Malware

Tsunami Backdoor Can Be Used for Denial of Service Attacks

Posted on October 26th, 2011 by Peter James

A new backdoor and hacker tool, Tsunami, has been discovered. This hacker tool seems to be a port of a Linux malware, which has been around for some time, and provides remote access to hackers by listening in on an IRC (Internet relay chat) channel for instructions.

Tools like this are often used for distributed denial of service (DDoS) attacks (more on that below). These attacks flood computers with standard network requests, with a goal of overloading them. If a server receives more requests than it can handle, it can slow down, or even crash.

The Tsunami backdoor accepts a number of commands, and can change servers, download files, such as updates, and send packets to a specified IP address.

```
* TSUNAMI <target> <secs>       = A PUSH+ACK flooder                *
* PAN <target> <port> <secs>    = A SYN flooder                     *
* UDP <target> <port> <secs>    = An UDP flooder                    *
* UNKNOWN <target> <secs>       = Another non-spoof udp flooder     *
* NICK <nick>                   = Changes the nick of the client    *
* SERVER <server>               = Changes servers                   *
* GETSPOOFS                     = Gets the current spoofing         *
* SPOOFS <subnet>               = Changes spoofing to a subnet      *
* DISABLE                       = Disables all packeting from this bot *
* ENABLE                        = Enables all packeting from this bot  *
* KILL                          = Kills the knight                  *
* GET <http address> <save as>  = Downloads a file off the web      *
* VERSION                       = Requests version of knight        *
* KILLALL                       = Kills all current packeting       *
* HELP                          = Displays this                     *
* IRC <command>                 = Sends this command to the server  *
* SH <command>                  = Executes a command                *
```

Source code for this backdoor has been publicly available since at least September 2009, and it is trivial to compile this code, using Apple's XCode, and create a Mac executable.

This tool requires installation, and may actually be installed manually by people who choose to participate in DDoS attacks, such as those in the Anonymous group.

Individual users generally have little to fear from these tools. However, servers connected to the Internet can be vulnerable to remote installation. Hackers can take advantage of weaknesses in server tools, or especially PHP vulnerabilities, to gain access to a server and install a tool like this. In addition, once such a tool has been installed, the remote hacker can install other software onto the infected Mac.

What is a denial of service attack?

A denial of service attack, or a distributed denial of service attack (DDoS), occurs when one or many computers "gang up" on a web site or server by sending a flood of traffic to that server. Most web servers can handle standard traffic of a certain number of connection attempts per second. Large web sites, such as the biggest online retailers, can handle thousands of connections a second or more. But when thousands of computers get together and send requests all at the same time, sending "floods" of requests, servers have trouble remaining operable. When this type of attack happens, most firewalls will act and block the sending address, but in sophisticated attacks, these addresses are forged, and may change with each new packet.

Denial of service attacks are illegal; they are done for malicious purposes, such as to prevent a web site from functioning, or to block network traffic to and from a specific server. In some cases, such as Operation Payback, denial of service attacks were launched by a company paid by some Bollywood movie studios to attack websites that would not take down copyrighted material. After this, a retaliatory attack was made against a number of copyright organizations, law firms and others. Another attack was made on financial organizations that refused to process donations to Wikileaks.

Some users may install the Tsunami backdoor intentionally, to be part of such attacks. It is also possible that this tool is installed remotely on servers to increase the number of computers participating in such attacks, and, therefore, their effectiveness.

Hacker tools and their usage

Tsunami is one of the many dozens of hacker tools that Intego VirusBarrier X6 protects against. These are tools that are used to attack a machine other than the one on which it is installed, and include tools for executing DDoS attacks, scanning ports, sniffing network traffic, searching for known vulnerabilities and much more.

Most hacker tools are in limited circulation, and are not used for direct attacks; they need to be manually installed on computers, after which they are operated remotely. As such, their threat level is generally very low. Nevertheless, VirusBarrier X6 protects against all such tools, notably to protect servers where they may be installed via exploits that take advantage of vulnerabilities in third-party code, such as PHP.

In any case, Intego has updated the threat filters for VirusBarrier X6 to protect against this backdoor; threat filters dated October 25, 2011 or later, will spot and block this malware as OSX/Tsunami.A.