Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

02 August 2018

Alert Number

I-080218-PSA

Cyber Actors Use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious Cyber Activities

Cyber actors actively search for and compromise vulnerable Internet of Things (IoT) devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and computer network exploitation. IoT devices, sometimes referred to as "smart" devices, are devices that communicate with the Internet to send or receive data. Examples of targeted IoT devices include: routers, wireless radios links, time clocks, audio/video streaming devices, Raspberry Pis, IP cameras, DVRs, satellite antenna equipment, smart garage door openers, and network attached storage devices.

IoT proxy servers are attractive to malicious cyber actors because they provide a layer of anonymity by transmitting all Internet requests through the victim device's IP address. Devices in developed nations are particularly attractive targets because they allow access to many business websites that block traffic from suspicious or foreign IP addresses. Cyber actors use the compromised device's IP address to engage in intrusion activities, making it difficult to filter regular traffic from malicious traffic.

Cyber actors are using compromised IoT devices as proxies to:

- Send spam e-mails;
- Maintain anonymity;
- Obfuscate network traffic;
- Mask Internet browsing;
- Generate click-fraud activities;
- Buy, sell, and trade illegal images and goods;
- Conduct credential stuffing attacks, which occurs when cyber actors use an automated script to test stolen passwords from other data breach incidents on unrelated web-sites; AND
- Sell or lease IoT botnets to other cyber actors for financial gain.

Cyber actors typically compromise devices with weak authentication, unpatched firmware or other software vulnerabilities, or employ brute force attacks on devices with default usernames and passwords.

Compromised devices may be difficult to detect but some potential indicators include:

- A major spike in monthly Internet usage;
- A larger than usual Internet bill;
- Devices become slow or inoperable;
- Unusual outgoing Domain Name Service queries and outgoing traffic; or
- Home or business Internet connections running slow.

Protection and Defense

- Reboot devices regularly, as most malware is stored in memory and removed upon a device reboot. It is important to do this regularly as many actors compete for the same pool of devices and use automated scripts to identify vulnerabilities and infect devices.
- Change default usernames and passwords.
- Use anti-virus regularly and ensure it is up to date.
- Ensure all IoT devices are up to date and security patches are incorporated.
- Configure network firewalls to block traffic from unauthorized IP addresses and disable port forwarding.
- Isolate IoT devices from other network connections.

Additional Resources

For additional information on cyber threats to IoT devices, please refer to "Common Internet of Things Devices May Expose Consumers to Cyber Exploitation," available at https://www.ic3.gov/media/2017/171017-1.aspx.

Victim Reporting

If you suspect your IoT device(s) may have been compromised, contact your local FBI office and/or file a complaint with the Internet Crime Complaint Center at www.ic3.gov.