Endpoint Protection

symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things

Apr 18, 2017 01:20 PM

Migration User

A battle is raging for control of Internet of Things (IoT) devices. There are many contenders, but two families stand out: the remains of the Mirai botnet, and a new similar family called Hajime.

Hajime was first discovered by researchers in October of last year and, just like Mirai (Linux.Gafgyt), it spreads via unsecured devices that have open Telnet ports and use default passwords. In fact, Hajime uses the exact same username and password combinations that Mirai is programmed to use, plus two more.

But that's where the similarities end.

Unlike Mirai, which uses hardcoded addresses for its command and control (C&C) server, Hajime is built on a peer-to-peer network. There isn't a single C&C server address, instead the controller pushes command modules to the peer network and the message propagates to all the peers over time. This is typically considered a more robust design as it makes takedowns more difficult.

Hajime is also stealthier and more advanced in comparison to Mirai. Once on an infected device, it takes multiple steps to conceal its running processes and hide its files on the file system. The author can open a shell script to any infected machine in the network at any time, and the code is modular, so new capabilities can be added on the fly. It is apparent from the code that a fair amount of development time went into designing this worm.

Over the past few months, Hajime has been spreading quickly. Symantec has tracked infections worldwide, with large concentrations in Brazil and Iran. It is hard to estimate the size of the peer-to-peer network, but modest estimates put it in the tens of thousands.

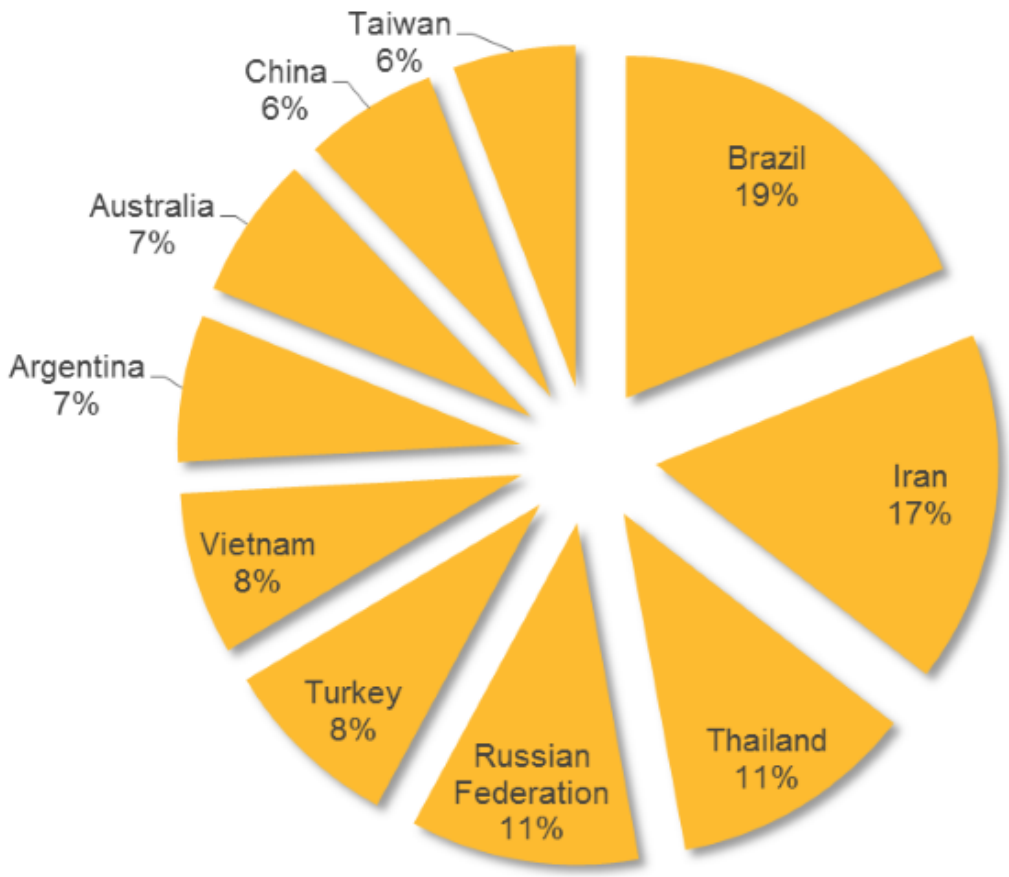

Figure 1. Top 10 Hajime-infected countries

Reasons behind the worm

There are some features that are noticeably missing from Hajime. It currently doesn't have any distributed denial of service (DDoS) capabilities or any attacking code except for the propagation module. Instead, it fetches a statement from its controller and displays it on the terminal approximately every 10 minutes. The current message is:

Just a white hat, securing some systems.

Important messages will be signed like this!

Hajime Author.

Contact CLOSED

Stay sharp!

The above message is cryptographically signed and the worm will only accept messages signed by a hardcoded key, so there is little question that this message is from the worm's true author. However, there is a question around trusting that the author is a true white hat

and is only trying to secure these systems, as they are still installing their own backdoor on the system. The modular design of Hajime also means if the author's intentions change they could potentially turn the infected devices into a massive botnet.

To the author's credit, once the worm is installed it does improve the security of the device. It blocks access to ports 23, 7547, 5555, and 5358, which are all ports hosting services known to be exploitable on many IoT devices. Mirai is known to target some of these ports.

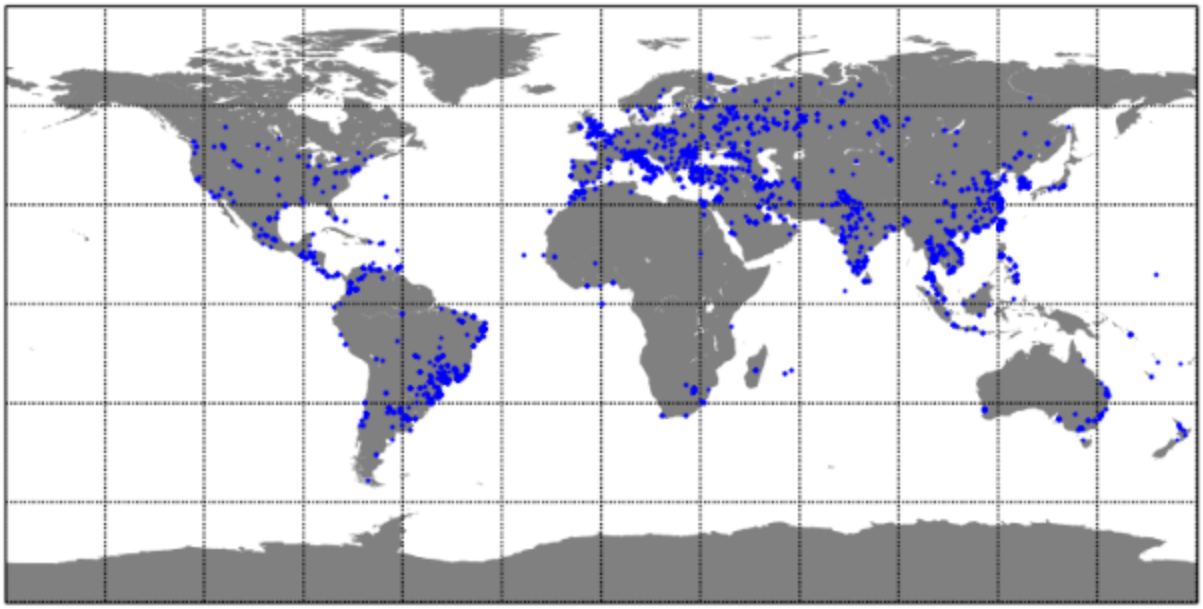

Figure 2. The volume of observed Hajime infections, by location

White worms

This isn't the first case of a vigilante attempting to secure vulnerable IoT devices. In 2014/2015, the Linux.Wifatch malware was observed. This was written by "The White Team", which attempted to secure IoT devices in much the same way as Hajime is now. Brickerbots also try to take IoT devices offline by deleting critical system files or corrupting the system in similar ways.

The problem with these white worms is that they usually turn out to have a short lifespan. That is because their effects are only temporary. On the typical IoT system affected by these worms the changes made to improve the security are only in RAM and not persistent.

Once the device is rebooted it goes back to its unsecured state, complete with default passwords and a Telnet open to the world. To have a lasting effect, the firmware would need to be updated. It is extremely difficult to update the firmware on a large scale because the process is unique to each device and in some cases is not possible without physical access. And so, we are left with embedded devices stuck in a sort of *Groundhog Day* time loop scenario. One day a device may belong to the Mirai botnet, after the next reboot it could belong to Hajime, then the next any of the many other IoT malware/worms that are out there scanning for devices with hardcoded passwords. This cycle will continue with each reboot until the device is updated with a newer, more secure firmware.

Security researchers doubling as QA

There is another aspect of the worm that stands out. In the broadcast message, the author refers to themselves as the “Hajime Author” but the name Hajime appears nowhere in the binaries. In fact, the name “Hajime” didn’t come from the author but rather from the researchers who discovered the worm and spotted similarities between it and the Mirai botnet and wanted to maintain the Japanese naming theme (Mirai means “future” in Japanese, Hajime means “beginning”). This shows that the author was aware of the researchers’ report and seemed to have liked the name.

The report also identified bugs in the worm and provided signatures for detecting them. It appears that the worm’s author took note. Now, each of the noted bugs has been fixed and none of the signatures still work. It appears that the report, in a way, served as free quality assurance for the worm’s author; showing them what bugs they still needed to fix.

In this case, helping the author fix the bugs may not have caused that much damage, but the thought of security researchers inadvertently assisting malware authors is worrying. There is a fine balance between deciding how much information to put into a malware report to help IT teams identify compromises, while at the same time not exposing so much information as to serve as training and critical review for the attackers. Highlighting mistakes in malware is rarely worth it as it provides very little actionable intelligence for defenders. Just like in poker, security researchers must remember to never show someone their hand if they don’t have to.

Guarding against attack

Users of IoT devices should take the following steps to help prevent their devices from becoming infected with malware.

- Research the capabilities and security features of an IoT device before purchase
- Perform an audit of IoT devices used on your network
- Change the default credentials on devices. Use strong and unique passwords for device accounts and Wi-Fi networks
- Use a strong encryption method when setting up Wi-Fi network access (WPA)
- Disable features and services that are not required
- Disable Telnet login and use SSH where possible
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary
- Modify the default privacy and security settings of IoT devices according to your requirements and security policy
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Regularly check the manufacturer’s website for firmware updates
- Ensure that a hardware outage does not result in an unsecure state of the device

Protection

Symantec and Norton products detect the threats mentioned in this blog as:

Further reading

To learn more about the security of IoT devices, read our whitepaper: Insecurity in the Internet of Things