More security,
More freedom

May the Shadow Force be with Maggie

– Shadow Force Group Characteristics and Relationship to Maggie

CHA Minseok (Jacky), KIM Junseok, LEE Jaejin

ASEC

@VB2023 (October 5, 2023)

AhnLab

:~$whoarewe

CHA Minseok (Jacky)

LEE Jaejin

KIM Junseok

Contents

1 Operation Shadow Force

2 Leaked Certificates

3 Malware

4 Tools

5 Maggie

6 Attribution

7 Conclusion

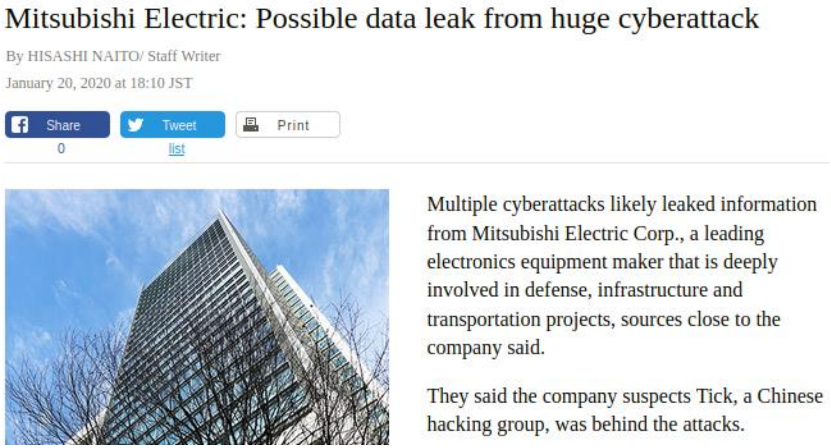
1
Operation Shadow Force

AhnLab

Data Breach of Mitsubishi Electric

- Mitsubishi Electric Hack (2020.1)

- Suspicious details first found in June 2019
- Exploited the Trend Micro OfficeScan's Arbitrary File Upload with Directory Traversal Vulnerability (CVE-2019-18187)
- Approached 14 company department networks including sales branches and headquarters
- Personal data of 1,987 job applicants, 4,566 employees, and 1,569 retirees breached or corrupted
- First, Tick Group -> Now, BlackTech is presumed to be behind the attack
- Aurora Panda and Emdivi also attempted attacks in the past



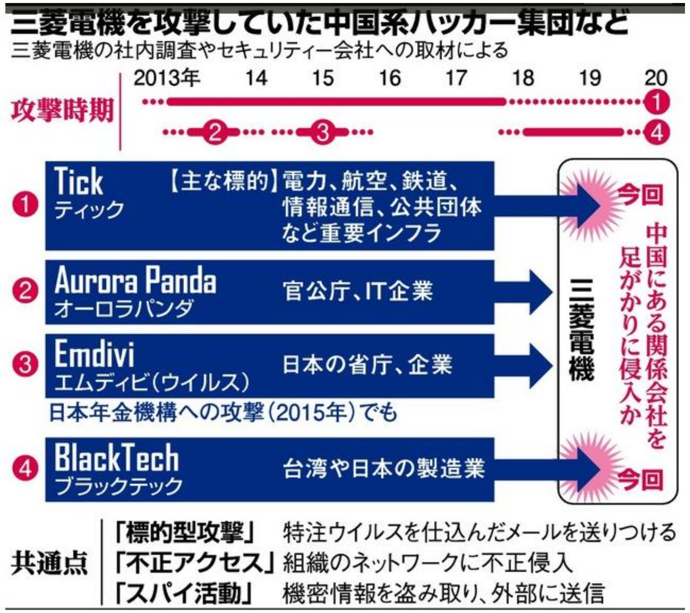
Mitsubishi Electric: Possible data leak from huge cyberattack

By HISASHI NAITO/ Staff Writer

January 20, 2020 at 18:10 JST

Multiple cyberattacks likely leaked information from Mitsubishi Electric Corp., a leading electronics equipment maker that is deeply involved in defense, infrastructure and transportation projects, sources close to the company said.

They said the company suspects Tick, a Chinese hacking group, was behind the attacks.



三菱電機を攻撃していた中国系ハッカー集団など

三菱電機の社内調査やセキュリティー会社への取材による

攻撃時期

2013年 14 15 16 17 18 19 20

①–④

① Tick ティック 【主な標的】電力、航空、鉄道、情報通信、公共団体など重要インフラ

② Aurora Panda オーローラパンダ 官公庁、IT企業

③ Emdivi エムディビ(ウイルス) 日本の省庁、企業

日本年金機構への攻撃(2015年)でも

④ BlackTech ブラックテック 台湾や日本の製造業

三菱電機

今回

中国にある関係会社を足がかりに侵入か

今回

共通点

「標的型攻撃」 特注ウイルスを仕込んだメールを送りつける

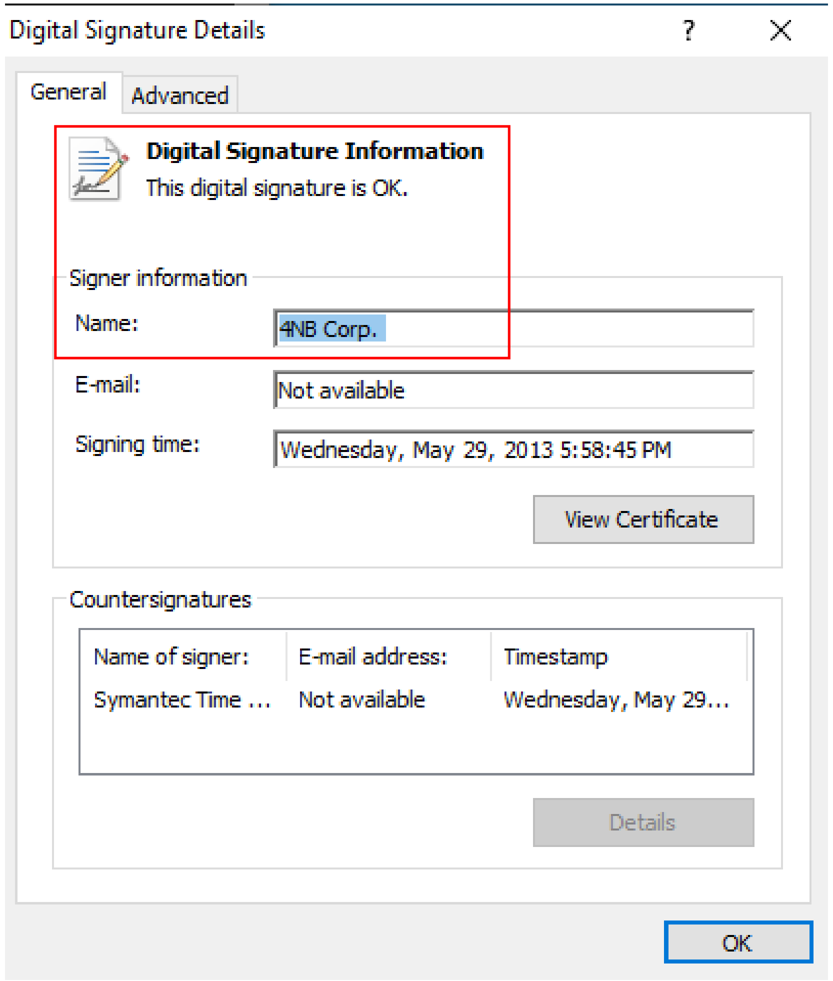
「不正アクセス」 組織のネットワークに不正侵入

「スパイ活動」 機密情報を盗み取り、外部に送信

* Source: http://www.asahi.com/ajw/articles/AJ202001200047.html & http://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf , https://www.asahi.com/articles/photo/AS20200121004397.html

Malware - ZoxPNG

- ZoxPNG (BLACKCOFFEE)
  - Created by Zhang Peng (missll) in Jinan, China
  - FireEye ‘Hide and Seek’ report
  - Known to have been used in attacks by Aurora Panda
  - Signed with a certificate from a Korean video conference company (4NB) (serial: 4e1aa28fa46d6088d27178f4a59f57be)
  - Could there be more malware signed with the 4NB certificate?



Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information
Name: 4NB Corp.
E-mail: Not available
Signing time: Wednesday, May 29, 2013 5:58:45 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	Wednesday, May 29...

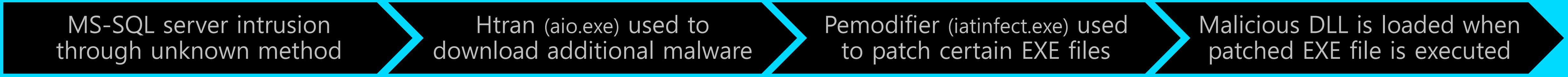
* md5 : ba86c0c1d9a08284c61c4251762ad0df

Operation Shadow Force

- Active in the Asia-Pacific region including Korea since 2013
- Target: IT operations management, medical, media, transport, foodservice, political institutions, etc.
- First analysis report by Trend Micro in 2015
- No clear attack vector identified (SQL server vulnerability suspected)
- Malware signed with forged or stolen digital certificates of Korean companies
- Consists of PE modifier, backdoor, keylogger, and tools

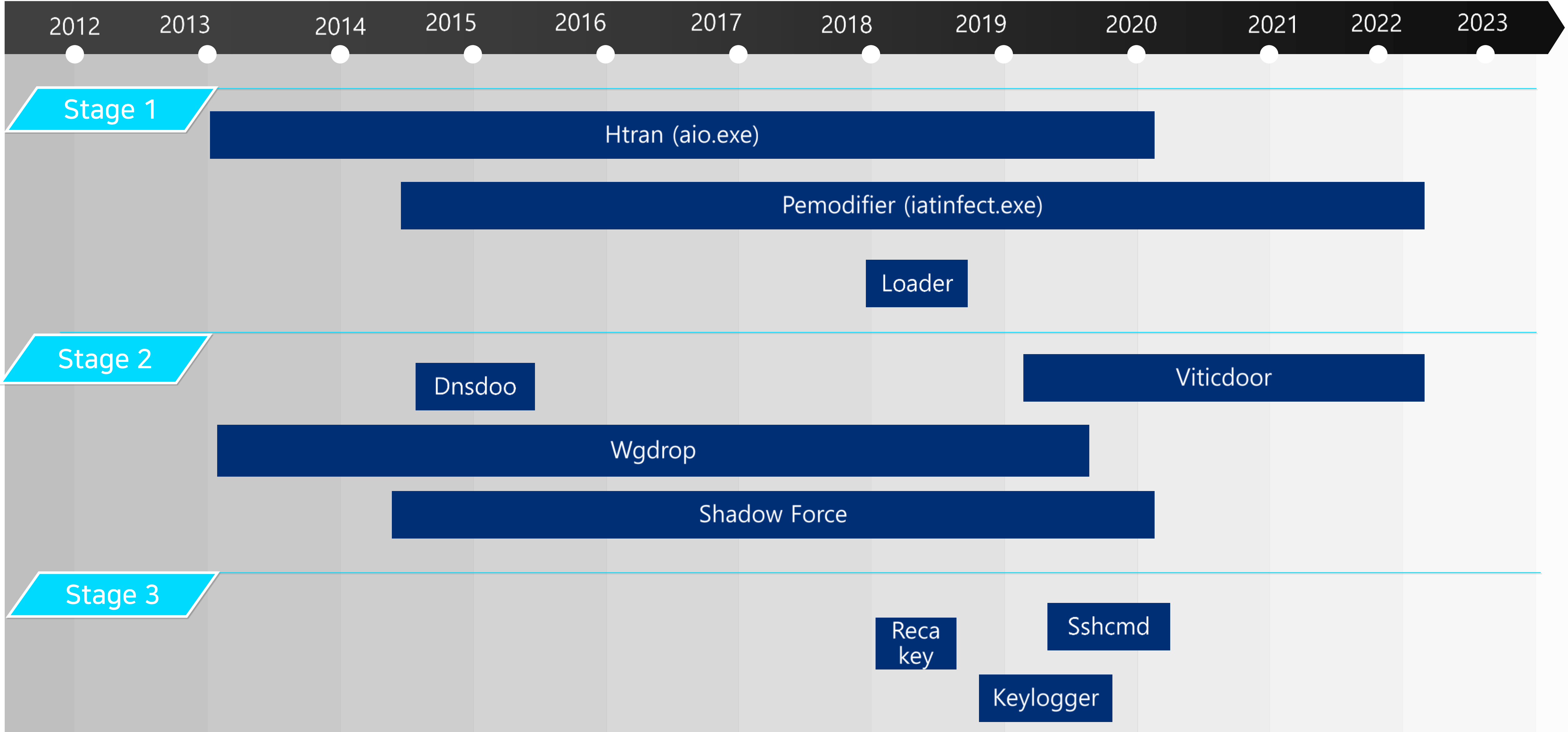
2013 —— **Operation Shadow Force** —— 2022

Attack Process



MS-SQL server intrusion through unknown method → Htran (aio.exe) used to download additional malware → Pemodifier (iatinfect.exe) used to patch certain EXE files → Malicious DLL is loaded when patched EXE file is executed

Operation Shadow Force



2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

Stage 1

Htran (aio.exe)

Pemodifier (iatinfect.exe)

Loader

Stage 2

Dnsdoo

Viticdoor

Wgdrop

Shadow Force

Stage 3

Reca key

Sshcmd

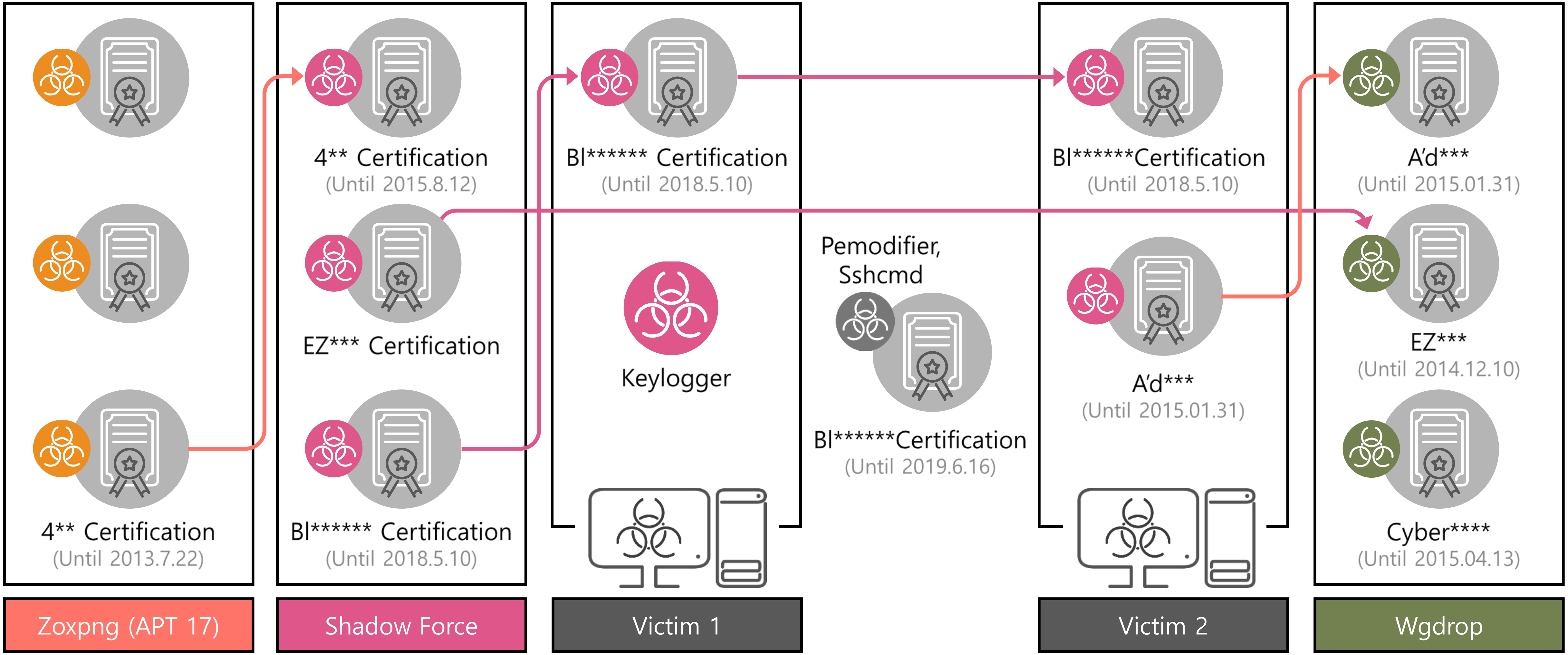
Keylogger

2
Leaked Certificates

AhnLab

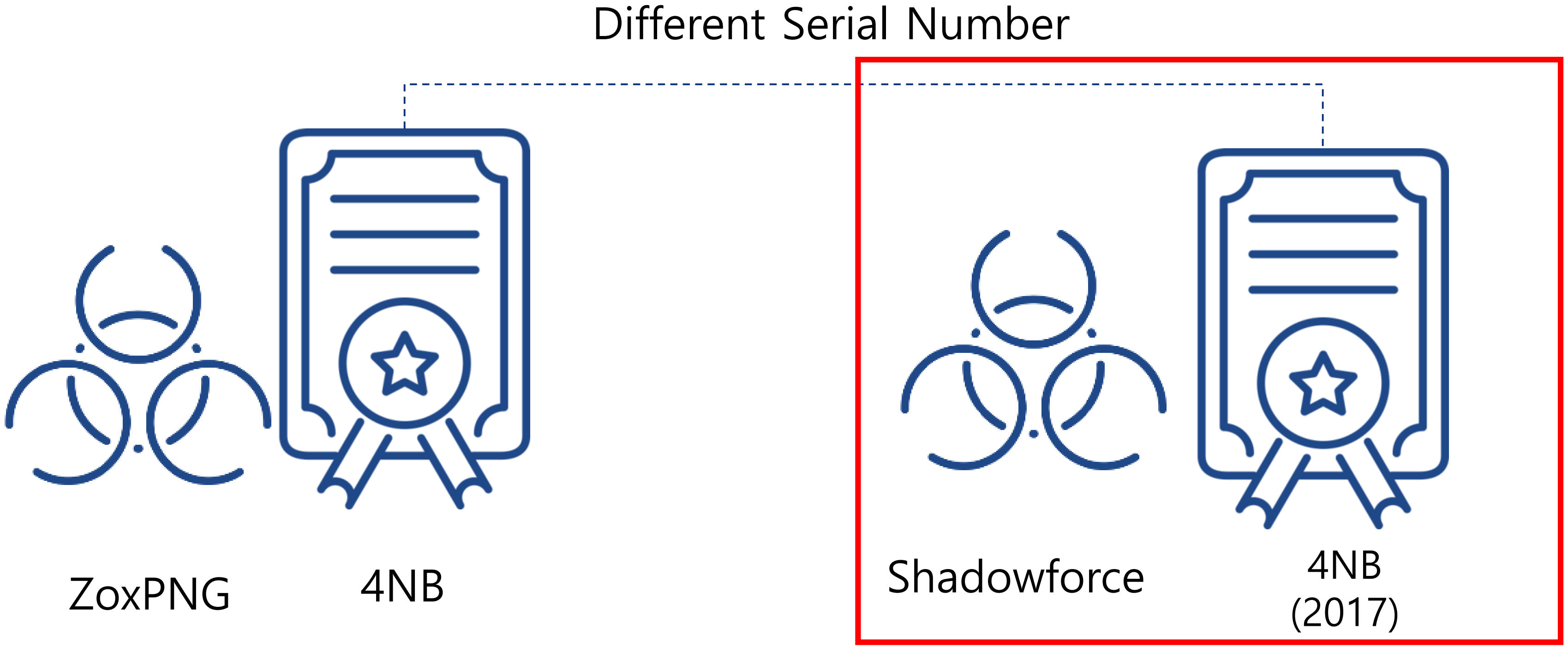
Digital Certificate Relationship

Relationship Chart



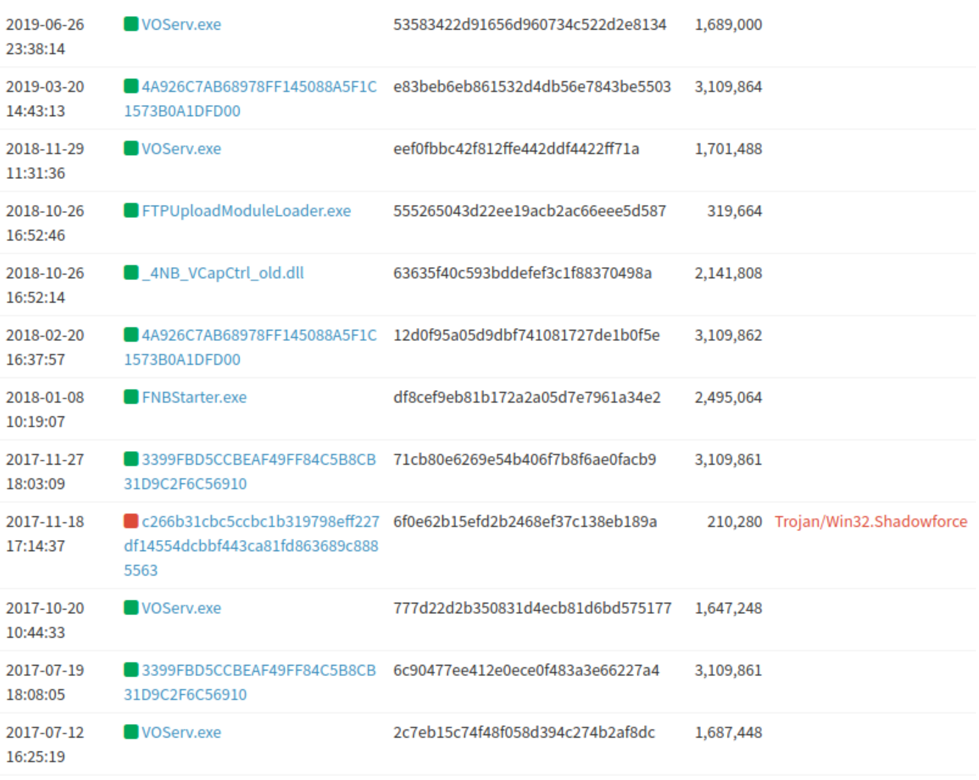
Tracking – Step 1

- Step 1 – Investigated files signed with the 4NB certificate
  - The serial numbers of the 4NB certificates are different
  - Unlikely to be the same developer

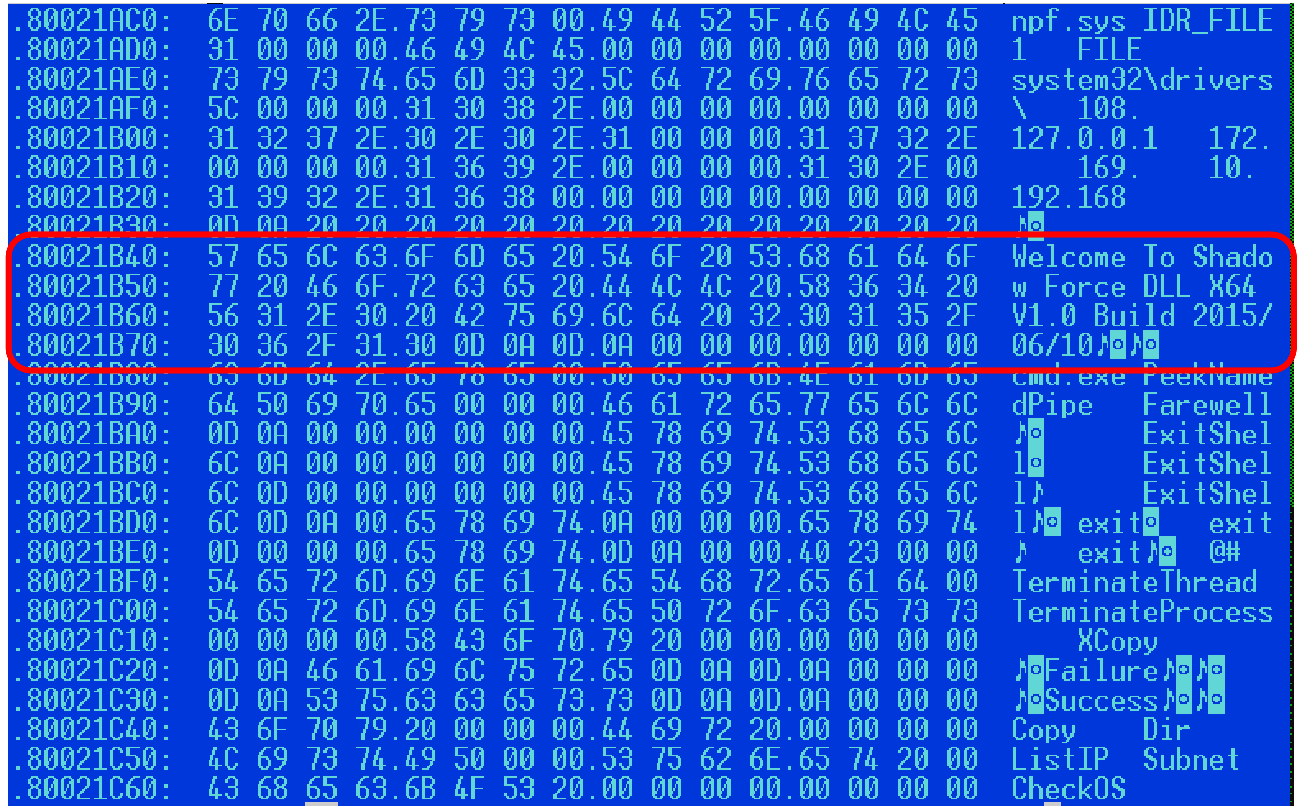


Investigation of Files Signed with 4NB Certificates

- Investigated files signed with the 4NB certificate
  - 672 signed files in total
  - Strange string found in a signed file from 2017: "Welcome To Shadow Force DLL X64 V1.0 Build 2015/06/10"



2019-06-26 23:38:14	🟩 VOServ.exe	53583422d91656d960734c522d2e8134	1,689,000	
2019-03-20 14:43:13	🟩 4A926C7AB68978FF145088A5F1C1573B0A1DFD00	e83beb6eb861532d4db56e7843be5503	3,109,864	
2018-11-29 11:31:36	🟩 VOServ.exe	eef0fbbc42f812ffe442ddf4422ff71a	1,701,488	
2018-10-26 16:52:46	🟩 FTPUploadModuleLoader.exe	555265043d22ee19acb2ac66eee5d587	319,664	
2018-10-26 16:52:14	🟩 _4NB_VCapCtrl_old.dll	63635f40c593bddefef3c1f88370498a	2,141,808	
2018-02-20 16:37:57	🟩 4A926C7AB68978FF145088A5F1C1573B0A1DFD00	12d0f95a05d9dbf741081727de1b0f5e	3,109,862	
2018-01-08 10:19:07	🟩 FNBStarter.exe	df8cef9eb81b172a2a05d7e7961a34e2	2,495,064	
2017-11-27 18:03:09	🟩 3399FBD5CCBEAF49FF84C5B8CB31D9C2F6C56910	71cb80e6269e54b406f7b8f6ae0facb9	3,109,861	
2017-11-18 17:14:37	🟥 c266b31cbc5ccbc1b319798eff227df14554dcbbf443ca81fd863689c8885563	6f0e62b15efd2b2468ef37c138eb189a	210,280	Trojan/Win32.Shadowforce
2017-10-20 10:44:33	🟩 VOServ.exe	777d22d2b350831d4ecb81d6bd575177	1,647,248	
2017-07-19 18:08:05	🟩 3399FBD5CCBEAF49FF84C5B8CB31D9C2F6C56910	6c90477ee412e0ece0f483a3e66227a4	3,109,861	
2017-07-12 16:25:19	🟩 VOServ.exe	2c7eb15c74f48f058d394c274b2af8dc	1,687,448	

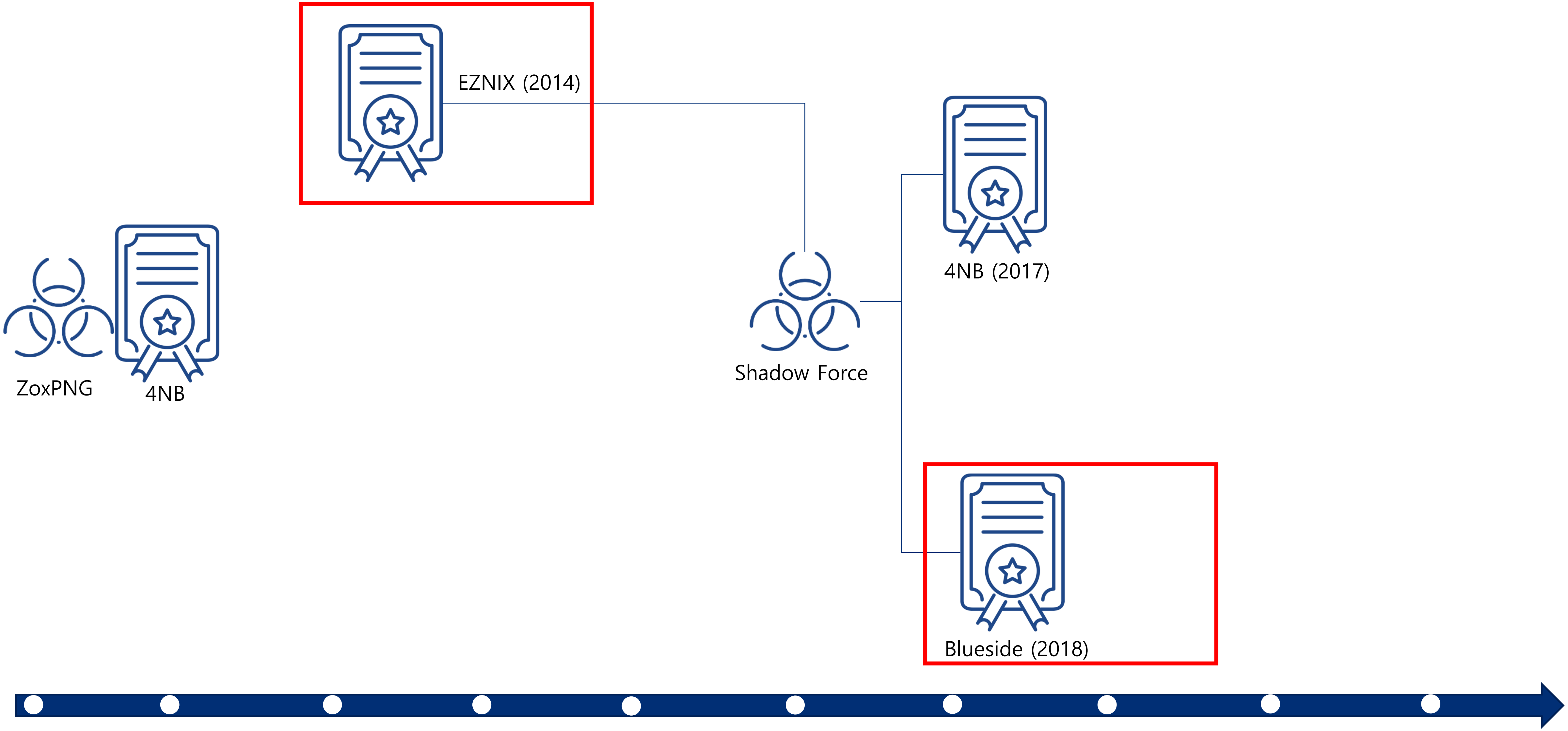


```
.80021AC0:  6E 70 66 2E.73 79 73 00.49 44 52 5F.46 49 4C 45  npf.sys IDR_FILE
.80021AD0:  31 00 00 00.46 49 4C 45.00 00 00 00.00 00 00 00  1   FILE
.80021AE0:  73 79 73 74.65 6D 33 32.5C 64 72 69.76 65 72 73  system32\drivers
.80021AF0:  5C 00 00 00.31 30 38 2E.00 00 00 00.00 00 00 00  \   108.
.80021B00:  31 32 37 2E.30 2E 30 2E.31 00 00 00.31 37 32 2E  127.0.0.1   172.
.80021B10:  00 00 00 00.31 36 39 2E.00 00 00 00.31 30 2E 00      169.    10.
.80021B20:  31 39 32 2E.31 36 38 00.00 00 00 00.00 00 00 00  192.168
.80021B30:  0D 0A 20 20.20 20 20 20.20 20 20 20.20 20 20 20  ♪◙
.80021B40:  57 65 6C 63.6F 6D 65 20.54 6F 20 53.68 61 64 6F  Welcome To Shado
.80021B50:  77 20 46 6F.72 63 65 20.44 4C 4C 20.58 36 34 20  w Force DLL X64
.80021B60:  56 31 2E 30.20 42 75 69.6C 64 20 32.30 31 35 2F  V1.0 Build 2015/
.80021B70:  30 36 2F 31.30 0D 0A 0D.0A 00 00 00.00 00 00 00  06/10♪◙♪◙
.80021B80:  63 6D 64 2E.65 78 65 00.50 65 65 6B.4E 61 6D 65  cmd.exe PeekName
.80021B90:  64 50 69 70.65 00 00 00.46 61 72 65.77 65 6C 6C  dPipe   Farewell
.80021BA0:  0D 0A 00 00.00 00 00 00.45 78 69 74.53 68 65 6C  ♪◙      ExitShel
.80021BB0:  6C 0A 00 00.00 00 00 00.45 78 69 74.53 68 65 6C  l◙      ExitShel
.80021BC0:  6C 0D 00 00.00 00 00 00.45 78 69 74.53 68 65 6C  l♪      ExitShel
.80021BD0:  6C 0D 0A 00.65 78 69 74.0A 00 00 00.65 78 69 74  l♪◙ exit◙   exit
.80021BE0:  0D 00 00 00.65 78 69 74.0D 0A 00 00.40 23 00 00  ♪   exit♪◙  @#
.80021BF0:  54 65 72 6D.69 6E 61 74.65 54 68 72.65 61 64 00  TerminateThread
.80021C00:  54 65 72 6D.69 6E 61 74.65 50 72 6F.63 65 73 73  TerminateProcess
.80021C10:  00 00 00 00.58 43 6F 70.79 20 00 00.00 00 00 00      XCopy
.80021C20:  0D 0A 46 61.69 6C 75 72.65 0D 0A 0D.0A 00 00 00  ♪◙Failure♪◙♪◙
.80021C30:  0D 0A 53 75.63 63 65 73.73 0D 0A 0D.0A 00 00 00  ♪◙Success♪◙♪◙
.80021C40:  43 6F 70 79.20 00 00 00.44 69 72 20.00 00 00 00  Copy    Dir
.80021C50:  4C 69 73 74.49 50 00 00.53 75 62 6E.65 74 20 00  ListIP  Subnet
.80021C60:  43 68 65 63.6B 4F 53 20.00 00 00 00.00 00 00 00  CheckOS
```

* md5 : 6f0e62b15efd2b2468ef37c138eb189a

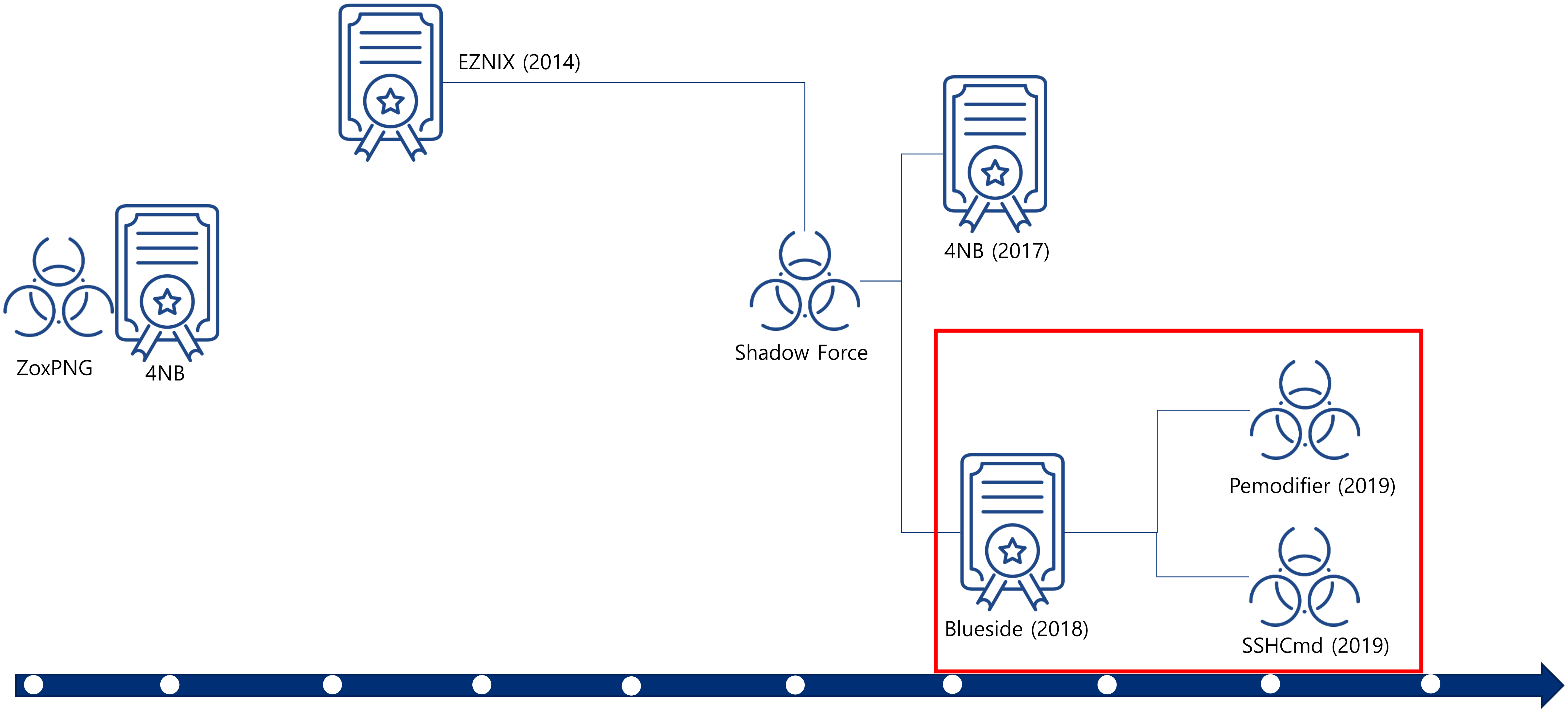
Tracking – Step 2

- Step 2 – Tracked Shadowforce variants and found two additional certificates



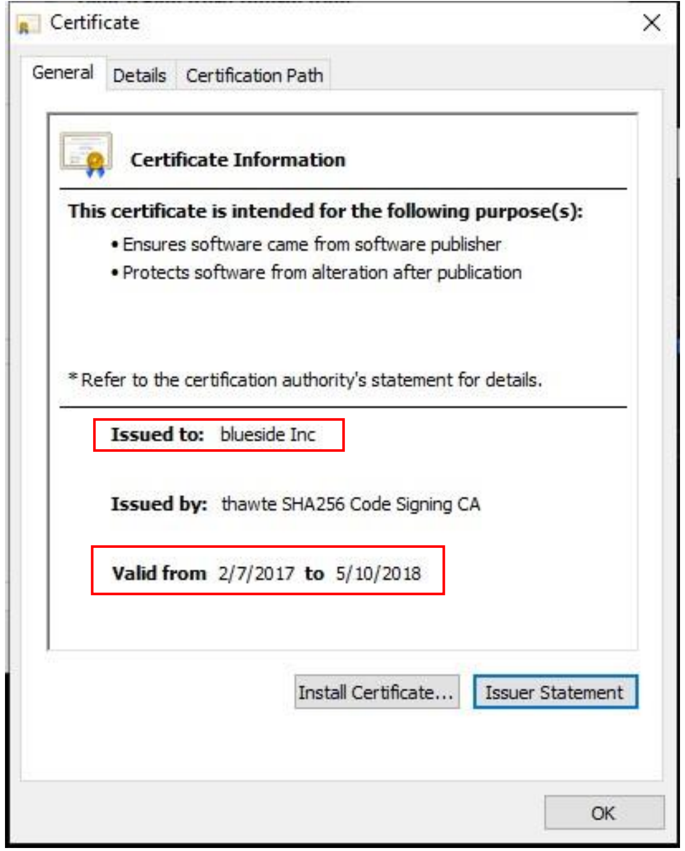
Tracking – Step 3

- Step 3 – Tracked malware signed with the Blueside certificate



Suspicious Files Signed with Blueside Certificates

- Found an additionally compromised Blueside certificate (serial: 6613fd5935f1bb8f1d355c28f920b028)
  - Presumed to be leaked before Nov 2018
  - Compared the two certificates



Certificate Information

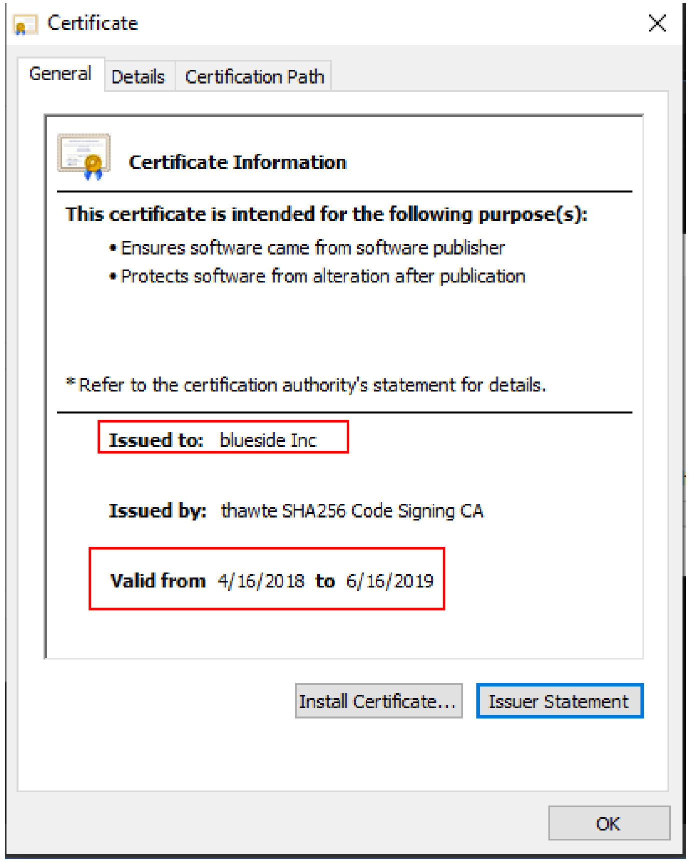
This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: blueside Inc

Issued by: thawte SHA256 Code Signing CA

Valid from 2/7/2017 **to** 5/10/2018



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: blueside Inc

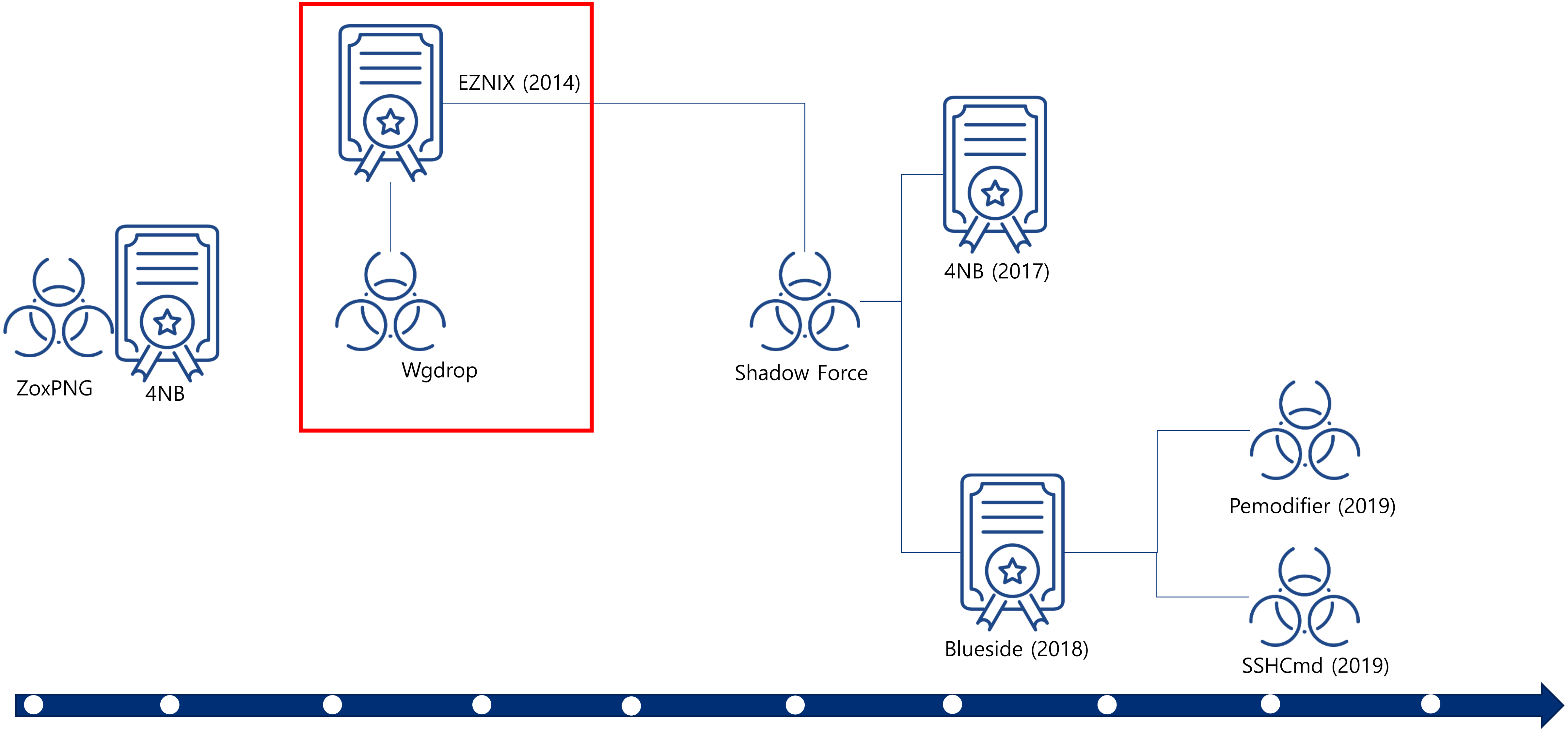
Issued by: thawte SHA256 Code Signing CA

Valid from 4/16/2018 **to** 6/16/2019

* md5 : e94d2ac3dd6f315e32960583be42d2ce , b4021d49e0478ac6436a22498e699976

Tracking – Step 4

- Step 4 – Tracked the malware signed with an EZNIX certificate and found a Wgdrop variant



Certificate Counterfeiting and Theft

Certificate	Serial Number	Country	Period	Method	Status
4NB	483f0bf7a6d84c6cf429d4eb4988e686	Korea	2017	Presumed to be a counterfeit	?
A'd* **	456e967a815aa5cbb99fb86aca8f7f69	Korea	2012 - 2013	Stolen (key leakage presumed)	Revoked
Blueside	706ac96953034b9d9926d4cc1d3248b3, 6613fd5935f1bb8f1d355c28f920b028	Korea	2018 - 2022	Stolen (key leakage presumed)	Valid
Cyber****	1d226108cbb0eb7b504697bdfec66a8b	Taiwan	2012	Presumed to be a counterfeit	Revoked
EZNIX	73e78017a7bf71b6762a603dc41fb6b5	Korea	2014	Stolen (key leakage presumed)	Valid
Pa*** TV**	39880be01fe37120ad98698509663f92	Korea	2018	Presumed to be a counterfeit	?

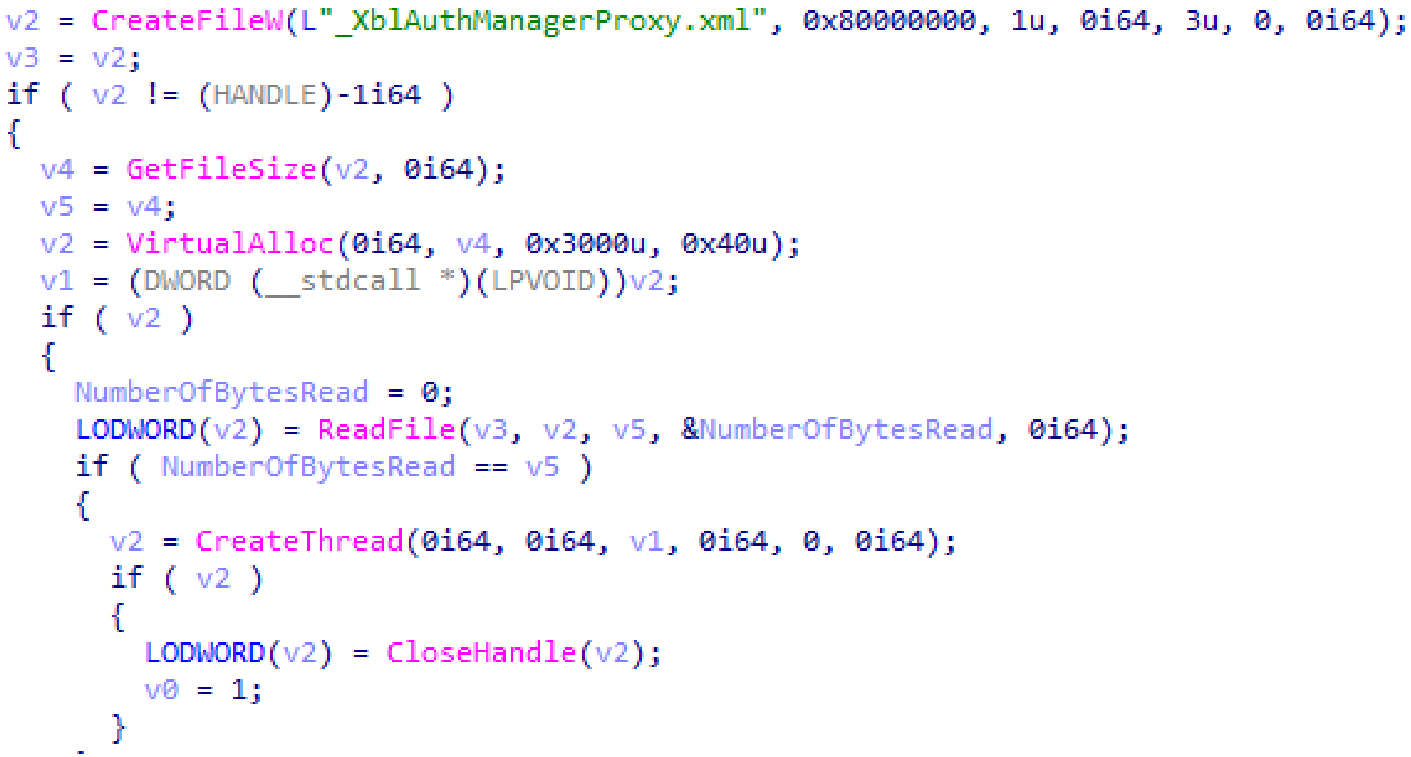
3
Malware

Malware Types

Period	Name	Type
2013 – 2020	Htran (aio.exe)	General hacking tool
2014 – 2020	Pemodifier (iatinfect.exe)	Modifies PE files and loads additional DLL files when executed
2018	Loader	Malware loader
2013 – 2014	Dnsdoo	Backdoor
2012 – 2015	Wgdrop	Ircbot. Initially in EXE format, then in DLL format
2013 – 2020	Shadow Force	Backdoor
2018	Recakey	Screen recording, keylogging, RAR console program
2018 – 2019	Keylogger	Keylogging
2019 - 2020	Sshcmd	Hacking helper tool
2019	LoginInfoStealer	Breaches user login information
2019 - 2022	Viticdoor	VTCP.dll backdoor
2020 - Present	Maggie	MS SQL backdoor

Loader

- TSMSISrv.dll (38,912 bytes)
  - Other file name: oci.dll
  - _XblAuthManagerProxy.xml (not confirmed) loads the actual code
  -

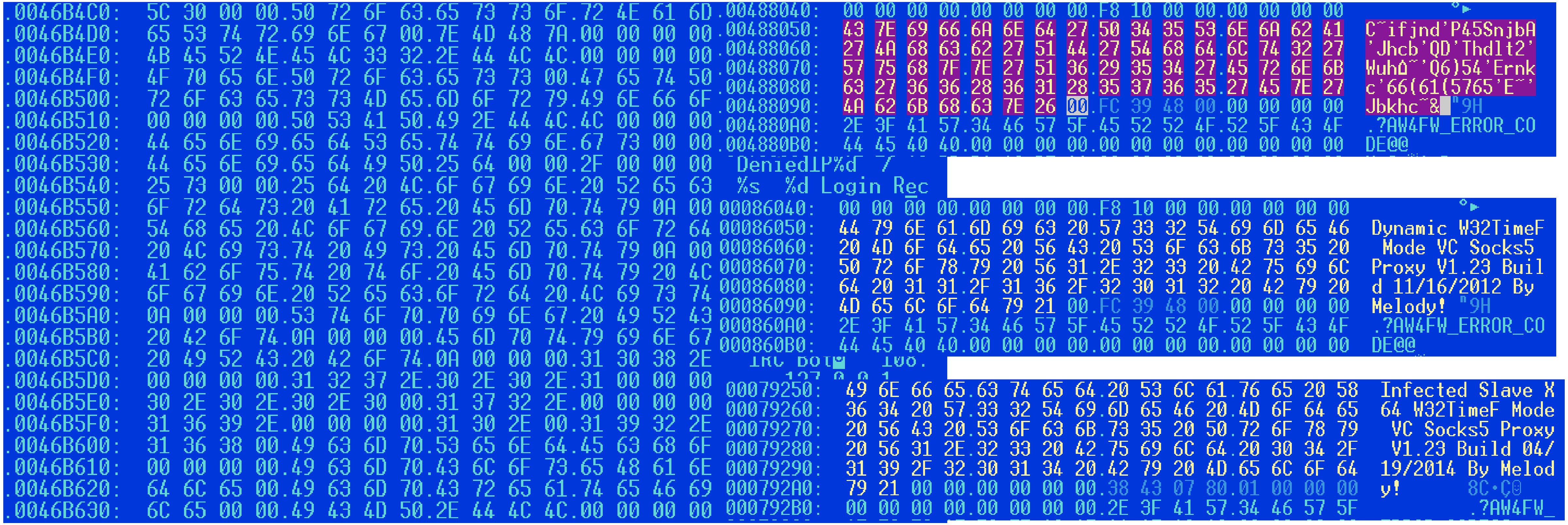


```
v2 = CreateFileW(L"_XblAuthManagerProxy.xml", 0x80000000, 1u, 0i64, 3u, 0, 0i64);
v3 = v2;
if ( v2 != (HANDLE)-1i64 )
{
  v4 = GetFileSize(v2, 0i64);
  v5 = v4;
  v2 = VirtualAlloc(0i64, v4, 0x3000u, 0x40u);
  v1 = (DWORD (__stdcall *)(LPVOID))v2;
  if ( v2 )
  {
    NumberOfBytesRead = 0;
    LODWORD(v2) = ReadFile(v3, v2, v5, &NumberOfBytesRead, 0i64);
    if ( NumberOfBytesRead == v5 )
    {
      v2 = CreateThread(0i64, 0i64, v1, 0i64, 0, 0i64);
      if ( v2 )
      {
        LODWORD(v2) = CloseHandle(v2);
        v0 = 1;
      }
```

* md5 : 7b329a6bcdc15cff1eb3c5bd31176b2c

Ircbot - Wgdrop

- Wgdrop
  - Ircbot discovered between 2013-2015 (Actual development seems to have been until 2014)
  - Filename: sqlwriter.dll, winisec.dll, cissesrv.dll, NCleanService.dll
  - String encrypted with XOR 0x07



```
.0046B4C0:  5C 30 00 00.50 72 6F 63.65 73 73 6F.72 4E 61 6D
.0046B4D0:  65 53 74 72.69 6E 67 00.7E 4D 48 7A.00 00 00 00
.0046B4E0:  4B 45 52 4E.45 4C 33 32.2E 44 4C 4C.00 00 00 00
.0046B4F0:  4F 70 65 6E.50 72 6F 63.65 73 73 00.47 65 74 50
.0046B500:  72 6F 63 65.73 73 4D 65.6D 6F 72 79.49 6E 66 6F
.0046B510:  00 00 00 00.50 53 41 50.49 2E 44 4C.4C 00 00 00
.0046B520:  44 65 6E 69.65 64 53 65.74 74 69 6E.67 73 00 00
.0046B530:  44 65 6E 69.65 64 49 50.25 64 00 00.2F 00 00 00
.0046B540:  25 73 00 00.25 64 20 4C.6F 67 69 6E.20 52 65 63
.0046B550:  6F 72 64 73.20 41 72 65.20 45 6D 70.74 79 0A 00
.0046B560:  54 68 65 20.4C 6F 67 69.6E 20 52 65.63 6F 72 64
.0046B570:  20 4C 69 73.74 20 49 73.20 45 6D 70.74 79 0A 00
.0046B580:  41 62 6F 75.74 20 74 6F.20 45 6D 70.74 79 20 4C
.0046B590:  6F 67 69 6E.20 52 65 63.6F 72 64 20.4C 69 73 74
.0046B5A0:  0A 00 00 00.53 74 6F 70.70 69 6E 67.20 49 52 43
.0046B5B0:  20 42 6F 74.0A 00 00 00.45 6D 70 74.79 69 6E 67
.0046B5C0:  20 49 52 43.20 42 6F 74.0A 00 00 00.31 30 38 2E
.0046B5D0:  00 00 00 00.31 32 37 2E.30 2E 30 2E.31 00 00 00
.0046B5E0:  30 2E 30 2E.30 2E 30 00.31 37 32 2E.00 00 00 00
.0046B5F0:  31 36 39 2E.00 00 00 00.31 30 2E 00.31 39 32 2E
.0046B600:  31 36 38 00.49 63 6D 70.53 65 6E 64.45 63 68 6F
.0046B610:  00 00 00 00.49 63 6D 70.43 6C 6F 73.65 48 61 6E
.0046B620:  64 6C 65 00.49 63 6D 70.43 72 65 61.74 65 46 69
.0046B630:  6C 65 00 00.49 43 4D 50.2E 44 4C 4C.00 00 00 00
```

```
 DeniedIP%d  /
 %s  %d Login Rec
```

```
.00488040:  00 00 00 00.00 00 00 00.F8 10 00 00.00 00 00 00          °▶
.00488050:  43 7E 69 66.6A 6E 64 27.50 34 35 53.6E 6A 62 41  C~ifjnd'P45SnjbA
.00488060:  27 4A 68 63.62 27 51 44.27 54 68 64.6C 74 32 27  'Jhcb'QD'Thdlt2'
.00488070:  57 75 68 7F.7E 27 51 36.29 35 34 27.45 72 6E 6B  WuhΔ~'Q6)54'Ernk
.00488080:  63 27 36 36.28 36 31 28.35 37 36 35.27 45 7E 27  c'66(61(5765'E~'
.00488090:  4A 62 6B 68.63 7E 26 00.FC 39 48 00.00 00 00 00  Jbkhc~& "9H
.004880A0:  2E 3F 41 57.34 46 57 5F.45 52 52 4F.52 5F 43 4F  .?AW4FW_ERROR_CO
.004880B0:  44 45 40 40.00 00 00 00.00 00 00 00.00 00 00 00  DE@@
```

```
00086040:  00 00 00 00.00 00 00 00.F8 10 00 00.00 00 00 00          °▶
00086050:  44 79 6E 61.6D 69 63 20.57 33 32 54.69 6D 65 46  Dynamic W32TimeF
00086060:  20 4D 6F 64.65 20 56 43.20 53 6F 63.6B 73 35 20   Mode VC Socks5
00086070:  50 72 6F 78.79 20 56 31.2E 32 33 20.42 75 69 6C  Proxy V1.23 Buil
00086080:  64 20 31 31.2F 31 36 2F.32 30 31 32.20 42 79 20  d 11/16/2012 By
00086090:  4D 65 6C 6F.64 79 21 00.FC 39 48 00.00 00 00 00  Melody! "9H
000860A0:  2E 3F 41 57.34 46 57 5F.45 52 52 4F.52 5F 43 4F  .?AW4FW_ERROR_CO
000860B0:  44 45 40 40.00 00 00 00.00 00 00 00.00 00 00 00  DE@@
```

```
   IRC bot     108.
       127.0.0.1
```

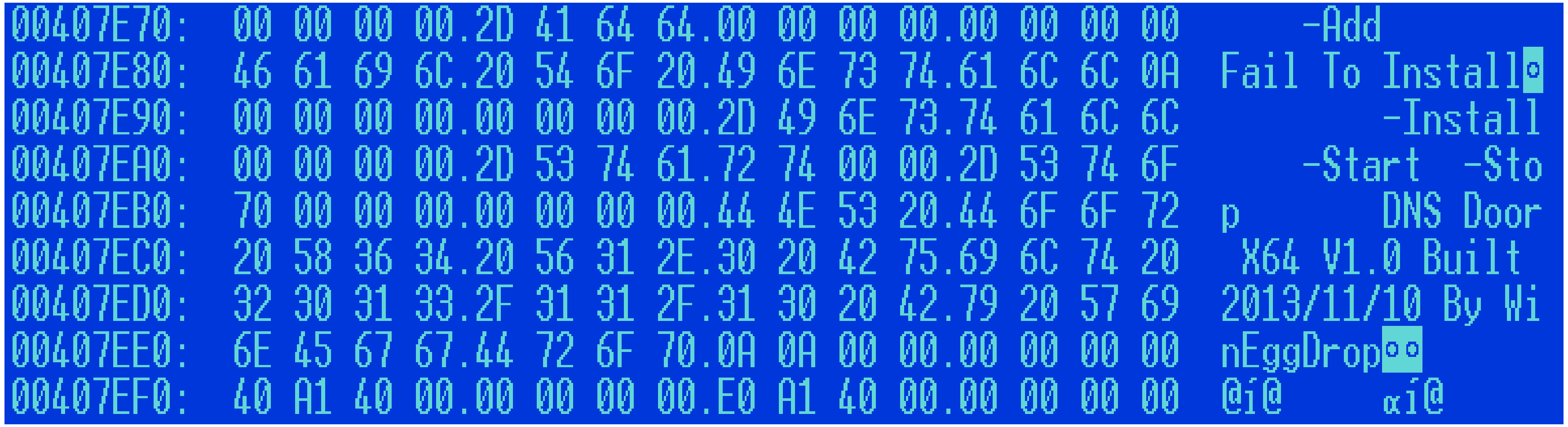
```
00079250:  49 6E 66 65.63 74 65 64.20 53 6C 61.76 65 20 58  Infected Slave X
00079260:  36 34 20 57.33 32 54 69.6D 65 46 20.4D 6F 64 65  64 W32TimeF Mode
00079270:  20 56 43 20.53 6F 63 6B.73 35 20 50.72 6F 78 79   VC Socks5 Proxy
00079280:  20 56 31 2E.32 33 20 42.75 69 6C 64.20 30 34 2F   V1.23 Build 04/
00079290:  31 39 2F 32.30 31 34 20.42 79 20 4D.65 6C 6F 64  19/2014 By Melod
000792A0:  79 21 00 00.00 00 00 00.38 43 07 80.01 00 00 00  y!      8C•Ç©
000792B0:  00 00 00 00.00 00 00 00.2E 3F 41 57.34 46 57 5F          .?AW4FW_
```

* md5 : 9552c356950daf907f30da1ca2dcb755

Backdoor - Dnsdoo

- Dnsdoo

- Filename: dns.exe
- "DNS Door X64 V1.0 Built 2013/11/10 By WinEggDrop"
- Executes cmd.exe



```
00407E70:  00 00 00 00.2D 41 64 64.00 00 00 00.00 00 00 00      -Add
00407E80:  46 61 69 6C.20 54 6F 20.49 6E 73 74.61 6C 6C 0A  Fail To Install◙
00407E90:  00 00 00 00.00 00 00 00.2D 49 6E 73.74 61 6C 6C          -Install
00407EA0:  00 00 00 00.2D 53 74 61.72 74 00 00.2D 53 74 6F      -Start  -Sto
00407EB0:  70 00 00 00.00 00 00 00.44 4E 53 20.44 6F 6F 72  p       DNS Door
00407EC0:  20 58 36 34.20 56 31 2E.30 20 42 75.69 6C 74 20   X64 V1.0 Built
00407ED0:  32 30 31 33.2F 31 31 2F.31 30 20 42.79 20 57 69  2013/11/10 By Wi
00407EE0:  6E 45 67 67.44 72 6F 70.0A 0A 00 00.00 00 00 00  nEggDrop◙◙
00407EF0:  40 A1 40 00.00 00 00 00.E0 A1 40 00.00 00 00 00  @í@     αí@
```

* md5 : 44aaa2ec4ab02bb86a39dc72394471a4

Backdoor - Shadowforce

- Shadowforce

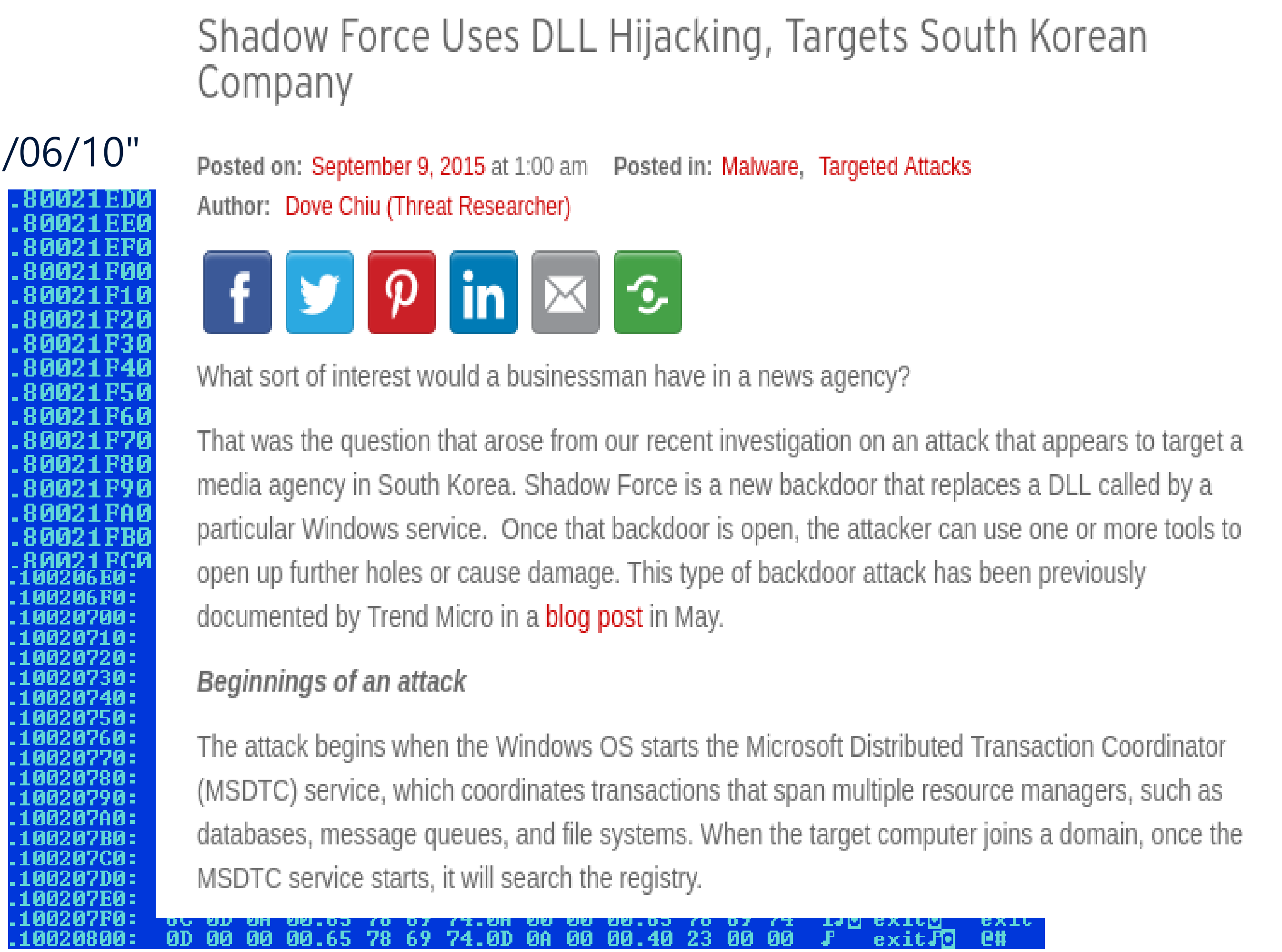
- Filename: oci.dll, sqlwriter.dll, msvcr70.dll

- "Welcome To Shadow Force DLL X64 V1.0 Build 2015/06/10"

- Attack on a Korean corporation in Sep 2015 (revealed by Trend Micro)

- Used to attack a Korean political institute in Mar 2019 (!)

- A total of 22 variants found including files signed with a Korean work management program and game company's certificates



```
.80021ED0
.80021EE0
.80021EF0
.80021F00
.80021F10
.80021F20
.80021F30
.80021F40
.80021F50
.80021F60
.80021F70
.80021F80
.80021F90
.80021FA0
.80021FB0
.80021FC0
.100206E0:
.100206F0:
.10020700:
.10020710:
.10020720:
.10020730:
.10020740:
.10020750:
.10020760:
.10020770:
.10020780:
.10020790:
.100207A0:
.100207B0:
.100207C0:
.100207D0:
.100207E0:
.100207F0:  0C 0D 0A 00.65 78 69 74.0A 00 00 00.65 78 69 74   exit   exit
.10020800:  0D 00 00 00.65 78 69 74.0D 0A 00 00.40 23 00 00      exit   @#
```

Shadow Force Uses DLL Hijacking, Targets South Korean Company

Posted on: September 9, 2015 at 1:00 am **Posted in:** Malware, Targeted Attacks
Author: Dove Chiu (Threat Researcher)

What sort of interest would a businessman have in a news agency?

That was the question that arose from our recent investigation on an attack that appears to target a media agency in South Korea. Shadow Force is a new backdoor that replaces a DLL called by a particular Windows service. Once that backdoor is open, the attacker can use one or more tools to open up further holes or cause damage. This type of backdoor attack has been previously documented by Trend Micro in a blog post in May.

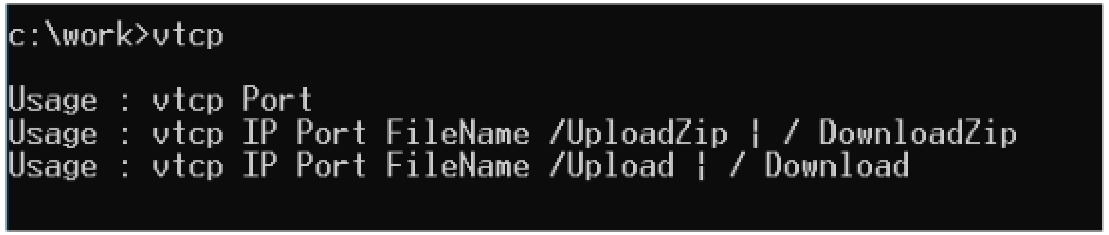
Beginnings of an attack

The attack begins when the Windows OS starts the Microsoft Distributed Transaction Coordinator (MSDTC) service, which coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. When the target computer joins a domain, once the MSDTC service starts, it will search the registry.

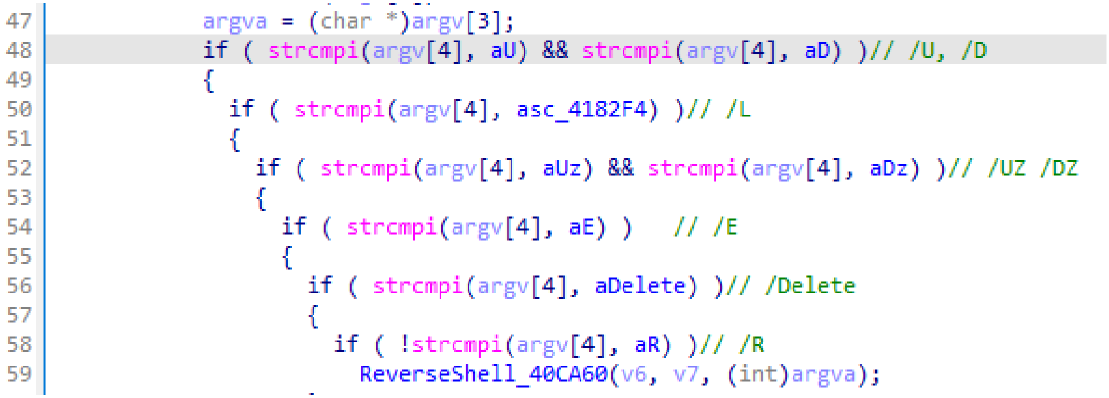
* Source: 6f0e62b15efd2b2468ef37c138eb189a, https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/

Backdoor - Viticdoor

- Viticdoor
  - VTCP.exe + VTCP.dll
  - Discovered in Mar 2019

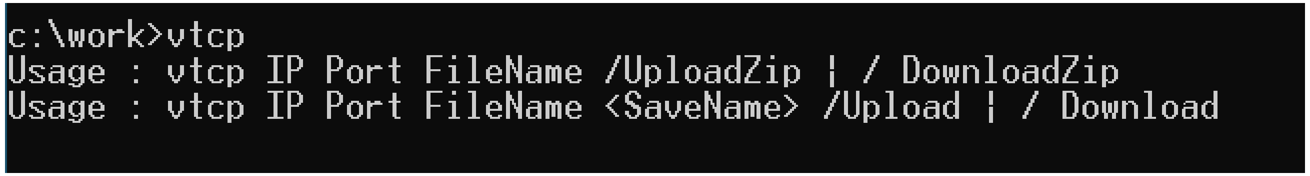


```
c:\work>vtcp

Usage : vtcp Port
Usage : vtcp IP Port FileName /UploadZip | / DownloadZip
Usage : vtcp IP Port FileName /Upload | / Download
```

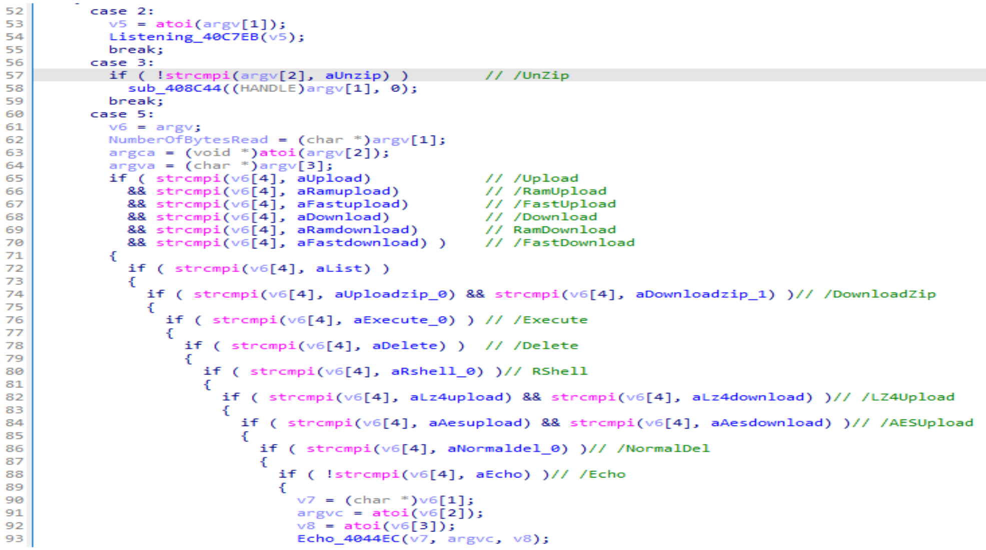


```
argva = (char *)argv[3];
if ( strcmpi(argv[4], aU) && strcmpi(argv[4], aD) )// /U, /D
{
  if ( strcmpi(argv[4], asc_4182F4) )// /L
  {
    if ( strcmpi(argv[4], aUz) && strcmpi(argv[4], aDz) )// /UZ /DZ
    {
      if ( strcmpi(argv[4], aE) )   // /E
      {
        if ( strcmpi(argv[4], aDelete) )// /Delete
        {
          if ( !strcmpi(argv[4], aR) )// /R
            ReverseShell_40CA60(v6, v7, (int)argva);
```

  - 2021: FastDownload, FastUpload, RamDownload, and RamUpload commands added
  - 2022



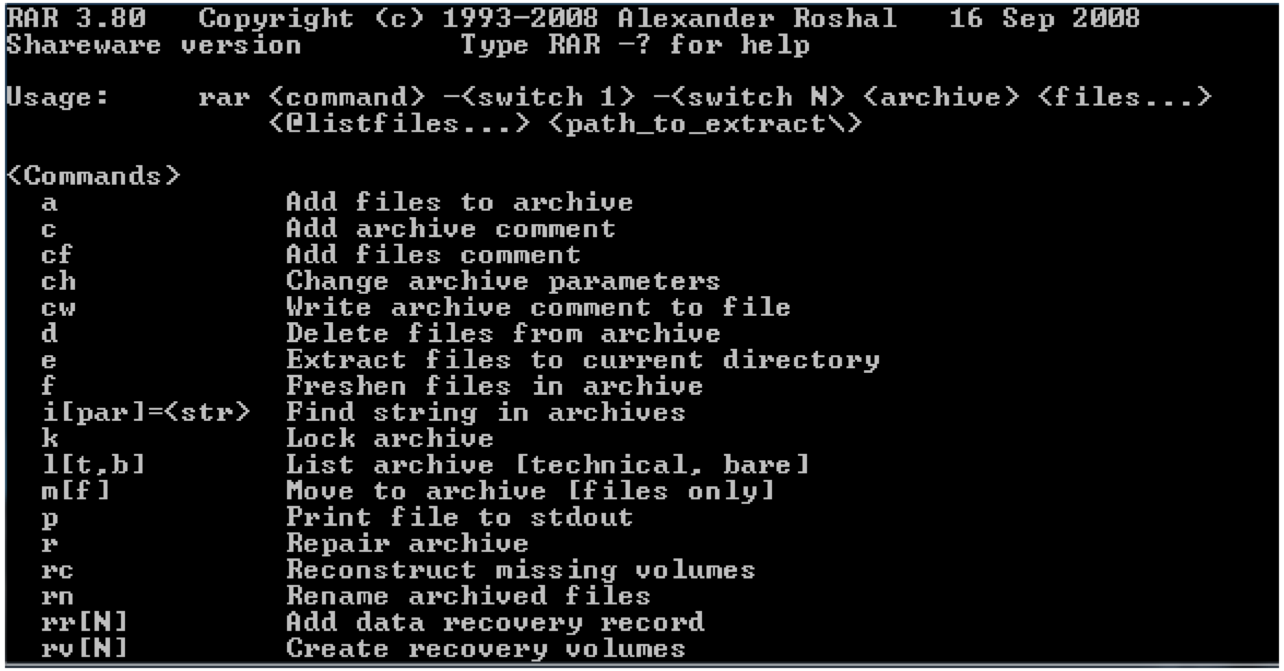
```
c:\work>vtcp
Usage : vtcp IP Port FileName /UploadZip | / DownloadZip
Usage : vtcp IP Port FileName <SaveName> /Upload | / Download
```



```
case 2:
  v5 = atoi(argv[1]);
  Listening_40C7EB(v5);
  break;
case 3:
  if ( !strcmpi(argv[2], aUnzip) )        // /UnZip
    sub_408C44((HANDLE)argv[1], 0);
  break;
case 5:
  v6 = argv;
  NumberOfBytesRead = (char *)argv[1];
  argca = (void *)atoi(argv[2]);
  argva = (char *)argv[3];
  if ( strcmpi(v6[4], aUpload)              // /Upload
    && strcmpi(v6[4], aRamupload)           // /RamUpload
    && strcmpi(v6[4], aFastupload)          // /FastUpload
    && strcmpi(v6[4], aDownload)            // /Download
    && strcmpi(v6[4], aRamdownload)         // RamDownload
    && strcmpi(v6[4], aFastdownload) )      // /FastDownload
  {
    if ( strcmpi(v6[4], aList) )
    {
      if ( strcmpi(v6[4], aUploadzip_0) && strcmpi(v6[4], aDownloadzip_1) )// /DownloadZip
      {
        if ( strcmpi(v6[4], aExecute_0) ) // /Execute
        {
          if ( strcmpi(v6[4], aDelete) )  // /Delete
          {
            if ( strcmpi(v6[4], aRshell_0) )// RShell
            {
              if ( strcmpi(v6[4], aLz4upload) && strcmpi(v6[4], aLz4download) )// /LZ4Upload
              {
                if ( strcmpi(v6[4], aAesupload) && strcmpi(v6[4], aAesdownload) )// /AESUpload
                {
                  if ( strcmpi(v6[4], aNormaldel_0) )// /NormalDel
                  {
                    if ( !strcmpi(v6[4], aEcho) )// /Echo
                    {
                      v7 = (char *)v6[1];
                      argvc = atoi(v6[2]);
                      v8 = atoi(v6[3]);
                      Echo_4044EC(v7, argvc, v8);
```

Stealer - Recakey

- Recakey
  - Screen recording and keylogging features
  - Filename: Linkinfo.dll (399,984 bytes)
  - Includes RAR 3.80
    - The initial version discovered in 2011 only had a RAR console and a screen video recording feature -> keylogging feature added in the 2018 version



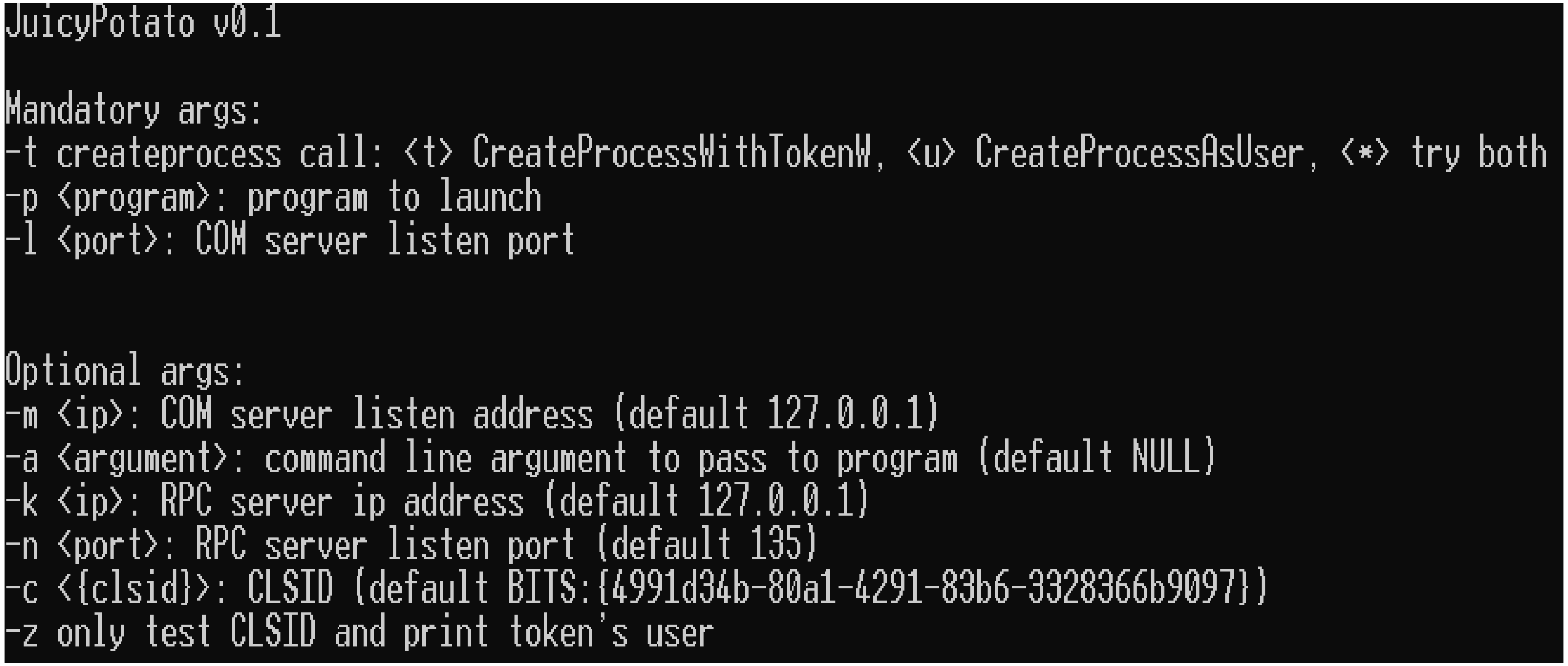
```
RAR 3.80   Copyright (c) 1993-2008 Alexander Roshal   16 Sep 2008
Shareware version         Type RAR -? for help

Usage:     rar <command> -<switch 1> -<switch N> <archive> <files...>
               <@listfiles...> <path_to_extract\>

<Commands>
  a             Add files to archive
  c             Add archive comment
  cf            Add files comment
  ch            Change archive parameters
  cw            Write archive comment to file
  d             Delete files from archive
  e             Extract files to current directory
  f             Freshen files in archive
  i[par]=<str>  Find string in archives
  k             Lock archive
  l[t,b]        List archive [technical, bare]
  m[f]          Move to archive [files only]
  p             Print file to stdout
  r             Repair archive
  rc            Reconstruct missing volumes
  rn            Rename archived files
  rr[N]         Add data recovery record
  rv[N]         Create recovery volumes
```

* md5 : e94d2ac3dd6f315e32960583be42d2ce

4
Tools

JuicyPotato

- JuicyPotato
  - Privilege escalation
  - filename is JP.exe
  - Packed with VMProtect



```
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port


Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user
```

Htran (aio.exe)

