Background

The publication of the Mirai botnet source code in late 2016 has resulted in two major outcomes:

- The first - and most obvious – is it has given cybercriminals and perpetrators worldwide not only a functioning program for creating and operating botnets, but also a customizable one.

- The second is it has demonstrated the sheer vulnerability of IoT devices and their operating systems to simple malware infection and enslavement attempts. Not only are the devices vulnerable, a large variety and number of devices are ALREADY infected.

Since the publication of the source code, there has been a race to enslave more and more IoT devices by hackers and bot-herders. Though there are more than 6 billion connected devices today (and expected to grow to 20 billion by 2020)[i], there is a fierce competition between these hackers, leading to the introduction of malwares that can expunge other malwares from controlling the device. These devices facilitate espionage, data theft or launch massive DDoS attacks, and also scan other vulnerable devices and add them to the botnet.

The expanding list of devices is startling. It includes everything from routers, online cameras and DVRs to “smart” phones, watches, and TVs all the way to appliances such as toys, vending machines and even light bulbs.

Spreading the Epidemic

While the devices may seem different from one another, they all share common vulnerabilities and are all compromised in the same manner.

Using default credentials (normally provided by manufacturers) – they manage to infect additional devices and increase the potential power of the botnet. Many of the victims are actually newly connected devices.

IoT botnets are targeting several different architectures including ARM, ARM7, PowerPC and other processors. Scanners will look for vulnerable devices connected to the Internet and attempt to gain access by brute forcing the login with a set of default passwords. Once it gains access, it will load the malicious source code appropriate to the architecture and enslave the device into the botnet. Since Radware began tracking the Mirai botnet, it has witnessed 2,790 attacks utilizing attack vectors from basic UDP floods to powerful DNS water torture attacks.

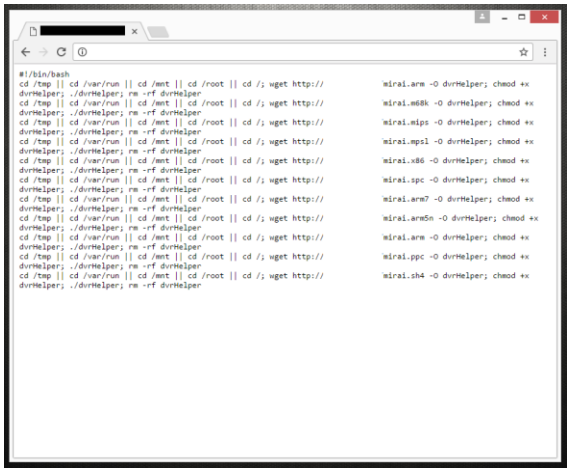


Figure 1: Server hosting Mirai malware (Credit @VessOnSecurity)

Common Vulnerabilities of IoT Devices

- **Default credentials** – IoT device credentials are by default very weak. They are often root:root or admin:admin and are hardly every changed by the end users. Once these devices become infected, the malware will change the default password to prevent the user from logging in and to prevent other attackers from taking over their infected bots. The most common attempts include root:root and admin:admin.

- **Open ports** – IoT devices come from the manufacturer vulnerable in the form of number of services and ports that are open by default. Users who don't change the default password will hardly be able to know how to reconfigure the device and close a port 23 (telnet).

- **Large-scale attacks** – IoT botnets are always active. Unlike a PC botnet, when an IoT bot-herder wants to launch a DDoS attack, they will have most of his bots ready to go. The increase of available devices participating in an attack, in combination with faster Internet connections, results in massive 1Tbps DDoS attacks.

- **Targeting** - Devices are scanned and even targeted within minutes since being initially activated and connected and are attacked hundreds of time a day by other IoT devices that have already been infected. Since the publication of Mirai, a number of hackers from amateur to criminals have deployed their own IoT botnets and are actively scanning and looking for new victims. Even just a botnet with a few thousand infected IoT devices could cause major problems to businesses – from mere resource consumption to significant service degradation or even a complete outage.

Enslaving Digital Appliances

Vending Machines

Digital vending solutions and kiosks around the world are rapidly becoming more advanced. They are connected to the Internet with a mobile router so they can help improve accuracy and efficiency of the service. Vendors with this new technology can connect to these devices to view sales reports, check inventory and monitor service issues. Some of these devices are used for remote monitoring and have been found to have multiple vulnerabilities,[ii] including weak credentials management (default credentials like admin:admin or user:12345). Consequently, the devices were exposed to online attacks.

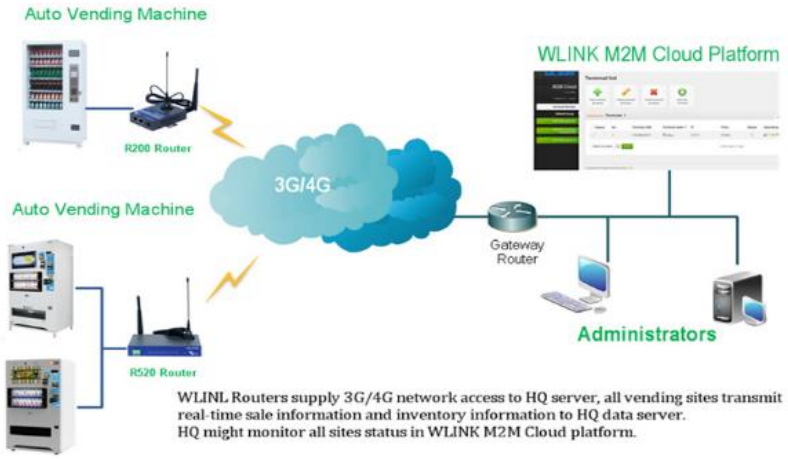
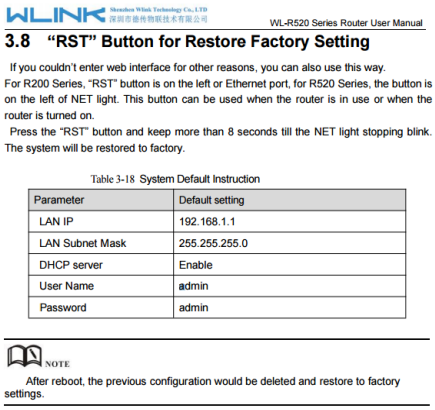


Figure 2: WLINK Router for Smart Vending Solution

Some street light systems rely on wireless nodes as well and can be accessed by any other device in the wireless network.



WLINK Shenzhen Wlink Technology Co., LTD 深圳市基伟物联技术有限公司 WL-R520 Series Router User Manual

3.8 "RST" Button for Restore Factory Setting

If you couldn't enter web interface for other reasons, you can also use this way.
For R200 Series, "RST" button is on the left or Ethernet port, for R520 Series, the button is on the left of NET light. This button can be used when the router is in use or when the router is turned on.
Press the "RST" button and keep more than 8 seconds till the NET light stopping blink. The system will be restored to factory.

Table 3-18 System Default Instruction

Parameter	Default setting
LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP server	Enable
User Name	admin
Password	admin

NOTE
After reboot, the previous configuration would be deleted and restore to factory settings.

Figure 3: WLINK R520 Router has default credentials

Research

Attackers scan the Internet looking for devices that are vulnerable to specific command injection-based attacks. The commands used in these IoT-based botnet attacks instruct the targeted device to download and run malware hosted on an external server. Once executed the malware enslaves the device into a botnet and is used to launch DDoS attacks.

A Radware Honeypot that monitors activity on Port 23, Telnet, saw a number of 300 login attempts a day from devices located around the world. These devices are IoT devices like routers, NAS's, DVRs and web cameras. One device being commonly used is primarily located in Vietnam. This device, VNPT's GPON IGATE GW040, has become infected because it was exposed to the Internet with default credentials. This device also supports the TR-069 remote management protocol and has open Telnet/SSH access. **Most manufacturers provide documentation on their websites that contain these default passwords**. GPON IGATE GW040's manual provides the default credentials - admin:vnpt. Scanners for IoT-based botnets like qBot, Hajime, Mirai and other use a set of default credentials. Mirai's file scanner.c included 62 default passwords of various devices and bot-herders can search for more credentials from other manufactures so they can enslave new devices into their botnet.

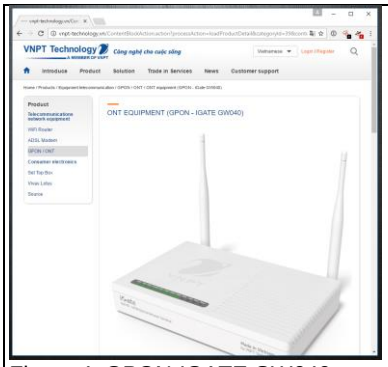


Figure 4: GPON-IGATE GW040 router

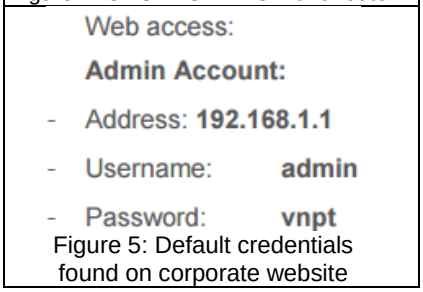


Figure 5: Default credentials found on corporate website

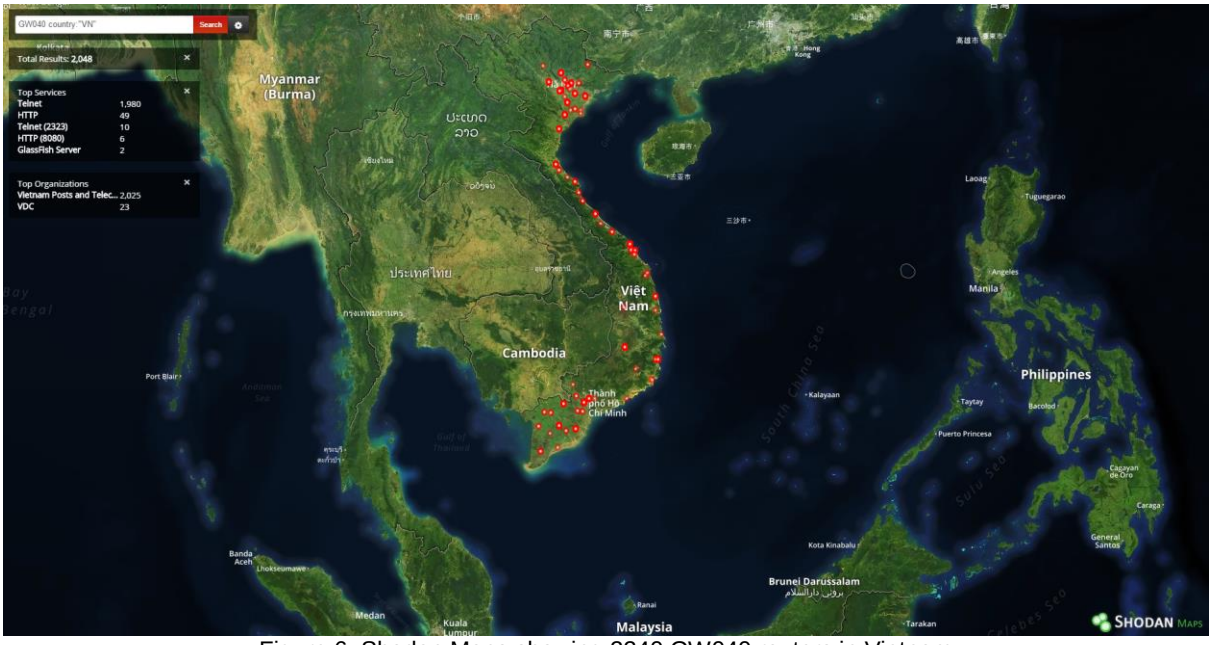


Figure 6: Shodan Maps showing 2240 GW040 routers in Vietnam

Another device is the ZTE, ZXHN H108N router. This device, just like VNPT's devices, ship with default credentials and open ports exposing the device to unnecessary risk and injection-based attacks. These devices see daily attempts to brute force port 23.

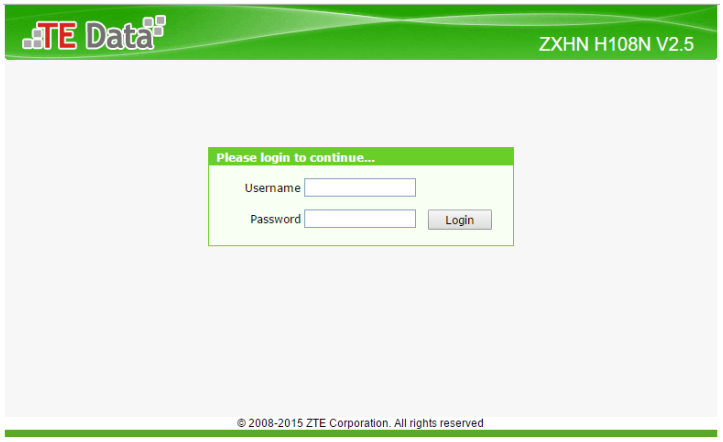


Figure 7: ZTE, ZXHN H108N router

Attack vectors

DDoS attacks are expected to gain in strength and power as the average bot-herder is now able to take control of hundreds of thousands of IoT devices with nearly zero cost.

- UDP Flood
- VSE Valve Source Engine Flood
- NTP Refection
- DNS Water Torture
- SYN with options
- ACK + bypass
- GRE Generic Routing Encapsulation
- HTTP Layer 7 Flood

Notable Hacks

Routers, Internet Cameras and DVRs – These devices are the major contributors to the power of the Mirai botnet and the 1Tbps DDoS attacks against Brian Krebs, OVH and DynDNS[iii] in late 2016 and the takeover attempt against 900,000 routers of Deutsche Telekom[iv]

Vending Machines, Light Bulbs – Verizon's RISK team discovered a university's hijacked vending machines and 5,000 other IoT devices were making false DNS requests every 15 minutes, thus slowing down the network operation and legitimate lookups were being dropped. The botnet spread from device to device by brute forcing default passwords and then changed them to lock the network operators out.[v]

Toys -

- Germany's Federal Network Agency issued a warning directing parents to destroy Cayla (a talking doll) because its smart technology can reveal personal data. It has been reported by researches that a Bluetooth component embedded in the doll can be exploited to listen and talk to children.[vi]
- A manufacturer of wirelessly connected stuffed pets revealed that the data of more than 800,000 user accounts was stolen by criminals who later tried to extort the company for ransom. Allegedly, the data was accessible from within the network without authentication prompts. Together with personal details, including the personal data of children, these puppets recorded and stored conversations between children and other people. [vii]

Smart TVs –

- Samsung revealed that the voice activation feature on its smart TVs captures nearby conversations. The TV sets can share the information, including sensitive data, with Samsung as well as third-party services.[viii] That poses a risk of having voice samples of individual consumers making their way to unauthorized parties.
- Devices with microphones and cameras can obviously be used for eavesdropping. In addition, LG smart TVs have been infected with an Android version of the Cyber.Police ransomware.[ix]

Recommendations

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

Four Steps to Prepare

- **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 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 0-day attacks
- **A cyber-security emergency response plan** - that includes a dedicated emergency team of experts who have experience handling IoT outbreaks

Effective Web Application Protection Against Bots and Data Theft

- **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
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

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.

---

[i] gartner.com/newsroom/id/3165317
[ii] http://seclists.org/fulldisclosure/2016/Jun/60
[iii] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/mirai-botnet/
[iv] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/deutsche-telekom-routers-takeover/
[v] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf
[vi] http://www.bbc.com/news/world-europe-39002142
[vii] https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/
[viii] http://theweek.com/speedreads/538379/samsung-warns-customers-not-discuss-personal-information-front-smart-tvs
[ix] http://www.techspot.com/news/67573-smart-tvs-arent-immune-ransomware-one-user-recently.html