Background

Using a customized Mirai botnet variant, hackers are attempting to takeover Internet routers around the world. With a simple remote code execution (RCE), a hacker took advantage of a SOAP (an XML-based application communication protocol) vulnerability in DSL modems with port 7547 opened for communication with third parties, beyond service providers IP range. This remote code execution attack is exploiting a vulnerability found in the TR-069 configuration protocol in combination with the Mirai IoT botnet.

A metasploit (a common penetration testing tool) module for the exploit can be found at exploit-db.[1] Eir D1000 modem, Zyxel AMG1302 and the D-Link DSL-3780 routers appeared to be the main target as the binaries targeted microprocessor without interlocked pipeline stages (MIPS) and ARM (advanced RISC - reduced instruction set computing - machine) devices. This vulnerability was mentioned earlier this month among the hacker community when research discovered that TR-064 commands can be sent to D1000 modems supplied by Ireland-based ISP Eir.

Figure 1: Example of a request to an open device

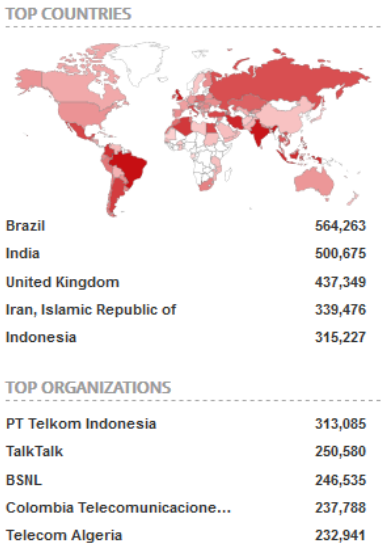

Figure 2: List of devices with that port (shodan)

[1] https://www.exploit-db.com/exploits/40740/

Motivation

The purpose was to inject malware and enslave new devices, thereby turning them into a botnet for future attacks. This attempt failed and the routers where not infected. Yet, the devices crashed due to an overload caused by the attack. The code is a variant of Mirai with the addition of scanning for the SOAP vulnerability in an attempt to hijack other routers and modems. It is an alarming development that underscores the sheer volume of vulnerable devices and the subsequent risk of multi-Gpbs traffic generation capabilities.

Method

The hacker attempted to remotely execute malicious commands on vulnerable devices via an injection attack on the network time protocol, NTP, server name field. Ultimately the NTP server name was parsed as a command that lead to the RCE vulnerability. The malicious code was inserted into the NTP server name field via the TR-069 protocol. This protocol is designed to allow Internet Service Providers (ISP's) to remotely manage devices on their network. The devices that suffered the attack where configured to accept TR-064 commands from the Internet which lead to a change in their NTP settings. TR-064 is based on HTTP and SOAP and its default port is TCP 7547. Commands are sent to the vulnerable devices as POST a request to this port.

By sending specific commands, the attacker can instruct the modem to open port 80 on the firewall, allowing access to the web administration interface. This piece of malware was designed to scan for vulnerable devices just like the original Mirai bot. Once the devices have become infected, the malware prevents further access by killing the telnet service and closing the port used by TR-064[2]

Service Providers Response

Internet service providers should block all IP address, except for their own range, to prevent anyone else from accessing port 7547. The update from Deutsche Telekom and UK ISP's now prevents third party access to the remote maintenance interface. Users have been advised to power off their devices for thirty seconds. Once the device reboots, it retrieves the new firmware update from the service provider that patches this vulnerability and prevents recurring attempts.

Radware Solution

Radware's Attack Mitigation System (AMS) can detect specific remote access attempts to these routers and prevent the remote code execution. In a full AMS deployment, AppWall, Radware's web application firewall can verify the content of the NTP server name fields in the SOAP request to reject any malicious OS command injections. It then uses DefenseMessaging to signal DefensePro to block any packets matching this signature at the perimeter and prevents malicious traffic from entering the network.

DDoS Protection Considerations for Organizations Under Threat

- **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 zero-day attacks.

---

[2] Exploit code:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9222
https://github.com/hackingyseguridad/cwmp
https://detux.org/report.php?sha256=1fce697993690d41f75e0e6ed522df49d73a038f7e02733ec239c835579c40bf

- **Cyber-Security Emergency Response Plan** - that includes a dedicated emergency team of experts.

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