protiviti®
Global Business Consulting

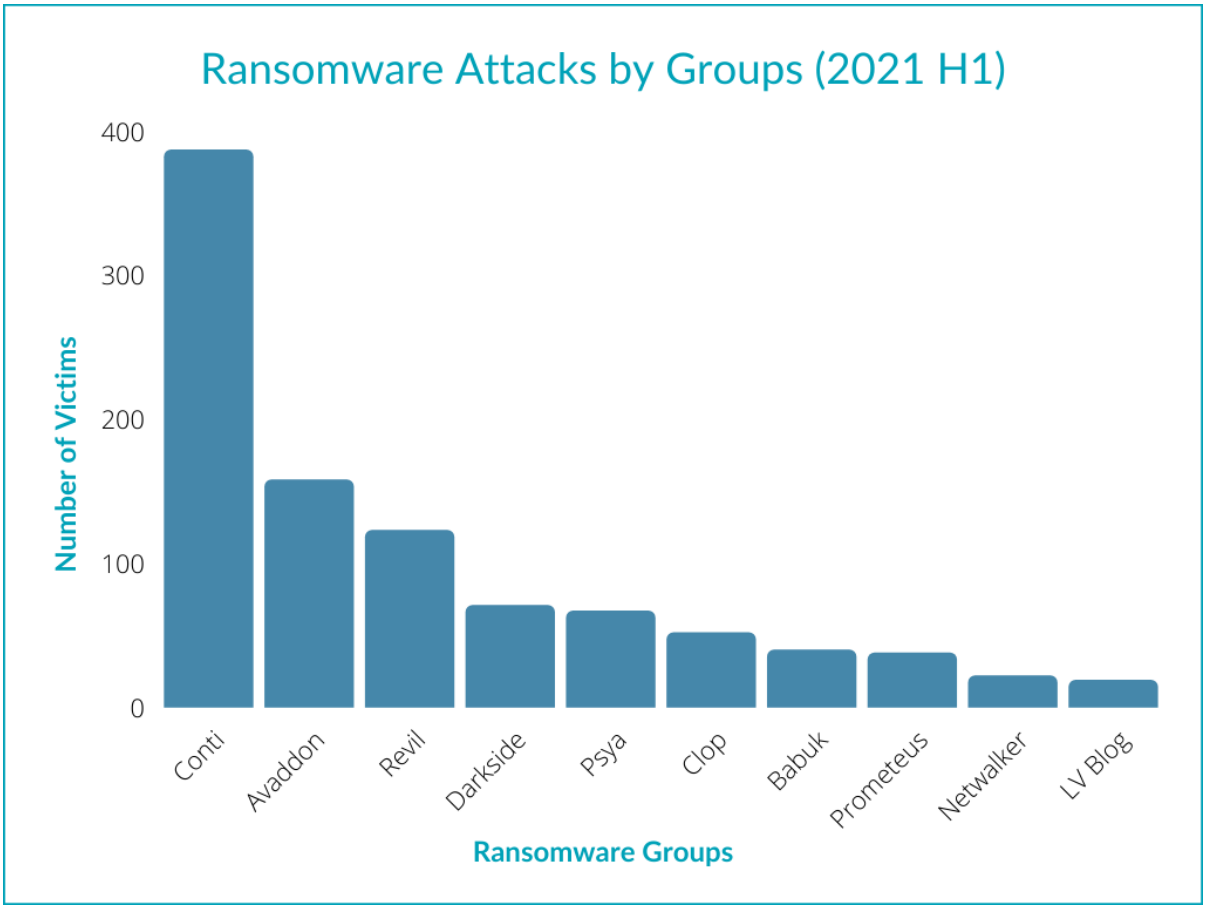
26% Rampant Rise in Ransomware Attacks Leaving APAC Companies Defenseless

Three Notorious Ransomware as a Service (RaaS) groups accounted for more than 60% of all ransomware attacks

According to Cognyte's Cyber Threat Intelligence Research Group[1], ransomware attacks nearly doubled in the first half of 2021, with 1,097 organisations experiencing a ransomware event, compared to 1,112 events for all of 2020. But while the number of attacks increased by nearly 100%, three ransomware groups are responsible for 60 percent of the attacks – Conti, Avaddon and Revil.

The prevalence of these ransomware groups can be attributed to their ransomware-as-a-service (RaaS) nature. As a branch of software-as-a-service (SaaS), RaaS is an offering of pay-for-use malware and follow-up support by sophisticated ransomware developers to those with less technical skills, who deploy them into potential victims' systems. This significantly lowers the hurdle of initiating ransomware attacks, incentivising more groups to enter this illegal industry for profit.

Ransomware is a type of malware that encrypts victim's data in exchange for a ransom payment. Different from a virus, which is signature-based with malicious code attached, ransomware does not aim to downgrade the system performance but to block the victim's access to the system itself.



Adapted from "Ransomware Attack Statistics 2021 – Growth & Analysis," Cognyte, August 8, 2021

To illustrate the kill-chain of ransomware, let's use Conti as an example. Through means like spear phishing emails, stolen remote-desktop-protocol (RDP) credentials or unpatched vulnerabilities, the group gains initial access to the victim's networks. It then exploits different internal tools and software available to escalate privileges and identify critical systems with valuable data. After the critical data is identified, the group uploads the data elsewhere with the original data encrypted and backup data deleted. A ransom note is left in the system for the victim to contact Conti for ransom payment —or the information will be published.

APAC Companies being the New Targets of Cyber Criminals

One of the victims attacked by Conti is JVCKenwood. In September 2021, attackers obtained unauthorised access to the servers of the Japan-based electronics supplier. The Conti group demanded a ransom of US$7 million for the recovery of the 1.7TB of data stolen, which included personal details of employees and customers as well as documents of internal departments. While the firm issued a press release reporting that a cybersecurity agency had

been hired to investigate the incident with the relevant authorities, its act suggested it refused to accept the ransom demand[2].

Similar incidents happened to the Taiwan-based motherboard manufacturer Gigabyte in October 2021. This time the ransomware group AvosLocker had stolen personal details of employees and job candidates, as well as the NDA with third-party companies and the file directory list[3]. It was the second ransomware attack for the company within 3 months after the theft of 112GB of business data by RansomExx in August 2021, which led to the temporary shutdown of internal servers together with external customer support websites[4].

The True Cost of a Ransomware Attack to your Business

The above two incidents are just a tip of the iceberg. In Hong Kong alone, on average more than 750,000 ransomware incidents occurred every month from April to June 2021[5]. While most of the attacks failed, the cost of a single successful incident to a business could be large.

The actual ransom may be the first cost of an attack that comes to mind. In 2021 Q2, the average ransomware payments for organisations reached US$136,576[6], and it is always a question of whether to pay or not. In recent years, double extortion techniques have become the mainstream. In this technique, if the business refuses to pay the ransom, the attacker can choose to leak out the data in dark web or sell it to third parties who value those data.

Even if an organisation reluctantly pay the ransom, it is not the end of the incident, as there is no guarantee that the cybercriminals will provide the correct decryption key for file restoration. In fact, in APAC region only 5% of victims managed to get back all their data, while 19% had no more than half of the data restored[7]. The slow recovery of data in turn affects the resumption-to-normal process. The average downtime for a ransomware attack has increased to 23 days on average in 2021, compared to 16 days in 2022[8], and downtime may be even longer if the victim does not have a well-developed plan in response to such scenario.

Another cost of ransomware attacks comes from reputation damage. As seen from Gigabyte incident, the data that is held at ransom could involve customer or business partner information. This type of data breach could cause customers and business partners to form a negative impression towards the company. In a study conducted by cybereason, 77% of respondents said they would retract their loyalty to brands following a ransomware incident, and 61% would switch some or all of their business to another provider within a year[9]. In some jurisdictions, data breaches, as well as failure to notify of such on time, would also attract regulatory fines and even criminal penalty from relevant authorities.

Time to Armor in Full before Next Attack

In APAC region, the average cost to rectify the impacts of a ransomware incident has reached US$2.34 million10, suggesting the urgent need to invest in ransomware solutions. However, having the most sophisticated security solutions isn't a silver bullet against ransomware attacks. In fact, humans are the biggest risk of an organisation's data falling into the hands of cyber criminals. All levels of an organisation are responsible to take proactive measures to prevent, respond and recover from ransomware attacks. Below are a few examples of key actions that many companies often overlook:

Role	Before Attack	After Attack
C-Suite Level	• Establish expectations for CISO and accountabilities for performance in the case of ransomware management • Establish the appropriate target level of operational resilience • Explore the feasibility of cyber insurance by understanding the extortion coverage and the prerequisite security measures	• Consider thoroughly the reasons for and against paying the ransom and choose the option that minimises damage and cost • Reflect on the attack and amend existing ransomware strategy
CISO	• Conduct compromise assessment to identify hidden compromised systems • Ensure the company's Cyber Incident Response Plan covers the scenario of ransomware attacks • Establish clear data retention guidelines to clean up excessive data • Consider multiple backups (including offsite and physical) as ransomware could delete backup	• Deliver the attack information in the most concise manner (e.g., dashboard) to management • Notify the third party at stake (e.g., regulatory authorities, cyber insurer) at once for follow-up
IT Department	• Stay updated on ransomware attack techniques and corresponding defense measures	• Analyse the root cause and suggest areas requiring external assistance

Every employee	• Not just ignore but timely report suspicious emails to IT • Stay updated to current cybersecurity news	• Be familiar with the Cyber Incident Response Plan and business continuity plan

Despite the fact that ransomware can be acting in the dark without an organisation's knowledge, it doesn't mean organisations should be passive about it. Instead, being proactive by conducting regular compromise assessments allows an early detection of hidden ransomware and shields companies to be more prepared for the attack. Furthermore, engaging employees in ransomware attack simulations helps develop their vigilance and understanding on actions taken during actual ransomware attacks. Good data handling practice also helps organisations to avoid excessive sensitive data being exposed to cyber criminals. When it comes to the decision of paying the ransom or not, company executives should stay calm and carefully assess the significance of the data held by cyber criminals. Last but not least, learn from mistakes. Post-incident analysis and follow-up to strengthen the organisation's cyber resilience is crucial to forbid cyber criminals a second attempt.

To learn more, get in touch with

Michael Pang
michael.pang@protiviti.com

Franklin Yeung
franklin.yeung@protiviti.com

[1] "Ransomware Attack Statistics 2021 – Growth & Analysis," Cognyte, August 8, 2021, available at https://www.cognyte.com/blog/ransomware_2021/

[2] "JVCKenwood hit by Conti ransomware attack", ComputerWeekly.com, October 1, 2021, available at JVCKenwood hit by Conti ransomware attack (computerweekly.com)

[3] "Gigabyte victim to ransomware again", Security, October 22, 2021, available at https://www.securitymagazine.com/articles/96364-gigabyte-victim-to-ransomware-again

[4] "Motherboard vendor GIGABYTE hit by RansomExx ransomware gang", The Record, August 6, 2021, available at https://therecord.media/motherboard-vendor-gigabyte-hit-by-ransomexx-ransomware-gang/

[5] "Over 750,000 ransomware attacks HK firms monthly", Hong Kong Business, available at https://hongkongbusiness.hk/information-technology/news/over-750000-ransomware-attacks-hk-firms-monthly

[6] "Modern Ransomware Shakes Up Banking, Government, Transportation Sectors in 1H 2021", Trend Micro, October 20, 2021, available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomware-shake-up-banking-government-transportation-sectors-in-1h-2021#cover

[7] The State of Ransomware 2021, Sophos, April 29, 2021, downloaded from https://mysecuritymarketplace.com/reports/the-state-of-ransomware-2021/

[8] Modern Ransomware (n 6).

[9] Ibid.

[10] The State of Ransomware (n 7).

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®