ENISA's Threat Landscape and the Effect of Ransomware

Ransomware attacks are complex, intricate activities that involve various cybersecurity threat actors. They are financially lucrative, and the motivation behind the attacks varies depending on the perpetrator (e.g., committed by an independent ransomware attacker or cartel), the target and the threat actor's intent. Ransomware attacks could result in improper financial gain, an enterprise advantage arising from stolen data or intellectual assets, societal disruption because of paralyzed critical infrastructure, or a weakened government. Death might also be a collateral consequence.

The European Union Agency for Cybersecurity (ENISA) *Threat Landscape 2021* report provides a general overview of current cybersecurity threats for policymakers and the technical cybersecurity community from a variety of open-source online references strategically picked based on ENISA's cyberthreat intelligence capabilities, covering multiple sectors, technologies and contexts.[1] The report named ransomware as the biggest among the nine major cyberthreats:

1. Ransomware
2. Cryptojacking
3. Threats against data
4. Malware
5. Disinformation/misinformation
6. Nonmalicious threats
7. Threats against availability and integrity
8. Email-related threats
9. Supply chain threats[2]

Four cybersecurity threat actor groups—entities that commit malicious acts by taking advantage of existing vulnerabilities intending to harm their victims—are responsible for these threats: state-sponsored actors, cybercrime actors, hackers for hire and hacktivists. Understanding the threats and the threat actors is helpful when planning cybersecurity defenses and mitigation strategies.

Ransomware: The Biggest Threat

ENISA considered ransomware the most prominent threat in 2021. Attackers demanding ransom payments sometimes make layered demands. Direct victims receive peremptory ultimatums involving substantial sums of money, while inconvenienced individuals and other affected third parties receive lesser orders. Attackers' use of this triple extortion scheme compounds the ransomware threat.[3]

Cryptocurrency is the most common payout method used by those threat actors providing Ransomware as a Service (RaaS).[4] Monero is their dominant cryptocurrency because it allows for anonymity and transactional indistinguishability.[5] These RaaS providers have created cartels to strengthen collaboration and facilitate the sharing of tactics. They even help one another publicly shame their victims, which includes media amplification, cold

ANTONIO M. VILLAMOR, JR. | CISA, CISM, CDPSE, CFE, CIA, CPA, CRMA, MIEE

Is the head of the internal audit unit of the International Center for Agricultural Research in the Dry Areas, a research institution dealing with international food security.

> The increase in policy initiatives in the European Union, the United States and worldwide is proof of the significance and impact of ransomware threats as a growing national security issue.

calling and harassment. Attacks orchestrated by RaaS cartels make individual attribution difficult.[6]

Ransomware attackers execute their attacks using these two most common ransomware infection vectors: compromise through phishing emails and brute-forcing on Remote Desktop Protocol (RDP) services. They use these vectors because they are the cheapest and most profitable methods. Until government agencies shut down their operations in 2021, Conti and Revil/Sodinokibi were the biggest players in the ransomware industry, amassing US$24.7 million.[7] In 2022, the reported global ransomware payments amounted to US$457 million.[8] Enterprises giving in to these RaaS providers' demands risk violating multiple government laws and regulations, such as the EU General Data Protection Regulation (GDPR) and the US Department of Treasury's Office of Foreign Assets Control (OFAC) advisory.[9] Despite the regulatory consequences, ENISA noted that Europeans tend to give in to RaaS demands.

Exploiting Opportunities

According to ENISA, cybersecurity threats continued to grow during the COVID-19 pandemic.[10] The pandemic increased cybersecurity threats and attack surfaces. It also provided attackers opportunities to exploit the new normal, partly because of the growth in people's online presence (e.g., social media), hybrid working models and the transition to more cloud-based solutions. The boom in the transportation industry's courier, express and parcel (CEP) business was also a factor because, during the pandemic, CEP delivery services became a critical infrastructure. The acceleration in new artificial intelligence (AI) technology and advanced features (e.g., AI adaptability through machine learning [ML] and automated phishing email distributions) also spurred the growth of the cybersecurity threat. These cyberattacks become more mainstream, leading to more targeting of enterprises through home offices.

In addition, state-backed or state-sponsored groups have taken advantage of the pandemic to conduct cyberespionage and implement COVID-19–related social engineering lures. This approach includes supply chain compromises that have reached new levels of sophistication and impact (e.g., software update process hijacking). The COVID-19 contact tracing systems deployed by governments provided valuable personal data for intelligence-gathering and spear phishing campaigns carried out by other state-sponsored actors or cybercriminals.[11] These data could also be sold in underground markets through data auctions.

A Geopolitical Chess Game

The increase in policy initiatives in the European Union, the United States and worldwide is proof of the significance and impact of ransomware threats as a growing national security issue. In April 2021, Alejandro Mayorkas, the US Department of Homeland Security (DHS) secretary, stated that he considered ransomware a national security issue.[12] He also pledged to implement the recommendations issued by the Institute for Security and Technology.[13] In July 2021, the United States criticized the People's Republic of China, citing its Ministry of State Security's irresponsible behavior and complicity in harboring and sponsoring groups that launch cyberattacks, including ransomware.[14] ENISA found that these state-backed or state-sponsored groups disguise their disruptive and destructive operations as ransomware. The involvement of these state-backed or state-sponsored groups can weaken, demoralize and discredit their sponsors' adversaries.

ENISA observed that state-backed or state-sponsored groups use offensive security tools (OSTs), living-off-the-land (LOTL) tactics, published proof-of-concept code and false flags. These groups take advantage of operational scalability, ease of use, deniability, operational effectiveness and reduced costs. Together with their cybercriminal hackers' network (applying elevated levels of operational security to conduct cyberoperations), these groups provide Crime or Crimeware as a Service. Their involvement complicates detection, response and attribution efforts. These cybercriminals are indispensable to their nation-state sponsors because they supply revenue-generating cyberintrusions.

Nation-states use cyberoperations as tools to further national interests. In particular, nations with advanced cybercapabilities can get favorable positions in the cyberarms race. State backing or sponsorship becomes elemental as it advances the host nation's strategic global, political, military, economic and ideological power. ENISA expects the lines between cyberespionage and cybercrime to blur even further. Under the auspices of nation-states, these state-backed or state-sponsored groups will increase their cyberintrusion activities, especially in the regions of trade routes and areas of armed conflict, launching attacks against strategic targets such as governmental organizations. Thus, cyberoperations enable large-scale espionage and theft of personally identifiable information (PII) and intellectual property in pursuit of sponsors' interests.

Ransomware Threat Mitigation Strategy

ENISA provided recommendations to mitigate ransomware threats. Some of its proposals include substantial investments, such as implementing secure and redundant backup strategies, implementing segregation of duties (SoD), separating development and production environments, and reviewing management response and recovery plans periodically. It also included cheap cyberhygiene components such as using products or services that block access to known ransomware sites and providing user security awareness.

> Organizational cyberhygiene is a better and cheaper way to address ransomware threats.

ENISA noted that adopting and implementing cloud-first strategies will not weaken the position of the four most prominent cybersecurity threat actors because they have already developed the ability to breach cloud infrastructure and services using cryptomining and cryptomining worms. Cloud security providers (CSPs) such as Black Baud, Swiss Cloud, Equinix and Cloudstar have all reported security compromises and have received ransomware demands. Enterprises that outsource their IT infrastructure management through managed service providers (MSPs) are also vulnerable to ransomware attacks. From the attackers' point of view, CSPs and MSPs already have access to these enterprises' data, which might be of value.

Interestingly, ENISA did not include ransomware insurance as a mitigation strategy. It pointed out that insurance policies encourage the ransomware industry's proliferation, fueling a ransomware economy.

Conclusion

Individual and organizational data are central to ransomware threats, which intertwine with other threats, such as threats against data availability and integrity. Successful threat actors make data unavailable and tarnish the technical and managerial competence and capabilities of those entrusted to protect data, such as chief information officers (CIOs), chief information security officers (CISOs), CSPs and MSPs. The major threats are the threat actors' ecosystems creating quasi-supply chains. Only after paying the ransom are the data accessible again. However, payment does not guarantee data availability or protect against later extortion (given the triple extortion ransomware scheme).

And having a ransomware insurance policy is not a panacea. Organizational cyberhygiene is a better and cheaper way to address ransomware threats. The blurred lines between cyberespionage and cybercrime, especially if state-sponsored actors carry out the attack, confirm that ransomware is a national security issue.

Endnotes

1 European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2021*, Greece, 2021, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021*

2 European Union Agency for Cybersecurity (ENISA), *Threat Landscape for Supply Chain Attacks*, Greece, 2021, *https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*

3 Whitney, L.; "Ransomware Attackers Are Now Using Triple Extortion Tactics," *TechRepublic*, 12 May 2021, *https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/*

4 *Op cit* ENISA, *ENISA Threat Landscape 2021*

[5] *Ibid*.

[6] *Ibid*.

[7] *Ibid*.

[8] Chainalysis Team; "Ransomware Revenue Down as More Victims Refuse to Pay," Chainalysis, 19 January 2023, *https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/*

[9] US Department of the Treasury Office of Foreign Assets Control (OFAC), "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," 1 October 2020, *https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf*

[10] *Op cit* ENISA, *ENISA Threat Landscape 2021*

[11] *Ibid.*

[12] Williams, B. D.; "DHS: Ransomware Is National Security Threat," Breaking Defense, 29 April 2021, *https://breakingdefense.sites.breakingmedia.com/2021/04/ransomware-a-national-security-issue-new-report-argues-yes/*

[13] Ransomware Task Force, "Combating Ransomware—A Comprehensive Framework for Action: Key Recommendations From the Ransomware Task Force," Institute for Security and Technology, September 2021, *https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf*

[14] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," USA, 19 July 2021, *https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/*