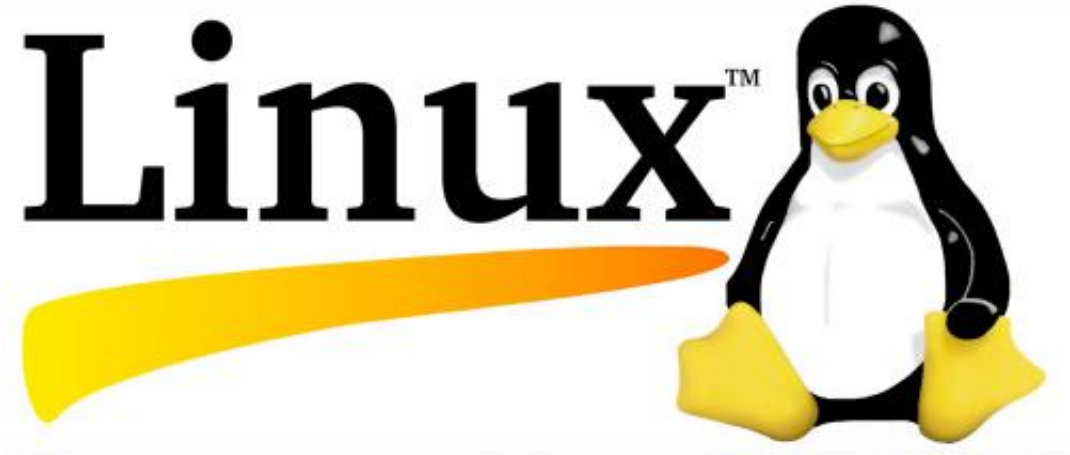
Operation Windigo: Linux server-side malware campaign exposed

March 19 2014, by Nancy Owano



(Phys.org) —Security researchers announced Tuesday a multi-year cybercriminal campaign called Windigo in which a malicious group compromised thousands of Linux and Unix servers. Once infected, victims' systems were used to steal credentials, redirect web traffic to malicious content and send millions of spam messages per day.

The security solutions company ESET said that Windigo, while largely unnoticed by the security community, has been in operation for more

than two and a half years. Pierre-Marc Bureau, security intelligence program manager at ESET, said Windigo currently has 10,000 servers under its control. "This number is significant if you consider each of these systems have access to significant bandwidth, storage, computing power and memory." Exploring this campaign, the ESET security research team collaborated with CERT-Bund, the Swedish National Infrastructure for Computing and other agencies, observing that, once infected, victims' systems are used to redirect web traffic to malicious content and send spam.

With thousands of Linux and Unix servers compromised, the Windigo operation is recognized as a large-scale effort. Its purpose seems to be monetary profit, the team said. The main components of the Windigo operation are an OpenSSH backdoor, a web redirection module and a spam-sending program. Servers located throughout the U.S., Germany, France and the UK are among those infected

A detailed report by the ESET team was published on Tuesday, titled Operation Windigo, and the report is described as a "vivisection" of a Linux server-side campaign of malware. This operation. ongoing since 2011, affected servers and companies and organizations. Among those who fell victim included the Linux Foundation. The ESNET team said the Windigo operation does not leverage any new vulnerability against Linux or Unix systems. Known systemic weaknesses were exploited by the malicious actors in order to build and maintain their botnet.

Among the team's key findings: Malicious modules used in Operation Windigo are designed to be portable. The spam-sending module has been seen running on all kinds of operating systems while the SSH backdoor has been witnessed both on Linux and FreeBSD servers. More than 25,000 unique servers have been compromised in the last two years. The quality of the various malware pieces is high, with stealthy, portable, sound cryptography (session keys and nonces) and shows a deep

knowledge of the Linux ecosystem.

ESET researchers are advising webmasters and system administrators on what actions may be taken if a compromise is discovered,. "If IT administrators discover their systems are infected, they are advised to wipe affected computers and reinstall the operating system and software. For a higher level of protection in the future, technology such as two-factor authentication should be considered."

The report's conclusion also talks about the issue of password authentication. "We conclude that password-authentication on servers should be a thing of the past." The team stated that "the game has changed regarding the management of servers on the Internet. Password-based login to servers should be a thing of the past. One should seriously consider two-factor authentication or, at least, a safe use of SSH keys."

The company has global headquarters in Bratislava (Slovakia), with malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow, Montreal, and Moscow and a partner network.

More information: www.welivesecurity.com/wp-cont … peration_windigo.pdf

Citation: Operation Windigo: Linux server-side malware campaign exposed (2014, March 19) retrieved 25 April 2024 from https://techxplore.com/news/2014-03-windigo-linux-server-side-malware-campaign.html