The Cyber-Criminals Behind Ransomware and How they Succeed

According to a report by BleepingComputer, March 2023 set a new record for ransomware attacks, with 459 reported worldwide. The report attributed the surge to the activity of several ransomware groups, such as Royal, BlackCat, Medusa, and Ransomhouse. Prominent victims of the criminals behind ransomware in March include André Mignot Hospital in France, and several schools and universities in the US.

The Criminals Behind Ransomware

A type of malicious software, ransomware attacks encrypt the victim's data and demand a ransom to unlock the information. One of the most profitable and widespread cybercrimes in the world, ransomware plagues millions of individuals and organizations every year. But who are the cyber-criminals behind ransomware and how do they succeed?

The ransomware network is complex and diverse, involving multiple actors with varying roles and motivations. They include:

- **Developers:** These technically skilled individuals and organizations create and update the ransomware code, often selling it as a service to other criminals.

For example, the developers of REvil ransomware claimed to make over $100 million in 2020 by providing their software to affiliates.

- **Distributors:** Organized to spread the ransomware to potential victims, they employ various methods such as phishing emails, malicious websites, or compromised networks.

  The distributors of Emotet malware have infected millions of computers worldwide by sending spam emails with malicious attachments.

- **Operators:** These professionals manage the ransomware campaigns, setting the ransom amount, communicating with the victims, and collecting the payments.

  The operators of DarkSide ransomware have targeted several large companies, such as Colonial Pipeline and JBS, demanding millions of dollars in ransom.

- **Affiliates:** Partners who share a percentage of the profits with the developers or operators, affiliates provide access to the ransomware service or tools.

  For example, the affiliates of Ryuk ransomware earned over $150 million in 2019 by using the malware provided by TrickBot distributors.

- **Money Launderers:** They help criminals to convert ransom payments, usually in cryptocurrencies, into cash or other assets.

  The money launderers of Maze ransomware employ various cryptocurrency mixing services and exchanges to hide their tracks.

How the Criminals Behind Ransomware Succeed

The criminals behind ransomware succeed because they exploit several weaknesses in our defense. These include the lack of adequate cybersecurity measures and awareness among individuals and organizations, making them vulnerable to ransomware attacks. Other success factors include:

- The availability and affordability of ransomware services and tools on the dark web. This allows anyone with malicious intent to launch a ransomware campaign with minimal effort and risk.
- The difficulty of tracing and prosecuting the ransomware criminals. They often operate from countries with weak or nonexistent cyber laws or cooperation agreements.
- The willingness of many victims to pay the ransom. They relent either because they lack data backups, or because they fear losing sensitive or valuable information.

Ransomware attacks can cripple any organization, regardless of its size, sector, or location. This highlights the importance of having strong cyber security measures in place, such as backup systems, antivirus software, employee training, and incident response plans.

How to Prevent Ransomware Attacks

Most successful ransomware attacks compromise one or more highly privileged user accounts. To guard against the compromise of privileged accounts, organizations need to implement information security governance. Least privilege and zero trust policies, multi-factor authentication (MFA), and randomized administrator passwords provide needed additional security.

Microsoft security tools and training can play a critical role in reducing the risk of ransomware and other cyber-attacks. Sometimes difficult for organizations with limited cyber security expertise to configure, these tools are known by cyber security consultants who provide valuable assistance in setting them up properly.

Ransomware a Serious Threat

In August 2021, the Hive attack extorted more than $100 million from various organizations, including a major hospital chain and a telecom company. And in February 2022, the Vice Society attack focused on the education sector, encrypted data from dozens of schools and universities.

A serious threat, Ransomware requires a coordinated response from all stakeholders, including governments, law enforcement, cyber security experts, and users. By raising awareness, adopting cyber security best practices, disrupting the ransomware infrastructure, and holding the criminals accountable, the impact and prevalence of this cyber-crime can be reduced.

Ransomware Prevention Experts

The cyber security consultants at eMazzanti Technologies possess the expertise necessary to protect your organization from ransomware attack. They help business leaders choose and configure the tools required, including access management, email protection, cloud backups, data encryption, and continuous network monitoring.