Cryptominers hit 10x more organisations than ransomware in 2018

Check Point Software Technologies has published the second instalment of its 2019 Security Report. It highlights how the tools and services used to commit cyber-crime have become democratised, with advanced attack methods now available to anyone willing to pay for them, as part of the growing 'malware-as-a-service' industry.

Source: pixabay.com

The second instalment of the 2019 Security Report reveals the key cyber-attack trends observed by Check Point researchers during 2018, and shows the significant growth in stealthy, complex attacks designed to stay below the radar of enterprise security teams. It also shows the types of cyberattacks which enterprise IT and security teams rate as the biggest threats to their organisations. Highlights include:

Report reveals 37% of organisations impacted by cryptomining

11 Feb 2019

Cryptominers digging undetected on networks: cryptominers infected 10x more organisations than ransomware in 2018, but only one in five IT security professionals were aware their company's networks had been infected by mining malware. Thirty-seven percent of organisations globally were hit by cryptominers in 2018, and 20% of companies continue to be hit every week despite an 80% fall in cryptocurrency values.

Threat risk of cryptominers underrated by organisations: when asked what they rated as the biggest threats to their organisation, just 16% stated cryptomining, compared with DDoS attacks (34%), data breaches (53%), ransomware (54%) and phishing (66%). This is concerning, as cryptominers can easily act as stealth backdoors to download and launch other

types of malware.

Malware-as-a-service rises: the GandCrab Ransomware-as-a-Service affiliate program shows how amateurs can now profit from the ransomware extortion business as well. Users keep up to 60% of the ransoms collected from victims, and its developers keep up to 40%. GandCrab has over 80 active affiliates, and within two months in 2018 had infected over 50,000 victims and claimed between $300,000 and $600,000 in ransoms.

“The second instalment of our 2019 Security Report shows how cyber-criminals are successfully exploring stealthy new approaches and business models, such as malware affiliate programs, to maximize their illegal revenues while reducing their risk of detection. But out-of-sight shouldn’t mean out-of-mind: even though cyberattacks during 2018 have been lower-profile, they are still damaging and dangerous,” said Peter Alexander, chief marketing officer of Check Point Software Technologies.

“By reviewing and highlighting these developments in the Report, organisations can get a better understanding of the threats they face, and how they prevent them impacting on their business.”

Check Point’s 2019 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 fifth-generation cyber-attacks and threats.

Get the full report here.

For more, visit: https://www.bizcommunity.com