MUST READ WinRAR zero-day open million users to hack

The mystery behind the Internet-of-Things vigilante malware

October 2, 2015 By Pierluigi Paganini

A new strain of malware identified by Symantec as the Vigilante malware, aka Wifatch, has infected tens of thousands of IoT devices across the world.

Who is infecting thousands of IoT devices across the world, and why?

A new strain of malware, identified by Symantec as Linux.Wifatch has infected tens of thousands of

IoT devices across the world, but the strange thing is that the botmaster hasn't used them for any illegal activities.

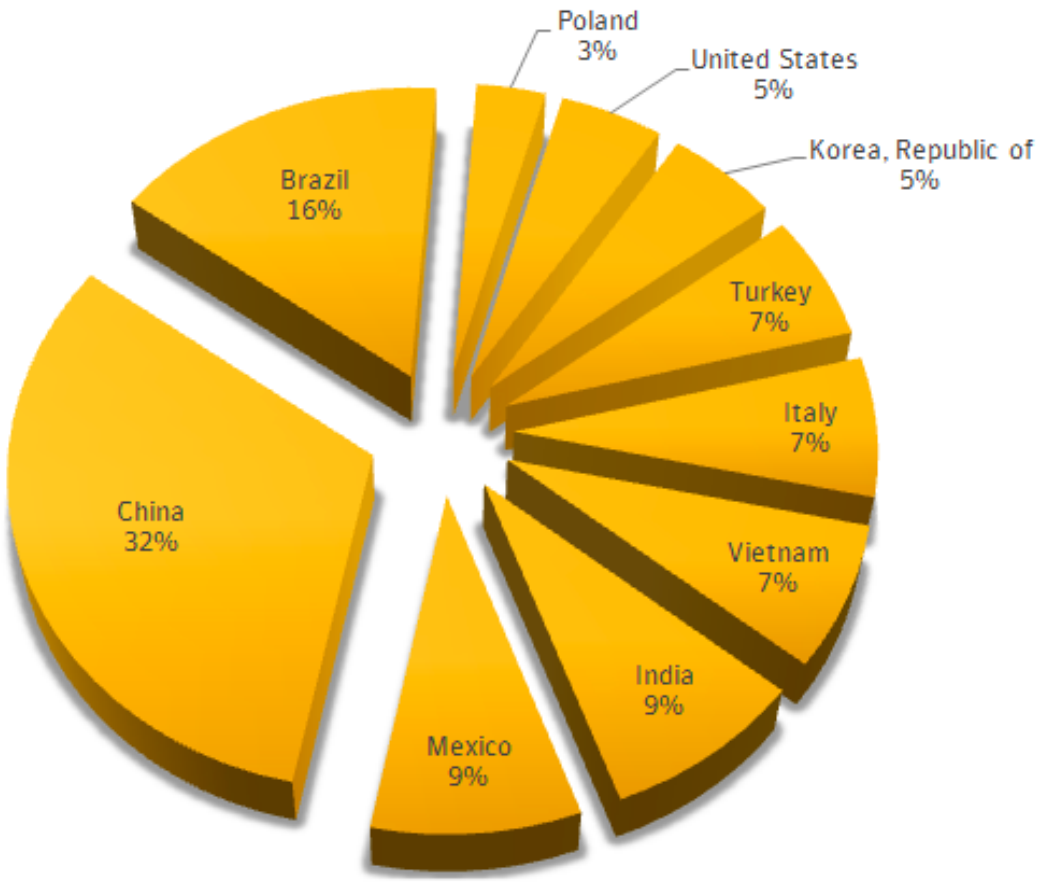
The backdoors set up by Wifatch would allow a potential attacker to use bots for different activities, from DNS poisoning and traffic redirection to distributed denial-of-service (DDoS) attacks. However, the threat actor seems to have a different purpose, it scans the web search for compromised IoT devices by searching for most popular malware signatures. If it discovers the presence of a malware on a device and it is able to hack it, **Wifatch** disables telnet to keep others out.

For this reason, the expert avoided to call the malware Wifatct and are calling it "Internet of Things (IoT) vigilante."

Symantec has identified tens of thousands of devices infected with the vigilante malware across the world, most of them are routers and IP cameras.

Wifatch is designed to target several the principal IoT architecture, analyzing the victims by architecture we can observe that compromised devices are based on ARM (83%), followed by MIPS (10%), and SH4 (7%).

The majority of the infections was observed in China, followed by Brazil (16%), Mexico (9%), India (9%), Vietnam (7%), Italy (7%), Turkey (7%), South Korea (5%), and the United States (5%).



The researchers speculate that the "Internet of Things (IoT) vigilante" malware was that work of someone that apparently monitors routers and other IoT devices from threat actors.

The malware is developed in Perl, but experts noticed that each instance of the vigilante malware detected uses its own Perl interpreter. The botnet uses a peer-to-peer (P2P) model that makes it very efficient.

The vigilante malware, aka Wifatch, scan the Web for devices that it can infect over Telnet, also in this case exploiting poorly configured systems likely IoT components using weak credentials. Once the vigilante malware infects a device, it allows botmaster to control it by using commands signed with a private Elliptic Curve Digital Signature Algorithm (ECDSA) key.

It is interesting to note that when the vigilant malware gain the control of an IoT device, it informs users trying to connect over Telnet that the service has been disabled for security reason and e
provides recommendations for preventing attacks.

*"*Wifatch's *code is not obfuscated; it just uses compression and contains* minified *versions of th
source code. It would have been easy for the author to obfuscate the Perl* code but *they chose
to. The* threat *also contains a number of debug messages that enable easier analysis. It looks li
the author wasn't particularly worried about others being able to inspect the code." state Syma
in its* analysis*. "The threat has a module (*dahua.*pm) that seems to be an exploit for Dahua DVR
CCTV systems. The module allows Wifatch to set the configuration of the device to automaticall
reboot every week. One could speculate that because Wifatch may not be able to properly defe
this type of device, instead, its strategy may be to reboot it* periodically which *would kill running
malware and set the device back to a clean state."*

The author of the Vigilant malware seems to be an expert in cryptography and he its botnet implements security mechanisms that make it resilient to cyber attacks, the experts confirmes t
usage of the Tor anonymity network for hiding control infrastructure.

Stay Tuned!

Pierluigi Paganini

(Security Affairs – Vigilante malware, IoT malware)

Hacking IoT malware security Symantec Vigilante malware

Breaking News Hacking Malware Security

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
An Amazon employee became owner of Google.com for a few minutes

YOU MIGHT ALSO LIKE

New Apple Gatekeeper bypass can allow running rouge applications

October 1, 2015 By Pierluigi Paganini

WinRAR zero-day open million users to hack

October 1, 2015 By Pierluigi Paganini