Mumblehard targets servers running Linux and BSD

May 4 2015, by Nancy Owano

Credit: Victorgrigas/Wikideia/ CC BY-SA 3.0

Security watchers are talking about a family of malware that infects Linux and BSD servers. Marc-Etienne M. Léveillé, ESET malware researcher, has provided details about Linux/Mumblehard, which targets servers running Linux and BSD.

The spamming malware is described as "sophisticated"—sophisticated in

terms of having successfully flown under the radar for over five years (Mumblehard has been active since at least 2009) and sophisticated in terms of being what *Ars Technica* called "the brainchild" of "experienced and highly skilled programmers."

"We got interested in this threat because the way the Perl scripts used by the cybercriminals are packed inside ELF executables is uncommon and more complex than the average server threat," wrote Léveillé in his ESET report, titled "Unboxing Linux/Mumblehard: Muttering spam from your servers." It has a back door and a spam daemon, sending out large batches of junk mail.

The main components, said *Ars Technica*'s Dan Goodin, are written in Perl and "obfuscated" inside a custom packer written in assembly, a programming language which corresponds to the native machine code of the computer hardware it runs on.

"Some of the Perl script contains a separate executable with the same assembly-based packer that's arranged in the fashion of a Russian nesting doll. The result is a very stealthy infection," said Goodin.

The ESET researchers are not yet certain how Mumblehard is installed but they suspect the malware may take hold by exploiting vulnerabilities in two content-management systems. Their other theory is that the infections are the result of installing pirated versions of a mailer program which is Perl-based software for sending bulk e-mail messages.

What's the spam like? Léveillé wrote that the spam content which they witnessed on their tracker was mostly for promoting pharmaceutical products with links to various online stores. Another feature unique to the spam template, said the report, was the use of random message headers that seems to be built using two or three random words, e.g., Formants-Carmichael-Cutlet (possibly to fool anti-spam solutions).

ESET researchers" sinkholed" the backdoor module of Mumblehard and collected statistics on infected servers. They were able to count the population of infected hosts, determine who the victims were and work with third parties to notify them.

The report concludes with the observation that "Malware targeting Linux and BSD servers is becoming more and more complex," but also raises some important questions that merit further consideration. "It is unclear if spamming is the only goal of this group. In theory, it is possible for the cybercriminals to deploy other executable files to thousands of servers at once. Do they send other types of spam with their botnet? Is a pharmaceutical online store lucrative enough to justify the effort?"

We Live Security, ESET's editorial outlet, carried this advice: "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."

More information: www.welivesecurity.com/2015/04 … tering-spam-servers/