ERT Threat Alert
Reaper Botnet
October 25th 2017

Abstract

Researchers claim to have discovered a new Internet of Things (IoT) botnet named Reaper, which is currently self-propagating. Reaper has not been observed launching attacks at the time of writing, as the IoT botnet was deployed without attack scripts. While there is debate whether this is a new botnet or a Mirai variant (as reported by virus total), research by Radware's Emergency Response Team (ERT) has been investigating Reaper to understand how it operates and what are the risks associated with it. At the moment, the Reaper botnet is not fully functional and it's in early stages of development. Reaper is not sophisticated and has been found to use a fixed domain and IPs for its command and control (C&C) server, thereby allowing it to be blocked at an ISP level. In addition, IPS signatures can be crafted to prevent further discovery and spread of Reaper.

IoT Botnets

An IoT botnet is a collection of compromised IoT devices such as cameras, routers, DVRs, wearables and other embedded technology that is infected with malware. It allows an attacker to control them and carry out tasks just like a traditional PC botnet.

IoT devices come with poor security features such as predictable admin credentials and open ports for remote access. Hackers typically compromise these devices via brute force login or inject malware via an open port or vulnerable service. In many cases, hackers leverage these exploits after researchers disclose a vulnerability.

Scanning

Reaper conducts scanning before delivering the payload. The first wave consists of SYN scans on TCP ports in the following order: 20480, 20736, 36895, 37151, 22528, 16671, 14340, 20992, 4135, 64288, 45090, 21248, 21504, 31775, 39455, 47115 and 42254. This first wave of scans is performed with an identical source IP and source port in every SYN packet. The scan is likely an attempt to fingerprint the devices. Once it finds an IoT device, its IP address is passed on to the exploit worker process.

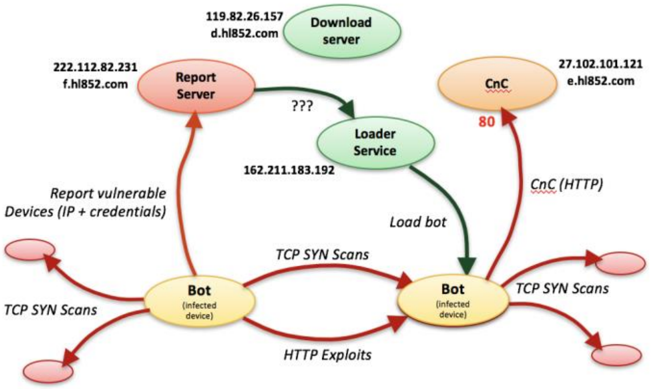

Figure 1: Exploit flowchart

Attack Vectors

Reaper begins its last phase of scanning once the IP is passed to the exploit process. Unlike previous IoT botnets or Mirai variants, Reaper does not leverage Telnet brute force with default credentials, but rather leverages HTTP-based exploits of known vulnerabilities in IoT. Reaper scans on TCP Ports 80, 8080, 81, 88, 8081, 82, 83, 8060, 10000, 8443, 8880, 3000, 3749, 1080, 84, 8090, 8001 and 1080 and attempts to open the server port and run one of the nine exploits included in the botnet.

- DLink DIR-600 and DIR-300[i]
- Goahead Webserver-based IP cams; multiple vendors[ii]
- Netgear ReadyNAS Surveillance [NAS][iii]
- Vacron NVR RCE [Surveillance Network Video Recorder][iv]
- DLink 850L [Wireless Router][v]
- Linksys E1500/E2500 [Wireless router][vi]
- Netgear DGN devices [DSL modems and routers][vii]
- AVTech [IP cams, NVRs, DVRs][viii]
- JAWS HTTP Server based DVRs [ix]

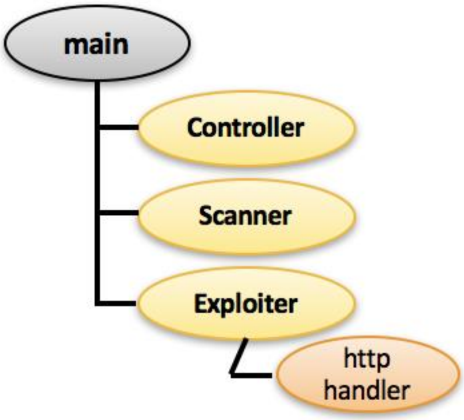

Figure 2: Malware process tree

Upon executing the main process:

