Threat Map shows African nations under cyber attack

Check Point Software Technologies Ltd released the October 2015 statistics for its ThreatCloud World Cyber Threat Map. Statistics found that for the month of October, Tanzania was the most attacked country in the world when it comes to cybercrime.

Mohamed Mbussa via Wikimedia Commons

Six other African countries - Malawi (4), Namibia (5), Mauritius (7), Tunisia (8), Ethiopia (9) and Nigeria (20) - were ranked in the top 20 most-attacked countries, ahead of Kenya (52) and South Africa (67).

"Many African countries have well-developed mobile internet networks that make it affordable for people to be online all the time. Hackers often target less developed countries, which may be behind the likes of South Africa and Kenya in terms of IT security, to gain backdoor access into larger countries or organisations," says Doros Hadjizenonos, Country Manager of Check Point South Africa.

"A large bank in South Africa could have a small branch in Tanzania. Hackers could exploit weaker security controls in Tanzania to gain entry into the bank's larger network. This is why third-party links should be subject to even more stringent security controls," said Hadjizenonos.

Based on threat intelligence, the Threat Map tracks how and where cyber attacks are taking place worldwide in real time, and identified more than 1,500 different malware families during October. The three most common malware types focus on remote control of infected PCs, enabling them to be used for launching DDoS and spam campaigns. Attacks using two malware families that enable ransomware scams and theft of users' credentials also rose sharply.

The top three malware families, which accounted for nearly 40% of the total recognised attacks in October, were:

1. Conficker - accounted for 20% of all recognised attacks, down from 28% in September. Machines infected by Conficker are controlled by a botnet. It also disables security services, leaving computers even more vulnerable to other infections.

2. Sality - the second most common attack, making up 10% of the total identified. Sality allows remote operations and downloads of additional malware to infected systems by its operator. Its main goal is to persist in a system to enable remote control and instaling further malware.

3. Cutwail - the third most common attack, a botnet mostly used for sending spam, as well as some DDoS attacks.

Changes to the top-ranking malware compared with September were the emergence in 4th place of the Neutrino EK exploit kit, which is linked with ransomware attacks. Also, the use of Fareit malware, which steals users' credentials from web browsers and emails, increased dramatically, taking it from 93 up to number 10.

"The data shows how established malware families are still being used to try and gain a foothold on organisations' networks, and highlights the rapid emergence of new attack types. It's easy for hackers to make small changes to malware code to enable it to bypass conventional defences, so companies need to deploy advanced technologies that can stop malware from entering their networks. By highlighting the top malware families and trends, organisations can better understand what methods attackers are currently favouring, and take steps to strengthen their security stance," said Hadjizenonos.

Cybercriminals are also targeting mobile devices to try and access sensitive data. **The top three mobile malware families in October were all Android-based exploits:**

1. Ztorg - a Trojan that uses root privileges to download and install applications on the mobile phone without the user's knowledge. This malware grew by 30% from September.

2. Xinyin - a Trojan-Clicker that performs click fraud mostly on Chinese advertising sites.

3. Plankton - a Trojan that collects data and sends it to a remote server. It has the ability to download additional code and run it on the mobile device, as well as accepting and executing various commands from the C&C server.

"In the past three months we have seen an increase of 20-35% per month in the amount of attacks for recognised mobile malware families, which is much higher than the growth of general malware families," says Hadjizenonos. "Threats targeting mobile devices are growing rapidly, but many organisations are not applying adequate security measures to protect them or their users, putting sensitive corporate data at risk. Companies need to be aware of these risks and apply security to stop mobile malware."

The ThreatCloud Map is powered by Check Point's ThreatCloudTM intelligence, the largest collaborative network to fight cybercrime that 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, over 11 million malware signatures and over 5.5 million infected websites, and identifies millions of malware types daily.