DDoS Trojans attack Linux

news.drweb.com/

Doctor Web

Back to news

May 15, 2014

The fallacy that Linux is fully protected against malware thanks to the specific features of its architecture makes life much easier for intruders distributing such software. In May 2014, Doctor Web's security analysts identified and examined a record-high number of Trojans for Linux, a large portion of which is designed to (distributed denial of service) attacks.

These programs share common features: first, they carry out DDoS attacks via various protocols, and second, they appear to have been created by the same person, according to Doctor Web specialists who have examined all the circumstantial evidence.

The malicious program that was added to the Dr.Web virus database as **Linux.DDoS.3**has a wide array of features. When launched, it determines the address of its command and control server (C&C server) and stands by for the parameters of the current task (once the task has been completed, it reports back to the criminals). **Linux.DDoS.3** can launch DDoS

attacks on the specified server over the TCP/IP (TCP flood) and UDP (UDP flood) protocols. It can also send DNS requests to enhance the effectiveness of the attacks (DNS Amplification).

Another modification of the threat, dubbed **Linux.DDoS.22**, targets Linux ARM distributions, while **Linux.DDoS.24** can infect servers and desktops running 32-bit versions of Ubuntu and CentOS. The Trojan **Linux.DDoS.24**installs in the system as pktmake and modifies the start-up scripts so that it will be launched automatically. Once launched, it also collects system hardware information, including the CPU type and available memory, and sends it in encrypted form to the C&C server belonging to the cybercriminals. The main purpose of this malware is to perform DDoS attacks upon command by the remote host.

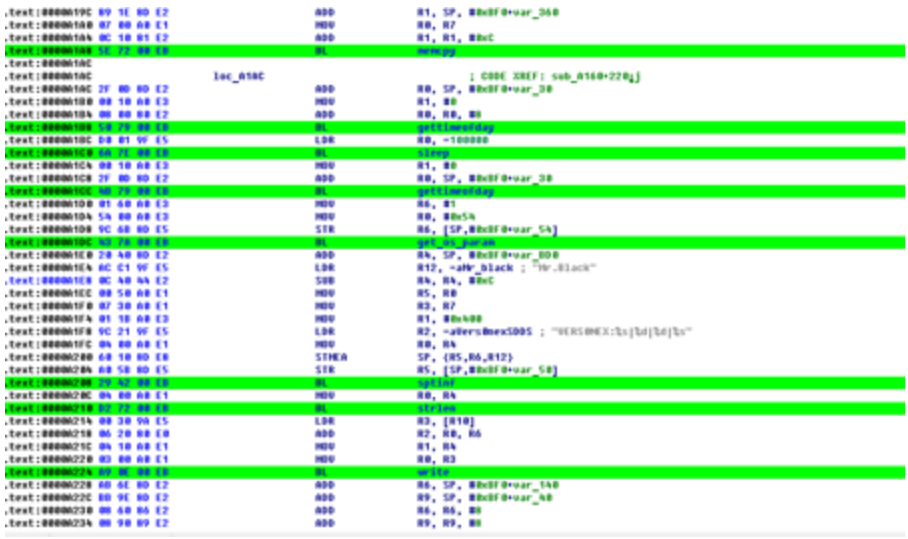
Another group of threats to Linux, studied by Doctor Web's security researchers this month, includes **Linux.DnsAmp.1**, **Linux.DnsAmp.2**, **Linux.DnsAmp.3**, **Linux.DnsAmp.4** and **Linux.DnsAmp.5**. Some malware of the Linux.DnsAmp family communicates with two control servers and can infect both 32- (**Linux.DnsAmp.1**, **Linux.DnsAmp.3**, **Linux.DnsAmp.5**) and 64-bit (**Linux.DnsAmp.2**, **Linux.DnsAmp.4**) versions of Linux. Like other members of this class of DDoS Trojans, **Linux.DnsAmp** modifies the start-up scripts, collects and sends to the remote server the infected machine’s configuration information (OS version, CPU, amount of free memory and swap file) and then waits for commands. Trojans of this family have the following features:

- SYN Flood (sending SYN requests to the target node to render it non-responsive).
- UDP flood (the Trojan makes sure that the remote host responds to requests and attempts to send 1,000 UDP packets to the target host).
- Ping Flood (an ICMP echo request that uses the PID of the process as the identifier and 0xA1B0A1B0 as data is dispatched to incapacitate the target).
- DNS Amplification
- NTP Amplification is implemented in various versions of the Trojan but remains unused.

Also upon command by a remote server, **Linux.DnsAmp** can write information into the log file, repeat the attack or update itself.

The Trojans **Linux.DnsAmp.3**(for 32-bit versions of Linux) and **Linux.DnsAmp.4**(for 64-bit Linux distributions) are modifications of the first version of Linux.DnsAmp with a limited set of features. In fact, these Trojan modifications can perform only three commands from the C&C server: start a DDoS attack, stop the attack and save the log file. It should be noted that many of the malware programs mentioned above connect to the same control servers.

Finally, we need to mention a malicious program for ARM-compatible Linux distributions that has been dubbed **Linux.Mrblack**. This Trojan is also designed to perform DDoS attacks via TCP/IP and HTTP. It features a fairly primitive design and, like other similar threats, acts on control server commands.



The command servers facilitating control over the Trojans are located mainly in the territory of China, and the corresponding DDoS attacks are directed mainly against Chinese websites. All these malicious applications are detected and removed by Dr.Web Anti-virus for Linux and, therefore, pose no danger to systems protected by the application.

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments