

Alleged ‘Satori’ IoT Botnet Operator Sought Media Spotlight, Got Indicted

krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/

A 20-year-old from Vancouver, Washington was indicted last week on federal hacking charges and for allegedly operating the “**Satori**” botnet, a malware strain unleashed last year that infected hundreds of thousands of wireless routers and other “Internet of Things” (IoT) devices. This outcome is hardly surprising given that the accused’s alleged alter ego has been relentless in seeking media attention for this global crime machine.



Schuchman, in an undated photo posted online and referenced in a “dox,” which alleged in Feb. 2018 that Schuchman was Nexus Zeta.

The Daily Beast’s **Kevin Poulsen** broke the [news](#) last week that federal authorities in Alaska indicted **Kenneth Currin Schuchman** of Washington on two counts of violating the Computer Fraud and Abuse Act by using malware to damage computers between August and November 2017.

The [3-page indictment](#) (PDF) is incredibly sparse, and includes few details about the meat of the charges against Schuchman. But according to Poulsen, the charges are related to Schuchman’s alleged authorship and use of the Satori botnet. Satori, also known as “Masuta,” is a variant of [the Mirai botnet](#), a powerful IoT malware strain that first came online in July 2016.

“Despite the havoc he supposedly wreaked, the accused hacker doesn’t seem to have been terribly knowledgeable about hacking,” Poulsen notes.

Schuchman reportedly went by the handle “**Nexus Zeta**,” the nickname used by a fairly inexperienced and clumsy ne’er-do-well who has tried on multiple occasions to get KrebsOnSecurity to write about the Satori botnet. In January 2018, Nexus Zeta changed the

login page for his [botnet control panel](#) that he used to remotely control his hacked routers to include a friendly backhanded reference to this author:



The login prompt for Nexus Zeta’s IoT botnet included the message “Masuta is powered and hosted on Brian Kreb’s [sic] 4head.” To be precise, it’s a 5head.

This wasn’t the first time Nexus Zeta said hello. In late November 2017, he chatted me up on on Twitter and Jabber instant message for several days. Most of the communications came from two accounts: “**9gigs_ProxyPipe**” on Twitter, and **ogmemes123@jabber.ru** (9gigs_ProxyPipe would later change its Twitter alias to Nexus Zeta, and Nexus Zeta himself admitted that 9gigs_ProxyPipe was his Twitter account.)

In each case, this person wanted to talk about a new IoT botnet that he was “researching” and that he thought deserved special attention for its size and potential disruptive impact should it be used in a massive Distributed Denial-of-Service (DDoS) attack aimed at knocking a Web site offline — something for which Satori would soon become known.

ogmemes123@jabber.ru

(04:39:25 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: hi

(04:41:14 PM) ogmemes123@jabber.ru: Has nobody noticed the mirai variant cnc hanging out with a fluctuating 300-500k devices infected ?

(04:42:48 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: i don't know. where is the c2?

(04:42:58 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: hard to imagine a botnet that big would go unnoticed

(04:43:47 PM) ogmemes123@jabber.ru: It's literally jumped from leaseweb to digital ocean then to some other host now psych networks

(04:45:02 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: i see. do you know the IP of the C2?

(04:45:29 PM) ogmemes123@jabber.ru: Let me check

(04:45:46 PM) ogmemes123@jabber.ru: I have two that appear to be active c2 servers

(04:46:46 PM) ogmemes123@jabber.ru: 172.93.97.219

(04:49:37 PM) ogmemes123@jabber.ru: From what I noticed the bot port was on port 7645

(05:01:02 PM) ogmemes123@jabber.ru: Have you obtained any further information?

(05:16:28 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: no. did you say there were 2 C2s?

(05:17:09 PM) ogmemes123@jabber.ru: Yes from what I found but I don't know the host ip from memory

(05:17:21 PM) ogmemes123@jabber.ru: I am currently working on a mobile device

(05:33:54 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: how is it you came to learn about this?

(05:35:23 PM) ogmemes123@jabber.ru: I pop up here and there within the hacking community and I also have my own sources

(05:36:02 PM) ogmemes123@jabber.ru: I apologize if it sounds rude, but I prefer not to disclose my sources

(05:37:17 PM) ogmemes123@jabber.ru: I wouldn't want to create a misunderstanding and incriminate myself.

(05:39:58 PM) krebsjabber@jabber.se/106677253125125026391511991439276646: fair enough. so do we know if this botnet has actually attacked anyone? or what it's made out of ?

A Jabber instant message conversation with Nexus Zeta on Nov. 29, 2017.

Nexus Zeta's Twitter nickname initially confused me because both 9gigs and ProxyPipe are names claimed by **Robert Coelho**, owner of ProxyPipe hosting (9gigs is a bit from one of Coelho's Skype account names). Coelho's sleuthing was quite instrumental in helping to unmask 21-year-old New Jersey resident Paras Jha as the author of the original Mirai IoT botnet (Jha later pleaded guilty to co-authoring and using Mirai and is due to be sentenced this month in Alaska and New Jersey). "Ogmemes" is from a nickname used by Jha and his Mirai botnet co-author.

On Nov. 28, 2017, 9gigs_ProxyPipe sent a message to the KrebsOnSecurity Twitter account:







"I have some information in regards to an incredibly dangerous IoT botnet you may find interesting," the Twitter message read. "Let me know how you would prefer to communicate assuming you are interested."

We connected on Jabber instant message. In our chats, Ogmemes123 said he couldn't understand why nobody had noticed a botnet powered by a Mirai variant that had infected hundreds of thousands of IoT devices (he estimated the size of the botnet to be about 300,000-500,000 at the time). He also talked a lot about how close he was with Jha. Nexus Zeta's Twitter account profile photo is a picture of Paras Jha. He also said he knew this new botnet was being used to attack ProxyPipe.

Less than 24 hours after that tweet from Nexus Zeta, I heard from ProxyPipe's Coelho. They were under attack from a new Mirai variant.

"We've been mitigating attacks recently that are about 270 gigabits [in volume]," Coelho wrote in an email. "Looks like somebody tagged you on Twitter pretending to be from ProxyPipe — likely the attacker? Just wanted to give you a heads up since that is not us, or anyone that works with ProxyPipe."

From reviewing Nexus Zeta’s myriad postings on the newbie-friendly hacker forum [Hackforums-dot-net](#), it was clear that Nexus Zeta was an inexperienced, impressionable young man who wanted to associate himself with people closely tied to [the 2017 whodunnit over the original Mirai IoT botnet variant](#). He also asked other Hackforums members for assistance in assembling his Mirai botnet:

	Thread / Author	Forum	Replies	Views	Last Post [asc]
	help me setup the mirai telnet bot-net - 1 tbps instantly (1 2) Nexus Zeta	Botnets, IRC Bots, and Zombies	10	425	11-27-2017, 06:29 PM Last Post: Finty
	Notice: Killing all Mirai bots (1 2 3 4) Nexus Zeta	Botnets, IRC Bots, and Zombies	35	2,685	08-08-2017, 08:24 AM Last Post: VEXTRACTF128
	Compiling for armv6b (1 2) Nexus Zeta	Botnets, IRC Bots, and Zombies	11	306	01-24-2017, 08:15 PM Last Post: caiveman
	Need server to bruteforce scans will give spot on net (1 2 3) Nexus Zeta	Botnets, IRC Bots, and Zombies	28	841	09-16-2016, 07:40 AM Last Post: /pH/
	Need vuln lists to scan into telnet and IRC- will give access i have 5 dedis 4 scan Nexus Zeta	Botnets, IRC Bots, and Zombies	3	362	08-30-2016, 03:03 PM Last Post: Transcendent
	Professional Botnet Support and Setup Services (FREE) Nexus Zeta	Botnets, IRC Bots, and Zombies	7	360	12-06-2015, 04:29 PM Last Post: Syria

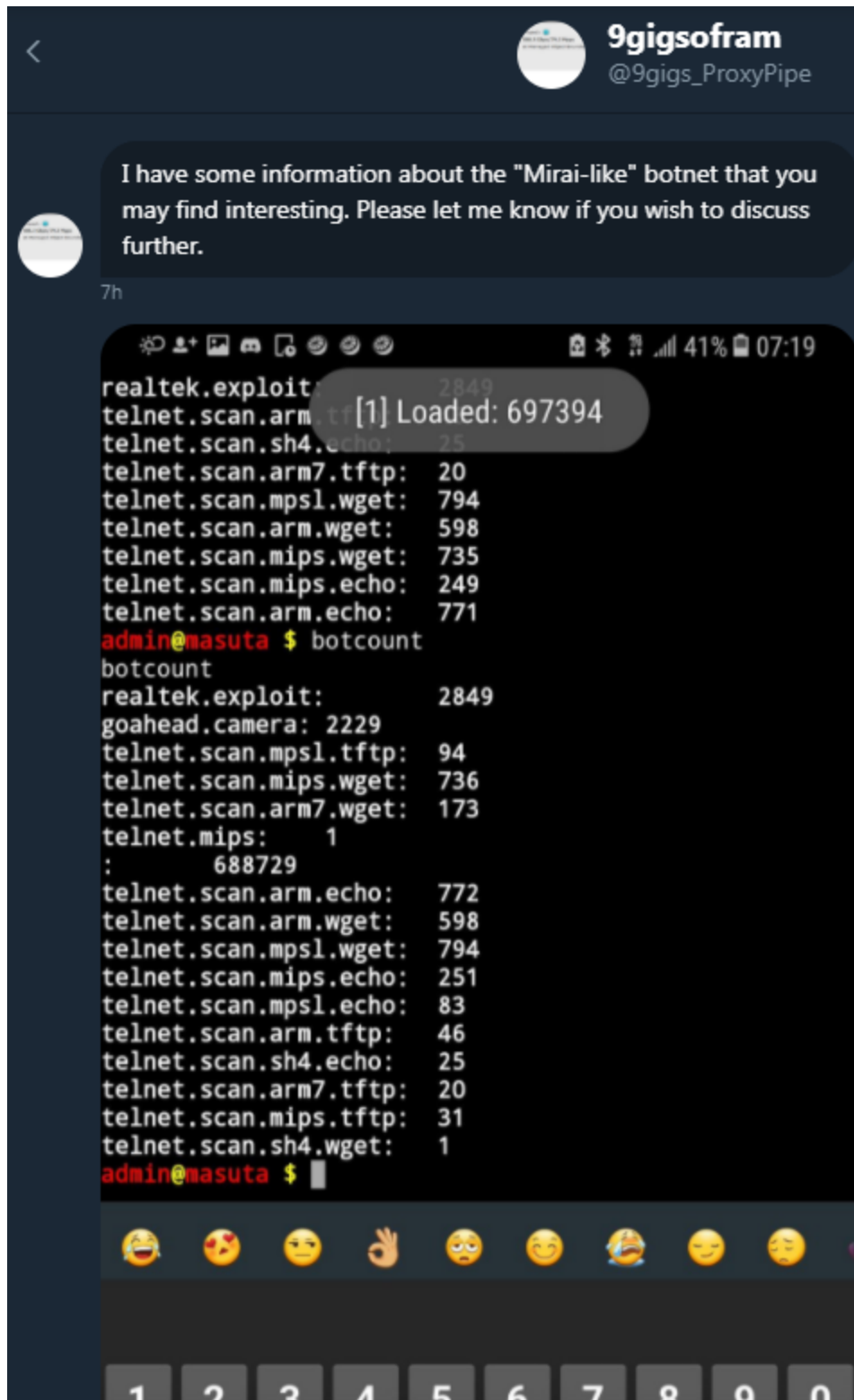
Some of Nexus Zeta’s posts on Hackforums, where he asks for help in setting up a Mirai botnet variant. Click to enlarge.

In one conversation with Ogmemes123, I lost my cool and told him to quit running botnets or else go bore somebody else with his quest for publicity. He mostly stopped bugging me after that. That same day, Nexus Zeta spotted [a tweet](#) from security researcher [Troy Mursch](#) about the rapid growth of a new Mirai-like botnet.

“This is an all-time record for the most new unique IP addresses that I’ve seen added to the botnet in one day,” Mursch tweeted of the speed with which this new Mirai strain was infecting devices.

For weeks after that tweet, Nexus Zeta exchanged private twitter messages with Mursch and his team of botnet hunters at [Bad Packets LLC](#) in a bid to get them to Tweet or write about Satori/Masuta.

The following screenshots from their private Twitter discussions, republished with Mursch’s permission, showed that Nexus Zeta kept up the fiction about his merely “researching” the activities of Satori. Mursch played along, and asked gently probing questions about the size, makeup and activities of a rapidly growing Satori botnet.



9gigs_ProxyPipe (a.k.a. Nexus Zeta allegedly a.k.a Kenneth Schuchman) reaches out to security researcher Troy Mursch of Bad Packets LLC.

Early in their conversations, Nexus Zeta says he is merely following the visible daily Internet scanning that Satori generated in a constant search for newly infectable IoT devices. But as their conversations continue over several weeks, Nexus Zeta intimates that he has much deeper access to Satori.



In this conversation from Nov. 29, 2017 between Nexus Zeta/9gigs_ProxyPipe and Troy Mursch, the former says he is seeing lots of Satori victims from Argentina, Colombia and Egypt.

Although it long ago would have been easy to write a series of stories about this individual and his exploits, I had zero interest in giving him the attention he clearly craved. But thanks to naivete and apparently zero sense of self-preservation, Nexus Zeta didn't have to wait long for others to start connecting his online identities to his offline world.

On Dec. 5, Chinese cybersecurity firm **Netlab360** released [a report on Satori](#) noting that the IoT malware was spreading rapidly to Chinese-made **Huawei** routers with the help of two security vulnerabilities, including one "zero day" flaw that was unknown to researchers at the time. The report said a quarter million infected devices were seen scanning for vulnerable systems, and that much of the scanning activity traced back to infected systems in Argentina, Colombia and Egypt, the same hotspots that Nexus Zeta cited in his Nov. 29 Twitter chat with Troy Mursch (see screen shot directly above).

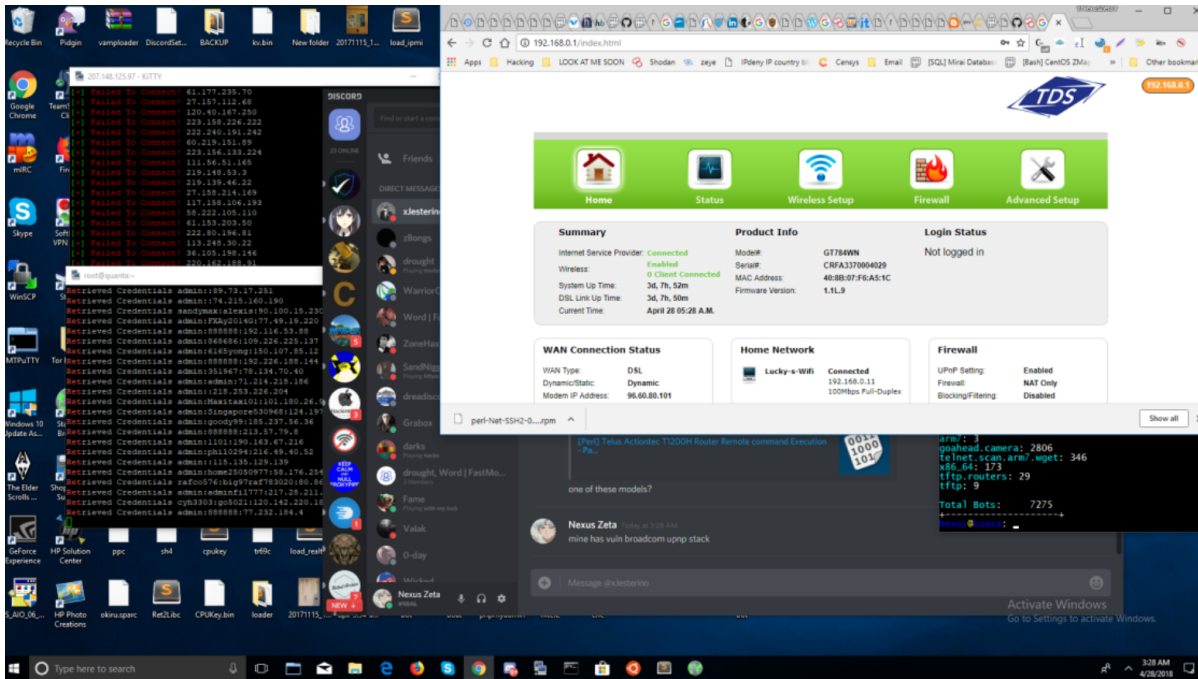
In a taunting post published Dec. 29, 2017 titled "[Good Zero Day Kiddie](#)," researchers at Israeli security firm **CheckPoint** pointed out that the domain name used as a control server to synchronize the activities of the Satori botnet — **nexusiotsolutions-dot-net** — was

registered in 2016 to the email address **nexuszeta1337@gmail.com**. The CheckPoint report noted the name supplied in the original registration records for that domain was a “Caleb Wilson,” although the researchers correctly noted that this could be a pseudonym.

Perhaps the CheckPoint folks also knew the following tidbit, but chose not to publish it in their report: The email address **nexuszeta1337@gmail.com** was only ever used to register a single domain name (**nexusiotsolutions-dot-net**), according to a historic WHOIS record search at DomainTools.com [full disclosure: DomainTools is an advertiser on this site.] But the phone number in that original domain name record was used to register one other domain: **zetastress-dot-net** (a “stresser” is another name for a DDoS-for-hire-service). The registrant name listed in that original record? You guessed it:

Registrant Name: kenny Schuchman
Registrant Organization: ZetaSec Inc.
Registrant Street: 8709 Ne Mason Dr, No. 4
Registrant City: Vancouver
Registrant State/Province: Washington
Registrant Postal Code: 98662
Registrant Country: US
Registrant Phone: +1.3607267966
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kenny.windwmx79@outlook.com

In April 2018 I heard from a source who said he engaged Nexus Zeta in a chat about his router-ravaging botnet and asked what kind of router Nexus Zeta trusted. According to my source, Nexus Zeta shared a screen shot of the output from his wireless modem’s Web interface, which revealed that he was connecting from an Internet service provider in Vancouver, Wash., where Schuchman lives.



The Satori botnet author shared this screen shot of his desktop, which indicated he was using an Internet connection in Vancouver, Washington — where Schuchman currently lives with his father.

“During our discussions, I learned we have the same model of router,” the source said. “He asked me my router model, and I told him. He shared that his router was also an ActionTec model, and sent a picture. This picture contains his home internet address.”

This matched a comprehensive “dox” that someone published on **Pastebin** in Feb. 2018, declaring Nexus Zeta to be 20-year-old Kenneth Currin Schuchman from Vancouver, Washington. The dox said Schuchman used the aliases Nexus Zeta and Caleb Wilson, and listed all of the email addresses tied to Nexus Zeta above, plus his financial data and physical address.

“Nexus is known by many to be autistic and a compulsive liar,” the dox begins.

“He refused to acknowledge that he was wrong or apologize, and since he has extremely poor opsec (uses home IP on everything), we have decided to dox him.

He was only hung around by few for the servers he had access to.

He lies about writing exploits that were made before his time, and faking bot counts on botnets he made.

He’s lied about having physical contact with Anna Senpai (Author of Mirai Botnet).”

As detailed in the *Daily Beast* story and Nexus Zeta’s dox, Schuchman was diagnosed with Asperger Syndrome and autism disorder, and at one point when he was 15 Schuchman reportedly wandered off while visiting a friend in Bend, Ore., briefly prompting a police search before he was found near his mother’s home in Vancouver, Wash.

Nexus Zeta clearly had limited hacking skills initially and almost no operational security. Indeed, his efforts to gain notoriety for his illegal hacking activities eventually earned him just that, as it usually does.

But it's clear he was a quick learner; in the span of about a year, Nexus Zeta was able to progress from a relatively clueless newbie to the helm of an international menace that launched powerful DDoS attacks while ravaging hundreds of thousands of systems.