying the ransom often only serves to increase the overall costs for a victim.
- Ransomware risk is not homogenous for various reasons:
  - The number of victims who pay significantly varies among regions, industries, and business size due to different capabilities, government regulations, and access to cryptocurrencies.
  - Protection against ransomware groups that use different monetization strategies requires defenders to have different qualifications and resources.
  - Business models focusing on targeted ransomware monetization require a deep knowledge of potential victims before data encryption, or before the purchase of access to the victim's infrastructure.
- Shifting left in the cyber kill chain can help minimize the impact of ransomware attacks by detecting and mitigating attacks before these can reach the encryption and data exfiltration stage. Increasing the cost of operations for ransomware actors at this point in the kill chain decreases the number of cybercriminals' potentially profitable targets, alongside the profitability of ransomware business models