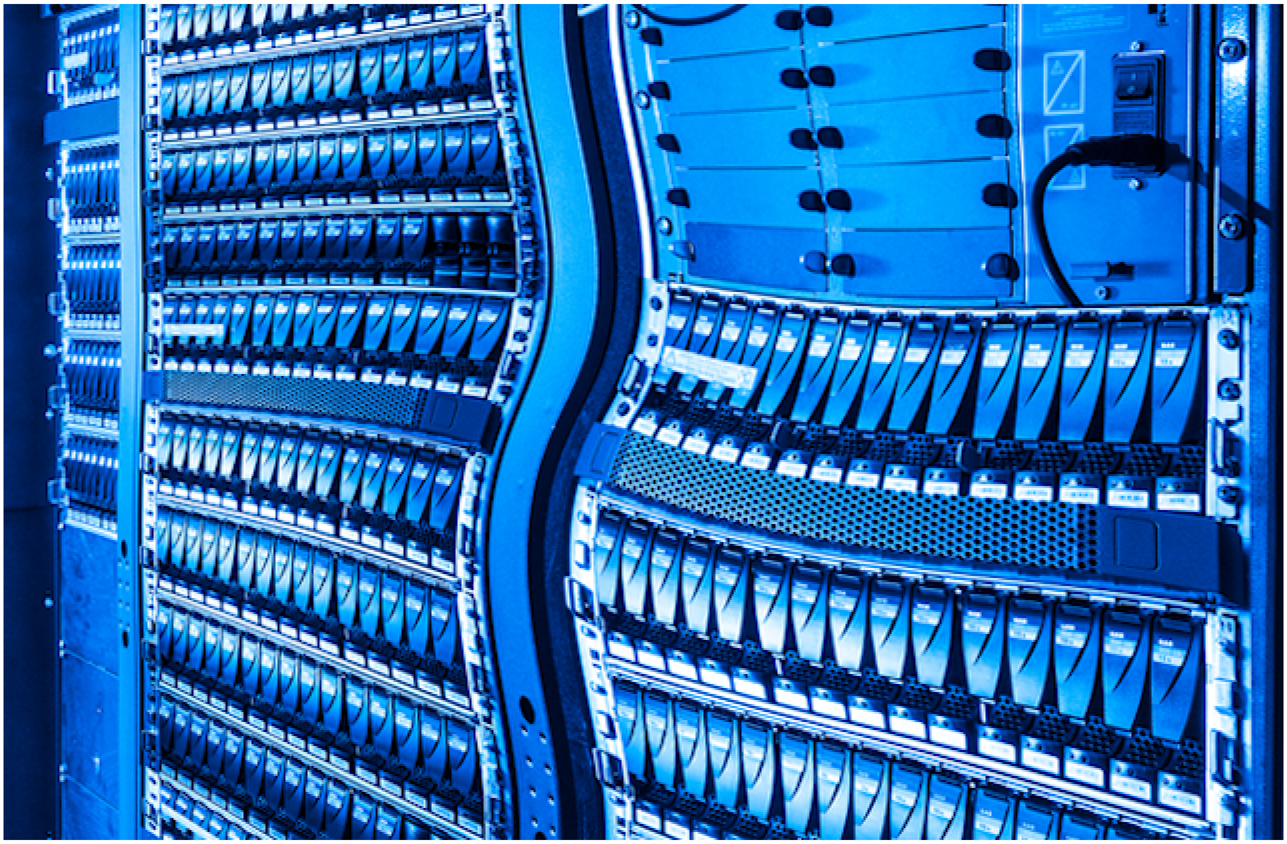
Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign

welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

March 18, 2014



Our report titled “Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign" details our analysis of a set of malicious programs that infect servers and desktop PCs, and send nearly 500,000 web users to malicious content daily."

18 Mar 2014 - 01:30PM

Our report titled “Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign” details our analysis of a set of malicious programs that infect servers and desktop PCs, and send nearly 500,000 web users to malicious content daily.”

A month ago, ESET published a technical analysis on Linux/Ebury. This malware is a clever OpenSSH backdoor and credential stealer. Since last year, ESET’s research team has been investigating the operation behind Linux/Ebury. We discovered an infrastructure used for malicious activities that is all hosted on compromised servers. We were also able to find a link between different malicious components such as Linux/Cdorked, Perl/Calfbot and Win32/Glupteba.M and realized they are all operated by the same group.

Today, we are publishing the results of significant amounts of research effort in a report titled “Operation Windigo – The vivisection of a large Linux server-side credential stealing malware campaign”. This report details our analysis of a set of malicious programs that are used together to infect servers and desktop computers. We chose the name “Windigo” for its North American first nation roots and for its references to a malevolent half-beast.

The gang behind Operation Windigo uses infected systems to steal credentials, redirect web traffic to malicious content, and send spam messages. According to our analysis, **over 25,000 servers** have been affected over the last two years. More than 10,000 of them are still infected today. These servers have all been compromised with the Linux/Ebury OpenSSH backdoor. This number is significant if you consider each of these systems have access to significant bandwidth, storage, computing power and memory. Well known organizations such as cPanel and kernel.org were on the list of victims, although they have now cleaned their systems.

The infected servers are used to redirect **half of a million** web visitors to malicious content on a daily basis. Our research also shows that the attacker is able to send more than 35,000,000 spam messages per day with his current infrastructure. Operating systems affected by the spam component include Linux, FreeBSD, OpenBSD, OS X, and even Windows (with Perl running under Cygwin).

During the course of our analysis, we have had the opportunity to collaborate with various international organizations, including CERT -Bund, the Swedish National Infrastructure for Computing, the European Organization for Nuclear Research (CERN) and others forming an international Working Group. With the help of the working group, thousands of victims have been notified that their servers were infected, in an effort to clean as many systems as possible. We are now releasing a complete white paper in hopes of raising awareness around Operation Windigo and motivating administrators to clean up their compromised servers.

We have been working hard to prepare this report. First of all because the threats we have analyzed are complex and stealthy. Secondly, because we have accumulated massive amounts of data, ranging from traffic capture to malicious URLs and binaries. Lastly, because we wanted to provide extensive guidance to help system administrators and network operators determine if servers are compromised and what can be done about it. We hope you enjoy reading our report as much as we enjoyed putting it together.

18 Mar 2014 - 01:30PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion