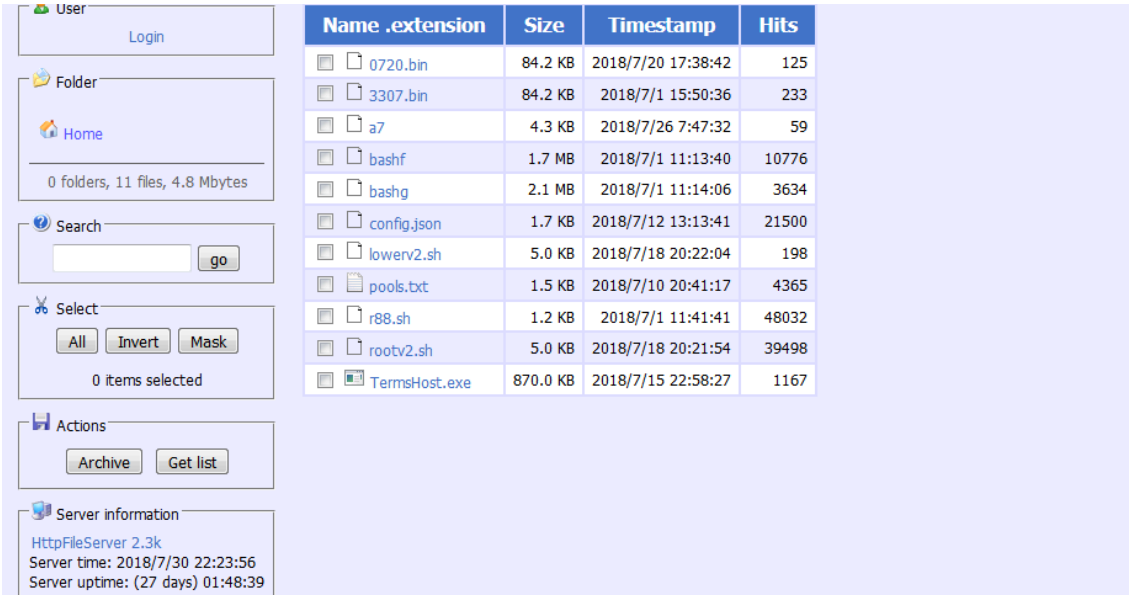
Rocke: The Champion of Monero Miners

By William Largent

Published: 2018-08-30 · Archived: 2026-04-02 10:34:33 UTC



Thursday, August 30, 2018 11:26

This post was authored by David Liebenberg.

Summary

Cryptocurrency miners are becoming an increasingly significant part of the threat landscape. These malicious miners steal CPU cycles from compromised devices to mine cryptocurrencies and bring in income for the threat actor.

In this post, we look at the activity of one particular threat actor: Rocke. We will examine several of Rocke's campaigns, malware, and infrastructure while uncovering more information about the actor. After months of research, we believe that Rocke is an actor that must be followed, as they continue to add new features to their malware and are actively exploring new attack vectors.

Introduction

Talos has written widely about the issue of cryptomining malware and how organizations should protect systems against this threat. We continue to actively research developments in this threat through research that includes monitoring criminal forums and deploying honeypot systems to attract these threats. It is

through these intelligence sources that the Chinese-speaking actor which we refer to as "Rocke" came to our attention.

Rocke actively engages in distributing and executing cyrptomining malware using a varied toolkit that includes Git repositories, HttpFileServers (HFS), and a myriad of different payloads, including shell scripts, JavaScript backdoors, as well as ELF and PE miners.

Early campaigns

This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability.

Several files were downloaded to our Struts2 honeypot from the Chinese repository site gitee.com for a user named "c-999." Subsequently, the Gitee user page transitioned to "c-888." Around the same time, we observed similar activity pulling down files from a gitlab.com repository page for a user named "c-18."

The repositories on both Gitee and GitLab were identical. All the repositories had a folder called "ss" that contained 16 files. The files were a collection of ELF executables, shell scripts, and text files that execute a variety of actions, including achieving persistence and the execution of an illicit cryptocurrency miner.

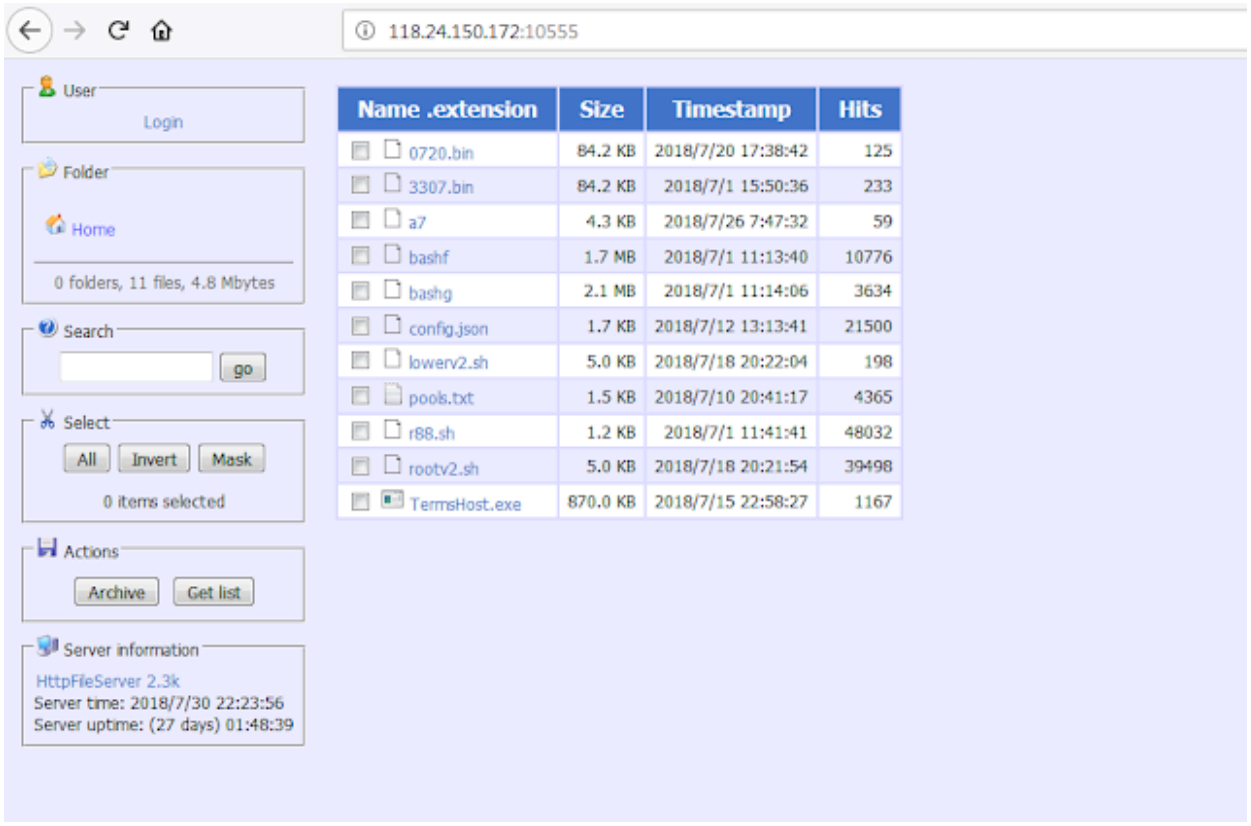
Once the threat actor had compromised a system, they achieved persistence on the device by installing a cron job that downloads and executes a file "logo.jpg" from "3389[.]space." This file is a shell script which, in turn, downloads mining executables from the threat actor's Git repositories and saves them under the filename "java." The exact file downloaded depends on the victim's system architecture. Similarly, the system architecture determines if "h32" or "h64" is used to invoke "java."

Although we first observed this actor exploiting vulnerabilities in Apache Struts, we've also observed what we believe to the same individual exploiting an Oracle WebLogic server vulnerability (CVE-2017-10271), and also exploiting CVE-2017-3066, a critical Java deserialization vulnerability in the Adobe ColdFusion platform.

Recent campaign

In late July, we became aware that the same actor was engaged in another similar campaign. Through our investigation into this new campaign, we were able to uncover more details about the actor.

We observed a wget request from our Struts2 honeypot for a file named "0720.bin" located on 118[.]24[.]150[.]172:10555. We visited this IP and found it was an open HFS hosting "0720.bin" along with 10 additional files: "3307.bin," "a7," "bashf," "bashg," "config.json," "lowerv2.sh," "pools.txt," "r88.sh," "rootv2.sh" and "TermsHost.exe." We set about examining these files.



Screenshot of HFS system

We had previously observed this same IP scanning for TCP port 7001 throughout May 2018. This was potentially a scan for Oracle WebLogic servers, which listens on TCP port 7001 by default.

Both "0720.bin" and "3307.bin" are similar ELF files of similar size (84.19KB) that reach out to 118[.]24[.]150[.]172, and were marked clean in VirusTotal at the time of discovery. Morpheus Labs described a similar file that connects to the same IP address, which could open a shell on the victim's machine if a password-verified instruction was issued from the C2. In both our samples, as well as the ones that Morpheus Labs described, the hard-coded password was not only identical, but also located at the same offset.

Hard-coded password

"A7" is a shell script that kills a variety of processes related to other cryptomining malware (including those with names matching popular mining malware such as "cranberry," "yam," or "kworker"), as well as mining in general (such as "minerd" and "cryptonight"). It detects and uninstalls various Chinese AV, and also downloads and extracts a tar.gz file from blog[.]sydwzl[.]cn, which also resolves to 118[.]24[.]150[.]172. The script downloads a file from GitHub called "libprocesshider," which hides a file called "x7" using the ID preloader. The script looks for IP addresses in known_hosts and attempts to SSH into them, before downloading "a7" again from the actor's HFS at 118[.]24[.]150[.]172, and execute it.

```
#/bin/bash
if [ -f /tmp/.a7 ]; then
  exit 101
fi
touch /tmp/.a7
function clean () {
  rm -f /tmp/.a7
}

for f in /var/spool/cron/* /var/spool/cron/crontabs/* /etc/*crontab /etc/cron.d/*; do
  if grep -i -q redis "$f"; then echo > "$f"; fi
done

if [ -f /etc/ld.so.preload ]; then
  mv -f /etc/ld.so.preload /etc/ld.so.pre
fi
chmod -x /etc/xig
chmod -x /root/cranberry /tmp/cranberry /root/yam
chmod -x /etc/root.sh
chmod -x /usr/bin/gpg-agentd
chmod -x /usr/bin/kworker
chmod -x /usr/local/bin/gpg-agentd
killall -9 xig
killall -9 cranberry
killall -9 root.sh
killall -9 gpg-agentd
killall -9 .gpg-agent
killall -9 xmr-stak
killall -9 kworker
killall -9 .gpg
killall -9 pnscan
killall -9 netfs
killall -9 geth
pkill -f stratum
pkill -f nativesvc
pkill -f cryptonight
pkill -f minerd
```

Extract of Source Code of "a7"

"Config.json" is a mining config file for XMRig, an open-source Monero miner. The file sets the mining pool as xmr[.]pool[.]MinerGate[.]com:45700 and the actor's wallet as rocke@live.cn. This is why we have named the actor "Rocke" (note that for MinerGate, an email can be used in place of a Monero wallet number — it's simply the login email for the MinerGate platform). "Pools.txt" appears to be a config file for XMR-stak, an open-source universal Stratum pool miner that mines Monero, Aeon and more. This configuration file contains the same actor pool and wallet information as the first.

"Bashf" is a variant of XMR-stak while "bashg" is a variant of XMRig.

"Lowerv2.sh" and "rootv2.sh" are similar shell scripts that attempt to download and execute the mining malware components "bashf" and "bashg," hosted on 118[.]24[.]150[.]172. If the shell scripts do not download a miner from 118[.]24[.]150[.]172, they attempt to download a file called "XbashY" from 3g2upl4pq6kufc4m[.]tk.

"R88.sh" is a shell script that installs a cron job and attempts to download "lowerv2.sh" or "rootv2.sh."

"TermsHost.exe" is a PE32 Monero miner. Based on the config file it uses, it appears to be the Monero Silent Miner. This miner can be purchased online for $14 and targets malicious actors. Advertising for the miner promotes it as offering startup registry key persistence, mining only while idle, and the ability to inject the miner into "Windows processes to bypass firewalls." The sample grabs the config file "xmr.txt," which contains the same configuration information as the previous files, from Rocke's command and control (C2) server hosted on sydwzl[.]cn. The sample then injects code into notepad.exe, which then proceeds to communicate with the MinerGate pool. The sample also creates the UPX-packed file "dDNLQrsBUE.url" in the Windows Start Menu

Folder. Intriguingly, this file appears to share some similarities with Cobalt Strike, the popular penetration testing software, which would allow the attacker to have greater control over the infected system.

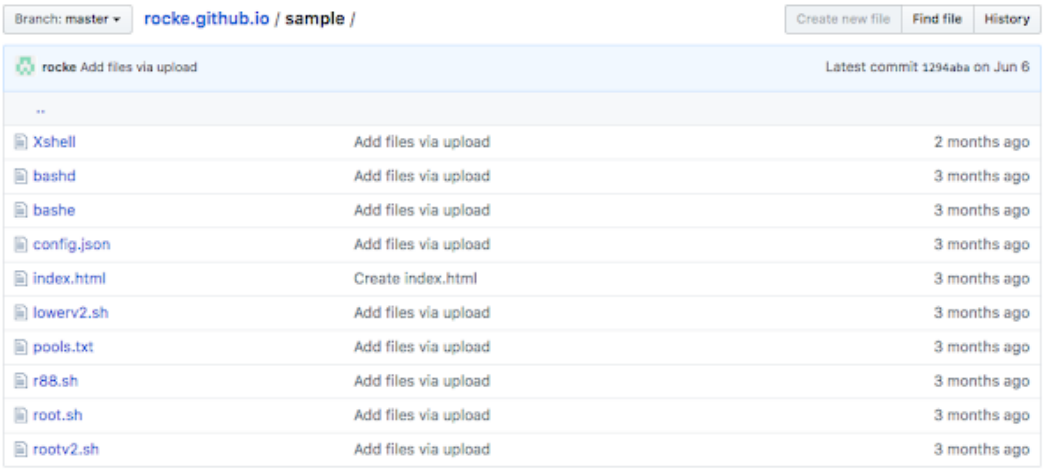
The payload appears to be similar to one used by the Iron Cybercrime Group, as reported by cybersecurity firm Intezer in May. Both Iron and Rocke's malware behave similarly, and reach out to similar infrastructure. So, while we can asses with high confidence that the payloads share some code base, we are still unsure of the exact relationship between Rocke and Iron Cybercrime Group.

Rocke has been observed seeking access to cloud storage services, as well as obtaining manuals for programming in the Chinese Easy language.

The majority of websites registered to Rocke list Jiangxi Province addresses for their registration. Some of these websites were for Jiangxi-based businesses, such as belesu[.]com, which sells baby food. We had had additional indications that Rocke is from Jiangxi based on their GitHub (see below). It is possible that the "jx" in jxci@vip.qq.com stands for Jiangxi. Therefore, we assess with high confidence that Rocke operates from Jiangxi Province.

The GitHub

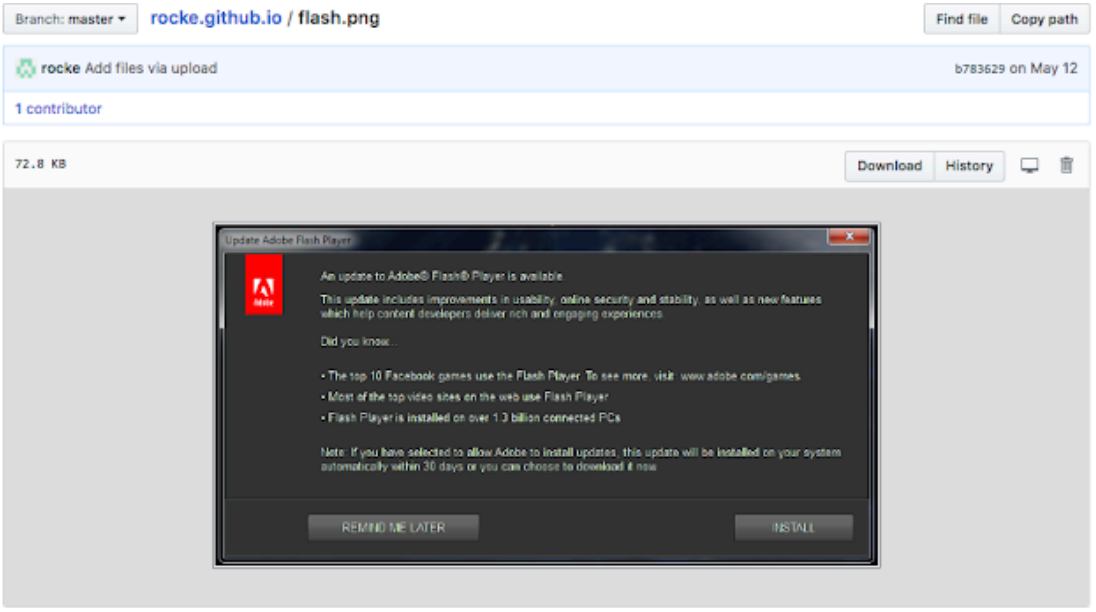
We identified a GitHub page apparently associated with Rocke. The GitHub page lists Rocke as being affiliated with Jiangxi Normal University. In one repository folder, we found several of the same files which were found on the HFS system, including several of the shell scripts with their wallet information included, as well as variants of the miner.

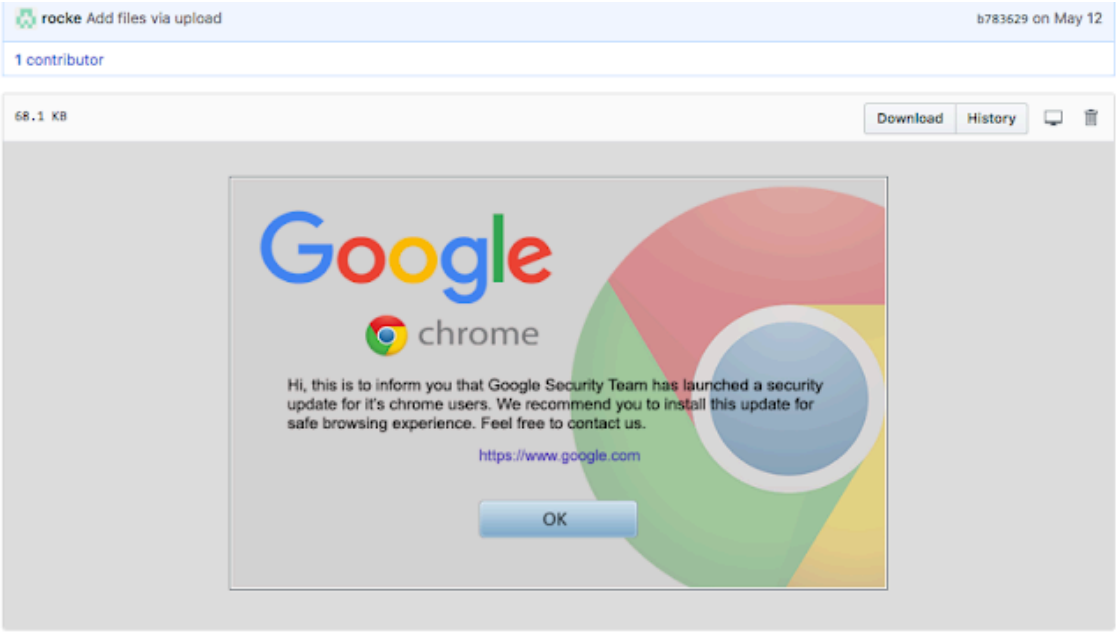


We found additional repositories for the same account. Within these repositories, we found scripts similar to those found in previous campaigns, with the exception that they reached out to sydwzl[.]cn in addition to the previously observed domain 3389[.]space. These findings support the link between Rocke and the activity we previously observed in April and May.

We also found an additional repository through Rocke's page that's hosting nearly identical content, but with a different C2. However, we are unable to determine how that page is being used or who is using it.

The files within their various repositories show that Rocke has become interested in browser-based JavaScript mining through the tool CryptoNote, as well as browser-based exploitation through the Browser Exploitation Framework. It appears that they are relying on fake Google Chrome alerts, fake apps, and fake Adobe Flash updates to social engineer users into downloading malicious payloads.





One of the JavaScript files in the repository, named "command.js," uses hidden IFrames to deliver payloads hosted on CloudFront domains. The payload that we were able to obtain was UPX packed and behaved very similarly to the file "dDNLQrsBUE.url" dropped by "TermsHost.exe."

Rocke has also shown interest in other security-related repositories. They have forked repositories with exploit information, including those related to Apache Struts 2, JBoss and Shadow Brokers, as well as more general-use tools such as masscan, proxy tools and brute forcers.

Despite the volatility in the value of various cryptocurrencies, the trend of illicit cryptocurrency mining activity among cybercriminals shows no signs of abating. Rocke's various campaigns show the variety of infection vectors, malware, and infrastructure that these criminals will employ to achieve their goals.

IOCs:

Earlier campaign:

Attacking IPs targeting Struts:

52[.]167[.]219[.]168: Attacking IP using repo at gitlab
120[.]55[.]226[.]24: Attacking IP using repo at gitee

Attacking IP targeting WebLogic:

27[.]193[.]180[.]224

Attacking IPs targeting ColdFusion:

112[.]226[.]250[.]77
27[.]210[.]170[.]197
112[.]226[.]74[.]162

Domains
3389[.]space

URLs
hxxps://gitee[.]com/c-999/ss/raw/master/ss/a
hxxps://gitee[.]com/c-999/ss/raw/master/ss/config[.]json
hxxps://gitee[.]com/c-999/ss/raw/master/ss/dir[.]dir
hxxps://gitee[.]com/c-999/ss/raw/master/ss/h32
hxxps://gitee[.]com/c-999/ss/raw/master/ss/upd
hxxps://gitee[.]com/c-999/ss/raw/master/ss/x86_64
hxxps://gitee[.]com/c-999/ss/raw/master/ss/h64
hxxps://gitee[.]com/c-999/ss/raw/master/ss/x
hxxps://gitee[.]com/c-999/ss/raw/master/ss/run
hxxps://gitee[.]com/c-999/ss/raw/master/ss/logo[.]jpg
hxxps://gitee[.]com/c-888/ss/raw/master/ss/a
hxxps://gitee[.]com/c-888/ss/raw/master/ss/cron[.]d
hxxps://gitee[.]com/c-888/ss/raw/master/ss/dir[.]dir
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/x
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/x86_64
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/run
hxxps://gitee[.]com/c-888/ss/raw/master/ss/upd

hxxps://gitlab[.]com/c-18/ss/raw/master/ss/upd
hxxps://gitee[.]com/c-888/ss/raw/master/ss/x
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/cron[.]d
hxxps://gitee[.]com/c-888/ss/raw/master/ss/h64
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/a
hxxps://gitee[.]com/c-888/ss/raw/master/ss/config[.]json
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/config[.]json
hxxps://gitee[.]com/c-888/ss/raw/master/ss/run
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/h32
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/dir[.]dir
hxxps://gitee[.]com/c-888/ss/raw/master/ss/x86_64
hxxps://gitee[.]com/c-888/ss/raw/master/ss/h32
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/h64
hxxp://93[.]174[.]93[.]149/[.]xxxzlol[.]tar[.]gz
hxxps://gitee[.]com/c-888/ss/raw/master/ss/logo[.]jpg
hxxps://gitlab[.]com/c-18/ss/raw/master/ss/logo[.]jpg

Hashes:
Logo.jpg: ad68ab153623472bbd8220fb19c488ae2884d9b52bc65add5d54b1821b4b743a
a: 6ec8201ef8652f7a9833e216b5ece7ebbf70380ebd367e3385b1c0d4a43972fb
cron.d: f6a150acfa6ec9d73fdecae27069026ecf2d833eac89976289d6fa15713a84fe
dir.dir: a20d61c3d4e45413b001340afb4f98533d73e80f3b47daec42435789d12e4027
h32: 45ed59d5b27d22567d91a65623d3b7f11726f55b497c383bc2d8d330e5e17161
h64: 7fe9d6d8b9390020862ca7dc9e69c1e2b676db5898e4bfad51d66250e9af3eaf

logo.jpg (from gitee[.]com): f1f041c61e3086da8157745ee01c280a8238a379ca5b4cdbb25c5b746e490a9b

logo.jpg (from gitlab[.]com): ad68ab153623472bbd8220fb19c488ae2884d9b52bc65add5d54b1821b4b743a

run: 0c358d826c4a32a8c48ce88eb073f505b555fc62bca6015f5270425c58a0d1c5
upd: 187d06f1e6020b6787264e2e700c46c463a7818f07db0b051687f3cba65dbe0b
x (32-bit miner): 6e80a9d843faf27e239b1a767d29c7443972be1ddf5ff5f5f9fc9a2b55a161f5
x86_64 (64-bit miner): 2ad07f8d1985f00cd05dafacbe5b6a5b1e87a78f8ae8ecdf91c776651c88a612

More recent campaign:

IPs
123[.]249[.]9[.]149: Issues get request for 0720.bin
118[.]24[.]150[.]172: Rocke's HFS, also resolves to C2 sydwzl[.]cn

Domains:
sydwzl[.]cn
blockbitcoin[.]com: Reached out to by Install.exe
dazqc4f140wtl[.]cloudfront[.]net: file server

3g2upl4pq6kufc4m[.]tk: file server
d3goboxon32grk2l[.]tk: file server
enjoytopic[.]tk: file server
realtimenews[.]tk: file server
8282[.]space: older C2

Domains registered to Rocke (not all are necessarily malicious):

5-xun[.]com
88180585[.]com
firstomato[.]com
jxtiewei[.]com
ncyypx[.]net

URLs
hxxp://d20blzxlz9ydha[.]cloudfront[.]net/Install.exe
hxxp://www[.]amazon[.]com:80/N4215/adj/amzn.us.sr.aps?sz=160x600&oe=oe=ISO-8859-1;&sn=12275&s=3717&dc_ref=http%3A%2F%2Fwww.amazon.com
hxxp://www[.]amazon[.]com:80/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books

Hashes
55dbdb84c40d9dc8c5aaf83226ca00a3395292cc8f884bdc523a44c2fd431c7b 0720.bin
38066751cb6c39691904ffbef86fe3bdfa737e4ba64add4dd90358245fa2b775 3307.bin
89b3463664ff13ea77256094844c9cf69d3e408d3daf9ffad3aa18af39bab410 TermsHost.exe
d341e3a9133e534ca35d5ccc54b8a79f93ff0c917790e7d5f73fedaa480a6b93 a7
442e4a8d35f9de21d5cbd9a695a24b9ac8120e548119c7f9f881ee16ad3761e6 bashf
7674e0b69d848e0b9ff8b82df8671f9889f33ab1a664f299bcce13744e08954c bashg
7051c9af966d1c55a4096e2af2e6670d4fc75e00b2b396921a79549fb16d03d4 lowerv2.sh
2f5bf7f1ea7a84828aa70f1140774f3d4ce9985d05a676c8535420232e2af87e pools.txt
ba29d8a259d33d483833387fad9c7231fbb3beb9f4e0603b204523607c622a03 config.json
7c2dbc0d74e01a5e7c13b4a41d3a1f7564c165bd532e4473acea6f46405d0889 r88.sh
d44e767132d68fdb07c23c848ff8c28efe19d1b7c070161b7bd6c0ccfc858750 rootv2.sh
35cb971daafd368b71ad843a4e0b81c80225ec20d7679cfbf78e628ebcada542 Install.exe
654ec27ea99c44edc03f1f3971d2a898b9f1441de156832d1507590a47b41190 ZZYO
F808A42B10CF55603389945A549CE45EDC6A04562196D14F7489AF04688F12BC XbashY
725efd0f5310763bc5375e7b72dbb2e883ad90ec32d6177c578a1c04c1b62054 reg9.sct
d7fbd2a4db44d86b4cf5fa4202203dacfefd6ffca6a0615dca5bc2a200ad56b6 m.png
ece3cfdb75aaabc570bf38af6f4653f73101c1641ce78a4bb146e62d9ac0cd50 hidden executable in m.png

---