

“BrickerBot” Results In Permanent Denial-of-Service

security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/



- [THREAT ALERTS](#)
- “BrickerBot” Results In Permanent Denial-of-Service

PDoS: Bricker Bot Results In Permanent Denial of Service - Radware Security

Called Permanent Denial of Service attacks (PDoS attacks), this form of cyber-attack is becoming increasingly popular in 2017 as more incidents involving this hardware-damaging assault occur.

[Download a Copy Now](#)

Abstract

Imagine a fast moving bot attack designed to render the victim’s hardware from functioning. Called Permanent Denial of Service attacks (PDoS attacks), 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, this type of cyber attack can destroy the firmware and/or basic functions of system. It is a contrast to its well-known cousin, [DDoS attacks](#), 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 Permanent Denial of Service 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 Permanent Denial of Service 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 Permanent Denial of Service 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 Permanent Denial of Service bots:

 Command sequence of BrickerBot.1 **Figure 1: Command sequence of BrickerBot.1**

Among the  An accessible device for a Bricker Bot PDoS Attack **Figure 2: An accessible device** 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.

 Geo mapped source IPs of BrickerBot.1 **Figure 3: Geo mapped source IPs of BrickerBot.1**

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

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:

 Command sequence of BrickerBot.2 **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 Internet of Things security and emergency assistance, [Contact us](#) with the code "Red Button".

[Click here](#) to download a copy of the ERT Threat Alert.

[Download Now](#)