Unboxing Linux/Mumblehard: Muttering spam from your servers

welivesecurity.com/2015/04/29/unboxing-linuxmumblehard-muttering-spam-servers/

April 29, 2015

Today, ESET researchers reveal a family of Linux malware that stayed under the radar for more than 5 years. We have named this family Linux/Mumblehard. A white paper about this threat is available for download on WeLiveSecuriy.

29 Apr 2015 - 12:50PM

Today, ESET researchers reveal a family of Linux malware that stayed under the radar for more than 5 years. We have named this family Linux/Mumblehard. A white paper about this threat is available for download on WeLiveSecuriy.

Today, **ESET researchers** reveal a family of Linux malware that stayed under the radar for more than 5 years. We have named this family Linux/Mumblehard. A white paper about this threat is available for download on WeLiveSecuriy.

There are two components in the **Mumblehard** malware family: a backdoor and a spamming daemon. They are both written in Perl and feature the same custom packer written in assembly language. The use of assembly language to produce ELF binaries so as to obfuscate the Perl source code shows a level of sophistication higher than average.

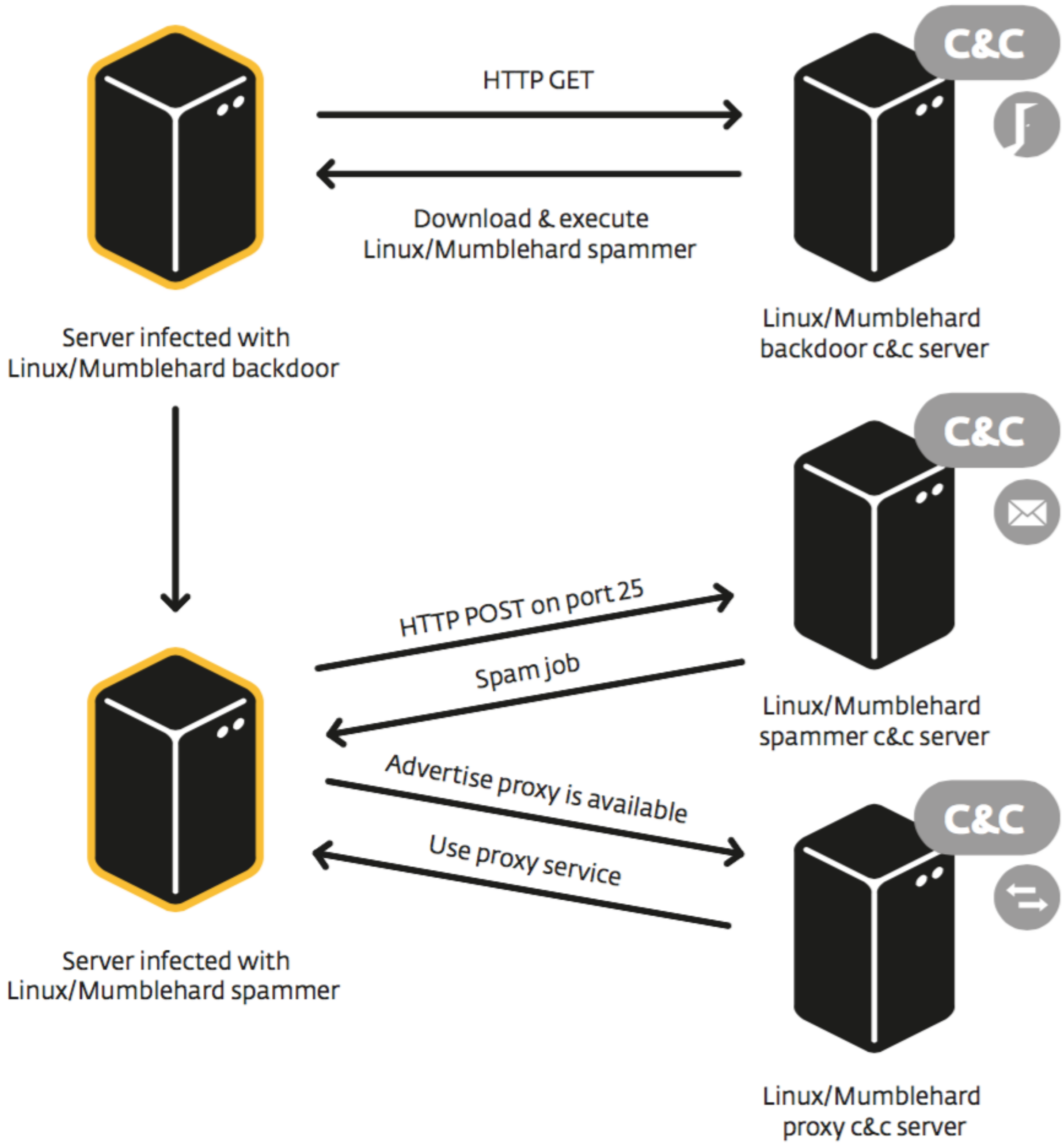
Check out Alexis Dorais-Joncas explaining how Mumblehard works:

Watch Video At:

https://youtu.be/XsxOvAlr45k

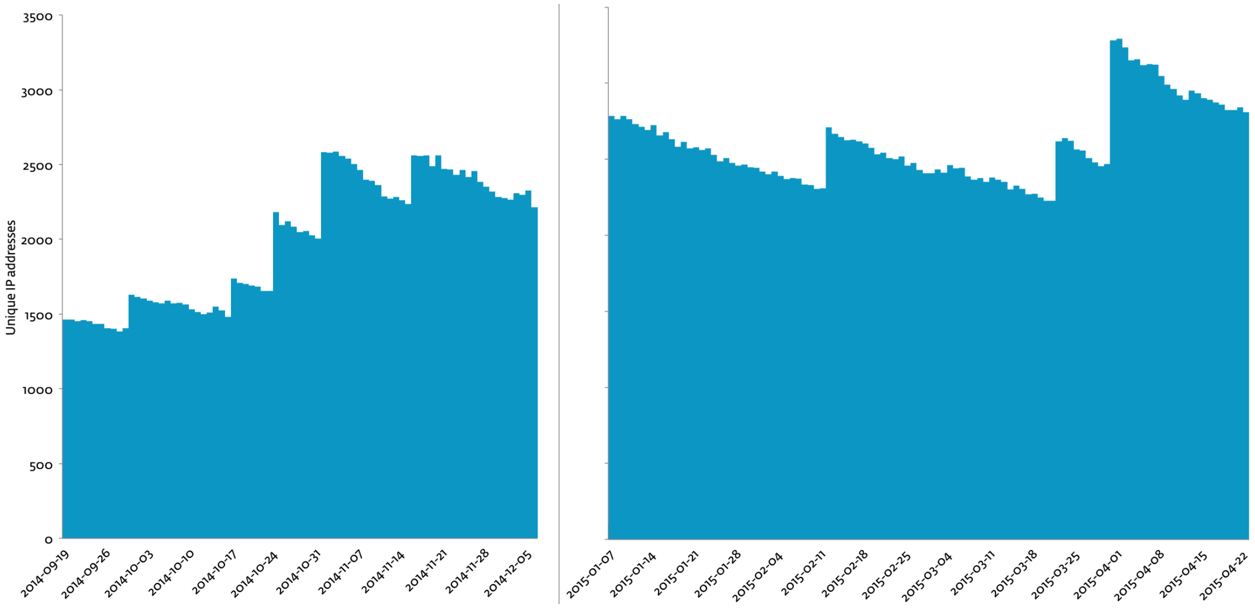
Monitoring of the botnet suggests that the main purpose of Mumblehard seems to be to **send spam messages** by sheltering behind the reputation of the legitimate IP addresses of the infected machines.

The relationship between the components and their command and control servers are illustrated in the following diagram:



Prevalence

ESET Researchers were able to monitor the Mumblehard backdoor component by registering a domain name used as one of the C&C servers. More than **8,500 unique IP addresses** hit the sinkhole with Mumblehard behavior while we were observing the requests coming in. The following chart shows the number of unique IP addresses seen each day over that period.



We can see from the chart that during the first week of April, **more than 3,000 machines were affected by Mumblehard**. The number of infected hosts is slowly decreasing, but the overall view shows that infection happens at specific times and that the botnet size has doubled over a **6-month period**.

A quick look at the list of victims suggests that Mumblehard mostly targets web servers.

Links with Yellsoft

Our analysis and research also shows a strong link between Mumblehard and Yellsoft. Yellsoft sells software, written in Perl, designed to send bulk e-mails. This program is called **DirectMailer**. The first link between them is that the IP addresses used as C&C servers for both the backdoor and spamming components are located in the same range as the web server hosting *yellsoft.net*. The second link is that we have found pirated copies of DirectMailer online that actually silently install the Mumblehard backdoor when run. The pirated copies were also obfuscated by the same packer used by Mumblehard's malicious components.

Prevention

Victims should look for **unsolicited cronjob entries for all the users** on their servers. This is the mechanism used by the Mumblehard backdoor to activate the backdoor every 15 minutes. The backdoor is usually installed in /tmp or /var/tmp. Mounting the tmp directory with the noexec option prevents the backdoor from starting in the first place.

The white paper with all the technical details is available for download on WeLiveSecurity.

Picture Credits: Flickr/Christian Barmala

29 Apr 2015 - 12:50PM

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

Newsletter

Discussion