Africa more vulnerable to mobile malware

Quarterly analysis of the global Threat Index by Check Point Software Technologies reveals deep disparities in the threat environments in Africa, and the potential for increased attacks as cyber-criminals target mobile devices.

Rick Rogers

Check Point is the largest global pure-play network cyber security vendor and their Threat Index provides a data-based breakdown of new and prevalent threats, as well as the relative rankings of countries' risk profiles globally.

The higher the ranking, the greater the threat of cyber-attack. At the end of the first quarter of 2016 (January – March 2016), Nigeria ranks as the 16th highest ranked country, moving up two places from 18th position in the preceding quarter.

Developing and African nations are highly represented in the upper rankings of the index, and Nigeria was surpassed by a handful of other African countries, including Namibia and Malawi in second and fourth spots, respectively.

In stark contrast, Kenya improved its ranking by 24 places, moving from 45th position at the end of 2015, to 69th at the end of the quarter.

The Index is based on threat intelligence drawn from Check Point's ThreatCloud World Cyber Threat Map, which tracks how and where cyber attacks are taking place worldwide in real time.

Rick Rogers, area manager for East and West Africa at Check Point Software Technologies, says Nigeria's worsening ranking may be due to a dramatic increase in threats targeting mobile devices specifically, while Kenya's improvement could reflect a growing maturity in security awareness.

"It's not immediately clear why the East and West African hubs are experiencing such different moves in terms of cyber-

attacks, and we are generally seeing a lot of volatility month to month for many of the countries on the index. But this quarter, mobile malware ranked as one of the 10 most prevalent attack types affecting corporate networks and devices for the first time ever.

“With Africa being the ‘mobile-first’ and often ‘mobile-only’ continent, this new wave of threats is likely to have a strong impact on the number of attacks evidenced in the region,” he continued. “Individuals who run their businesses off mobile devices, as well as organisations which have a bring-your-own-device policy, will need to prepare for this in their security strategy. It is necessary to apply the same level of security to mobile as required by traditional networks and PCs, and security professionals must have a coherent, over-arching threat management approach that addresses this.”

It is necessary to apply the same level of security to mobile as required by traditional networks and PCs.

The previously-unknown HummingBad agent was a large contributor to the new top 10 positioning of mobile threats. Discovered by Check Point in February 2016, HummingBad immediately became the seventh most common malware detected targeting corporate networks and devices, and in March it moved up to the sixth top spot.

...With Africa being the ‘mobile-first’ and often ‘mobile-only’ continent, this new wave of threats is likely to have a strong impact...

Hummingbad targets Android devices specifically, facilitating malicious activity such as installing a key-loggers, stealing credentials and bypassing encrypted email containers used by companies, allowing for interception of corporate data. It was the third highest threat in Kenya in Q1 and seventh in Nigeria.

Check Point identified more than 1,500 different malware families during January, 1,400 in February and 1,300 in March. Throughout the quarter, the Conficker and Sality families were two of the most commonly used malware variants in the quarter, with Sality ranking first in both Nigeria and Kenya. In mobile devices specifically, Hummingbad ended the quarter as the top threat globally.

The decrease in the variety of malware families reflects a concentration trend, rather than a decrease in absolute volume of threats, and is perhaps an indicator of the sophistication of the threat environment: cyber criminals do not need to develop entirely new malware; rather it is often sufficient to make small changes to existing families to circumvent security.

The Threat Map is powered by Check Point’s ThreatCloudTM intelligence, the largest collaborative network to fight cybercrime, delivering threat data and attack trends from a global network of threat sensors. The ThreatCloud database holds over 250 million addresses analysed for bot discovery, over 11 million malware signatures and over 5.5 million infected websites, and identifies millions of malware types daily.

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