Report reveals no immunity from cyber attacks

Check Point Research, the threat intelligence arm of Check Point Software Technologies has published its 2020 Cyber Security Report which reveals the key attack vectors and techniques...

Source: pixabay.com

Check Point Research, the threat intelligence arm of Check Point Software Technologies, a provider of cybersecurity solutions globally, has published its 2020 Cyber Security Report. The Report highlights the main tactics cyber-criminals are using to attack organisations worldwide across all industries, and gives cybersecurity professionals and C-Level executives the information they need to protect their organisations from today's fifth-generation cyber-attacks and threats.

The 2020 Security Report reveals the key attack vectors and techniques observed by Check Point researchers during the past year. Highlights include:

- **Cryptominers still dominate malware landscape** – Even though cryptomining declined during 2019, linked to cryptocurrencies' fall in value and the closure of the Coinhive operation in March, 38% of companies globally were impacted by crypto-miners in 2019, up from 37% in 2018. This is because the use of crypto-miners remains a low-risk, high-reward activity for criminals

- **Botnet armies surge in size** – 28% of organisations globally were hit by botnet activity, an increase of over 50% compared with 2018. Emotet was the most common bot malware used, primarily because of its versatility in enabling malware and spam distribution services. Other botnet actions such as sextortion email activity and DDoS attacks also rose sharply in 2019.

- **Targeted ransomware hits hard** – While the number of impacted organisations is relatively low, the severity of the attack is much higher – as seen in 2019's damaging attacks against U.S. city administrations. Criminals are choosing their ransomware targets carefully, with the aim of extorting the maximum revenue possible.

- **Mobile attacks decline** – 27% of organisations worldwide were impacted by cyber-attacks that involved mobile devices in 2019, down from 33% in 2018. While the mobile threat landscape is maturing, organisations are also increasingly aware of the threat, and are deploying more protection on mobiles

- **The year Magecart attacks became an epidemic** – These attacks which inject malicious code into e-commerce websites to steal customers' payment data hit hundreds of sites in 2019, from hotel chains to from commerce giants to SMBs, across all platforms.

- **Rise in cloud attacks** – Currently, more than 90% of enterprises use cloud services and yet 67% of security teams complain about the lack of visibility into their cloud infrastructure, security, and compliance. The magnitude of cloud attacks and breaches has continued to grow in 2019. Misconfiguration of cloud resources is still the number one cause for cloud attacks, but now we also witness an increasing number of attacks aimed directly at cloud service providers.

"2019 presented a complex threat landscape where nation-states, cybercrime organisations and private contractors accelerated the cyber arms race, elevating each other's capabilities at an alarming pace, and this will continue into 2020," said Lotem Finkelsteen: Major Intelligence Officer, Check Point Software Technologies.

> *Even if an organisation is equipped with the most comprehensive, state-of-the-art security products, the risk of being breached cannot be completely eliminated. Beyond detection and remediation, organisations need to adopt a proactive plan to stay ahead of cybercriminals and prevent attacks. Detecting and automatically blocking the attack at an early stage can prevent damage. Check Point's 2020 Security Report shares what organisations need to look out for, and howthey can win the war against cyber-attacks through key best practices.*

Check Point's 2020 Security Report is based on data from Check Point's ThreatCloud intelligence, a collaborative network for fighting cybercrime which delivers threat data and attack trends from a global network of threat sensors; from Check Point's research investigations over the last 12 months; and on a brand new survey of IT professionals and C-level executives that assesses their preparedness for today's threats.

The report examines the latest emerging threats against various industry sectors and gives a comprehensive overview of the trends observed in the malware landscape, in emerging data breach vectors, and in nation-state cyber-attacks. It also includes expert analysis from Check Point's thought leaders, to help organisations understand and prepare themselves for today's and tomorrow's complex threat landscape.

For more details download the full report.