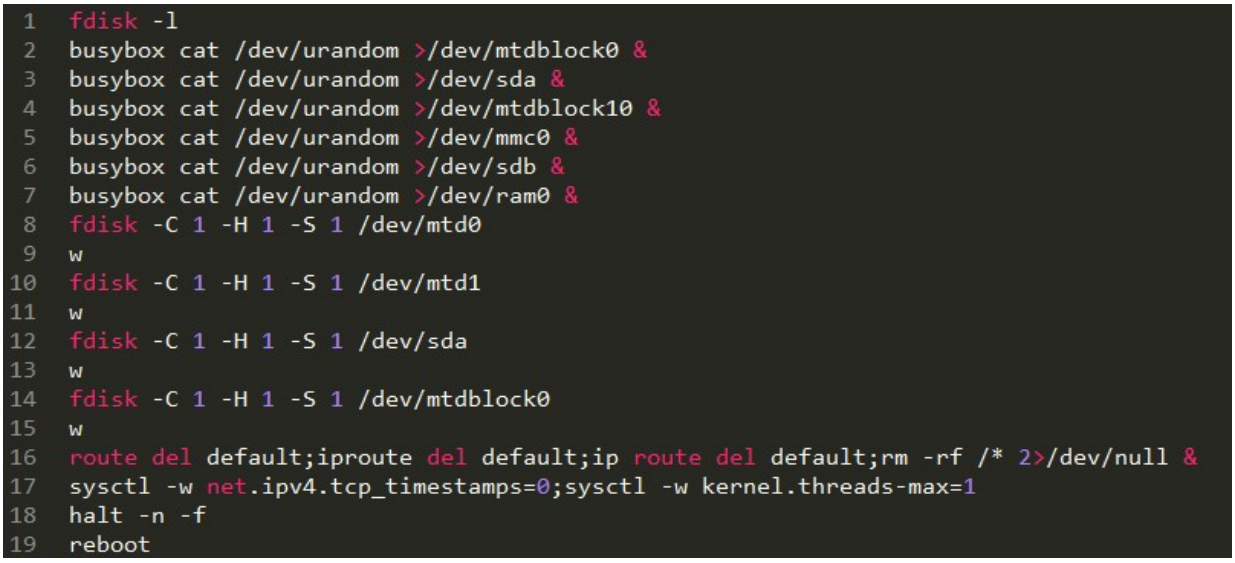
Honeypot reveals BrickerBot attacks: Internet of Things device wipeout

April 10 2017, by Nancy Owano



```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Command sequence of BrickerBot.

(Tech Xplore)—A new type of malware rendering Internet of Things devices useless is making a lot of security watchers simply scratch their heads. They know how the attacks are taking place; they just cannot figure out why.

Dan Goodin, *Ars Technica*, weighed in on the BrickerBot attacks. He said the attacks were "designed to damage routers and other Internet-connected appliances so badly that they become effectively inoperable."

Goodin said that "Once the bots find a vulnerable target, they run a series of highly debilitating commands that wipe all the files stored on the device, corrupt the device's storage, and sever its Internet connection."

The targets appear to be Linux BusyBox-based IoT devices that have their Telnet port open and exposed.

Radware is the security firm that discovered the malware. *SC Magazine* reported that the malware not only attacks but destroys unsecure iOT devices. There are two new forms of Denial of Service (DOS) malware involved in this, and they are bricking Internet of Things devices for reasons that are not yet clear. The two forms are BrickerBot.1 and BrickerBot.2.

Doug Olenick gave this account:

Such attacks began on March 20 when the forms began pinging a Radware honeypot, Radware said in its security alert.

"Within four days, 1,895 PDoS penetration attempts were recorded from locations worldwide. The malware MO has it searching for open Telnet ports and then brute forces its way into the device, in a manner similar to Mirai. It then corrupts the targets storage destroying it, concluding what is called a Permanent Denial of Service (PDOS) attack."

Reports said BrickerBot.2 was still active. All the same, " BrickerBot.2 can only access machines that expose a telnet service protected by default passwords—a requirement that greatly limits its destructive effects," said Dan Goodin, *Ars Technica*.

Useful at this point is what Dan Goodin described in his report. This was the situation at the time of his post which was on April 6.

"The attacks came from two separate botnets—dubbed BrickerBot.1 and BrickerBot.2—with nodes for the first located all around the world. BrickerBot.1 eventually went silent, but even now the more destructive BrickerBot.2 attempts a log-on to one of the Radware-operated honeypot devices roughly once every two hours."

Goodin said BrickerBot.2 uses the Tor anonymity service to conceal the IP addresses of its member nodes.

Here is how the same was described by Radware:

"Radware's honeypot recorded 1,895 PDoS attempts performed from several locations around the world. Its sole purpose was to compromise IoT devices and corrupt their storage. Besides this intense, short-lived bot (BrickerBot.1), Radware's honeypot recorded attempts from a second, very similar bot (BrickerBot.2) which started PDoS attempts on the same date – both bots were discovered less than one hour apart –with lower intensity but more thorough and its location(s) concealed by TOR egress nodes."

Here is how Radware spelled out targets of the attack: "The use of the 'busybox' command combined with the MTD and MMC special devices means this attack is targeted specifically at Linux/BusyBox-based IoT devices which have their Telnet port open and exposed publically on the Internet. These are matching the devices targeted by Mirai or related IoT botnets."

Radware also discussed protecting IoT devices moving forward. Change the device's factory default credentials; disable Telnet access to the device; network behavioral analysis can detect anomalies in traffic and combine with automatic signature generation for protection; user/entity behavioral analysis (UEBA) to spot granular anomalies in traffic early. Radware also said that "An IPS should block Telnet default credentials

or reset telnet connections. Use a signature to detect the provided command sequences."

Back to the earlier question though. Why is this attack being carried out? What is the goal? *SC Magazine US*: "There is no good explanation for why this malware was created or used."

Doug Olenick wrote, "Researchers said there remain many unanswered questions about BrickerBot, most importantly why is someone interested in using the malware to destroy a device instead of for financial gain."

As Catalin Cimpanu in *Bleeping Computer* commented, "All in all, BrickerBot isn't like anything we've seen before in the landscape of IoT malware." Often you can follow the money. Who is making the most off these attacks? With BrickerBot, he said, the attacks do not seem to benefit anyone.

" BrickerBot could also be the work of an Internet vigilante that wants to destroy insecure IoT devices."

Could it be the work of someone who wants to show the IoT devices that are not secure? JP Buntinx in *The Merkel*: "Deliberate destruction of a device is never a rightful course of action, regardless of the reasoning behind it."

More information: security.radware.com/ddos-thre … t-denial-of-service/

brickerbot-internet-device.html