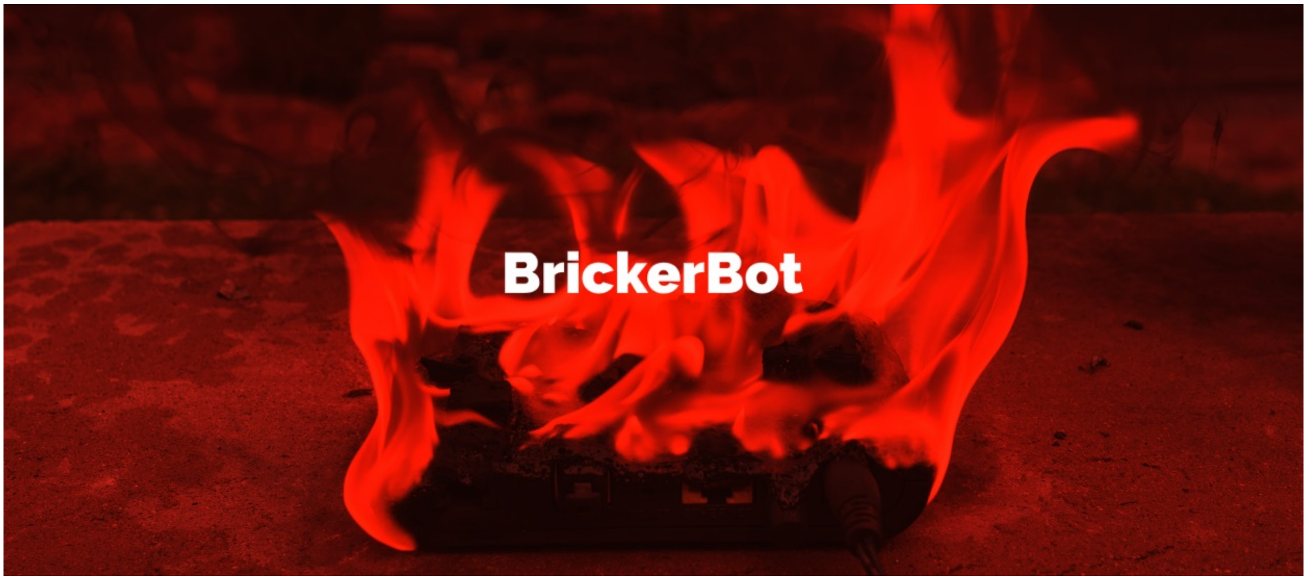
BrickerBot Author Claims He Bricked Two Million Devices

bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/

Catalin Cimpanu

By
Catalin Cimpanu

- April 21, 2017
- 01:30 AM
- 1



Just like Wifatch and Hajime, the BrickerBot malware is the work of a vigilante grey-hat, who goes online by the name of Janit0r, a nickname he chose on the Hack Forums discussion boards.

If you're unfamiliar, BrickerBot is a new malware family that was first identified at the start of the month by Radware researchers. The malware made headlines because it was the first threat of its kind that intentionally bricked IoT and networking devices, by rewriting the flash storage space of affected devices with random data.

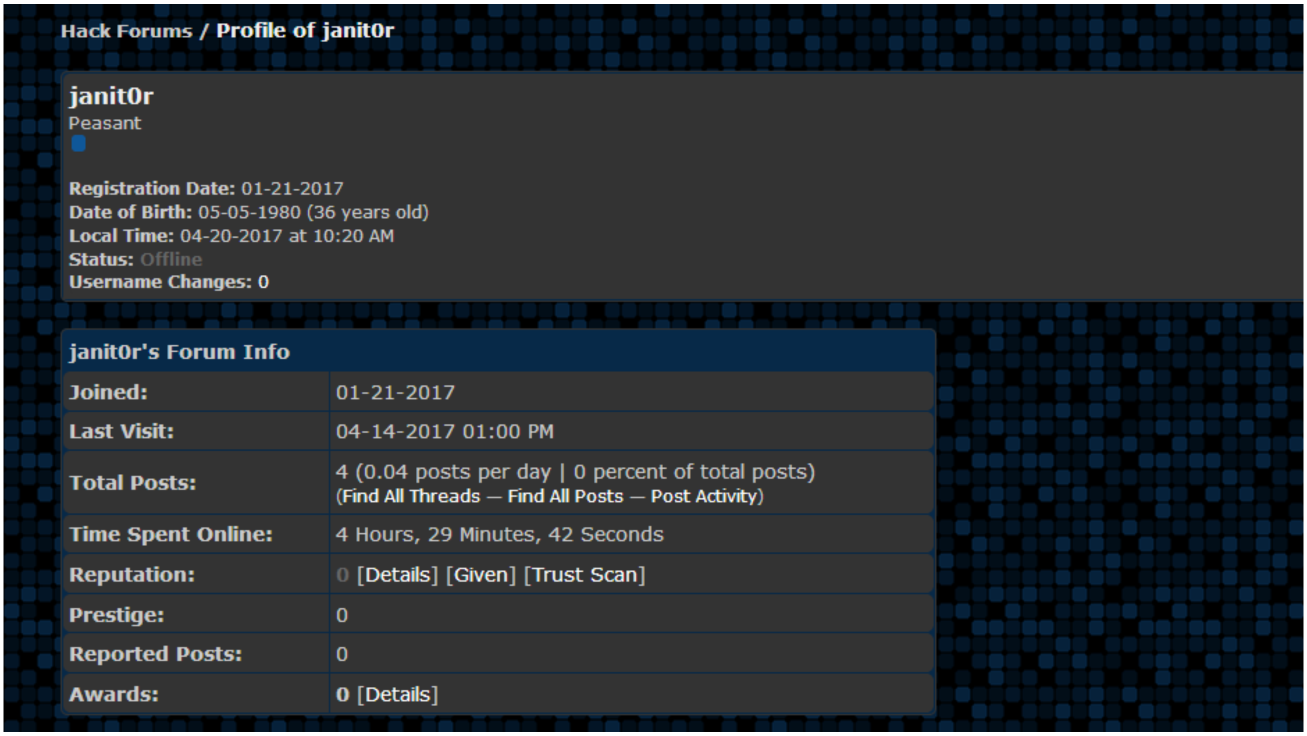
Such actions rendered troves of devices useless, many needing a firmware reinstall, but as many needing to be replaced altogether.

Destructive actions like these caught the attention of authorities. In the US, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an official alert last week, warning companies to disable Telnet and SSH access to their devices and asking owners to change their devices' default factory passwords.

Anonymous tip leads us to Hack Forums profile

Since BrickerBot's appearance, law enforcement and the infosec community have been on the hunt for new information regarding how BrickerBot operates and who's behind it.

New information surfaced over the Easter weekend when Bleeping Computer received an anonymous tip about the online identity of BrickerBot's creator. The tipster pointed us towards the profile of a Hack Forums user named janit0r.



Hack Forums / Profile of janit0r

janit0r
Peasant

Registration Date: 01-21-2017
Date of Birth: 05-05-1980 (36 years old)
Local Time: 04-20-2017 at 10:20 AM
Status: Offline
Username Changes: 0

janit0r's Forum Info	
Joined:	01-21-2017
Last Visit:	04-14-2017 01:00 PM
Total Posts:	4 (0.04 posts per day | 0 percent of total posts) (Find All Threads — Find All Posts — Post Activity)
Time Spent Online:	4 Hours, 29 Minutes, 42 Seconds
Reputation:	0 [Details] [Given] [Trust Scan]
Prestige:	0
Reported Posts:	0
Awards:	**0** [Details]

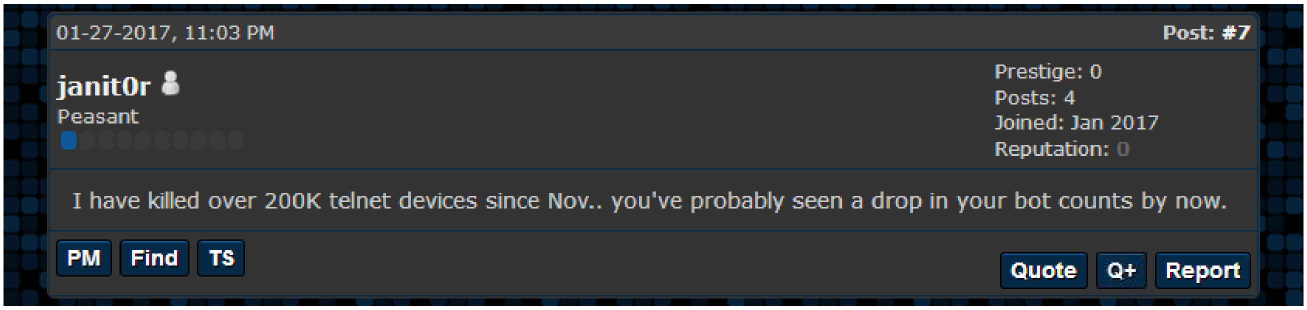
We ignored the tip at first since Hack Forums is known to attract a crowd of braggadocio hackers, many of whom tend to "embellish" their abilities or knowledge. We expected that that two weeks after BrickerBot's discovery, Hack Forums would be abuzz with people trying to take credit for BrickerBot, but it was strangely silent.

On Monday, feeling bad that we did not follow through with the same dilligence that the tipster had warned us with, we decided to have another look over janit0r's profile.

What we discovered was a user that registered on January 21, 2017, had the forum boards set up to use the Alaska timezone and had made four posts.

Right off the bat, his first post was the most interesting one. In a forum topic discussing a decline in the number of active Mirai bots, Janit0r made the following statement. Remind you, this still almost two months and a half before Radware's BrickerBot discovery.

I have killed over 200K telnet devices since Nov.. you've probably seen a drop in your bot counts by now.



01-27-2017, 11:03 PM Post: #7

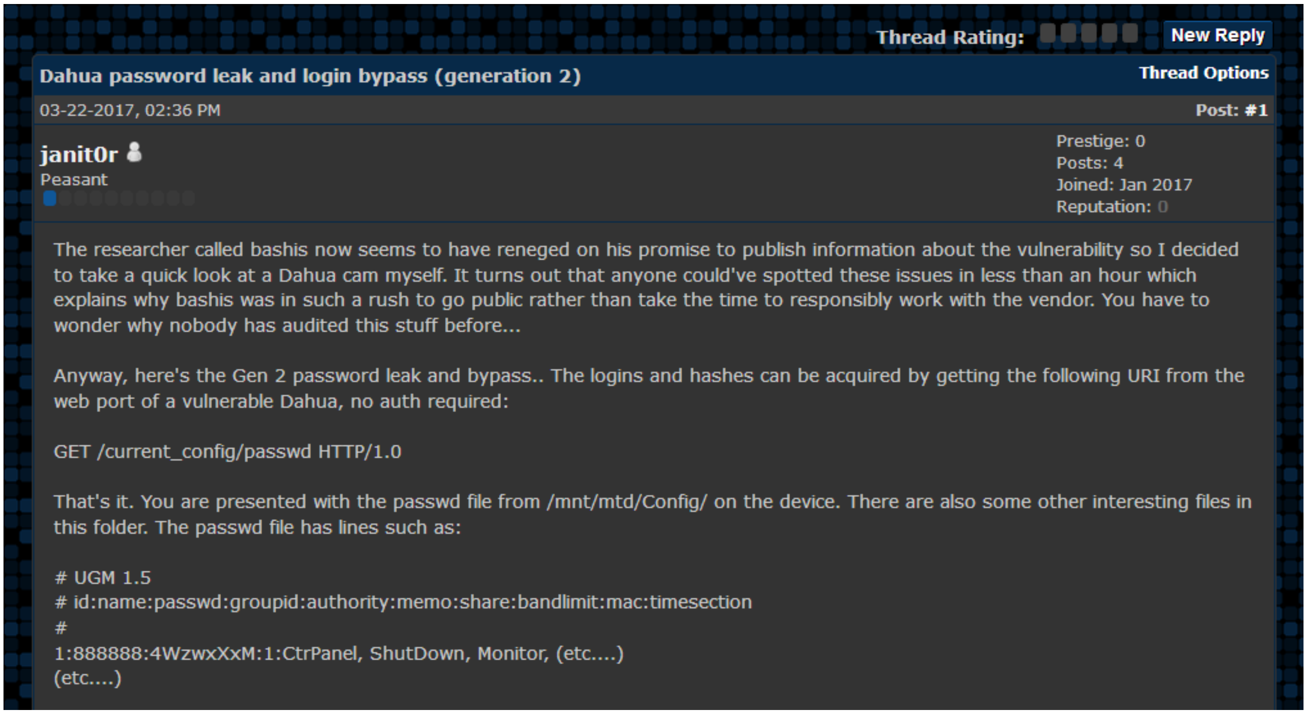
janit0r
Peasant

Prestige: 0
Posts: 4
Joined: Jan 2017
Reputation: 0

I have killed over 200K telnet devices since Nov.. you've probably seen a drop in your bot counts by now.

His second and third posts also came before BrickerBot became public and attested to his skills as a reverse engineer, in a topic he started himself, discussing a security flaw in Dahua 2nd and 3rd generation IP cameras.

The researcher who discovered and made public the flaw, withheld proof-of-concept exploit code for one month, to give Dahua customers time to apply a firmware update. Janit0r showed dissatisfaction with the researcher's action and published exploitation details for that particular bug himself.



Dahua password leak and login bypass (generation 2)

03-22-2017, 02:36 PM Post: #1

janit0r
Peasant

Prestige: 0
Posts: 4
Joined: Jan 2017
Reputation: 0

The researcher called bashis now seems to have reneged on his promise to publish information about the vulnerability so I decided to take a quick look at a Dahua cam myself. It turns out that anyone could've spotted these issues in less than an hour which explains why bashis was in such a rush to go public rather than take the time to responsibly work with the vendor. You have to wonder why nobody has audited this stuff before...

Anyway, here's the Gen 2 password leak and bypass.. The logins and hashes can be acquired by getting the following URI from the web port of a vulnerable Dahua, no auth required:

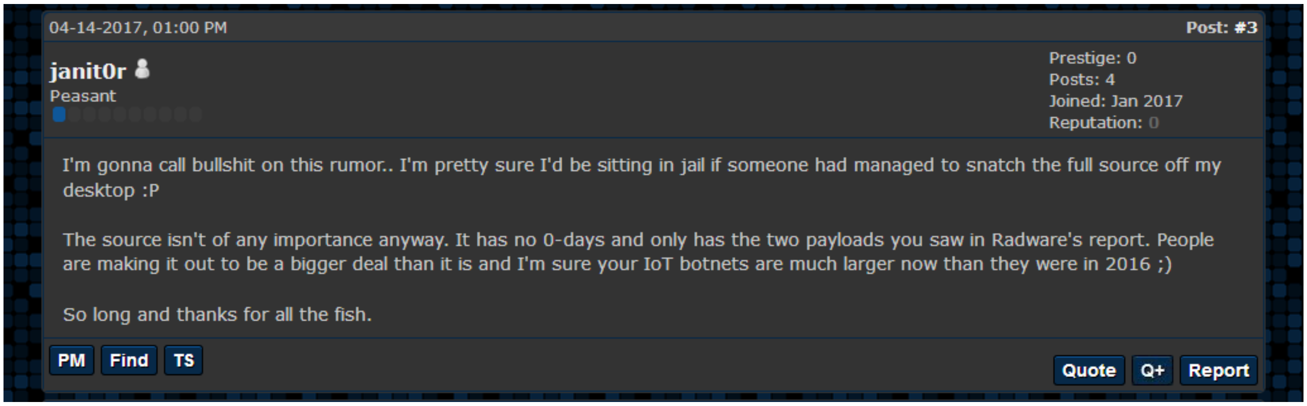
```
GET /current_config/passwd HTTP/1.0
```

That's it. You are presented with the passwd file from /mnt/mtd/Config/ on the device. There are also some other interesting files in this folder. The passwd file has lines such as:

```
# UGM 1.5
# id:name:passwd:groupid:authority:memo:share:bandlimit:mac:timesection
#
1:888888:4WzwxXxM:1:CtrPanel, ShutDown, Monitor, (etc....)
(etc....)
```

His last post was in a topic started by a user who "heard" that BrickerBot's source had leaked. Janit0r's response was quick and to the point.

I'm gonna call bullshit on this rumor.. I'm pretty sure I'd be sitting in jail if someone had managed to snatch the full source off my desktop :P


04-14-2017, 01:00 PM

Post: #3

janit0r

Peasant

Prestige: 0
Posts: 4
Joined: Jan 2017
Reputation: 0

I'm gonna call bullshit on this rumor.. I'm pretty sure I'd be sitting in jail if someone had managed to snatch the full source off my desktop :P

The source isn't of any importance anyway. It has no 0-days and only has the two payloads you saw in Radware's report. People are making it out to be a bigger deal than it is and I'm sure your IoT botnets are much larger now than they were in 2016 ;)

So long and thanks for all the fish.

At this point, we had to confirm that Janit0r was indeed BrickerBot's author and not just some guy bragging on Hack Forums. This is how we spent the next two days, scraping through the Dark Web, underground hacking forums, and getting in contact with a few threat intelligence analysts we knew.

By Wednesday, we didn't manage to find any other clue of Janit0r's existence, or anybody else claiming to be BrickerBot's author, with some solid proof on his side. That's when we just gave up, and launched a desperate tweet, asking BrickerBot's author to reach out.

BrickerBot's Author reaches out

Lo and behold, this was exactly what happened. The same day, we received an email from a person claiming to be BrickerBot's creator.

The email contained lots of details about BrickerBot's operation and internal structure. Nevertheless, at this point, we knew that there could be the possibility that someone was pulling a prank.

Chance had it that someone else had also seen our tweet. That person was Victor Gevers, a security researcher mostly known for tracking the destructive ransom attacks against MongoDB and other databases.

In the Bleeping Computer article that broke the news of BrickerBot's existence, we asked Victor for his expert opinion on this new malware's behavior and repercussions. Victor not only put BrickerBot in perspective for our readers, but also asked BrickerBot's creator to reach out and discuss an alternative method of dealing with unsecured IoT devices, instead of blindly destroying people's property.

Unknown to all was that BrickerBot author had reached out to Victor hours after our article went live. The two had shared notes and Victor was acting as an intermediary between Janit0r and various CERTs. All the operational details shared with us on Wednesday were the same Janit0r shared with Victor in the previous three weeks, confirming we were speaking with the same person.

"Yes, I am janit0r"

"Yes, I was janit0r on Hackforums," the BrickerBot author started his email, which then continued with Janit0r showing his anger at the sad state of affairs in the realm of IoT security.

Like so many others I was dismayed by the indiscriminate DDoS attacks by IoT botnets in 2016. I thought for sure that the large attacks would force the industry to finally get its act together, but after a few months of record-breaking attacks it became obvious that in spite of all the sincere efforts the problem couldn't be solved quickly enough by conventional means.

The IoT security mess is a result of companies with insufficient security knowledge developing powerful Internet-connected devices for users with no security knowledge. Most of the consumer-oriented IoT devices that I've found on the net appear to have been deployed almost exactly as they left the factory.

For example 9 out of every 10 Avtech IP cameras that I've pulled the user db from were set up with the default login admin/admin! Let that statistic sink in for a second.. and then consider that if somebody launched a car or power tool with a safety feature that failed 9 times out of 10 it would be pulled off the market immediately. I don't see why dangerously designed IoT devices should be treated any differently and after the Internet-breaking attacks of 2016 nobody can seriously argue that the security of these devices isn't important.

I hope that regulatory bodies will do more to penalize careless manufacturers since market forces can't fix this problem. The reality of the market is that technically unskilled consumers will get the cheapest whitelabel DVR they can find at their local store, then they'll ask their nephew to plug it into the Internet, and a few minutes later it'll be full of malware. At least with 'BrickerBot' there was some brief hope that such dangerous devices could become the merchant's and manufacturer's problem rather than our problem.

BrickerBot allegely wiped over two million devices

I joined Hackforums in January mainly to see if my activities had been noticed by the botnet kids. Back then 200,000 bricked units seemed like a lot and I was sure I was close to the end of it. Now when the count is **over 2 million** it's clear that I had no idea (and still have no idea) how deep the rabbit hole of IoT insecurity is. I'm certain that the worst is still ahead of us.

I hope the unconventional actions by 'BrickerBot' have helped in buying another year of time for governments, vendors and the industry in general to get the current IoT security nightmare under control.

Many other people have also done important things to combat IoT malware (Team White, Hajime author, @packetcop and his fellow sinkholers, etc) so I'm by no means claiming credit for Mirai being weak in Q1/2017, but if Imeij and Amnesia have suffered a little recently then it's probably mainly my fault ;)

Janit0r's email then goes on to detail a few operational details regarding BrickerBot's infrastructure, also dispelling the notion that he's a madman set on the random destruction of IoT devices.

In reality, Janit0r wants to be considered in the same class as the White Team, the self-proclaimed white-hat hackers behind the Wifatch malware, and the author of the Hajime malware, another vigilante who created a new malware family last October that tries to secure IoT devices by force.

The Radware writeup made 'BrickerBot' sound simplistic, but it actually carries 86 protocol and device-specific payloads and is relatively successful at mitigating commonly exploited devices. The bot's every action has a statistically determined purpose and what might've seemed like buggy behavior in the honeypot really isn't.

As a preference 'BrickerBot' will try to secure units without damaging them and the bricking behavior is a 'plan B' (yes the B stands for brick :) for units which are unlikely to be securable. A blogger on the net wondered about 'BrickerBot' simply trying to change his honeypot's login and this would've been due to the bot assuming the device had a persistent user db. Because the honeypots are often quite different from any actual devices the behaviors in them are usually weird.

If security researchers made their honeypots look more like actual devices (that one could actually find with default credentials on the net) and hosted them on dirtier networks they would find even more interesting things going on..

Victor Gevers, who confirmed Janit0r's bricking statistics also believes this person is only misguided, and hopes to convince him to abandon his ways. "The writer of the email does not strike me as a bad person," Gevers told Bleeping Computer based on his own communications with Janit0r. "Just some young guy who was too eager to solve a problem."

Janit0r wants a change in IoT security standards

For the time being, Janit0r doesn't seem interested in stopping BrickerBot attacks, or at least not until officials and hardware vendors take a look at IoT security and start changing things with a hurry.

Authorities have been talking about IoT security standards for years, but in the meantime, some of the same vendors participating in those discussions have continued to ship out insecure devices with the same ol' default passwords. In a follow-up email, Janit0r wrote the following.

I consider my project a form of "Internet Chemotherapy" I sometimes jokingly think of myself as The Doctor. Chemotherapy is a harsh treatment that nobody in their right mind would administer to a healthy patient, but the Internet was becoming seriously ill in Q3 and Q4/2016 and the moderate remedies were ineffective. The side effects of the treatment were harmful but the alternative (DDoS botnet sizes numbering in the millions) would have been worse. I can only hope hope that when the IoT relapse comes we'll have better ways to deal with it. Besides getting the number of IoT DDoS bots to a manageable level my other key goal has been to raise awareness. The IoT problem is much worse than most people think, and I have some alarming stories to tell.

Janit0r is a wanted man

Nonetheless, the actions of BrickerBot place this malware in the same category as other destructive e-threats, such as ransomware and banking trojans. Janit0r already knows he's a wanted man and has taken many precautions.

Tracking down Janit0r's real life persona may also be a little harder than going after teenagers that rent DDoS botnets with their father's credit card. While he signed his Hack Forums posts with the name "Rob," Janit0r also used different names within each email, said he never intends to log into his Janit0r Hack Forums account again, and has consistently changed email addresses every few days.

For what's worth it, Janit0r has been very careful with his OpSec, compared to many of today's hackers, who, according to a Flashpoint report released yesterday, prefer Skype as their main communications method, an IM service known to give up data on its users to law enforcement.

Janit0r: I'm not a security researcher

Current clues like Janit0r's reverse engineering skills, in-depth knowledge of the malware scene, and a desire to do good, point to the fact that we may be dealing with another security researcher or network engineer that has decided to do something about the ever-increasing number of unsecured network and IoT devices.

"For what it's worth I'll state that I've never actually worked in networking, systems administration, information security or anything of the sort, but I have a hobby interest in all of the above. I believe that basic knowledge in such things is good self-defense in the 21st century," Janit0r wrote in an email.

Right now, all users and companies can do is to follow Radware and ICS-CERT's recommendations, and block access to Telnet and SSH ports, and also change the device's default password. Otherwise, they may get a visit from BrickerBot, and it might reach Plan B.

Headline image credit: Simeon W & Bleeping Computer

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

Emotet botnet switches to 64-bit modules, increases activity

New stealthy BotenaGo malware variant targets DVR devices

- Botnet
- BrickerBot
- IoT
- Malware

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

DodoIso - 5 years ago

It would be interesting to know what actions are taken before PLAN B... Quickly browsing through the Radware article, it seems a better approach to fix the problem is to program the device's firewall to deny incoming and outgoing WAN traffic, and the device would still be usable locally by the innocent customer. If enough customers return their device to vendors because they do not perform as advertised, that would get the wheel turning. Bricking a device is kind of 'off-warranty', waste time, and raise the customers' cost tremendously to prove to the vendors that they did nothing wrong. The burden should be on the vendors, not the customers.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: