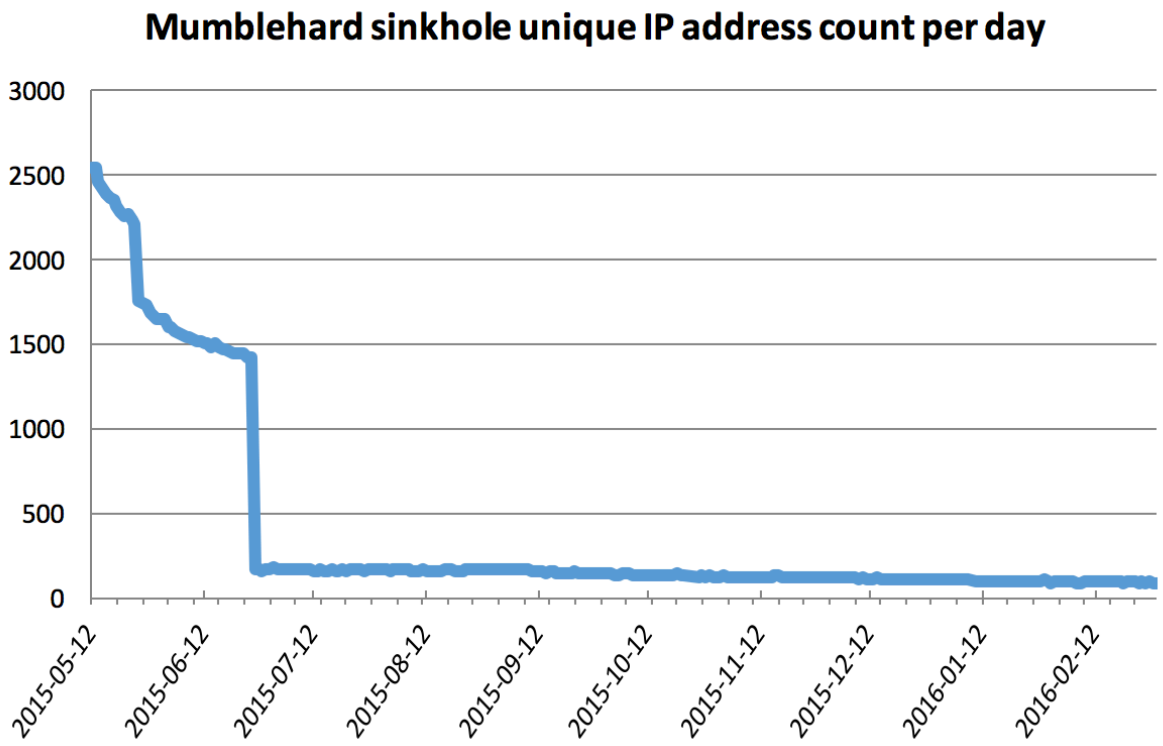
Mumblehard Linux botnet no longer active, takedown declared

April 11 2016, by Nancy Owano



Statistics from Mumblehard sinkhole after the publication. Credit: welivesecurity

(Tech Xplore)—The Mumblehard Linux botnet is out of the way. Malware researcher Marc-Etienne M. Léveillé trumpeted the good news on *WeLiveSecurity* from security company ESET: Mumblehard has been

struck down, which means an end to spamming as a result of Mumblehard for an army of Linux servers. He said, "we are pleased to report that it is no longer active," referring to the Linux botnet.

Who is raising the flag of victory here? ESET along with the Cyber Police of Ukraine and Cys Centrum LLC.

Spamming activities have been stopped for over a month, thanks to their efforts, according to the announcement."Mumblehard might not be the most prevalent, the most dangerous or the most sophisticated botnet out there, but shutting it down is still a step in the right direction and shows that security researchers working with other entities can help reduce the impact of criminal activity on the internet."

What's next: "ESET is operating a sinkhole server for all known Mumblehard components. We are sharing the sinkhole data with CERT-Bund, which is taking care of notifying the affected parties around the world through their national CERTs," said Léveillé. "CERT-Bund has recently started to notify the affected parties. We hope to see a faster decrease in the weeks to come." He also said, "We have not seen any new variants of Mumblehard, or any activities from this group, since the takedown."

What the team learned as they proceeded to get to the problem: "Spamming was their main business. We also found several different control panels that were used to simplify management of the botnet. Like the Mumblehard malicious components, the control panel was written in the Perl programming language."

Also, data collected during March showed that almost 4,000 Linux systems had been compromised with the Mumblehard botnet agent at the end of February, but the number went down.

What did the botnet do? It caused spam blasts for more than a year.

Cryptography reviews and technology site *Bitcoinist* shared the good news over the weekend, reminding readers: "As we all know, spam messages – such as the ones sent through Mumblehard – are one of the more common causes of Bitcoin ransomware infections." It may have taken a year in the making—it took quite some time to take control of the botnet, and eventually shut it down—but law enforcement and ESET pulled it off, they added, in managing to put an end to the Mumblehard Linux botnet.

What was so hard in getting rid of Mumblehard right away?

Bitcoinist had an answer: "Mumblehard was a unique botnet sending spam email messages, as it used packed quite a punch once it managed to get installed on a Linux machine. [Dan Goodin in *Ars Technica* said the botnet was the product of highly skilled developers.] Not only did the malware hide the source code from security solutions, but it also installed backdoor access on infected computers, and a mail daemon used to get the spam messages sent to other computer users."

More information: www.welivesecurity.com/2016/04 … rvers-from-spamming/