- Recursively unlinks /var/log directory
    - `execve("/bin/rm", ["rm", "-r", "/var/log"], [/* 13 vars */] <unfinished ...>`
- Forks 3 processes
    - Controller which listens on port TCP/23 (Telnet) on all interfaces
    - Scanner process used for TCP SYN Scanning
    - Exploit worker process in charge of exploiting the device using nine HTTP-based IoT exploits
        - Forks another helper process (supposedly to handle the HTTP exploits)
- All processes listen on port TCP 48099 on ‘localhost’ – supposedly IPC channel

Command and Control

Reaper uses a fixed domain and IPs for its C&C server, which resides at e.hl852.com. The botnet owner is taking a risk of being completely blocked at an ISP level. The communication from the infected devices to the central sever is done in clear text. The clients check in every 10 seconds with the server. It is likely that once the botnet is updated with attack scripts, the commands will be delivered via this channel.

The server domains, IP addresses and the HTTP requests can be easily identified and blocked at a gateway level. Blackholing the servers at the ISP level will render those devices in the botnet and once rebooted the malware is gone from the devices.

IoT Security Recommendations

Manufacturers and regulators must enforce incorporation of IoT security features into the design and production of these devices, in particular the IoT security of Telnet communication and its associated ports. Default passwords must be random and users should be advised to change them.

Four Steps to Protect IoT Devices From Being Compromised

- **Stay Current -** Update firmware and software regularly
- **Authentication** – Use unique credentials for each device
- **Configuration** – Close unnecessary ports and disable unnecessary services
- **Segment** – Create separate network zones for your IoT systems

Organizations Under IoT Attack Should Consider

- **Hybrid DDoS Protection** (on-premise + cloud) – for real-time **DDoS attack prevention** 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 zero-day attacks
- **A Cyber-Security Emergency Response Plan** - that includes a dedicated emergency team of experts who have experience with IoT security and handling IoT outbreaks

Specific Actions Against Reaper

- Block TCP SYN scans to below destination ports originating from the same IP and source port: 20480, 20736, 36895, 37151, 22528, 16671, 14340, 20992, 4135, 64288, 45090, 21248, 21504, 31775, 39455, 47115, 42254
- A second wave of TCP SYN scans originating from the same IP but with changing source ports – list of destination ports in the scan: 80, 81, 82, 83, 84, 88, 1080, 3000, 3749, 8001, 8060, 8080, 8081, 8090, 8443, 8880, 10000
- Block outbound HTTP communication to C&C server at e.hl852.com and DNS queries for weruuoqweiur.com. Remember the ten second intervals between attempts.

For further IoT security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

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, it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] http://www.s3cur1ty.de/m1adv2013-003

[ii] https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

[iii] https://blogs.securiteam.com/index.php/archives/3409

[iv] https://blogs.securiteam.com/index.php/archives/3445

[v] https://blogs.securiteam.com/index.php/archives/3364

[vi] http://www.s3cur1ty.de/m1adv2013-004

[vii] http://seclists.org/bugtraq/2013/Jun/8

[viii] https://github.com/Trietptm-on-Security/AVTECH

[ix] https://www.pentestpartners.com/security-blog/pwning-cctv-cameras

Appendix – Indicators of Compromise

- File - bot

MD5 03ac15c3cf698510aa928cb93175bf55
SHA-1 33ba46f7edbffca58d88e4b6ac03bf2dab762f45
ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), statically linked, with unknown capability 0x41000000 = 0xf676e75, not stripped

- File - sa

MD5 37798a42df6335cb632f9d8c8430daec
SHA-1 8f40a00effdc150d15f7a49ce7c72efc5fc364d9
ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped

- File - sa5

MD5 95b448bdf6b6c97a33e1d1dbe41678eb
SHA-1 955dd87b3eee817f87df2a0cac654746f40329c0
ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped

- File - server.armel

MD5 704098c8a8a6641a04d25af7406088e1
SHA-1 694ab441edcd6da67312df7f006a9ab1951a5c24
ELF 32-bit LSB executable, ARM, version 1 (SYSV), dynamically linked (uses shared libs), not stripped

- File - sm

MD5 f247b270f2710db884a2e48c61d55dd5
SHA-1 98da7c69e1a346e76505cf96d6ae7dc6a4d68394
ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped

- File - xget

MD5 6f91694106bb6d5aaa7a7eac841141d9
SHA-1 8756fc70cf05d558d086c669e449ca007f2b2f05
ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped