Report reveals 37% of organisations impacted by cryptomining

A new report, by Check Point Software Technologies, shows 20% of companies globally continue to be hit by cryptomining attacks every week; 33% of companies were hit by mobile malware, and just 4% by ransomware in the past 12 months.

Check Point Software Technologies, a global provider of cybersecurity solutions, has published the first instalment of its 2019 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.

Are we prepared for 2019's cyber security challenges?

Grant Hamilton 15 Jan 2019

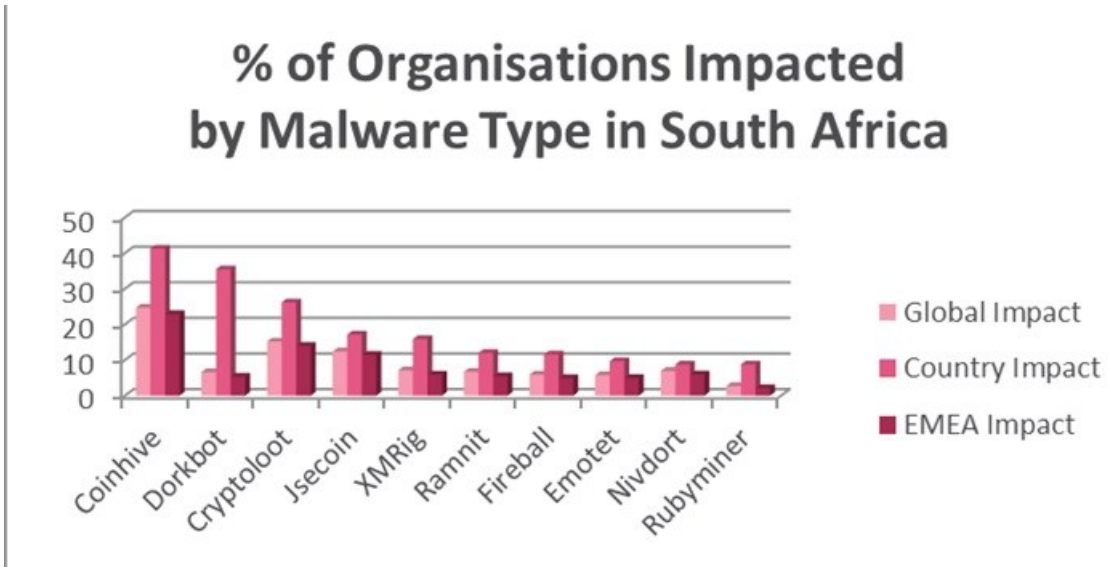
The first instalment of the 2019 Security Report reveals the key malware trends and techniques observed by Check Point researchers during the past year.

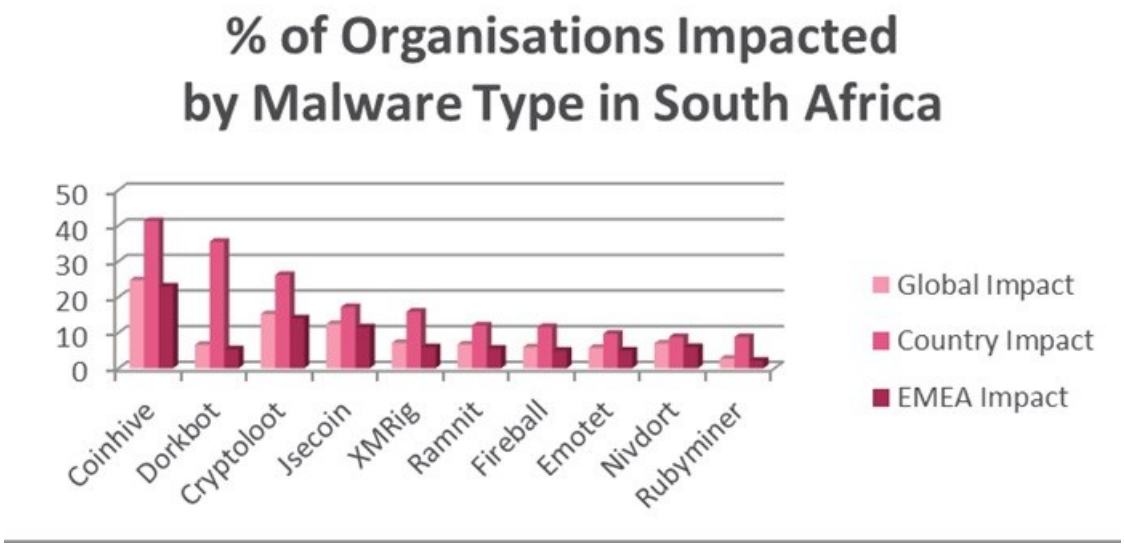
Highlights include:

