Wifatch: Atypical Malware

Technical Report · April 2018

DOI: 10.13140/RG.2.2.27854.77123

CITATION
1

READS
347

2 authors:

Nur Syazana Mohd. Adi Firdaus Tan
Universiti Sains Malaysia
1 PUBLICATION **1** CITATION
SEE PROFILE

Selvakumar Manickam
Universiti Sains Malaysia
272 PUBLICATIONS **1,787** CITATIONS
SEE PROFILE

Wifatch: Atypical Malware

More Good Than Harm?

Nur Syazana bt. Mohd. Adi Firdaus Tan
National Advanced IPV6 Centre
Universiti Sains Malaysia (USM)
Penang, Malaysia
SyazanaTan.student@usm.my

Dr. Selvakumar Manickam
National Advanced IPV6 Centre
Universiti Sains Malaysia (USM)
Penang, Malaysia
selva@usm.my

***Abstract*—This paper encompasses the review of the malware Wifatch that was discovered in 2014, how it has impacted Internet of Things (IoT) devices, how it has changed the typical perception of malware having a malicious nature, and what has been revealed in its role in security.**

Keywords—Malware; Linux; Symantec; Internet of Things; P2P.

I. INTRODUCTION

According to Fisher (2018), the composition of the word "malware" originates from the combination of "malicious", and "software". It is used to depict the nature of software that is created with ill intentions such as intrusion of permission on a computer to steal personal information through the usage of a backdoor. Software that behaves in such a way that it wasn't intended to could also be classified as a malware [1]. They exist in forms such as rootkits, spyware, Trojans, adwares, viruses, and worms – all of which are used to complete tasks such as stealing data that are protected, deleting, or even adding software without the user's approval, or acknowledgement [2].

In a modernized world, the need for a globalized devices, and network of machines that are capable of interacting with one another is the basis of Internet of Things – which is also known as Internet of Everything. In simpler terms, IoT is defined as devices that are linked to the Internet, and are equipped with sensors, and actuators [3] [4].

By infiltrating a vulnerable Telnet authentication, Wifatch uses a backdoor through routers at home to communicate with a Command & Control (C&C) server. What makes it unique is that although it is classified as a malware, it acts a guard against other forms of infection without any malicious intent to its host – hence, it is categorized as a white – hat Trojan [5].

II. THE DISCOVERY

In 2014, an unusual activity was detected on a home router by an independent security researcher in which the process was not part of the original device's software. Upon further investigation, an intricate, and sophisticated code - designed in Perl - was discovered that had caused the router to involuntarily connect to other infected network of peer – to – peer devices. This was further investigated by Symantec by setting up honeypots in efforts to collect samples of this embedded device targeted malware. Generally, home routers are often used by cyber criminals to perform acts such as Distributed Denial of Service (DDoS) attacks. Unsuspecting users would not have noticed the difference as it tends to go unnoticed as how other infections are [6].

Unlike other malwares, this particular subject is dubbed as the "vigilante" of its kind. This is due to the fact that it serves one purpose – to protect the devices that it infects. By identifying weak, or unchanged passwords through hacking Telnet, and other protocols. It would then disable Telnet after scanning for known malwares in the device to avoid further infections. Although there is potential in misusing the backdoor created by Wifatch, it was never put into use for anything of sorts – which leads to experts believing that it was part of the "IoT vigilantes" effort in securing devices that were at risk [7].

III. IMPACT ON IOT

It has been reported that there were speculations whereby Wifatch was created in attempts to fend against surveillance by governmental agencies – for instance, National Security Agency (NSA). A comment left in the piece of code quoted from Richard Stallman in this malware hints on defending constitutional rights of the people. Knowing the nature of how home routers could be used as a medium to spread updates without acknowledgement from the user – this malware will urge the device's owner to make use of stronger passwords, aside from updating the current firmware as such ignorance could lead to future mishaps. In order to "prevent" certain devices such as the CCTV (of which Wifatch is unable to "protect" against other malwares), it was designed to reboot the system after a certain period of time - taking advantage of the fact that malwares in embedded systems are not as persistent, and that a reinstallation must take place for them to take effect. Although it is concerning, the researchers have found that the commands that were passed through the backdoor were cryptographically signed. In other words, this indicates that only the original author would be able to control what it does. In turn, this cuts the chances of the said malware of being manipulated by malicious hijackers. Interestingly enough, the Internet is claimed to be at a safer state – all thanks to Wifatch [8][9].

IV. The Good and the Bad

Known for its "good" intentions", Symantec's Mario Ballano made a point that it could be manipulated to inflict detrimental damage at any given time through its general – purpose back doors. It is still regarded as a malware since it infects the device without the user's consent. Relying on a malware to "guard" one's system would not exactly be a wise choice, and thus it is still placed under careful watch [10].

The positives gained from Wifatch's release:

- For educational purposes, and to encourage learning.

  This is supported by the fact that the Perl code was not obscure, and that the creator was not concerned of having it being inspected, nor shared. The source code was only compressed, and minified. Released version of it did not contain the private key, selected parts of the C&C, and infection code to prevent misuse [7].

- To promote better understanding in the need to heighten security measures.

  If in the wrong hands, the botnets are able to carry out DDoS attacks through the infected routers. Hence, it raises the issue in the importance of addressing default security configurations before it is taken advantage of.

- Increasing security in general.
- Counteracting against illegal mining of Bitcoin.
- Saving bandwidth by cancelling out other malware scans.
- Reduces interruption of service, reboots, and overheat of device.
- Saving credentials from being stolen.

It is noted that the creation, and spread of the malware is originally caused by the neglect of the user themselves:

- Leaving default security configurations, and passwords.
- Lack of concern, and awareness among users.
- Poor habit, and encouragement by Internet Service Providers (ISP) to retain original credentials for easier maintenance.
- Insecure Telnet protocol.

V. Background

Inspired by Carna botnet, the idea of Wifatch was to challenge the idea of not being able to create something of similar sorts whereby it challenges the existing security level of embedded devices. It is considered to be "virtually nonexistent", and thus giving rise for the need to "protect" these vulnerable users. As Carna botnet before it, it was crucial to act against the vulnerability that existed.

With over a year spent on ways to reliably shut down the Telnet's port, implementing malware detection, and functions for disinfecting the system, on top of the technicalities within bootstrapping a botnet – everything within Wifatch's functionalities was a challenge.

Wifatch was never meant to be kept a secret, and upon agreement of free licensing under General Public License – it was made public. The creator firmly stated that although the created malware holds no ill intentions – users should not use this as a form of comfort, and safety. The known issues, and security holes must be dealt immediately. It does not utilize 0day exploits, nor elaborate backdoors to infiltrate a system, and its target only comprises of unprotected devices.

Users are open to experiment with the codes available on almost an x86 or AMD64 Linux Kernel by loading them on the same directory with a stable network access in order to connect to the P2P network with the option of obtaining the extension modules, and upgrading the bot. It will create a database directory upon finding a suitable mountpoint. Users must keep in mind that there is no warranty for self experimentation. Not only that, users are encouraged to volunteer to help as more reliable machines are needed in order to serve as a backend database for malware signatures. Generally, this botnet requires a full network access to enable it to scan vulnerable devices. It is reachable via UDP, and TCP with the range 32769 – 65534. Infections are carried out from a centralized point, and only a single keypress is needed if anything goes sour.

When asked if the same creator was behind Carna botnet, it was declined. Inspiration was derived from the collected data of the said botnet. The team remains anonymous, though goes by the name "The White Team".

VI. Infection Statistics

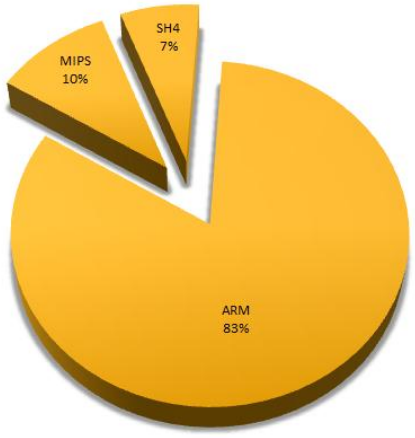

Figure 1: Infected Architecture Breakdown [6]

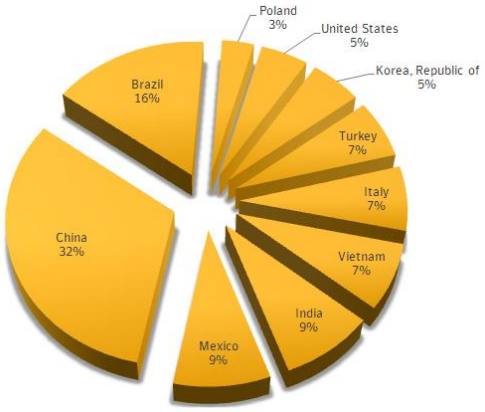

Figure 2: Infected Countries Breakdown [6]

Figure 1 depicts the three major architectures that were found to be infected with this malware. ARM architecture is most prevalent as it is the most used firmware partnered with complimenting cores known to be used by multiple successful companies such as Apple, Nvidia, Qualcomm, and even Samsung Electronics. This is makes up the majority of mobile devices, and embedded systems. MiPS is known to be used in gaming consoles, supercomputers, and even in automobiles. Certain embedded systems utilize SH4 in cellular phones, LCD TVs, and NAS. Whilst not included in the chart – it is reported that X86, and PowerPC holds a miniscule percentage of 0.132 of total infection percentage [6].

Based on figure 2, the countries affected are listed down accordingly. However, it is to be noted that the percentage breakdown may not be as depicted as the malware is removed upon resetting the said infected device. It may also become infected after time if the router's firmware is not up to date, or is still using its default password [6].

VII. Conclusion

While the creation is meant for good use, the users should never grow too comfortable in relying on a white – hat malware to take care of a security issue when it could have been issued with as simple as changing the default credentials of a router. As quoted by Harrington (n.d.), "Violating systems as a path to remediation is not the right way to go" [11].

There could never be a general consensus on whether or not this malware holds more potential in harming, or protecting one's device. The debate lies in the nature of how secure the device is to begin with. A protected hardware would not have contracted the malware in the first place. An invasion of privacy is still what it is even if it is doing no harm. In the end, there is little that could be done if not for the mindset of the users themselves to initiate the change.

References

[1] Fisher, T. (n.d.). What Is Malware? Retrieved April 09, 2018, from https://www.lifewire.com/what-is-malware-2625933

[2] What is Malicious Software (Malware)? - Definition from Techopedia. (n.d.). Retrieved April 09, 2018, from https://www.techopedia.com/definition/4015/malicious-software-malware

[3] Lee, In & Lee, Kyoochun. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 58. 10.1016/j.bushor.2015.03.008.

[4] Burgess, M. (2018, February 16). What is the Internet of Things? WIRED explains. Retrieved April 09, 2018, from http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

[5] Pastrana, S., Rodriguez-Canseco, J., & Calleja, A. (2016). ArduWorm: A Functional Malware Targeting Arduino Devices.

[6] Is there an Internet-of-Things vigilante out there? (n.d.). Retrieved April 09, 2018, from https://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there.

[7] Kovacs, E. (2015). Retrieved April 09, 2018, from https://www.securityweek.com/developers-mysterious-wifatch-malware-come-forward.

[8] Linux.Wifatch: The Router Virus That May Be Secretly Defending You From Other Malware. (n.d.). Retrieved April 09, 2018, from https://securityintelligence.com/news/linux-wifatch-the-router-virus-that-may-be-secretly-defending-you-from-other-malware/.

[9] Beneficial Malware? It's a Thing... (n.d.). Retrieved April 09, 2018, from https://www.pcrisk.com/internet-threat-news/9498-beneficial-malware-linux-wifatch.

[10] Russon, M. (2015, October 02). Linux.Wifatch: Routers hacked by 'white hat' virus that makes them more secure against malware. Retrieved April 09, 2018, from https://www.ibtimes.co.uk/linux-wifatch-routers-hacked-by-white-hat-virus-that-makes-them-more-secure-against-malware-1522214.

[11] Fox-Brewster, T. (2015, October 09). Meet The Mystery Vigilantes Who Created 'Malware' To Secure 10,000 Routers. Retrieved April 09, 2018, from https://www.forbes.com/sites/thomasbrewster/2015/10/06/mystery-white-team-vigilante-hackers-speak-out/#1ea56745689f.