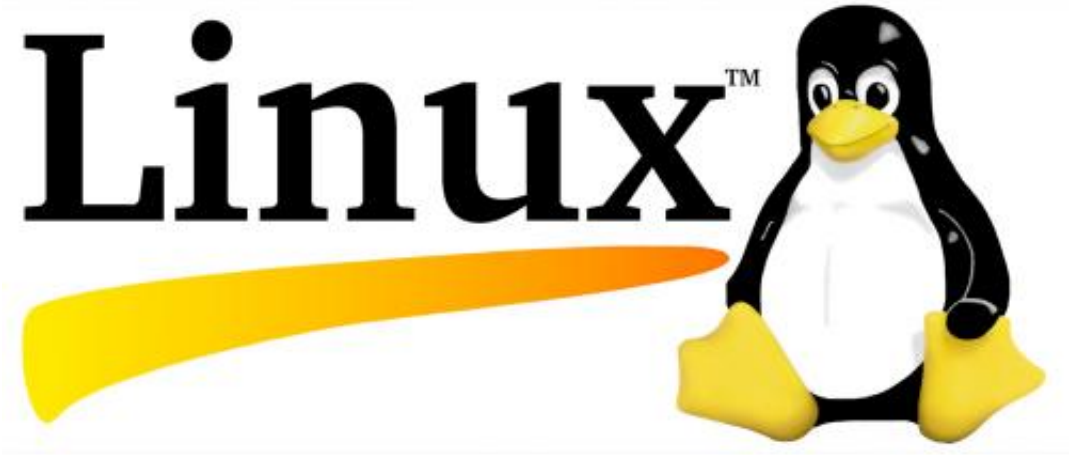
Crippling Linux botnet strikes gaming, education sites

October 1 2015, by Nancy Owano



The IT world was given the word this week that a botnet is preying on Linux computers and the attacks are powerful. Most of the targets are in Asia and security experts tracking these attacks say the botnet appears to be of Asian origin.

There is a network of Linux computers flooding gaming and education sites with as much as 150 gigabits per second of malicious traffic, said Dan Goodin of *Ars Technica*, enough in some cases to knock the targets

offline.

This is a distributed denial-of-service (DDoS) network. The findings are from Akamai Technologies. Akamai's Security Intelligence Response Team (SIRT) considered the botnet, XOR DDoS, as "High Risk" in an advisory posted on Tuesday.

The XOR DDoS botnet has grown and is now capable of mega DDoS attacks of 150+ Gbps—-they are using a Trojan malware to hijack the Linux systems. How do the attackers pull this off?

They first gain access by brute force attacks to discover the password to Secure Shell services on a Linux machine. Once the login is acquired, the attackers use root privileges to run a Bash shell script, downloading and executing the malicious binary.

"Akamai's Security Intelligence Response Team (SIRT) is tracking XOR DDoS, a Trojan malware that DDoS attackers have used to hijack Linux machines to build a botnet for distributed denial of service (DDoS) attack campaigns with SYN and DNS floods."

Here are some key points on what Akamai discovered: The gaming sector has been the primary target, followed by educational institutions. The botnet has attacked up to 20 targets per day, 90 percent of which were in Asia. The malware spreads via Secure Shell (SSH) services susceptible to brute-force attacks due to weak passwords.

The situation could travel from bad to worse. Akamai's team expected the XOR DDoS activity to continue "as attackers refine and perfect their methods, including a more diverse selection of DDoS attack types."

According to the Akamai team, the IP address of the bot is sometimes spoofed, but not always. The attacks observed in the DDoS campaigns

against Akamai customers were a mix of spoofed and non-spoofed attack traffic.

Lucian Constantin of IDG News Service said on Tuesday that this power to generate crippling attacks at over 150 Gbps represents many times greater than a typical company's infrastructure can withstand.

Meanwhile, an advisory detailing this threat in full, including DDoS mitigation payload analysis and malware removal information, is available for download from Akamai. Removing the XOR DDoS malware is a four-step process for which several scripts are provided in the advisory.

Wait a minute, isn't Linux considered especially secure? Stuart Scholly, senior vice president and general manager, Security Business Unit, Akamai, said " XOR DDoS is an example of attackers switching focus and building botnets using compromised Linux systems to launch DDoS attacks. This happens much more frequently now than in the past, when Windows machines were the primary targets for DDoS malware."

Constantin said the XOR DDoS-reflected a wider trend of "hijacking poorly configured Linux-based systems for use in DDoS attacks. Old and unmaintained routers are especially vulnerable to such attacks, as several incidents have shown over the past two years."

More information: www.stateoftheinternet.com/res … tion-yara-snort.html