BIZCOMMUNITY

South Africa experiences an increase in cyber attacks

Check Point Software Technologies has revealed that a rising number of people using video-on-demand services, as well as an increase in e-commerce over the festive season, could be why South Africa shot up the list of countries most attacked by cybercriminals in January 2016.

©Dmitriy Shironosov via 123RF

South Africa appeared at number 22 on the list last month, up from 67th in December. Namibia remains the most-attacked country for the second month in a row, with Ethiopia ranking in the 10th position. After spending two months in the top 20, Nigeria improved its ranking to 30th position, from 17th, while Kenya slid ten places to 54th.

“We’ve seen an increase in phishing attacks targeting video-on-demand users, who are tricked into handing over their passwords under the guise that their accounts need to be updated,” says Doros Hadjizenonos, country manager of Check Point South Africa. “These mails also install malware onto the user’s PC, which steals personal information, such as banking details, without the user knowing.”

Dodgy websites

A rise in e-commerce and online shopping over the festive season is another reason for the increase in cyber attacks, says Hadjizenonos. “Cybercriminals also use phishing to get users to visit dodgy websites and download fake apps. Tactics often involve ‘discounts’ when shopping online or through a retailer’s app. What consumers are often unaware of is that, even though the app or URL look legitimate, they have been designed with the sole purpose of stealing information.”

Based on threat intelligence drawn from its ThreatCloud World Cyber Threat Map, which tracks how and where cyber attacks are taking place worldwide in real time, Check Point identified more than 1,500 different malware families during January, continuing the trend first seen in December 2015 when the number of active families rose by 25%.

While the Conficker and Sality families remained the two most commonly used malware for the second month running, collectively accounting for 34% of all attacks globally, Dorkbot, associated with DDoS attacks and exploits targeting sensitive data, was a new entry to the top three, responsible for 5% of attacks during the month.

Top malware families

The top three malware families, which accounted for 39% of the total attacks in January were:

• ↔ Conficker - accounted for 24% of all recognised attacks; machines infected by Conficker are controlled by a botnet. It also disables security services, leaving computers even more vulnerable to other infections.

• ↑Sality - virus that allows remote operations and downloads of additional malware to infected systems by its operator. Its main goal is to persist in a system and provide means for remote control and installing further malware.

• ↑Dorkbot - IRC-based Worm designed to allow remote code execution by its operator, as well as download additional malware to the infected system, with the primary motivation being to steal sensitive information and launch denial-of-service attacks.

Check Point's research also revealed the most prevalent mobile malware during January 2015, and once again attacks against Android devices were significantly more common than iOS. **The top three mobile malware were:**

• ↑ AndroRAT - malware that is able to pack itself with a legitimate mobile application and install without the user's knowledge, allowing a hacker full remote control of an Android device.

• ↓ Xinyin - observed as a Trojan-Clicker that performs Click Fraud on Chinese ad sites.

• ↑Leech - malware designed to send text messages from infected mobile devices to premium rate numbers hard-coded within the file.

"The increase in DDoS attacks against public websites has been well publicised in the past couple of months, and the fact that the Dorkbot family is becoming more prevalent underlines the fact that businesses need to be taking steps to protect themselves against such attacks.

"The range and volume of attacks that organisations face have continued to grow in the early stages of 2016, highlighting the challenges they face in securing their networks. As such it is critical that organisations deploy protection to prevent them being exploited and ensure that their data is secure," concludes Hadjizenonos.