Newly Found Malware Threatens IoT Devices

lifars.com/2022/01/newly-found-malware-threatens-iot-devices/

January 12, 2022

A new malware has been identified by AT&T Alien Labs that exposed millions of Internet of Things devices. The BotenaGo backdoor vulnerability, written in Google's Golang programming language, uses the Internet of Things (IoT) with 19412 networking ports or associated modules. The said malware threatens IoT devices and can simultaneously exploit up to 30 separate vulnerabilities against its targets.

Mercenaries turned to Shodan to ensure that millions of devices were compromised by at least part of the malware's activities. Shodan is a search engine used for hunting internet-connected devices on the internet. Unfortunately, the number of antivirus solutions capable of protecting against infection is far lower. The software is believed to be similar to the Mirai botnet, which was responsible for shutting down internet connectivity for parts of the East Coast in 2016.

When BotenaGo was found, just six of the 62 vendors that the malware-scanning VirusTotal platform used to identify it as malware detected it as malware. A few recognized BotenaGo as malware because it was based on Mirai – a malicious software intended to construct

botnets. Its controllers may launch widespread denial of service attacks against its targets by doing so.

> LIFARS Managed Threat Hunting and Response Service (MTH&R) was designed to help customers uncover adversaries across your Endpoint, Network and SIEM data. Our elite team has decades of combined experience working within their Governmental CSIRT responding and hunting for adversaries from 100's of attacks, including Ransomware and APT's.

BotenaGo's Operational Structures

BotenaGo starts by presenting the total number of infected devices to the hacker's payload interface, which occurs before injecting shell script files into the host console's operating system. The attack surface is then assaulted by employing a function to map the victim's device to narrow down the scope of the assault. Each destination is defined in command terminal strings to launch malicious malware on the target device. Following that, a request is sent to the IoT endpoint to verify that the destination is legitimate. To send the malicious payload, the attackers must press the enter key.

BotenaGo looks for potentially susceptible targets during the scanning process as the malware threatens IoT devices. An examination of the code shows that the attacker is supplied with a real-time global infection counter, which indicates the number of affected devices on the network at any particular point in time. From this, the attackers can exploit vulnerabilities in internet-facing devices and execute remote shell commands, which attackers might utilize as a gateway to the broader network if the device is not adequately protected.

Additionally, attackers can use this option to spread malicious payloads. However, at the time of the researchers' analysis of BotenaGo, many of these payloads were deleted from the servers maintained by the attackers; thus, it was not feasible to analyze them.

What Vulnerabilities Can Be Compromised With BotenaGo

BotenaGo can hack millions of vulnerable systems. It can go as big as malware that threatens IoT devices. However, according to the researchers, there is no apparent connection with a command and control server at this time. Accordingly, there are three possible outcomes to consider. Initially, BotenaGo may be merely a broader malware suite module that isn't currently utilized in assaults. Another option is tied to Mirai, which individuals use to target particular computers when launching attacks.

Likewise, experts claim that BotenaGo is still under development and that a beta version was mistakenly published early, which explains why it doesn't seem to be doing anything. Even if BotenaGo is not actively exploiting any vulnerabilities, the sheer number of flaws it can attack implies that millions of devices are theoretically susceptible.

Methods for Keeping Your Organization Safe From a Potential IoT Attack

You can avoid any assault and malware that threatens IoT devices by keeping software up to date and applying security upgrades as soon as possible. That will reduce the time for attackers to exploit newly discovered vulnerabilities in IoT software. It is also advised that IoT devices not be exposed to the public internet and that a properly configured firewall be installed to give off better security.

Keep Firmware And Applications Up To Date

Firmware keeps you secure by installing the most recent security fixes and reducing the likelihood of a cyberattack occurring. You may patch any vulnerabilities or exploits as they are discovered and make your IoT devices more secure. If at all feasible, enable the option to check for updates automatically.

Modify The Router's Default Configuration

The majority of individuals forget to change their routers and instead use the name provided by the manufacturer instead. That might jeopardize the security of a personal Wi-Fi network. Any name you like, as long as it is not affiliated with you. Because so many IoT devices are linked to Wi-Fi, the network and Wi-Fi are the first line of defense against hackers when securing your IoT devices. Make sure that the default privacy and security settings are changed. Those configurations often serve the interests of manufacturers rather than you. Avoid online shopping when connected to a public Wi-Fi network since anybody may take your information.

Stay Away From Universal Plug and Play Devices

Even though Universal Plug and Play (UPnP) has its benefits, it may render printers, routers, cameras, and other Internet of Things (IoT) devices susceptible to cyber assaults. The underlying premise behind the design of UPnP is to make it simpler for network devices to communicate with one another without the need for extra setup and to assist them in automatically discovering one another. However, hackers will profit the most from this since they can find all IoT devices outside your local network. As a result, it is recommended that UPnP be turned off altogether.

Have A Complex Password And Do Not Reuse it

If you are still using the words "password" and "qwerty" as your password, you should reconsider your strategy. Using a common and basic password for Internet of Things devices is equivalent to opening the door to hackers. Passwords that are both strong and secure are the greatest safeguard against hackers. Make sure to use a different, one-of-a-kind password for each device. If hackers can guess one of your passwords, they might damage

every device you possess that relies upon that password to function correctly. Yes, it may be challenging to remember all passwords, but it is necessary to safeguard Internet of Things devices. You may jot them down in your journal but abstain from storing them on your technological device.

Turn Off Any IoT Devices Connected To The Network When Not In Use

You must be conscious of every feature you require from your Internet of Things device. Most modern products, including refrigerators and televisions, can connect to the internet. However, that does not imply that you must link them to the internet as well. It would help if you scrutinized the characteristics of your devices to determine which gadgets need internet access to work properly.

Final Thoughts

The bulk of IoT manufacturers send out frequent updates, and you can also check their websites to see if there are any new security patches or upgrades available. Because IoT devices do not have any additional layers of protection, keeping them up to date regularly is essential for their security. Software updates for Internet of Things devices guarantee that the device is equipped with the most recent antimalware and antivirus defenses. Furthermore, it assists the system in cleaning up the security weaknesses present in prior software versions. Hackers are continually refining their strategies for invading your personal information. It is preferable to keep software up to date and to be prepared for any external threats.

References

https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits
https://www.iotworldtoday.com/2021/11/16/botenago-malware-targets-millions-of-iot-devices/
https://sea.pcmag.com/security/47232/att-reveals-malware-targeting-millions-of-routers-iot-devices
https://www.zdnet.com/article/this-mysterious-malware-could-threaten-millions-of-routers-and-iot-devices/