



# Worm War: The Botnet Battle for IoT Territory

Stephen Hilt, Fernando Mercês, Mayra Rosario, and David Sancho



#### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by  
Trend Micro Research

Written by  
Stephen Hilt, Fernando Mercês,  
Mayra Rosario, and David Sancho

Stock image used under license from  
Shutterstock.com

*For Raimund Genes (1963 – 2017)*

# Contents

**4**

Introduction

**5**

What the Numbers Show

**8**

Mirai: The Grandfather

**11**

Kaiten: A Tsunami of Attacks

**13**

Qbot: The Third Brother

**16**

IoT Botnet Malware in the  
Cybercriminal Underground

**20**

Case Study: JenX

**25**

Conclusion



A war is being waged in the cybercriminal underground and across online devices, a war in which the most affected devices are routers. Even as they sit quietly in many homes around the world, routers are the battleground for a portion of cybercriminals today. Cybercriminals collect infected routers in what are known as botnets, specifically internet-of-things (IoT) botnets. The most powerful botnet has the greatest number of routers, fueling the battle for resources among cybercriminal groups.

In this research paper, we examine the nature of this so-called worm war and the groups that are waging it. We first look into the three main source codebases that have spawned numerous pieces of botnet malware: Mirai, Kaiten, and Qbot. These bot source codebases, which are readily available on the internet, allow malicious actors to snatch control of affected devices even from competing cybercriminal groups. We then explore the accessibility of IoT botnets as illustrated by their market in the cybercriminal underground. Finally, we present a case study to demonstrate one of the many ways botnets are used by cybercriminal groups.

With this research paper, we hope to help inform users who are caught in the crossfire of this war. We also aim to help users learn how to protect their routers and other connected devices — especially in a time when these devices are all the more essential to maintaining connectivity in homes, whether for work or otherwise.

# Introduction

One would be forgiven for thinking that surely there must be critical devices other than routers that cybercriminals could profit from targeting. The reality, however, is that being able to take over home routers is already advantageous to many cybercriminals since there are a number of ways to monetize infected routers.

Cybercriminals often use infected routers to launch distributed denial-of-service (DDoS) attacks on third parties. This is a tried and tested form of online extortion — making a machine on the internet inaccessible and refusing to stop doing so until a fee is paid. This is even more relevant nowadays, in a time when many businesses rely on their e-commerce revenue to survive.

Cybercriminals also use infected routers to let other people access the internet through them. In doing so, cybercriminals can use these channels to cover their tracks and essentially frame innocent victims: Any wrongdoing committed by cybercriminals while using an infected router will implicate the device owner's IP address.

With enough infected routers, cybercriminals could form powerful botnets to sell as individual services. “We can DDoS anybody on the internet and bring down their website,” or “We can let you access the internet anonymously by means of some random IP address,” their ads promise on some cybercriminal underground forums.

In summary, infected routers mean money. The more routers cybercriminals take over, the more power their botnet accumulates and, ultimately, the more lucrative the botnet becomes. Therefore, *cybercriminals compete to take over as many routers as they can*. As soon as a group of cybercriminals infects a router, they usually uninstall preexisting malware infections. They do not do this, though, to assume the role of heroic outlaws in the manner of Robin Hood, where a crime is committed to stop a greater evil. It is merely a case of thief versus thief, where both parties compete over potential victims. To be clear, there is no technical reason that a device could not be infected by different pieces of botnet malware. It is just that botnet owners simply do not want to share the bandwidth of an infected router with other botnet owners.

There is another nasty side effect for end users after their routers become infected. Whenever an IP address is flagged as being part of an active IoT botnet, it will often turn up in blacklists for different security solutions. If blacklisted, the victims' machines would not only be carrying out or facilitating crime, but they would also be unable to properly access parts of the internet — or the environment of the victims' own companies, for that matter. In today's world, where numerous people are working from home, the security of home routers is even more critical.

# What the Numbers Show

There are millions of routers around the world, with more being added or some taken offline every moment. The widespread and disparate nature of routers makes it impossible for a single holistic view of all the routers that are infected globally. However, solutions such as the Trend Micro™ Home Network Security software track several data points that indicate the overall growth of botnets over time. Two that we think are among the most directly relevant are brute-force login attempts and Telnet login attempts.

In a brute-force login attempt, a malicious actor aims to gain access to a device by guessing the necessary password. This is systematically done using a program that tries every possible password until one finally works. With IoT devices such as routers, it is often a fairly quick process since many routers use publicly known default passwords. Specific to botnets, brute-force logins might be part of a botnet that is trying to log in to additional routers so as to widen its presence and effectiveness. As previously mentioned, the more routers a botnet accumulates, the more powerful it becomes and the more money it earns its owner.

According to Trend Micro's telemetry, as visualized in Figure 1, brute-force login attempts on routers grew steadily in 2019. The growth was incremental at first, until October. Beginning in that month, the figures drastically increased and pushed the numbers in a different ballpark altogether. We cannot say for sure how many of these login attempts came from routers, but routers are the likeliest source of and explanation for such a spike in attempts. The war for botnet control has shifted, becoming more powerful and abusing more routers than ever before.

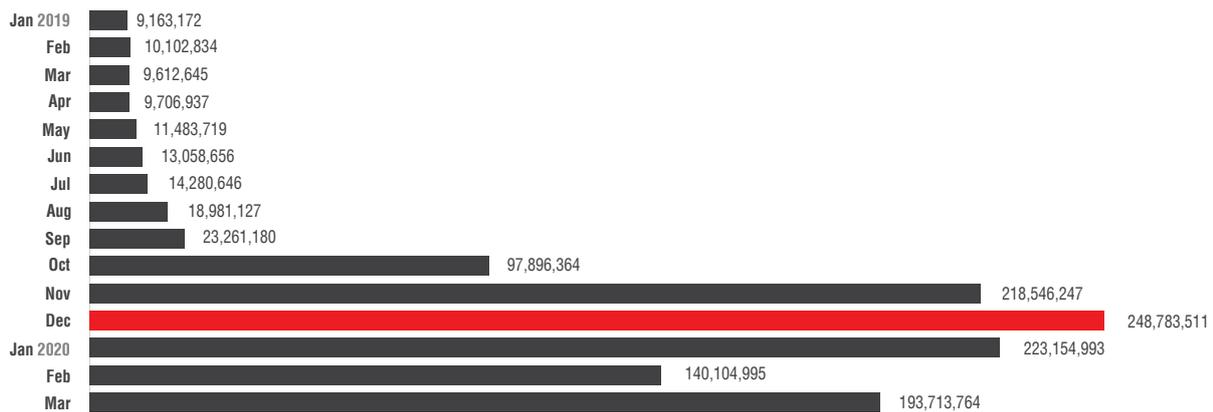


Figure 1. Brute-force login attempts from January 2019 to March 2020

Telnet activity related to IoT worms or botnet malware paints a similar picture. Telnet is another means used by malicious actors to extend the reach of their IoT botnets. Telnet data points can provide further insight into the magnitude of this recent phenomenon. Although we do not have data specific to infected routers, Telnet login attempts can serve as a proxy statistic. While Telnet is not as widely used today as in the past, IoT devices still largely rely on it for its remote access capabilities. Telnet communication is unencrypted, making it easy for a malicious actor or a botnet to sniff user credentials. Botnets can thus use this open protocol to further spread by infecting more routers.

Trying to open Telnet sessions with other devices is not normal behavior for a router and is an earmark of an infection attempt. We can therefore use this metric as a close indicator of the “number of infected routers.” In Figure 2, which is based on Trend Micro’s telemetry from July 2019 to April 2020, the bars represent Telnet connection attempts, and the line represents the sources of those attempts, which we consider to be the number of infected devices. At the peak of the latter metric, nearly 16,000 devices were attempting to open Telnet sessions with other IoT devices in a single week. This could indicate that previous activity meant to grow a botnet’s size had been successful, allowing active botnets to have a larger number of devices under their control than previously possible.

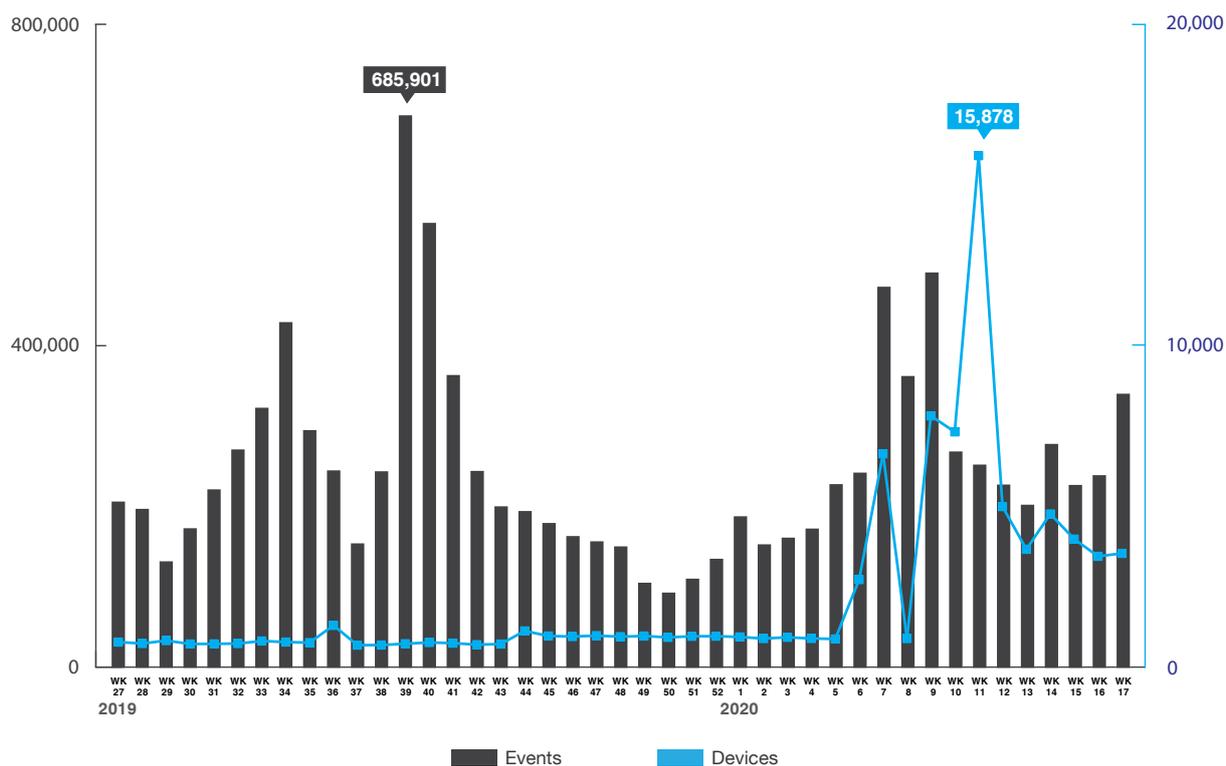


Figure 2. Telnet activity coming from IoT devices from July 2019 to April 2020 and the number of devices starting those suspicious connections

From the two data indicators, we see that IoT botnet activity is on the rise. Now we take a look at the most popular botnet malware families and analyze whether they have ways that they use in common to “clean up” an existing infection soon after they infect a router. As part of our ongoing IoT botnet research, we have observed that there are three main bot source codebases that are most often used by cybercriminal groups and script kiddies: Mirai, Kaiten, and Qbot. The codes for these three are all freely available, that is, any enterprising crook can easily download, modify, and recompile them to start infecting routers and create their own IoT botnet. As we discuss in the succeeding sections, these three form the basis of and are the main cyberweapons in the ongoing router turf war.

# Mirai: The Grandfather

Among the three, Mirai is the most common code we see — and with good reason. Mirai, a botnet malware family that came out in late 2016, changed the landscape of IoT threats. A computer science major from New Jersey created the malware, with some help from others, to see how DDoS attacks could be monetized.<sup>1,2,3</sup> This led to one of the most crippling DDoS attacks in recent history. The original Mirai botnet malware was responsible for the DDoS attack, on Sept. 20, 2016, that caused an outage of four days to the Krebs on Security website. Reaching 620 gigabits per second (Gbps), this attack was so damaging that the site’s content delivery network provider, Akamai, could not keep up with it and had to stop servicing the targeted website.<sup>4,5</sup>

Mirai was built with the purpose of being a DDoS tool for sale to aid in “DDoSing” gamers and to monetize their fights with one another.<sup>6</sup> The first attack, observed on Sept. 19, 2016, was on the French internet service provider (ISP) OVH, which, as it turned out, was hosting many online games (most notably Minecraft).<sup>7</sup> Shortly after this attack, the Mirai source code was posted online. The largest DDoS attack from Mirai came nearly a month after the initial attack, on Oct. 12, 2016, when the malware was used against Dyn, a Domain Name System (DNS) hosting provider. This attack took down many services that people around the globe use daily, including Netflix, Reddit, and Twitter.<sup>8</sup>

Once the author open-sourced the botnet code, the IoT malware landscape was forever changed. The ability to add new hard-coded credentials and other exploits to the codebase enabled novice attackers to make new Mirai variants that were more effective and aggressive. For many, the Mirai code in some ways became their “gateway drug” into the cybercriminal community.

Currently, Trend Micro tracks many variants of Mirai. Some of these came out shortly after the code was open-sourced, while others are more recent variants, including ones that surfaced in the last year. The main reason that there is a narrow range of IoT botnet malware families is because attackers tend to gravitate toward the handful of very effective existing frameworks, such as Mirai.

Given the huge variability among all the variants, it is difficult to generalize Mirai’s features. What we can be sure of is that some of these variants do have the capability to clean up previous infections in order to completely “own” an infected router. This is a feature that can be divisive for cybercriminals who develop and use the Mirai code.

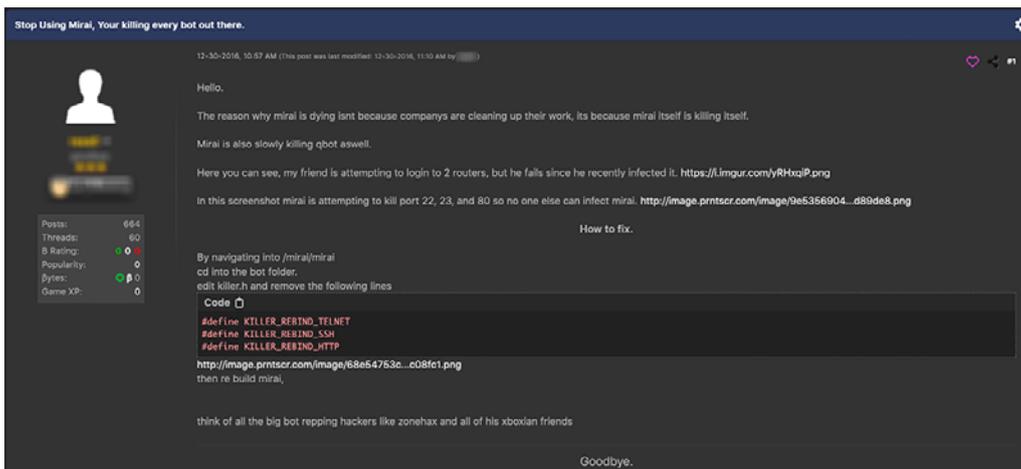


Figure 3. A cybercriminal forum post discussing the Mirai feature that shields an infected router's ports 22, 23, and 80 to effectively protect it from further infections

In fact, the original Mirai source code has the capability of killing other processes. The screenshot of the Mirai source code shown in Figure 4, for example, shows the default configuration for killing processes that match the string ".anime", tied to the Anime IoT malware.<sup>9</sup>

```
add_entry(TABLE_KILLER_SAFE, "\\x4A\x56\x56\x52\x51\x18\x0D\x0D\x5B\x4D\x57\x56\x57\x0C
add_entry(TABLE_KILLER_PROC, "\\x0D\x52\x50\x4D\x41\x0D\x22", 7);
add_entry(TABLE_KILLER_EXE, "\\x0D\x47\x5A\x47\x22", 5);
add_entry(TABLE_KILLER_DELETED, "\\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22", 11);
add_entry(TABLE_KILLER_FD, "\\x0D\x44\x46\x22", 4);
add entrv(TABLE_KILLER_ANIME. "\\x0C\x43\x4C\x4B\x4F\x47\x22". 7):
```

Figure 4. Mirai source code settings that kill the Anime malware

The piece of code that effectively kills matching processes is shown in Figure 5. In the code snippet, Mirai uses the `kill()` Linux system function to effectively send the `SIG_KILL (9)` signal to the desired processes.

```

187 // Resolve exe_path (/proc/$pid/exe) -> realpath
188 if ((rp_len = readlink(exe_path, realpath, sizeof (realpath) - 1)) != -1)
189 {
190     realpath[rp_len] = 0; // Nullterminate realpath, since readlink doesn't guarantee a null terminated string
191
192     table_unlock_val(TABLE_KILLER_ANIME);
193     // If path contains ".anime" kill.
194     if (util_stristr(realpath, rp_len - 1, table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
195     {
196         unlink(realpath);
197         kill(pid, 9);
198     }
199     table_lock_val(TABLE_KILLER_ANIME);
200

```

Figure 5. Part of the Mirai source code that ends the processes of competing malware

This feature in the most popular IoT botnet malware shows how Mirai is also being used as a weapon in the turf war among cybercriminals in order to displace other pieces of botnet malware from an infected router and thus collect as many bots as possible in a single botnet. This field is also highly configurable, so variants of Mirai can modify it to take out other variants, often belonging to rival cybercriminal groups.

# Kaiten: A Tsunami of Attacks

Kaiten is not quite well known to the public, but it is nonetheless a popular botnet malware family among cybercriminals and script kiddies alike. Kaiten, which has been open-source since 2001,<sup>10</sup> was one of the earliest IoT botnet malware families, with variants that remain popular today. Its communication with its command-and-control (C&C) servers is based on the popular IRC (Internet Relay Chat) protocol, allowing infected devices to receive commands from an IRC channel hard-coded within the Kaiten binaries. These can be compiled for a variety of hardware platforms, namely SH4, PowerPC, MIPSel, MIPS, and ARM.

```
addiu $v0, (aBigboatz - 0x410000) # "#BigBoatz"  
sw $v0, (chan - 0x450FA0)($v1)  
la $v1, key  
la $v0, unk_410000
```

Figure 6. An example of disassembly from Kaiten, where the IRC channel is “#BigBoatz”

Kaiten, also known as Tsunami, got its name from a trojan of the same name,<sup>11</sup> whose code the botnet malware seems to be based on. In fact, Kaiten shares the IRC and DDoS capabilities of the original Kaiten trojan, although the botnet malware uses the same infection script as a previous, less well-known piece of botnet malware called HeavyAidra.<sup>12</sup> This Python script has the capability of infecting devices by brute-forcing Telnet services. It also allows a malicious actor to, as indicated in Figure 8, choose the hardware architecture being targeted (lines 21 to 26) and set the download server (line 30).

```
136 passwords = [ #Some default SSH logins.  
137     "root:root", #This one is the least secure and ironically most effective.  
138     "root:toor",  
139     "admin:admin",  
140     "root:123qwe",  
141     "root:redtube",  
142     "root:admin",  
143     "root:1111",  
144     "test:test",  
145     "root:ferrari",  
146     "root:1q2w3e4r5t",  
147     "root:test",  
148     "root:1234",  
149     "root:1q2w3e",  
150     "root:qwerty"  
151 ]
```

Figure 7. A hard-coded password list in the Kaiten infection script

```

17 import threading, paramiko, random, socket, time, sys
18
19 paramiko.util.log_to_file("/dev/null") #Prevents paramiko error spam.
20
21 files = [ #Files in which we would like to execute upon the routers.
22     "kaiten-sh4",
23     "kaiten-powerpc",
24     "kaiten-mipsel",
25     "kaiten-mips",
26     "kaiten-armv5l"
27
28 ]
29
30 website = "123.123.123.123" #Public facing IP hosting the IRC bot binaries.

```

Figure 8. A Kaiten infection script snippet showing payloads for different hardware architectures

The original source code for Kaiten, as previously mentioned, has also been released in the wild, prompting cybercriminals to modify it and add new and improved functionality.<sup>13</sup> Kaiten variants include Amnesia (2017),<sup>14</sup> Muhstik (2018),<sup>15</sup> and the sophisticated Capsaicin (2017).<sup>16</sup>

Recent Kaiten variants have also implemented the “bot-killing” feature that effectively cleans any previous infection from a Kaiten-infected router. Some cybercriminals boast about this feature on underground forums, as shown in Figure 9.

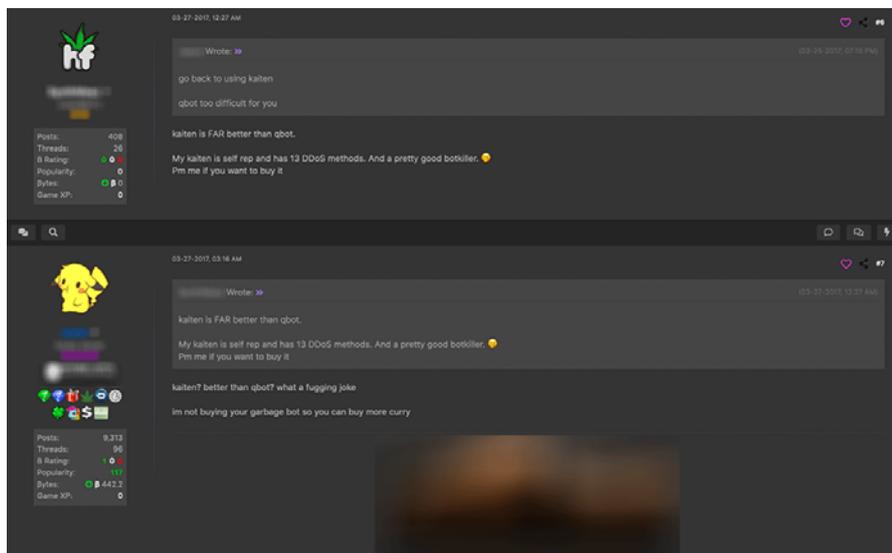


Figure 9. A cybercriminal underground forum post showing a seller boasting some of the features added to Kaiten, including a “pretty good botkiller”

Evidently, much like Mirai, Kaiten allows cybercriminals to grow their botnets and compete against others for control over devices.

# Qbot: The Third Brother

Despite being older than Mirai, Qbot is still commonly used by cybercriminals; it has been active since 2008.<sup>17</sup> Also known as Bashlite, Gafgyt, Lizkebab, or Torlus,<sup>18</sup> this botnet malware has been around for a while,<sup>19</sup> but more so than with the other two, time has not affected its popularity.

Qbot's main feature is that its source code is made up of only a few files. Since the main configuration needs to be done directly from the source code, using Qbot might be difficult to the uninitiated. Its difficulty has resulted in many threads on cybercriminal forums that teach newbies how to configure this botnet malware. Plenty of cybercriminals are also peddling their "help" in correctly setting up Qbot botnets.

Qbot also supports a number of hardware architectures, as shown in Figure 10. However, unlike Kaiten, Qbot uses C&C servers based on TCP (Transmission Control Protocol) and does not rely on high-layer protocols such as IRC.

```
20  compileas = ["ntpd", #mips
21              "sshd", #mipsel
22              "openssh", #sh4
23              "bash", #x86
24              "tftp", #Armv6l
25              "wget", #i686
26              "cron", #ppc
27              "ftp", #i586
28              "pftp", #m68k
29              "sh",
30              "' '",
31              "apache2",
32              "telnetd"]
~~
```

Figure 10. A Qbot installation script snippet showing supported architectures

After infecting a device, Qbot tries to contact each of its hard-coded C&C servers until one of them replies. It then waits for commands before starting different types of common DDoS attacks, such as HTTP and UDP (User Datagram Protocol) floods.

More recent Qbot variants have added the ability to uninstall other pieces of botnet malware. As a result, should a Qbot variant successfully attack an already infected device, it would be able to kill its competitors. Figure 11 shows a code snippet that points to this feature.

```

64 const char *knownBots[] = {
65 "mips", "mipsel", "sh4", "x86", "i686", "ppc", "i586", "i586",
66 "jackmy*", "hackmy*", "arm*", "b1", "b2", "b3", "b4", "b5", "b6", "b7", "b8", "b9",
67 "busyboxterrorist", "DFhxdhdf", "dvrHelper", "FDFDHF", "FEUB", "FTUdfu1", "GHfjgvj",
68 "jhu0H", "JIPJIPJj", "JIPJuijph", "kmyx86_64", "lolmipsel", "mips", "mipsel", "RYrydry",
69 "tel*", "TwoFace*", "UYyuyioy", "wget", "x86_64", "XDzdfxzf", "xxb*", "sh",
70 "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15", "16",
71 "17", "18", "19", "20", "hackz", "bin*", "gtop", "ftp*", "tftp*", "botnet", "swatnet",
72 "ballpit", "fucknet", "cracknet", "weednet", "gaynet", "queernet", "ballnet", "unet",
73 "youngay", "sttftp", "sstftp", "sbtftp", "btftp", "y0u1sg3y", "bruv*", "ToT*",
74 };

```

Figure 11. A Qbot code snippet showing identifying strings for rival botnet malware

This process-killing feature in Qbot also signifies that a war is being carried out among IoT botnet authors as they all compete for control of valuable devices. A recent example of this war is the appearance of the powerful Momentum IoT botnet malware, which we described in an article posted in December 2019.<sup>20</sup> As shown in Figure 12, Momentum samples have a long list of process names related to other pieces of malware. These are the competing pieces of botnet malware that they are trying to get rid of. The complete list contains a staggering 438 process names, including ones that represent well-known botnet malware families such as Mirai.

```

.data:1006B5BC .globl knownBots
.data:1006B5BC knownBots: .long aLoligang # DATA XREF: botkill+3Cfo
.data:1006B5BC # botkill+54fo ...
.data:1006B5BC # "loligang*"
.data:1006B5C0 .long aFrostydvrhelpe # "frosty*dvrHelper"
.data:1006B5C4 .long a902i13 # "902i13"
.data:1006B5C8 .long aBzSxLxBxeY # "BzSxLxBxeY"
.data:1006B5CC .long aHohoLugo7 # "HOHO-LUGO7"
.data:1006B5D0 .long aHohoU79o1 # "HOHO-U79OL"
.data:1006B5D4 .long aJuyfouyf87 # "JuYfouyf87"
.data:1006B5D8 .long aNigger69xd # "NiGGeR69xd"
.data:1006B5DC .long aSo190Ij1x # "So190Ij1x"
.data:1006B5E0 .long aDvrhelper # "dvrhelper"
.data:1006B5E4 .long aDvrsupport # "dvrsupport"
.data:1006B5E8 .long aMirai # "mirai"
.data:1006B5EC .long aBlade # "blade"
.data:1006B5F0 .long aDemon # "demon"
.data:1006B5F4 .long aDemon_0 # "Demon"
.data:1006B5F8 .long aSmd # "smd"
.data:1006B5FC .long aSmd_0 # "smd*"
.data:1006B600 .long aFuck # "fuck"
.data:1006B604 .long aUn5 # "un5"
.data:1006B608 .long aKowai # "kowai"
.data:1006B60C .long aHoho # "hoho"
.data:1006B610 .long aHakai # "hakai"
.data:1006B614 .long aArmv41 # "armv41"
.data:1006B618 .long aCron # "cron"
.data:1006B61C .long aSshd # "sshd"
.data:1006B620 .long aNtpd # "ntpd"
.data:1006B624 .long aHoho_0 # "hoho*"
.data:1006B628 .long aPs23e # "ps23e"
.data:1006B62C .long aTron # "tron"
.data:1006B630 .long aNut # "nut"
.data:1006B634 .long aSbot # "sbot*"
.data:1006B638 .long aSbot_0 # "sbot"
.data:1006B63C .long aSora # "sora"
.data:1006B640 .long aSora_0 # "sora*"

```

Figure 12. A Momentum botnet malware code snippet with a list of process names to kill

```

lis      r9, knownBots@ha
addi    r9, r9, knownBots@1
slwi    r0, r0, 2
add     r9, r0, r9
lwz     r11, 0(r9)
addi    r0, r31, 0xC
mr      r3, r0
lis     r9, aPkill1958busybox@ha
addi    r4, r9, aPkill1958busybox@1 # "pkill -9 %s || busybox pkill -9 %s || /"...
mr      r5, r10
mr      r6, r8
mr      r8, r29
mr      r9, r11

```

Figure 13. A kill routine from Momentum samples compiled to PowerPC

In Qbot, we again see the same strategy we have observed in its two prominent competitors, Mirai and Kaiten: trying to “own” an infected device and taking it from its previous “owner.” These three botnet malware families are part of a competition to infect the most routers, where sharing a device is not an option. Figure 14 summarizes the characteristics of the three botnet malware families under discussion.

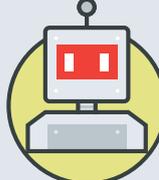
|  |   |   |
|--|---|---|
|  <p><b>Mirai</b></p> <ul style="list-style-type: none"> <li>Built with the purpose of being a DDoS tool for sale</li> <li>Open-source code enables novice attackers to make new, more aggressive variants</li> <li>Original source code contains the capability to kill competing processes</li> </ul> |  <p><b>Kaiten</b></p> <ul style="list-style-type: none"> <li>Also known as Tsunami</li> <li>C&amp;C servers are based on the popular IRC protocol</li> <li>Supports multiple hardware architectures</li> <li>Recent variants implement a bot-killing feature</li> </ul> |  <p><b>Qbot</b></p> <ul style="list-style-type: none"> <li>Also known as Bashlite, Gafgyt, Lizkebab, or Torlus</li> <li>Supports multiple hardware architectures</li> <li>Uses TCP-based C&amp;C servers and does not rely on high-layer protocols such as IRC</li> <li>Recent variants can uninstall other pieces of botnet malware</li> </ul> |
|--|---|---|

Figure 14. A summary of the three main IoT bot source codebases

In the next section, we discuss the availability of these botnet malware families in the cybercriminal underground by looking at the different forums or markets for them.

# IoT Botnet Malware in the Cybercriminal Underground

Cybercriminals are selling Qbot and a number of Mirai variants on underground forums, online stores, and even social media sites, including Twitter and Instagram. In general, IoT botnet malware rentals are very affordable and allows inexperienced low-level criminals to enter the field. Qbot rentals, for example, start at a mere US\$5. The original source codes for Qbot and Mirai are free, but the price for modifications and new variants starts at US\$30. This price varies depending on the presence or the absence of antimalware detection capabilities.

We have also observed several advertisements for guides on “how to make money off botnets” and the more basic “how to set up botnets.” The price range for these guides varies widely, with some offered for free and others sold at high rates.

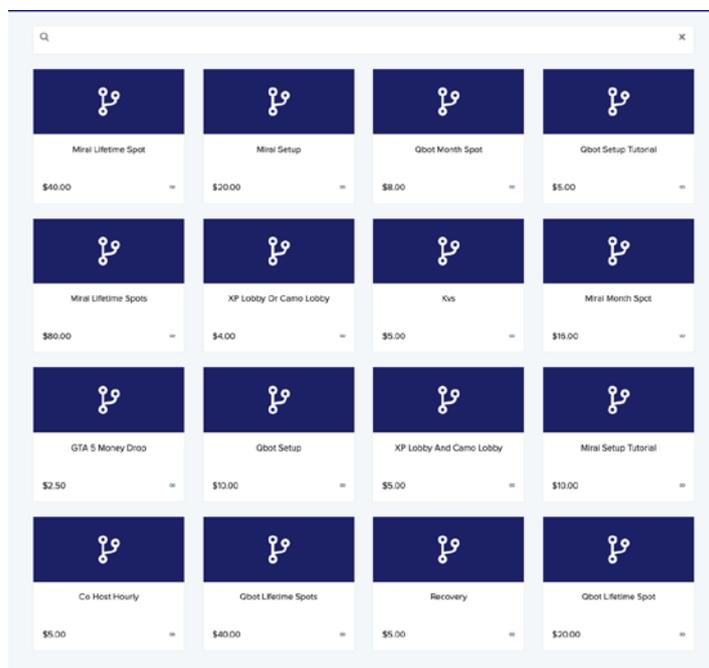


Figure 15. A store offering Qbot and Mirai rentals, including setup services

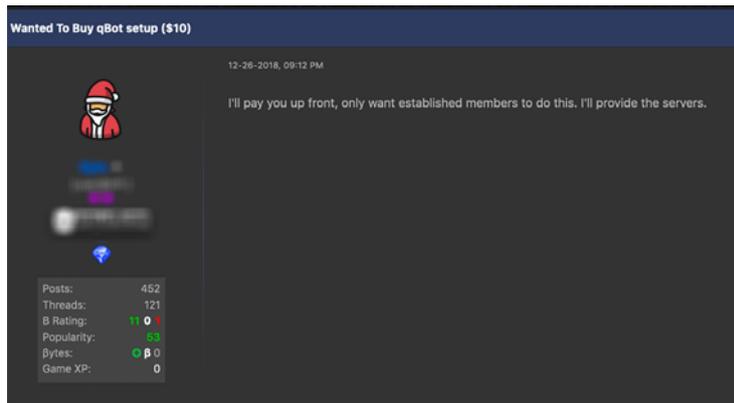


Figure 16. A forum user looking to purchase Qbot setup services

Some underground advertisements offer a one-stop shop, with a private botnet variant, infrastructure setup, a bot killer, and a Telnet “brute-forcer,” all in one package. These services are more expensive and can reach over US\$150.

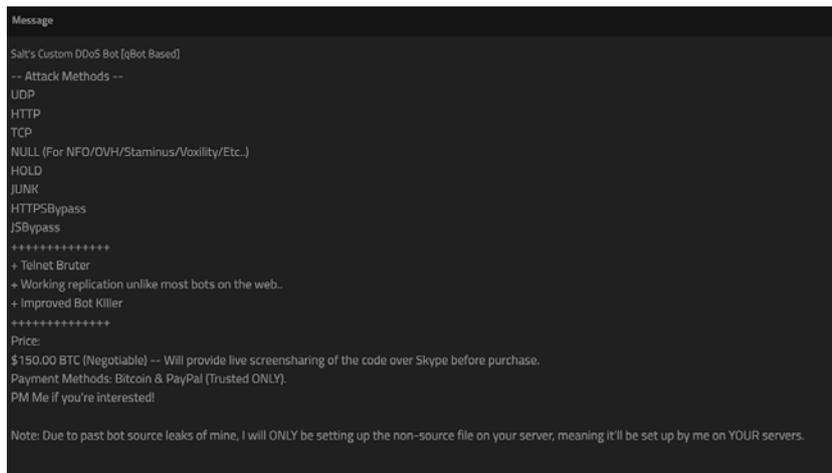


Figure 17. A Qbot-based DDoS service package

The screenshot from Twitter in Figure 18 shows that underground forums are not the only ways for cybercriminals to advertise their wares. Mainstream social networks are also used in much the same way. It is worth noting that cybercriminals are also offering a “mini DDoS attack,” which is capable of creating a delay of 5,500 seconds, a duration of about an hour and a half. This might not be enough to bring a website down, but in the gaming world this is more than enough to win a game or make a server unavailable for a rival clan.



Figure 18. A Twitter post advertising Mirai and Qbot rentals starting at US\$15 a month

The cybercriminal behind the advertisement on Instagram shown in Figure 19 is selling both denial-of-service (DoS) and virtual private network (VPN) services. This cybercriminal might be monetizing infected routers both ways. Not only is the victim's router being used to extort other internet users via DDoS, but their IP address is also being used and shown as logged evidence in other hacking attacks.



Figure 19. An Instagram post advertising Mirai and Qbot rentals

On Instagram, we found multiple advertisements for botnet reseller services. Ads often contain photos or videos showing off how much money one could make from the advertisers' botnets.



Figure 20. An IoT botnet seller showing off their success on Instagram

We summarize the range of prices for Mirai-, Kaiten-, and Qbot-related services we have seen available online in Table 1.

| Service                   | Price   |
|---------------------------|---|
| <b>Mirai</b>              |   |
| Rentals                   | From US\$5 to US\$15 a month<br>US\$35 and up for lifetime rentals        |
| Variants' source codes    | US\$30 and up   |
| Source code               | Free  |
| <b>Kaiten</b>             |   |
| Rentals                   | US\$15 a month  |
| Source code               | US\$300 with setup in 2016<br>US\$5 without setup in 2018<br>Free in 2020 |
| <b>Qbot</b>               |   |
| Rentals                   | From US\$5 to US\$15 a month<br>US\$35 and up for lifetime rentals        |
| Variants' source codes    | US\$30 and up   |
| Source code               | Free  |
| Setup                     | US\$5   |
| Botnet service with crypt | US\$25  |

Table 1. Prices for IoT botnet malware-related services as of March 31, 2020

As this section shows, IoT botnet malware-related services are not difficult to purchase and are available at affordable starting prices. Going beyond underground forums, some sellers have also boldly advertised their “products” on social media platforms. This could be reflective of how popular and accessible IoT botnets are in the cybercriminal world.

# Case Study: JenX

In this section, we present an example of how attackers used a piece of IoT botnet malware called JenX to infect routers for their own benefit. We found it remarkable that the attackers did not appear to have high technical knowledge in conducting their campaign, based on their use of ready-made tools and on forums discussing the group. This case helps illustrate the kind of people who are in this competition to infect routers. The attackers in this case study can be considered “soldiers” in this turf war.

JenX was used against the Spanish gaming community of the popular action-adventure video game series Grand Theft Auto (GTA). It is based on both the Masuta and Brickerbot codes.<sup>21</sup> That JenX and Masuta, which is believed to be a modification of Mirai,<sup>22</sup> are linked is suggested by the appearance of the rather objectionable string “gosh that chinese family at the other table sure ate alot,” as shown in Figure 21, in both their binaries.

```
In [3]: cspbertat = "\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x00"
In [4]: cleartat = "gosh that chinese family at the other table sure ate alot"
In [11]: for i in range(0, len(cspbertat)-1):
    print("%x" % cspbertat[i], cleartat[i], "--", ord(cspbertat[i]), ord(cleartat[i]), "diff=", ord(cspbertat[i]) - ord(cleartat[i]), "
    hex=", ord(cspbertat[i]) ^ ord(cleartat[i]))
0 : " g -- 34 100 diff= -66 hex= 69
1 : " 0 -- 42 111 diff= -69 hex= 69
2 : " 0 -- 56 115 diff= -61 hex= 69
3 : " h -- 45 104 diff= -59 hex= 69
4 : " - -- 101 97 diff= 40 hex= 60
```

Figure 21. JenX’s source code showing the same single string found in Masuta’s

The C&C server for JenX was hosted on the main website of a group called San Calvicie, located at sancalvicie[.]com. The website also provided GTA multiplayer mod servers and DDoS services with a guaranteed bandwidth of 290 to 300 Gbps at a minimum rate of US\$20.<sup>23</sup>

| SAMP                             | CORRIENTE DIVINA  | TEAMSPEAK 3                             |
|----------------------------------|---|---|
| \$16                             | \$20  | \$9                                     |
| Denon para su nuevo host de SAMP | La ip de disco será empleada en contra de la IP que nos proporcione | Denon para su nuevo host de TEAMSPEAK 3 |
| HOSTING                          | NULL IP   | HOSTING                                 |
| MAIL - MTA - PCU                 | DDOS/DOH  | USADOS 400 SLITS                        |
| 400 SLITS                        | 700 SCRIPTS   | 400000 SCRIPTS                          |
| 400000 FLOOD                     | QUEEN FLOOD   | 4000000 SCRIPTS                         |
| 4000000 FLOOD                    | 100   | 4000000000                              |
| 4000000000                       | \$99.990 Gbps de ancho garantizado                                  | 40000000000                             |
| PAGAR                            | PAGAR   | PAGAR                                   |

Figure 22. A pricing matrix including the price for a DDoS service called Corriente Divina (“Divine Current” in Spanish)

JenX exploits two known vulnerabilities: Realtek software development kit (SDK) Miniigd UPnP (Universal Plug and Play) SOAP (Simple Object Access Protocol) command execution (CVE-2014-8361)<sup>24</sup> and Huawei Router HG532 arbitrary command execution (CVE-2017-17215).<sup>25</sup> While these are old vulnerabilities, the unpatched nature of many routers means they could still be exploited successfully.

Posts on gaming forums have repeatedly pointed fingers at San Calvicie as the group responsible for DDoS attacks on other gaming communities. On one of these posts, a user has gone as far as establishing the nationality and other personal details of the group's leader, as shown in Figure 23.

Since 2016, the Spanish GTA gaming community has been dealing with San Calvicie's harassment of players, in addition to its own competitors in the DDoS gaming business, such as Fenixzone. Its other targets include Grand Theft Multiplayer (GTMP) servers and the aforementioned French ISP OVH.

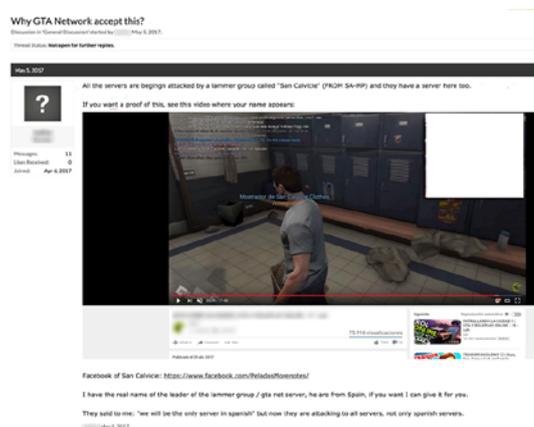


Figure 23. A 2017 complaint about San Calvicie's attack on GTA servers<sup>26</sup>

According to gaming forum posts, San Calvicie's leader has also attacked competitors in the DDoS business in order to coerce them into selling their servers to San Calvicie. In some instances, San Calvicie's leader shuts down the servers after purchasing them. Apparently, the worm war is not restricted only to taking control of victims' routers; it extends to taking advantage of armies of infected machines against the competition.

In 2018, GTMP switched owners when "DurdyFree," its original owner, decided to sell it as they could no longer maintain it. A user going by the name of "Julice," whom some have identified as San Calvicie's leader, outbid the then-best offer of €8,000 (around US\$9,000), which had been made by one of the coders of GTMP, who was looking to support the community. DurdyFree eventually sold GTMP and its source code to Julice for €30,000 (around US\$34,000). Gaming forum members voiced their concerns about having Julice as the new owner of GTMP seeing as San Calvicie had developed a reputation for harassing other players. Some believed Julice would use the GTMP client to expand their 25,000-member botnet.

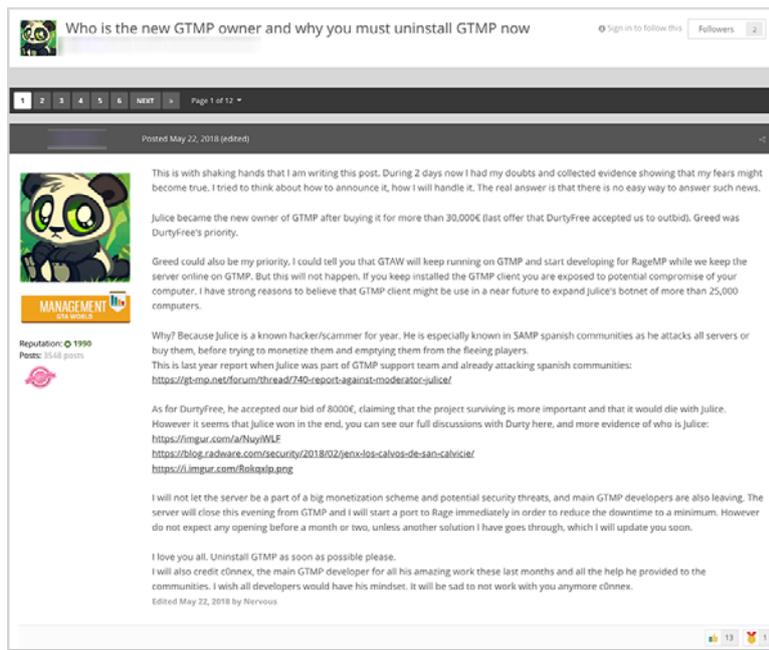


Figure 24. A forum post discussing Julice and their purchase of GTMP after outbidding one of its coders

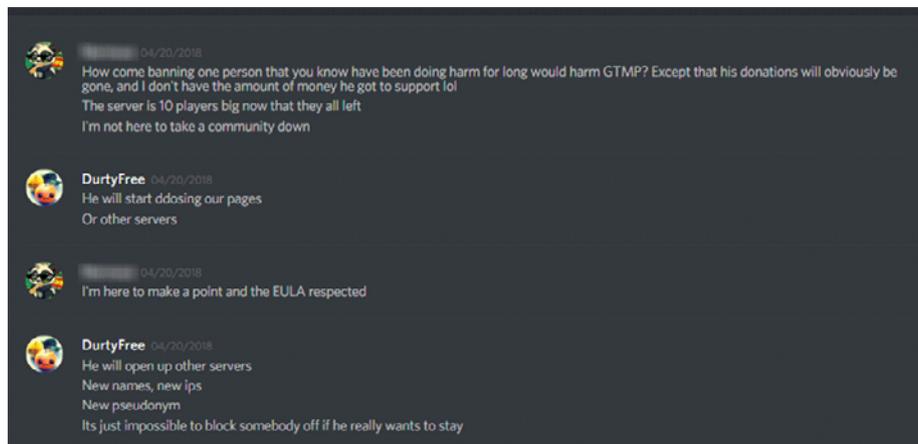


Figure 25. Chat messages from the owner of GTMP on how difficult it was to ban someone as its servers would undergo DDoS in retaliation

Several gaming channels on YouTube that occasionally include interviews with members of San Calvicio discuss the threat that the group presents to other gaming servers.<sup>27</sup> There is even a Change.org petition about this issue with more than 1,000 signatures calling for the banishment of Julice, who is also known as “Sergioo,” from the gaming community.<sup>28</sup>



Figure 26. A YouTube video discussing the ongoing DDoS war between San Calvicie and the Spanish GTA gaming community

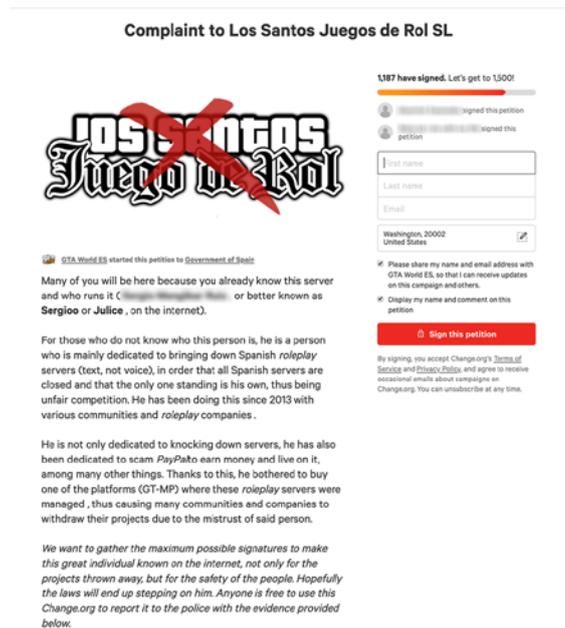


Figure 27. A Change.org petition to ban Julice aka Sergioo from the gaming community

Some forum posts have also accused the suspected San Calvicie leader of hacking Paypal accounts.<sup>29</sup> A GTA server that has been connected to San Calvicie, LS-RP, has also been involved in DDoS activity as recently as June 9, 2020, according to AbuseIPDB.<sup>30</sup>

San Calvicie and its followers participate on a Facebook page called “Calvos for Locos” (*calvos* meaning “bald” and *locos* meaning “crazy” in Spanish). Posts include conversations about DDoS activity against other gaming servers, gaming updates, and complaints about gaming members.

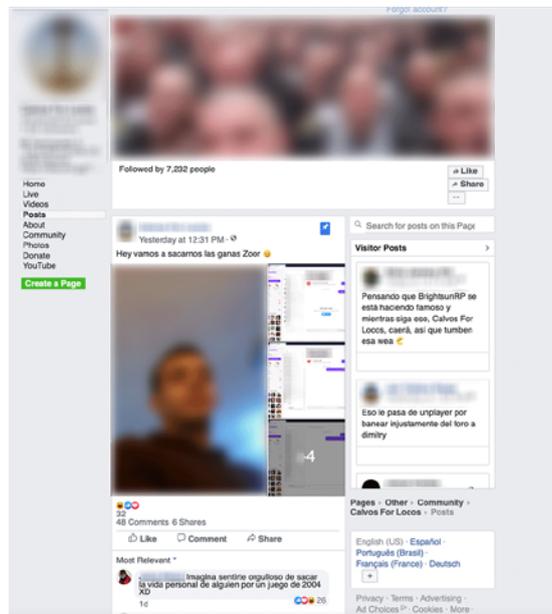


Figure 28. A San Calvicie fan page on Facebook

San Calvicie is a stereotypical attacker in this turf war, that is, the group has an objective. In the group’s case, it is to further the members’ own gaming community by destroying their adversaries. They use IoT botnets in order to reach their objective. This entails taking over as many routers as possible and using their bandwidth to perform DDoS on other gaming communities or selling their bandwidth for someone else to hire their power. These DDoS capability could end up being used by other gamers, extortionists, and other people for whatever purpose.

This is not an isolated incident. The price of these weapons is so ridiculously low — often they are simply free of charge — that virtually anybody can join this war.

## Conclusion

We have shown how malicious actors could use various tools to compromise as many online routers as possible, including those already in their rivals' hands. In this competition, the biggest botnet has the most power, and each group actively seeks to wrest control of resources from its competitors. Cybercriminals use infected routers for different purposes, from selling services based on infected routers to attacking their own enemies, normally other communities or servers. But one thing is very clear: In this worm war, it is not enough for attackers to know how to monetize infected routers, nor is it enough for them to just know who their rivals are, but they also have to know their rivals' weaknesses to be able to outplay the competition.

Ordinary internet users have no idea that this war is happening inside their own homes and how it is affecting them — which makes this issue all the more concerning. The bottom line is that responsible router owners in whatever setting should take proper care of their internet connections and devices. Otherwise, they run the risk of being victimized by cybercriminals, who could then use their devices to perform further attacks on others.

This issue cannot be more important in this time, when many people are staying at and working from home. Looking after the security of routers might mean the difference between being productive at home or not. Routers in a botnet expend resources attacking other people or letting cybercriminals go online, generally maximizing bandwidth meant for making work from home possible and convenient.

Taking charge of the security of routers and other IoT devices can save them from the interest of groups looking to expand their botnets. Users can narrow the battlefield and weaken the arsenal of these warring groups by reexamining the security measures for and the settings of their connected devices.

We recommend IT-savvy users to check the health of their routers at least once per quarter by following these steps:

- Check the logs for unusual behavior, strange accounts, and other anomalies.
- Make sure the router is running the latest firmware.
- Use a strong, hard-to-guess password and change the password from time to time.
- Disable remote login to allow only logins from the local network.

In this time of remote working, we also encourage IT staff to help other employees in securing their home routers. Each country usually has a limited number of router models issued by different ISPs. Creating a help guide for each of those is not only possible, but it will also help their supported users to stay secure while working from home.

Connected devices can also be protected by security software such as the Trend Micro™ Home Network Security<sup>31</sup> and Trend Micro™ Home Network Security SDK<sup>32</sup> solutions, which can check internet traffic between a router and all connected devices. These solutions, which also help users have better visibility over their devices and provide vulnerability assessment, can be essential tools for preventing botnet malware from taking over devices in a war where routers are the battlefield as well as the prize to be won.

# Appendix

Indicators of compromise for JenX and Momentum are shown in Table 2, including related file names, IP addresses, domains, and hashes derived from SHA-256 and Telfhash (Trend Micro ELF Hash), a new clustering algorithm we have developed to help group Linux IoT malware.<sup>33</sup>

| Malware  | File name, IP address, or domain | SHA-256  | Telfhash   |
|----------|----------------------------------|--|--|
| JenX     | jennifer.arm                     | a51c4e7bd27348bc24b694538e<br>ee9b19e60727c49b362fe4cbac<br>911caa015e21 | a621e248a7001fec2ff0894e83<br>5ae237b4663890aa172855c75f<br>9d5e4362fb77561833 |
|          | jennifer.mips                    | 04463cd1a961f7cd1b77fe6c9e<br>9f5e18b34633f303949a0bb072<br>82dedcd8e9dc | 24f03a5811381bf493818dddb<br>ddff38a4a184df99692f378d00<br>d9d9a721a829c01c3c  |
|          | jennifer.x86                     | 01ca8fe678b8375b60ba9571a4<br>790448bade3b30b5d29665565f<br>cbb1ab5f6ae  | 8a1128e4be7294f9f2e4ac4d8b<br>2e6726833606600f3364b944f2<br>6dc136f1193a8f5c48 |
|          | 50.63.202.73                     | x  | x  |
|          | 184.168.221.51                   | x  | x  |
|          | sancalvicie.com                  | x  | x  |
|          | skids.sancalvicie.com            | x  | x  |
| Momentum | x                                | 0c95e0a62a035c86ef534e3124<br>2ebf52ce1dfb3b420ca8bf8c7d<br>7d0e94030581 | 6ec1d8889c3b1dad5f131c0ca4<br>1e6e52095bb6abb484bf95ff35<br>ccc905a9029f868d0f |

Table 2. Indicators of compromise for JenX and Momentum

# References

1. Brian Krebs. (Oct. 26, 2018). *Krebs on Security*. "Mirai Co-Author Gets 6 Months Confinement, \$8.6M in Fines for Rutgers Attacks." Accessed on June 30, 2020, at <https://krebsonsecurity.com/2018/10/mirai-co-author-gets-6-months-confinement-8-6m-in-fines-for-rutgers-attacks/>.
2. Josh Fruhlinger. (March 9, 2018). *CSO Online*. "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet." Accessed on June 9, 2020, at <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>.
3. Ted Sherman. (Dec. 17, 2017). *NJ.com*. "How a Rutgers student went from Minecraft to internet warfare." Accessed on July 6, 2020, at [https://www.nj.com/news/2017/12/inside\\_the\\_massive\\_cyber\\_scam\\_launched\\_by\\_a\\_kid\\_fr.html](https://www.nj.com/news/2017/12/inside_the_massive_cyber_scam_launched_by_a_kid_fr.html).
4. Charlie Osborne. (May 9, 2018). *ZDNet*. "Mirai DDoS attack against KrebsOnSecurity cost device owners \$300,000." Accessed on June 9, 2020, at <https://www.zdnet.com/article/mirai-botnet-attack-against-krebsonsecurity-cost-device-owners-300000/>.
5. Charlie Osborne. (Sep. 23, 2016). *ZDNet*. "Krebs on Security booted off Akamai network after DDoS attack proves pricey." Accessed on July 1, 2020, at <https://www.zdnet.com/article/krebs-on-security-booted-off-akamai-network-after-ddos-attack-proves-pricey/>.
6. Garrett Graff. (Dec. 13, 2017). *Wired*. "How a Dorm Room Minecraft Scam Brought Down the Internet." Accessed on June 30, 2020, at <https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/>.
7. Josh Fruhlinger. (March 9, 2018). *CSO Online*. "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet." Accessed on June 30, 2020, at <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>.
8. Nicky Woolf. (Oct. 26, 2016). *The Guardian*. "DDoS attack that disrupted internet was largest of its kind in history, experts say." Accessed on June 9, 2020, at <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.
9. Evosec. (Sept. 5, 2016). *Evosec*. "New IoT Malware? Anime/Kami." Accessed on June 9, 2020, at <https://evosec.eu/new-iot-malware/>.
10. Steve Ragan. (Feb. 22, 2018). *CSO Online*. "Linux Mint hacked: Compromised data up for sale, ISO downloads backdoored." Accessed on July 6, 2020, at <https://www.csoonline.com/article/3035743/linux-mint-hacked-compromised-data-up-for-sale-iso-downloads-backdoored.html>.
11. McAfee. (Oct. 1, 2002). *McAfee*. "Linux/DDoS-Kaiten." Accessed on June 9, 2020, at <https://www.mcafee.com/enterprise/en-us/threat-intelligence.malwaretc.html?vid=99733>.
12. Georgios Kambourakis et al. (2019). *Google Books*. "Botnets: Architectures, Countermeasures, and Challenges." Accessed on June 30, 2020, at [https://books.google.com/books?id=rcO2DwAAQBAJ&dq=Botnets:+Architectures,+Countermeasures,+and+Challenges&source=gbs\\_navlinks\\_s](https://books.google.com/books?id=rcO2DwAAQBAJ&dq=Botnets:+Architectures,+Countermeasures,+and+Challenges&source=gbs_navlinks_s).
13. Charlie Osborne. (Nov. 1, 2016). *ZDNet*. "Hackers release new malware into the wild for Mirai botnet successor." Accessed on June 29, 2020, at <https://www.zdnet.com/article/hackers-release-new-malware-into-the-wild-for-mirai-botnet-successor/>.
14. Catalin Cimpanu. (April 8, 2017). *Bleeping Computer*. "Irresponsible Chinese DVR Vendor Still the Target of IoT Botnets One Year Later." Accessed on June 29, 2020, at <https://www.bleepingcomputer.com/news/security/irresponsible-chinese-dvr-vendor-still-the-target-of-iot-botnets-one-year-later/>.
15. Lindsey O'Donnell. (April 23, 2018). *Threatpost*. "Muhstik Botnet Exploits Highly Critical Drupal Bug." Accessed on June 29, 2020, at <https://threatpost.com/muhstik-botnet-exploits-highly-critical-drupal-bug/131360/>.

16. Georgios Kambourakis et al. (2019). *Google Books*. "Botnets: Architectures, Countermeasures, and Challenges." Accessed on June 30, 2020, at [https://books.google.com/books?id=rcO2DwAAQBAJ&dq=Botnets:+Architectures,+Countermeasures,+and+Challenges&source=gbs\\_navlinks\\_s](https://books.google.com/books?id=rcO2DwAAQBAJ&dq=Botnets:+Architectures,+Countermeasures,+and+Challenges&source=gbs_navlinks_s).
17. Doron Voolf. (June 11, 2020). *F5 Labs*. "Qbot Banking Trojan Still Up to Its Old Tricks." Accessed on July 6, 2020, at <https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks>.
18. New Jersey Cybersecurity and Communications Integration Cell. (Nov. 3, 2011). *NJCCIC*. "Bashlite NJCCIC Threat Profile." Accessed on June 30, 2020, at <https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/bashlite>.
19. Doron Voolf. (June 11, 2020). *F5 Labs*. "Qbot Banking Trojan Still Up to Its Old Tricks." Accessed on July 1, 2020, at <https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks>.
20. Aliakbar Zahravi. (Dec. 16, 2019). *Trend Micro Security Intelligence Blog*. "DDoS Attacks and IoT Exploits: New Activity from Momentum Botnet." Accessed on June 10, 2020, at <https://blog.trendmicro.com/trendlabs-security-intelligence/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet/>.
21. Radware. (Jan. 2, 2018). *Radware*. "JenX Botnet: A New IoT Botnet Threatening All." Accessed on June 11, 2020, at <https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx/>.
22. Ya Liu and Hui Wang. (2018). *Virus Bulletin*. "VB2018 paper: Tracking Mirai variants." Accessed on June 11, 2020, at <https://www.virusbulletin.com/virusbulletin/2018/12/vb2018-paper-tracking-mirai-variants/>.
23. Pascal Geenens. (Feb. 1, 2018). *Radware Blog*. "JenX – Los Calvos de San Calvicie." Accessed on June 11, 2020, at <https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/>.
24. National Vulnerability Database. (May 1, 2015). *National Vulnerability Database*. "CVE-2014-8361 Detail." Accessed on June 11, 2020, at <https://nvd.nist.gov/vuln/detail/CVE-2014-8361>.
25. National Vulnerability Database. (March 20, 2018). *National Vulnerability Database*. "CVE-2017-17215 Detail." Accessed on June 11, 2020, at <https://nvd.nist.gov/vuln/detail/CVE-2017-17215>.
26. GTA Network. (April 6, 2017). *GTA Network*. "Why GTA Network accept this?" Accessed on June 11, 2020, at <https://forum.gtanet.work/index.php?threads/why-gta-network-accept-this.4092/>
27. YouTube. (Feb. 6, 2017). *YouTube*. ""HACKERS" SAN CALVICIE AMENAZA A FENIXZONE." Accessed on July 15, 2020, at [https://www.youtube.com/watch?v=DH8\\_Pm-5fQY](https://www.youtube.com/watch?v=DH8_Pm-5fQY).
28. GTA World ES. (n.d.). *Change.org*. "Denuncia a Los Santos Juegos de Rol S.L.." Accessed on July 15, 2020, at <https://www.change.org/p/denuncia-a-los-santos-juegos-de-rol-s-l>.
29. Puto Informático. (May 10, 2011). *Puto Informático*. "Crackeo Play Station Network." Accessed on June 15, 2020, at <https://www.putoinformatico.net/crackeo-play-station-network/>.
30. AbuseIPDB. (n.d.). *AbuseIPDB*. "AbuseIPDB : 158[.]69[.]162[.]173." Accessed on June 30, 2020, at <https://www.abuseipdb.com/check/158.69.162.173>.
31. Trend Micro. (n.d.). *Trend Micro*. "Home Network Security." Accessed on July 6, 2020, at [https://www.trendmicro.com/en\\_us/forHome/products/homenetworksecurity.html](https://www.trendmicro.com/en_us/forHome/products/homenetworksecurity.html).
32. Trend Micro. (n.d.). *IoT Security*. "Trend Micro™ Home Network Security SDK." Accessed on July 6, 2020, at <https://www.trendmicro.com/us/iot-security/product/home-network-security-sdk?solutions=connected-consumer>.
33. Fernando Mercês. (April 20, 2020). *Trend Micro Security Intelligence Blog*. "Grouping Linux IoT Malware Samples With Trend Micro ELF Hash." Accessed on June 15, 2020, at <https://blog.trendmicro.com/trendlabs-security-intelligence/grouping-linux-ot-malware-samples-with-trend-micro-elf-hash/>.



## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)

