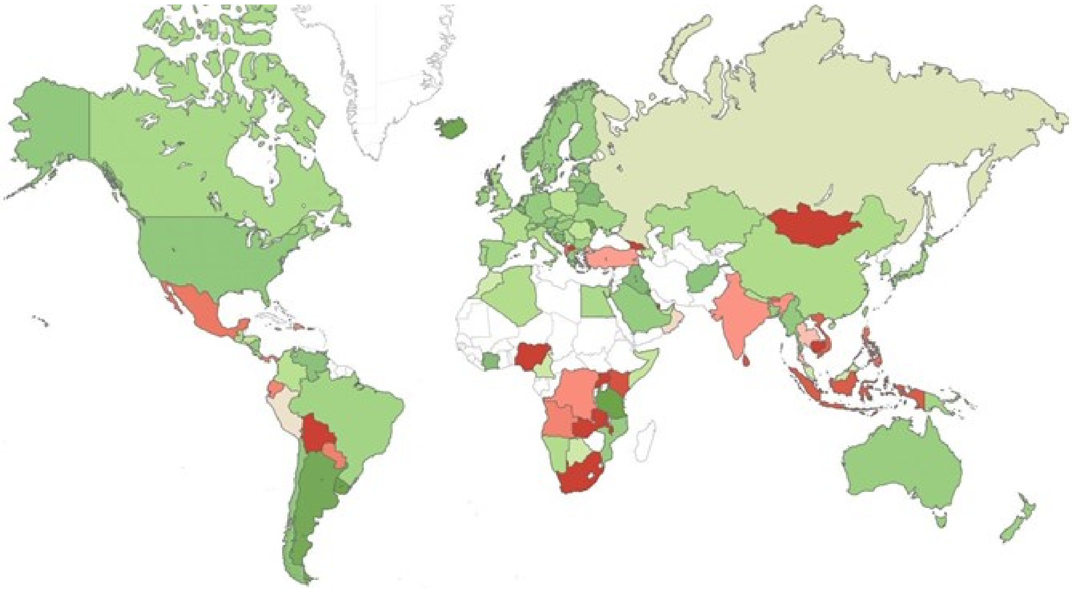
Top five highest cyber risk countries are in Africa

According to Check Point's latest Threat Index, African nations continue to top the list of countries prone to cyber attacks.



Zambia has the highest risk profile, with Nigeria in second position. Uganda, Malawi, and South Africa are ranked 7th, 8th, and 9th respectively. South Africa, in particular, demonstrated a significant jump in ranking, having moved up from 22nd position since last month.

The Index also revealed that more than one in four organisations globally was affected by the Fireball or WannaCry attacks during May.

Two of the top three malware families that impacted networks globally were zero-day, previously unseen attacks. Fireball impacted one in five organisations worldwide, with second-placed RoughTed impacting 16% and third-placed WannaCry affecting nearly 8% of organisations globally. The two malware variants, Fireball and WannaCry, rapidly spread worldwide throughout the month of May.

The most prevalent malware highlight the wide range of attack vectors and targets cyber-criminals are utilising, impacting all stages of the infection chain. Fireball takes over target browsers and turns them into zombies, which it can then use for a wide range of actions including dropping additional malware, or stealing valuable credentials.

RoughTed

By contrast, RoughTed is a large-scale malvertising campaign, and WannaCry takes advantage of a Windows SMB exploit called EternalBlue in order to propagate within and between networks. WannaCry was particularly high profile, bringing down a myriad of networks worldwide.

In addition to the top three, there were also other new variants of malware seen within the top ten of the index including Jaff (8th) another form of ransomware, demonstrating how profitable this particular attack vector is proving for malicious parties.

May 2017's top three 'most wanted' malware:

*The arrows relate to the change in rank compared to the previous month.

1. ↑ Fireball - Browser hijacker that can be turned into a full-functioning malware downloader. It is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware.
2. ↑ RoughTed - Large-scale malvertising used to deliver various malicious websites and payloads such as scams, adware, exploit kits and ransomware. It can be used to attack any type of platform and operating system, and utilises ad-blocker bypassing and fingerprinting in order to make sure it delivers the most relevant attack.
3. ↑ WannaCry - Ransomware that was spread in a large scale attack in May 2017 utilising a Windows SMB exploit called EternalBlue in order to propagate within and between networks.

In mobile malware, Hummingbad returned to the top of the list and was closely followed by Hiddad and Triada:

Top three 'most wanted' mobile malware:

1. Hummingbad - Android malware that establishes a persistent rootkit on the device, installs fraudulent applications, and with slight modifications could enable additional malicious activity such as installing a key-logger, stealing credentials and bypassing encrypted email containers used by enterprises.
2. Hiddad - Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is displaying ads, however it is also able to gain access to key security details built into the OS, allowing an attacker to obtain sensitive user data.
3. Triada - Modular Backdoor for Android which grants superuser privileges to downloaded malware, as this helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.

Commented Rick Rogers, area manager for East and West Africa at Check Point Software Technologies: "Organisations need to remember that the financial impact from cyber attacks goes way beyond the initial incident. Restoring key services and repairing reputational damage can be a very long and expensive process. As such, organisations in every industry sector need a multi-layered approach to their cybersecurity. Our SandBlast Zero-Day Protection and Mobile Threat Prevention, for example, protect against the widest range of continually evolving attack types, and also protect against zero-day malware variants."

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