Sucuri Blog

blog.sucuri.net/2014/03/windigo-linux-analysis-ebury-and-cdorked.html

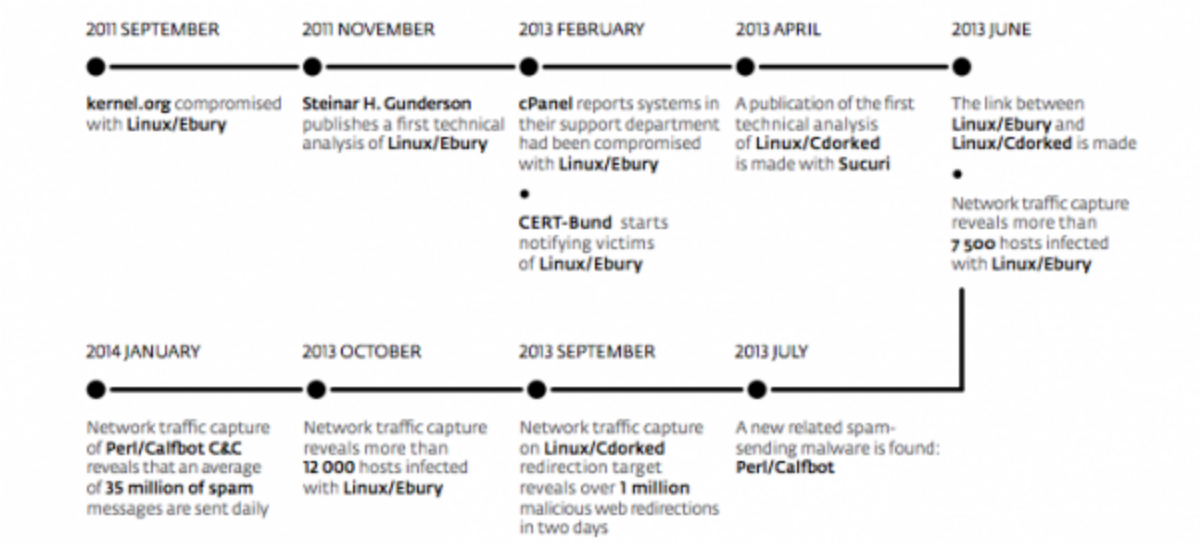
Daniel Cid March 18, 2014

Our friends over at ESET released a very detailed document about the Windigo Operation. The Windigo Operation has been responsible for the compromise of thousands of Linux servers over the years. When you hear terms like **Ebury, CDorked, Calfbot** and others, they are all related to each other.

Over the last few years, our team has been handling and fixing compromised servers and we can attest to how complex the clean up for this infection can be. We've seen that the servers we've fixed have been misused for distribution of malware, SPAM and, in some cases, to steal credit cards on compromised web servers used for e-commerce.

Windigo Timeline

The timeline released by ESET matches what we have been seeing and it goes back to 2011 when Linux/eBury was first seen. It goes through many evolutions, including our joint analysis of CDORKED on 2013 and the SSH backdoors:



Windigo Indicators of Compromise (IOC)

If you run a Linux server and you are worried it might be infected, they provide a few techniques (indicators of compromise) to check if the server is hacked.

- **For Linux/Ebury.** Run the **ssh -g** command. If it returns an error about missing argument, you know you are compromised.
- **For Linux/CDorked.** Run **curl** to **favicon.iso** and see if you get redirected to Google.com. If you do, you know you are compromised.

These apply to the latest versions of the malware. Old versions have different indicators and we explain them on our previous blog posts. Note that with the release of this document, the malware authors will likely change operations and the behavior of the code. So do not expect it to last long.

We recommend reading the whole PDF here: http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

If you need help cleaning up a compromised Linux server, let us know.