Analysis of SonicWall and Trellix Reports

Cyber security is constantly evolving, with new threats and trends emerging every year and attackers constantly developing new tactics. Therefore, staying informed about the latest threats and trends is crucial for both businesses and individuals to protect their data and systems. In this report, I review two important security reports by SonicWall and Trellix to provide insights into the current threat landscape and highlight developments and trends for 2023. I also completed this report with help from other companies' security reports.

Cyber Threat Report Analysis

This threat report examines the current cyber threat landscape, providing in-depth research on key trends, threats and forecasts for 2023. Some of the key findings include:

- **Decrease in ransomware attacks:** Ransomware attacks decreased by 36% in 2023 compared to the previous year. But it shows that ransomware is still a lucrative business for cybercriminals and organizations should be wary of such attacks.
- **Increasing cloud-based attacks:** As more businesses move to cloud environments, cybercriminals are adapting their tactics to target cloud infrastructure. For this reason, there has been a significant increase in cloud-based attacks. The report indicates that unauthorized cloud entries have increased by a total of 75%, with cloud-aware incidents rising by 110% year-on-year.
- **Growing interest in IoT devices and the proliferation of IoT devices:** The proliferation of Internet of Things (IoT) devices has created new opportunities for cybercriminals. And many IoT devices lack adequate security features, making them easy targets for hacking and exploitation.
- **Increase in AI-powered attacks:** Cybercriminals are increasingly using artificial intelligence (AI) and machine learning (ML) to create highly convincing social engineering attacks and avoid detection by security systems. In fact, recent blog posts from OpenAI and Microsoft reported that five major threat actors were found to be using OpenAI software for research, fraud and other malicious purposes and had their accounts closed.
- **Increase in the number of vulnerabilities:** There has been a significant increase in the number of vulnerabilities discovered in 2023, with more than 1,000 vulnerabilities discovered in the first half of the year alone. Therefore, it is critical to keep software and systems up to date.
- **Increase in the speed of cayber attacks:** Reports indicate that the average escape time has decreased by 22 minutes compared to the previous year, reaching 62 minutes. Additionally, the report notes that the fastest recorded attack lasted only 2 minutes and 7 seconds.
- **Focus on supply chain attacks:** Supply chain attacks are becoming more prevalent as cybercriminals begin to target third-party vendors and suppliers to gain access to sensitive information.

Threat Actors and Malware Mentioned in Reports

The threat actor groups that stand out in the two reports:

1. **APT28 and APT29:** APT groups linked to Russia. They are known to target government agencies, diplomatic organisations and other high-value targets.

2. **APT30 and APT41:** APT groups linked to the Chinese government. They can engage in both state-sponsored and for-profit activities. They can carry out wide-ranging attacks against a wide range of industries and organisations. APT30 usually carries out espionage attacks.
3. **APT34:** An APT group associated with the Iranian government. It is known to target organisations in the oil and gas sector. In the research conducted by Trellix, it was included in the list of the most common threat actors in the first quarter of 2023.
4. **Mustang Panda:** A hacker group based in China and often supported by the Chinese government. They are known for their financial theft and espionage activities, with a particular focus on financial institutions in Asia.
5. **Blind Eagle:** A hacker group associated with the Chinese government. It carries out cyber espionage activities and aims to steal military, political and economic information.
6. **Lazarus and UNC4191:** North Korea's government-sponsored hacker groups. They carry out attacks targeting international financial institutions and other organisations, espionage and enemies. UNC4191 was included in the list of the most common threat actors in the first quarter of 2023 in the research conducted by Trellix.
7. **Gamaredon Group: An** APT associated with Russia and targeting Ukraine. This group carries out attacks aimed at interfering in Ukraine's internal affairs and engages in cyber espionage activities.
8. **Sandworm Team:** A hacker group associated with Russia. They carry out cyber espionage activities and are particularly known for attacks on the energy sector. In addition, according to the SonicWall report, they have carried out attacks by actively using vulnerabilities in popular software such as WinRAR.
9. **Magecart Group**: It is a hacker group that attacks e-commerce sites to capture card information. Research conducted by Trellix shows that its activity has increased significantly.
10. **Common Raven:** It is a US government-sponsored hacker group and conducts cyber espionage activities. In the research conducted by Trellix, it was included in the list of the most common threat actors in the first quarter of 2023.

Notable malware include LockBit, Qakbot, AsyncRat, AgentTesla, RedLine, Cl0p, Emotet and Formbook. In addition, the reports also highlight the rise of malware types, particularly encrypted threats and the rise of cryptocurrency mining.

In addition, some of the trends experienced in 2023 are as follows:

- Malicious intrusions increased by 6 percent, encrypted threats rose by 117 percent, malware by 11 percent, and cryptocurrency mining surged by 659 percent.
- Small businesses are three times more likely to be targeted by threat actors than large organisations.
- Vulnerabilities are still the most common ransomware vector, with a record number of 28,834 CVEs published in 2023.
- Threat actors use innovative and different tactics, such as phishing campaigns and fake credit applications with spyware.
- Microsoft OneNote files have become a popular type of malicious Office files.
- Malware attacks on the financial industry have doubled.
- Ransomware attacks decreased by 36 per cent, but were still the third highest on record.
- The use of malicious PDFs has increased dramatically.

- Threat actors have started exploiting a new vulnerability in the popular Windows file archiving tool WinRAR.
- Ransom payments exceeded $1 billion for the first time.

Conclusion and Evaluation

Cyber security reports clearly show the complexity and diversity of threats and trends emerging in 2023. It also emphasises the need to raise cyber security awareness and take effective measures against threats. Therefore, it is critical for security experts and decision makers to continuously improve their security measures, keep their systems up-to-date, and adopt the latest technologies and strategies to deal with threats.

In conclusion, the increasing complexity and prevalence of cyber threats require increased cyber security awareness and measures. This is critical for ensuring a secure digital future.

REFERENCES

Trellix. (2023, June). The CybertThreat Report. Retrieved from https://www.trellix.com/assets/threat-reports/trellix-arc-threat-report-june-2023.pdf

SonicWall. (2024). SonicWall Cyber Threat Report. Retrieved from https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf

CrowdStrike. (2024). Global Threat Report. Retrieved from https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

CheckPoint. (2024) Ransomware Surge and AI Defense Innovations Highlighted in New Comprehensive 2024 Security Report. Retrieved from https://pages.checkpoint.com/2024-cyber-security-report

The World Economic Forum. (2024). Global Cybersecurity Outlook 2024 Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf