BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices

bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

Catalin Cimpanu

By
Catalin Cimpanu

- December 11, 2017
- 07:35 PM
- 1

The author of the BrickerBot malware has announced his retirement in an email to Bleeping Computer, also claiming to have bricked over 10 million devices since he started the "Internet Chemotherapy" project in November 2016.

Known as The Doctor (self-given name) and The Janit0r (HackForums nickname), this individual (or group) is the author of BrickerBot, a malware strain that was purposely created to brick IoT devices.

First spotted in April this year, BrickerBot operates by scanning the Internet for vulnerable devices and then using exploit code to gain a foothold on the exposed equipment to rewrite the device's flash storage with random data.

Devices infected with BrickerBot often need to be reinstalled, or in some cases, replaced altogether, as the malware sometimes rewrites their firmware.

BrickerBot is a controversial project

Following BrickerBot's public disclosure, The Janit0r reached out to Bleeping Computer and explained why he created BrickerBot. In an interview this spring, the Janitor explained that he refers internally to BrickerBot as "Internet Chemotherapy" and that he created the malware as a way to sabotage vulnerable devices before they were infected with the Mirai malware, which a hacker had used in the autumn of 2016 to launch some of the biggest DDoS attacks known to date.

That Mirai author also leaked the malware's source code online, in an attempt to hide his tracks by allowing other crooks to set up their very own Mirai botnet variations. His plan succeeded, and a free-for-all ensued with several Mirai botnets popping up everywhere online, powering on-demand DDoS cannons.

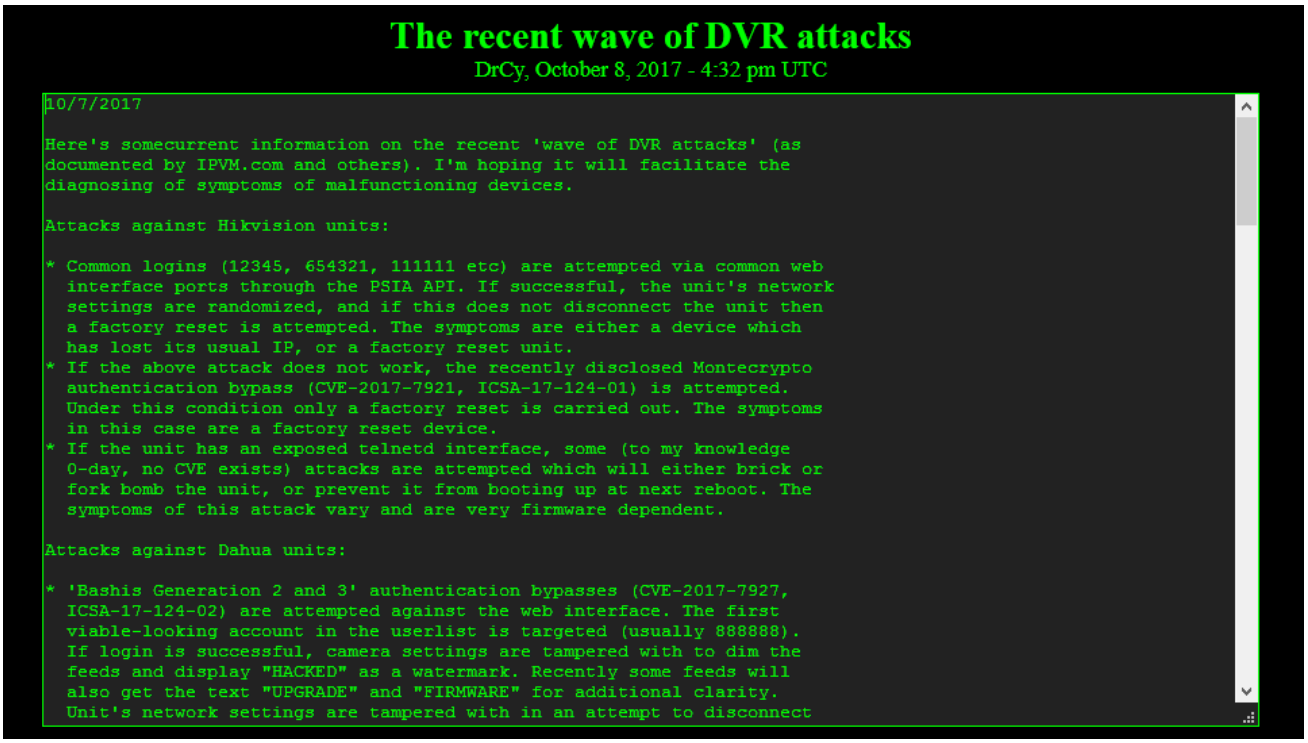
The Janit0r said this onslaught on the IoT scene determined him to create BrickerBot as a way to take vulnerable devices offline, force owners to install updated firmware, and take them out of the reach of Mirai botnets.

In all conversations, the Janit0r seemed an individual who believed he was fighting the good fight, albeit many users and experts have not seen his actions as neither "good" or even "legal."

BrickerBot continued to operate all year

Despite criticism, BrickerBot did not stop and Bleeping Computer reported on other attacks over the summer, such as the ones against a US ISP and several Indian Internet providers.

These were only the documented cases, and the BrickerBot author claimed in many emails to have been behind many other attacks and downtimes all over the world.



BrickerBot explains why he retired

In an email sent today to Bleeping Computer, The Janit0r announced his sudden retirement and explained why he reached this decision.

I believe that the project has been a technical success, but I am now starting to worry that it is also having a deleterious effect on the public's perception of the overall IoT threat. Researchers keep issuing high profile warnings about genuinely dangerous new botnets, and a few weeks or even days later they are all but gone. Sooner or later people are going to start questioning the credibility of the research and the seriousness of the situation.

The Janit0r cites the cases of Persirai, Hajime, or Reaper botnets that have been advertised as "the next big thing" in terms of IoT botnets, but have never lived up to the hype.

He now fears that because of his work in the shadows, people are not taking IoT devices to be a credible threat anymore. He believes that he needs to stop, so people truly understand how many vulnerable devices are out there.

It was rational to take action in an attempt to buy everyone time to get their affairs in order and there has been some progress over the past year in the form of new security standard proposals and so on. I however believe that people, organizations and goverments aren't doing enough nor moving quickly enough and we're running out of time. Because of this I've decided to make a public appeal regarding the severity of the situation. Taking credit for all the carnage of the past year has serious downsides for me and my mission. [...] However I

also recognize that if I keep doing what I'm doing then people of influence may simply perceive the IoT security disaster as less urgent when in reality they should consider it an emergency requiring immediate action.

The Janit0r then adds that once his efforts became public, the operators of IoT DDoS botnets also started taking precautions against BrickerBot, making his work even harder.

But Janit0r is also afraid of legal repercussions from authorities. The malware dev is fully aware that what he's been doing is highly illegal, as it might have caused financial losses to companies around the world. The DHS surely noticed his actions, because it issued an official alert after BrickerBot's public disclosure.

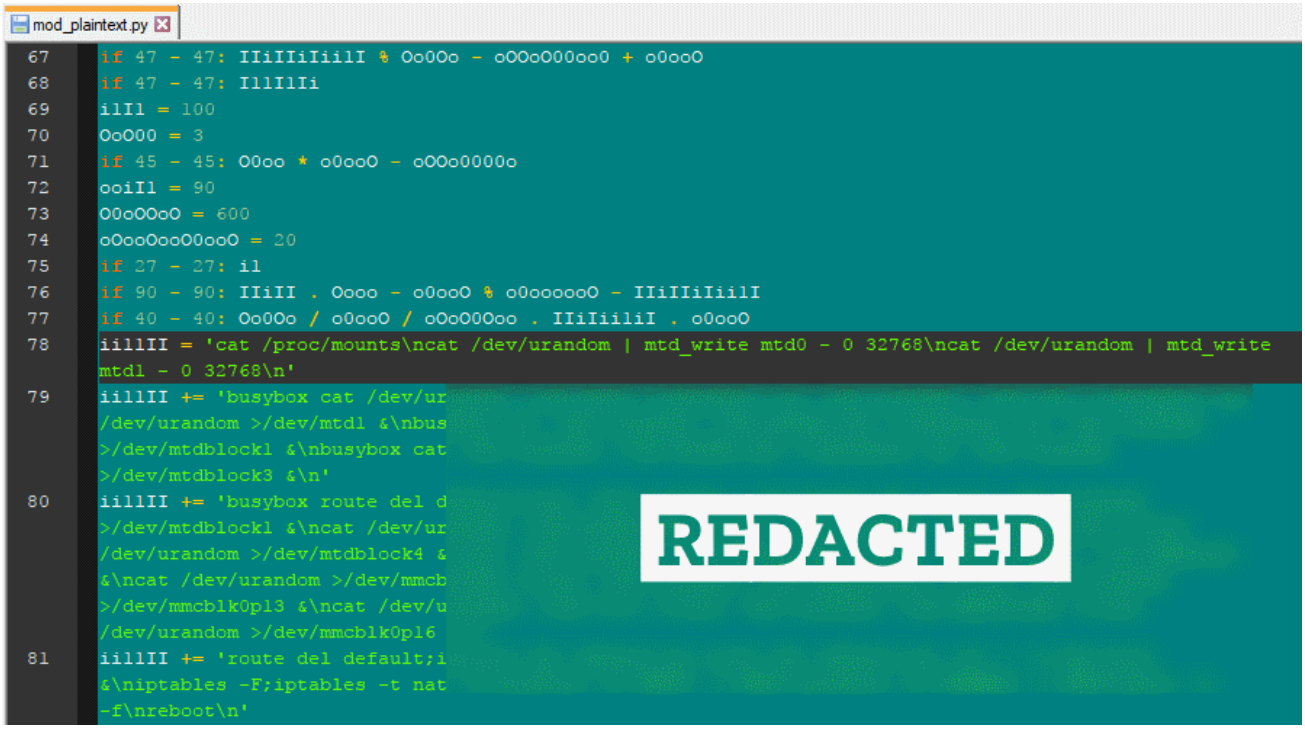
There's also only so long that I can keep doing something like this before the government types are able to correlate my likely network routes (I have already been active for far too long to remain safe). For a while now my worst-case scenario hasn't been going to jail, but simply vanishing in the middle of the night as soon as some unpleasant government figures out who I am.

Janit0r dumps some of BrickerBot's source code

These are the reasons the BrickerBot author invoked in the email Bleeping Computer received earlier today. Besides the email, Janit0r also published a manifesto on several compromised devices.

Bleeping Computer is not going to link to this manifesto since it also contains the source code for some of BrickerBot's attack (bricking) modules. We are also not publishing snippets from this manifesto, since a basic Google search could reveal copies of this file online.

We are doing this as a favor for industry experts who said the leaked code contains at least one zero-day that could be abused by other malware authors.



But Janit0r did not publish all his code.

My ssh crawler is too dangerous to publish. It contains various levels of automation for the purpose of moving laterally through poorly designed ISP networks and taking them over through only a single breached router. My ability to commandeer and secure hundreds of thousands of ISP routers was the foundation of my anti-IoT botnet project as it gave me great visibility of what was happening on the Internet and it gave me an endless supply of nodes for hacking back.

Janit0r behind long list of security incidents

All in all, the Janit0r quitting announcement focuses on trying to raise awareness to the fact that ISPs and device vendors play a major role in today's sad state of IoT security.

The BrickerBot author goes on to detail a case where he breached an ISP's network, disrupted devices for months, yet ISP employees failed to understand what was happening, let alone take precautionary actions.

He also lists a long list of incidents he claimed to have been behind, from events affecting Deutsche Telekom in Germany to Rogers in Canada, and various countries across Africa, Asia, and South America.

By far the most interesting incident is the one that has been previously classified as a "ransomware" attack, albeit it did not make any sense now or at the time.

The incident refers to a ransomware infection reported by the Washington Post that affected 70% of storage devices that record data from Washington DC's police surveillance cameras. The incident took place eight days before President Trump's inauguration, and caused some panic at the time.

According to the Janit0r, the incident can be attributed to BrickerBot running amok in some DC police-owned DVRs, which are typically the place where you find IoT malware and not ransomware.

The Janit0r preaches IoT security before going in the shadows

Janit0r's farewell message also includes some advice. For starters, he recommends that ISPs use basic tools like Shodan to audit their own networks and isolate ports and services that do not need to be exposed online.

Second, he advises users to sanction IoT vendors that do not deliver security updates in a timeline manner and refuse to purchase devices from a known offender.

Third, lobbying politicians about IoT security standards is also a good way to push IoT security forward.

Fourth, Janit0r advises security researchers to volunteer their free time to organizations such as GDI Foundation or the Shadowserver Foundation, which have been working to secure some of these vulnerable devices.

Last but not least, he advises that some of us that have too much time and money on our hands to start legal actions against the owners of some of these vulnerable devices. Janit0r believes that a constant legal threat could force companies and ISPs to install security updates and isolate equipment on private networks in a timely manner.

We'll end this article with a message from The Janit0r —original text preserved.

> YOU SHOULD WAKE UP TO THE FACT THAT THE INTERNET IS ONLY ONE OR TWO SERIOUS IOT EXPLOITS AWAY FROM BEING SEVERELY DISRUPTED.

Related Articles:

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Ukrainian imprisoned for selling access to thousands of PCs

Access:7 vulnerabilities impact medical and IoT devices

- Botnet
- BrickerBot
- Internet of Things
- IoT

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

Occasional - 4 years ago

Thanks for this story, CC. It's one of those where you can find yourself, arguing with yourself - as to whether, on balance, the actor/group's activities make things better or worse.

Criticisms of IoT hype, promotion and implementation are, if anything, not strong enough - but it's also troubling when individuals or groups take it on themselves to police the behavior of others though force. While actions speak loader than words; you can't have a debate, or find reasoned solutions to emerging problems, with sides imposing their will by force.

You may also like: