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)
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.
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..
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
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
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
Bandwidth Sharing Companies
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
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
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
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
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
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

```bash
d(){
cd /dev/shm && cp /bin/ls . && ./ls &>/dev/null && rm -f ls && return
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 axjfl [...] | grep [...] "$PACCT"; then
    echo "already running"
    exit
fi

if docker ps [...] | grep [...] peer2profit [...] p2pclient; then
    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.

<table>
<thead>
<tr>
<th>Traffic rate</th>
<th>for referrals networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>business: 0.35 GB</td>
<td>business: 0.15 GB</td>
</tr>
<tr>
<td>cellular: 1 GB</td>
<td>cellular: 0.55 GB</td>
</tr>
<tr>
<td>hosting: 0.35 GB</td>
<td>hosting: 0.15 GB</td>
</tr>
<tr>
<td>residential: 0.85 GB</td>
<td>residential: 0.45 GB</td>
</tr>
<tr>
<td>other networks: 0.35 GB</td>
<td>other networks: 0.15 GB</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>App Name &amp; Link</th>
<th>Residential/Home/Mobile IP or equivalent Proxy's IP</th>
<th>VPS/Datacenter/Hosting/Cloud IP or equivalent Proxy's IP</th>
<th>Max Devices per Account</th>
<th>Max Devices per IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Earnapp</td>
<td>✔</td>
<td>✗</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Go to HoneyGain</td>
<td>✔</td>
<td>✗</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Go to PROYAL</td>
<td>✔</td>
<td>✗</td>
<td>Unlimited</td>
<td>1</td>
</tr>
<tr>
<td>Go to PEER2PROFIT</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Go to PACKETSTREAM</td>
<td>✔</td>
<td>✗</td>
<td>Unlimited</td>
<td>1</td>
</tr>
<tr>
<td>Go to TRAFFMONETIZER</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Go to REPOCKET</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>2</td>
</tr>
<tr>
<td>Go to EARNFM</td>
<td>✔</td>
<td>✗</td>
<td>Unlimited</td>
<td>1</td>
</tr>
<tr>
<td>Go to PROXYRACK</td>
<td>✔</td>
<td>✔</td>
<td>500</td>
<td>1</td>
</tr>
<tr>
<td>Go to PROXYLITE</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>1</td>
</tr>
<tr>
<td>Go to BITPING</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>1</td>
</tr>
<tr>
<td>Go to MYSTNODE</td>
<td>✔</td>
<td>✔</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
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

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 your devices as 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

We also recommend using a safe and complicated password to secure your 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

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