Relativity® Trust

APAC Threat Landscape Update

Executive Summary

APAC is in a unique situation to be the new "hot" target for cybercrime and information theft. There are several threat actors that are specifically targeting the region, but there are also more generic, region-agnostic threats that need to be dealt with.

Risks

Awareness of the risks specific to the APAC region is essential to architecting a defence-in-depth strategy to mitigate those risks. The current major risks to private, public, and government organisations in the region include:

- Financially motivated cybercrime/e-crime:
  - **Circus Spider:** A Russian-speaking actor, particularly active in the APAC region, known for using the NetWalker ransomware. Originally used phishing, but has shifted to a Ransomware as a Service (RaaS) model. Threatens to publicly release stolen data.[11, 12]
  - **DDoS Attacks:** Extortion attacks that require payment (usually Bitcoin) to get a DDoS to stop.
  - **Netfilim Ransomware:** A ransomware strain that threatens to release data to the public if victims fail to pay ransom.
- Cyber espionage activities: Includes government-sponsored initiatives such as "Made in China 2025."[3]
- Global COVID-19 vaccine race: Many COVID-19 vaccine related scams are making the rounds.
- Rollout of 5G technology and Internet-of-Things (IoT) technology: A new technology with limited security controls or full understanding of security implications.
- Targeting of the video gaming industry: Attacks against video gamers and developers are ramping up.
- Supply chain vulnerability risks: Supply chain attacks focused on vendors used by the targets. Solarwinds is a recent example.
- Data privacy regulations across borders[15]

Notable Events

2019

Feb: Targeting of the Australian Parliament three months prior to general elections [Chinese Cyber Espionage][1]

Aug: Toll Group ransomware attack [Circus Spider, Netfilim ransomware][2, 14]

Nov: Targeting of Hong Kong District Council elections with a malicious macro-containing document [Chinese Cyber Espionage][1]

2020

Mar: NetWalker moves to RaaS model. "Netwalker affiliates are prohibited from going after organisations located in Russia or other post-Soviet republics that are part of the Commonwealth of Independent States (CIS)"[14]

Apr: NetWalker recruits affiliates to single out large targets: private business, hospitals, or government agencies. Gains access via unpatched VPN applications (Pulse Secure VPN), weak RDP passwords, and web application vulnerabilities (Telerik UI)[13]

May: Port Kemla Steelworks and Bluescope attacks

Jun: Lion beverage manufacturer cyberattack[16, 17]

Aug: New Zealand Stock Exchange DDoS attack[18]

NZX, MoneyGram, Braintree, other Fiserv DDoS attacks[19]

Nov: Law In Order ransomware attack [Netwalker][9, 10]

Dec: Accellion File Transfer Appliance vulnerability. Patched 72 hours post-discovery.

2021

Jan: Data breach of the Australian Securities and Investments Commission [Accellion vulnerability][5, 8]

Reserve Bank of New Zealand Breach [Accellion vulnerability][6, 7]

Mitigation Strategies

It's essential to use threat intelligence to understand your adversaries, prepare detection and mitigation strategies, and predict problems before they occur.[4] Understanding the social and geopolitical landscape will help prepare employees for specific lures that will be used against them.

Netwalker has recently been exploiting CVE-2019-11510 and CVE-2019-18935, with a recent move to Reflective Dynamic-Link-Library (DLL) injection. Because lures adapt quickly to events such as COVID-19, keeping patches for servers up to data is essential. Falling behind on patching results in an increased risk surface. Additionally, social engineering training – particularly phishing, conducted and tested regularly – will help reduce the risk of ransomware infection from that vector.

Mitigation of DDoS attacks is done by contacting your upstream internet provider and acquiring a reputable DDoS mitigation server that can react and remove the traffic before it can damage your infrastructure.

Supply chain attacks are going to continue to be a main entry point for many threat actors. The trust you have already established with vendors makes them a prime target. Do proper vetting of any vendors and monitor for any compromises they suffer. As in the case of the Accellion File Transfer Software vulnerability, be aware of the lifecycle of software and replace any that is coming to its end of life (EOL). Software is attacked more toward EOL and vulnerabilities are discovered that had been previously overlooked in such cases.

Finally, if you are in a particularly targeted industry such as medical research, video games, or are a supplier of goods and services to other industries, ensure you have a fully instituted and tested security program based on thereat intelligence in place. If you are required to hold certifications, be prepared to demonstrate those certifications and your testing results upon request.

As always, please reach out to **security@relativity.com** with any questions or concerns you may have.

About Relativity Trust

Thousands of organisations trust Relativity with their most sensitive data. We take every precaution to protect that data in a secure, performant system—as dependable as flipping a switch or turning on the tap.

Our internal security team, Calder7, includes cybersecurity, product security, compliance, and risk specialists with a simple mission: anticipate threats and stay ahead of the adversaries. Learn more about Calder7.

References

1. Election Cyber Threats in the Asia-Pacific Region
2. Netwalker Ransomware Explained: What You Need to Know
3. Threat intelligence and the importance of knowing your 'attackers'
4. Australian Financial Regulator Hit by Data Breach
5. ASIC reports server breached via Accellion vulnerability
6. Reserve Bank of New Zealand Investigates Data Breach
7. Reserve Bank of New Zealand investigates illegal access of third-party system
8. Australian Financial Regulator Hit by Data Breach
9. Law In Order – Cyber Security Incident
10. Law in Order Cyber Security Incident – King & Wood Mallesons response
11. NetWalker Ransomware Group Enters Advanced Targeting "Game"
12. Netwalker Ransomware Explained: What You Need to Know
13. Equinix breach: 7 things to know about netwalker ransomware attacks
14. Hackers Stole 220GB of Data in Toll Group Ransomware Attack
15. 5 Cybersecurity Issues to Address in the Asia-Pacific Region
16. Beverage maker Lion hit by cyber attack
17. Drinks giant Lion hit by cyber attack as hackers target corporate Australia
18. New Zealand Stock Exchange suffers day four disruption following DDoS attacks
19. DDoS extortionists target NZX, Moneygram, Braintree, and other financial services

Relativity

231 South LaSalle Street | 8th Floor | Chicago, Illinois 60604
+1 (312) 263-1177 | relativity.com