Forum: United Nations Office on Drugs and Crimes (UNODC)

Issue: Tackling the Rise of Ransomware Attacks

Chairs: Leyan Masri, Elana Tayeb, & Nada Himrane

Introduction

Ransomware is malware that encrypts a person's personal information and uses it as leverage to gain payment in exchange for decrypting it. This method of extortion is used against both public and private sector businesses. Ransomware attacks often block companies or organizations from their data. Once the data is encrypted, it is rendered useless unless decrypted. Attackers ensure a file stays encrypted by making it so only a decryption key is known by the attacker to decrypt the files stolen, once the ransom is paid. This also has implications for business revenue as it causes operational downtime. This not only means loss of customers but it can also impact brand reputation. Furthermore, after companies pay the ransom they most likely do not get their data returned due to the incomplete or flawed decryption that can impact data integrity. Although companies know this, they pay the ransom immediately to avoid brand damage or customer dissatisfaction.

Definition of Key Terms

Ransomware

Malicious software that encrypts data, blocking access until a ransom is paid. Modern variants may also threaten to leak sensitive data if the ransom isn't received, targeting both individuals and large organizations.

Cryptocurrency

Digital currency secured by cryptography, often used by ransomware attackers due to its anonymity, making it difficult for authorities to trace ransom payments or transactions.

Phishing

A cyber tactic where attackers send deceptive messages to trick users into revealing sensitive information or downloading malware. Phishing is commonly used to spread ransomware by gaining initial access to systems.

Drive-By-Downloads

Malware is automatically downloaded onto a user's device when they visit a compromised website, without needing user interaction.

Zero-Day Vulnerabilities

Security flaws in software attackers exploit before a patch is available. Ransomware groups use these vulnerabilities to infiltrate systems undetected, increasing the attack's effectiveness.

Background Information

Ransomware attacks first started in the late 1980s with the "AIDS Trojan," targeting people with very basic encryption by today's standards. It was a floppy disc distributed to healthcare professionals labeled “AIDS information”. Once used, it hid files and demanded ransom to decrypt the files. In 2010, strategies shifted as ransomware was now more often targeted against organizations beginning with CryptoLocker. CryptoLocker popularized the use of cryptocurrency as payment to avoid law enforcement tracing any payments. This increased ransomware payments as attackers began asking for more from successful organizations. Nowadays, attackers use a tactic called double extortion, where not only is data encrypted, but attackers also threaten to expose sensitive information. This gives attackers more control over companies which can affect brand reputation directly. Attackers use various methods to gain data such as phishing, drive-by downloads, and exploiting vulnerabilities such as zero-day flaws. These attacks have a consequence on our day-to-day life with it affecting healthcare, finance, education, and even public infrastructure. Hospitals that suffer these attacks have patient care disrupted, delayed treatment, and even the possibility of sensitive patient data being revealed. Attacks also have a big impact on essential services like fuel and power as seen in the Colonial Pipeline attack.

Major Parties Involved

United States

The United States has had the Federal Bureau of Investigation (FBI) investigate ransomware internationally and locally. Law enforcement authorities use predictive policing technologies to keep the public safe and prevent cybercrime, such as with the FBI.

United Kingdom

- The UK works closely with organizations such as Interpol and Europol to coordinate responses to ransomware threats.
- The UK government heavily assisted the National Health Service (NHS) during the WannaCry ransomware attacks. Following the incident, the government increased funds in order to improve cyber resilience after the disruption of services. The NHS experienced considerable losses financially, which allowed for the government to take

action in increasing the cyber security budget with a £61 million investment. This led to a three-year agreement with IBM in the development of a Cyber Security Operations Centre (CSOC), in order to improve the capabilities for threat monitoring and response.

Estonia

- Estonia is a major party that is involved in the current crisis after being a target of cyberattacks in the year of 2007. The country developed initiatives including the Cyber Security Strategy (CSS) to strengthen security and improve legal frameworks. Consequently, Estonia developed powerful organizations such as Cyber Security Council (CSS) and the Cyber Defence League (CDL) to take action against these cyberattacks. Not to mention, they actively collaborated with international organizations like NATO and the United Nations to ensure the success of their strategies. They prioritize addressing the issue behind ransomware through their national strategies and implementing ransomware defense with international cooperation. (Czosseck et al., 2011);

Timeline of Key Events

Date	**Description of event**
2017-2021	Early attacks like Cryptolocker and WannaCry marked the beginning of major ransomware attacks in Estonia.

	Organizations such as the NHS severely got affected across the UK.
2018–2021	Organizations such as Interpol and the FBI started campaigns such as "No More Ransom” to increase efforts to disrupt cybercrime.
2021 May	The Colonial Pipeline attack highlighted the risk of ransomware poses to essential services.
2022–2023	Global efforts focused on strengthening defenses and improving international cooperation to combat ransomware.

Previous Attempts to Resolve this Issue

1. **"No More Ransom" Initiative (2016)**

   This was a collaboration between government agencies such as Interpol and the FBI with cybersecurity companies to provide free decryption tools and to raise awareness helping victims recover without paying any ransom;

2. **International Cybersecurity Cooperation**

Countries have strengthened cooperation through organizations such as the European Union Agency for Cybersecurity (ENISA) and through agreements to share intelligence and respond to ransomware threats;

3. **Government Sanctions and Legislation**

Governments, particularly the US, have introduced sanctions against ransomware criminals and passed legislation to improve cybersecurity standards for both private and public sectors, aiming to reduce the risk of attacks and improve incident response.

Possible Solutions to Resolve this Issue

1. **Enhanced Cybersecurity Education and Training**

Providing cybersecurity awareness classes for organizations to recognize and prevent phishing and other ransomware methods;

2. **Stronger Legislation and International Cooperation**

Implementing stricter regulations and fostering deeper international collaboration to maintain effective security knowledge, instituting stronger strategies through international networks, and keeping people and companies safe;

3. **Improved Cyber Defense Technologies**

Investing in advanced security technologies like AI-powered threat detection, and multi-layered encryption to further increase protection against ransomware;

Bibliography

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 cyber attacks. *International Journal of Cyber Warfare and Terrorism*, *1*(1), 24–34. https://doi.org/10.4018/ijcwt.2011010103

ENISA. (2024, November 8). ENISA. https://www.enisa.europa.eu/

INTERPOL | The International Criminal Police Organization. (n.d.). https://www.interpol.int/en

KnowBe. (n.d.). AIDS Trojan | PC Cyborg | Original Ransomware | KnowBe4. https://www.knowbe4.com/aids-trojan

Vanderzielfultz, V. (2024, April 18). *2021 colonial pipeline ransomware attack*. Homeland Security Digital Library. https://www.hsdl.org/c/timeline/2021-colonial-pipeline-ransomware-attack/#:~:text

WannaCry ransomware attacks cost the NHS £92m. (2018). *Computer Fraud &amp; Security*, *2018*(11), 1–1. https://doi.org/10.1016/s1361-3723(18)30102-7