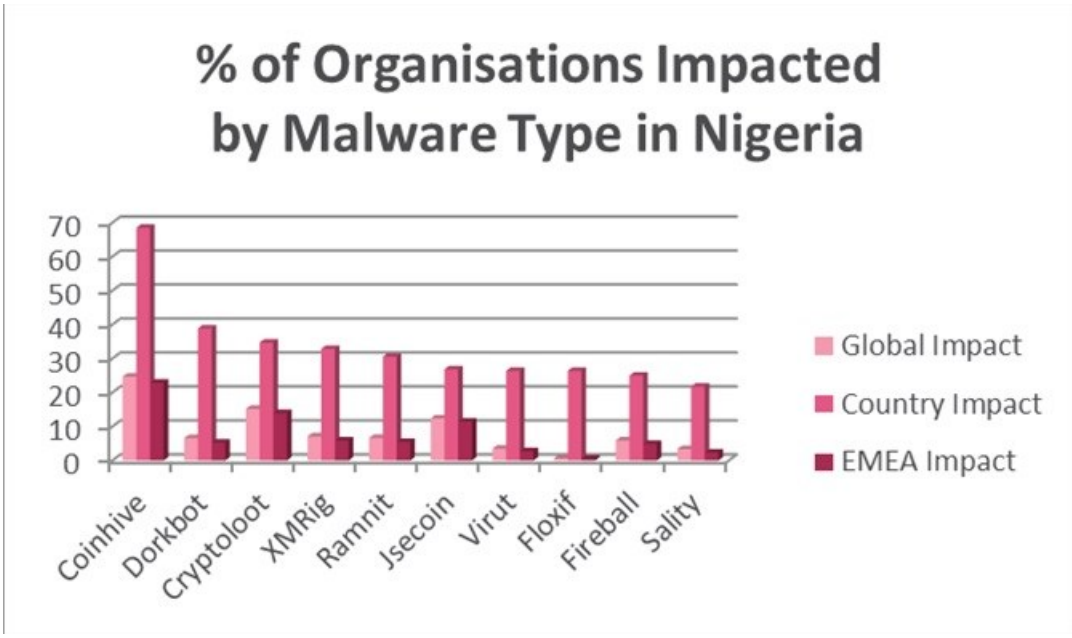
- **Cryptominers dominated the malware landscape**: Cryptominers occupied the top four most prevalent malware types and impacted 37% of organisations globally in 2018. Despite a fall in the value of all cryptocurrencies, 20% of companies continue to be hit by cryptomining attacks every week. Cryptominers have also highly evolved recently to exploit high profile vulnerabilities and to evade sandboxes and security products in order to expand their infection rates.

From a local perspective, cryptominers also dominated the malware landscape in 2018. Organisations in three of the key counties in Africa were highly impacted by Coinhive, which is a crypto-miner:

- 41.29% of organisations in South Africa
- 69.96% of organisations in Kenya
- 68.52% of organisations in Nigeria







Mobiles are a moving target: 33% of organisations worldwide were hit by mobile malware, with the leading three malware

types targeting the Android OS. 2018 saw several cases where mobile malware was pre-installed on devices and apps available from app stores that were actually malware in disguise.

- **Multi-purpose botnets launch range of attacks**: Bots were the third most common malware type, with 18% of organisations hit by bots which are used to launch DDoS attacks and spread other malware. Bot infections were instrumental in nearly half (49%) of organisations experiencing a DDoS attack in 2018.
- **Ransomware attacks in decline**: 2018 saw ransomware usage fall sharply, impacting just 4% of organisations globally.

“From the meteoric rise in cryptomining to massive data breaches and DDoS attacks, there was no shortage of cyber-disruption caused to global organisations over the past year. Threat actors have a wide range of options available to target and extract revenues from organisations in any sector, and the first instalment of the 2019 Security Report highlights the increasingly stealthy approaches they are currently using,” said Peter Alexander, chief marketing officer of Check Point Software Technologies.

“These multi-vector, fast-moving, large-scale Gen V attacks are becoming more and more frequent, and organisations need to adopt a multi-layered cybersecurity strategy that prevents these attacks from taking hold of their networks and data. The 2019 Security Report offers knowledge, insights and recommendations on how to prevent these attacks.”

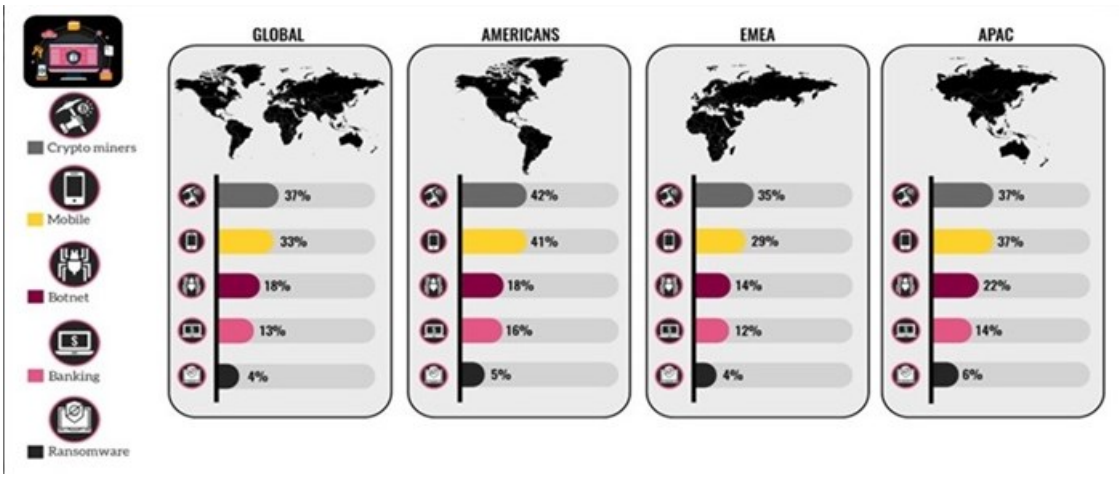


Diagram shows the top cyber-attack categories globally, and by region

Check Point’s 2019 Security Report is based on data from Check Point’s ThreatCloud intelligence, the largest 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 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.