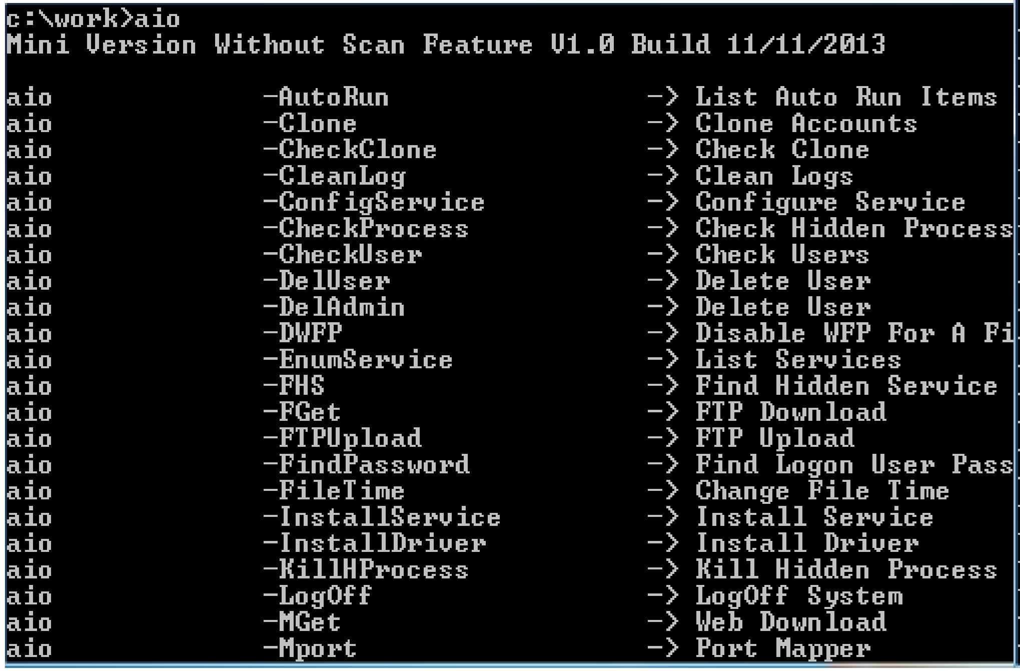
- Htran

- All file names are aio.exe

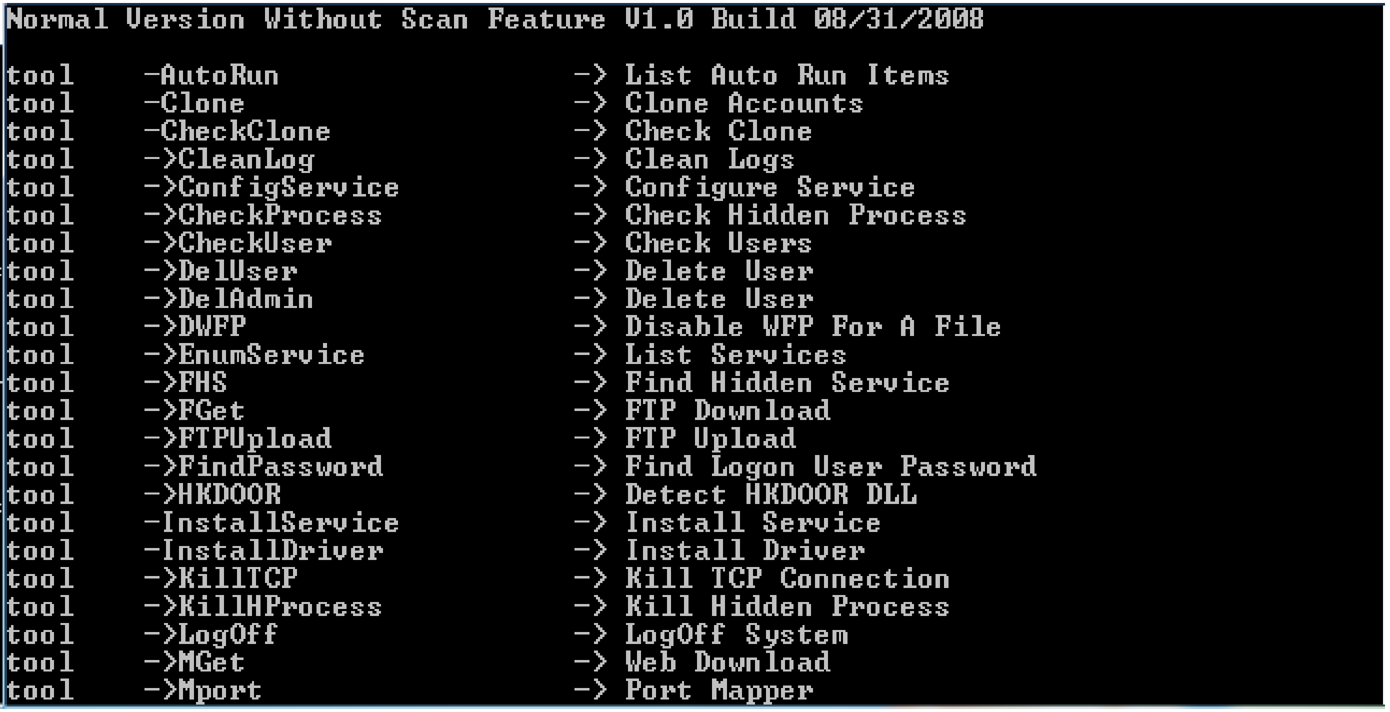
- "Mini Version Without Scan Feature V1.0 Build 11/11/2013"

- Provides features such as deleting logs, FTP, finding user passwords, and executing services and drivers.

- Initial version has been around since 2008



```
c:\work>aio
Mini Version Without Scan Feature V1.0 Build 11/11/2013

aio              -AutoRun                 -> List Auto Run Items
aio              -Clone                   -> Clone Accounts
aio              -CheckClone              -> Check Clone
aio              -CleanLog                -> Clean Logs
aio              -ConfigService           -> Configure Service
aio              -CheckProcess            -> Check Hidden Process
aio              -CheckUser               -> Check Users
aio              -DelUser                 -> Delete User
aio              -DelAdmin                -> Delete User
aio              -DWFP                    -> Disable WFP For A Fi
aio              -EnumService             -> List Services
aio              -FHS                     -> Find Hidden Service
aio              -FGet                    -> FTP Download
aio              -FTPUpload               -> FTP Upload
aio              -FindPassword            -> Find Logon User Pass
aio              -FileTime                -> Change File Time
aio              -InstallService          -> Install Service
aio              -InstallDriver           -> Install Driver
aio              -KillHProcess            -> Kill Hidden Process
aio              -LogOff                  -> LogOff System
aio              -MGet                    -> Web Download
aio              -Mport                   -> Port Mapper
```

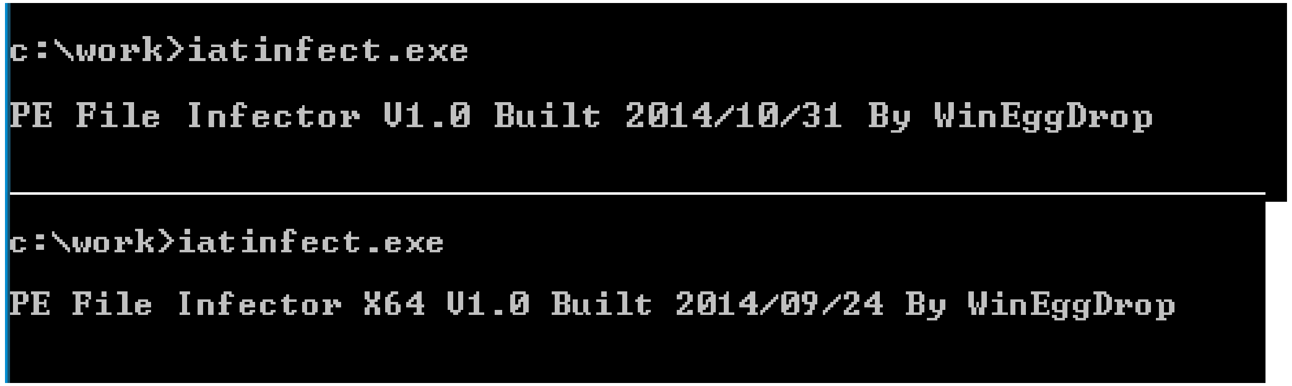


```
Normal Version Without Scan Feature V1.0 Build 08/31/2008

tool     -AutoRun                         -> List Auto Run Items
tool     -Clone                           -> Clone Accounts
tool     -CheckClone                      -> Check Clone
tool     ->CleanLog                       -> Clean Logs
tool     ->ConfigService                  -> Configure Service
tool     ->CheckProcess                   -> Check Hidden Process
tool     ->CheckUser                      -> Check Users
tool     ->DelUser                        -> Delete User
tool     ->DelAdmin                       -> Delete User
tool     ->DWFP                           -> Disable WFP For A File
tool     ->EnumService                    -> List Services
tool     ->FHS                            -> Find Hidden Service
tool     ->FGet                           -> FTP Download
tool     ->FTPUpload                      -> FTP Upload
tool     ->FindPassword                   -> Find Logon User Password
tool     ->HKDOOR                         -> Detect HKDOOR DLL
tool     -InstallService                  -> Install Service
tool     -InstallDriver                   -> Install Driver
tool     ->KillTCP                        -> Kill TCP Connection
tool     ->KillHProcess                   -> Kill Hidden Process
tool     ->LogOff                         -> LogOff System
tool     ->MGet                           -> Web Download
tool     ->Mport                          -> Port Mapper
```

* md5 : 07e5fbe4bf98da12af167fd8962339a1

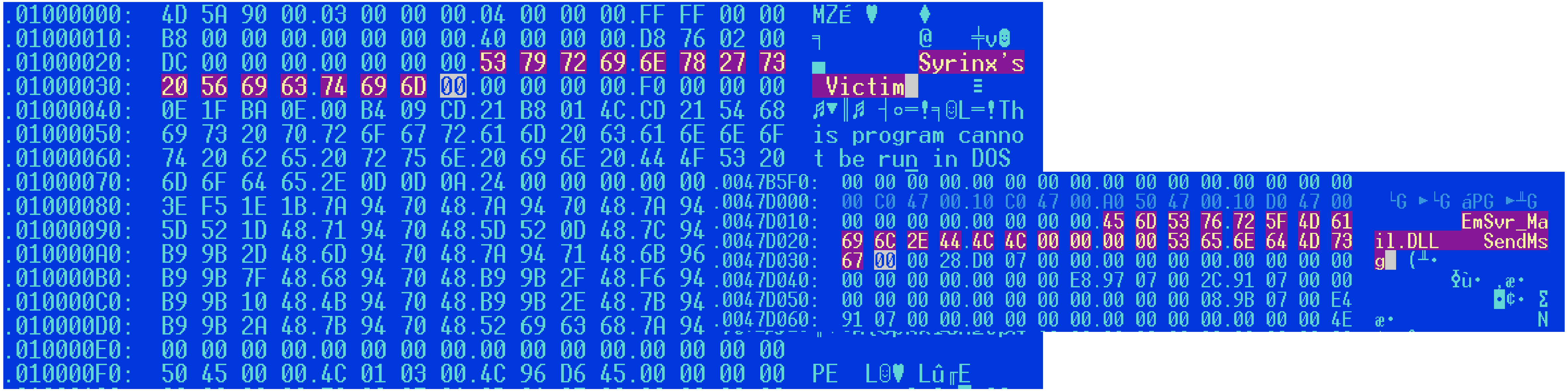
Tool - Pemodifier

- Pemodifier
  - Filename: iatinfect.exe (40,960 ~ 47,792 bytes)
  - Certificate: blueside (2019)
  - File infection tool
  - Contains "Syrinx's Victim" in the infection file



```
c:\work>iatinfect.exe
PE File Infector V1.0 Built 2014/10/31 By WinEggDrop
```

```
c:\work>iatinfect.exe
PE File Infector X64 V1.0 Built 2014/09/24 By WinEggDrop
```



```
.01000000:  4D 5A 90 00.03 00 00 00.04 00 00 00.FF FF 00 00  MZÉ ♥    ♦
.01000010:  B8 00 00 00.00 00 00 00.40 00 00 00.D8 76 02 00  ╕       @   ╪v☻
.01000020:  DC 00 00 00.00 00 00 00.53 79 72 69.6E 78 27 73  ▄       Syrinx's
.01000030:  20 56 69 63.74 69 6D 00.00 00 00 00.F0 00 00 00   Victim     ≡
.01000040:  0E 1F BA 0E.00 B4 09 CD.21 B8 01 4C.CD 21 54 68  ♬▼║♬ ┤○═!╕☺L═!Th
.01000050:  69 73 20 70.72 6F 67 72.61 6D 20 63.61 6E 6E 6F  is program canno
.01000060:  74 20 62 65.20 72 75 6E.20 69 6E 20.44 4F 53 20  t be run in DOS
.01000070:  6D 6F 64 65.2E 0D 0D 0A.24 00 00 00.00 00
.01000080:  3E F5 1E 1B.7A 94 70 48.7A 94 70 48.7A 94
.01000090:  5D 52 1D 48.71 94 70 48.5D 52 0D 48.7C 94
.010000A0:  B9 9B 2D 48.6D 94 70 48.7A 94 71 48.6B 96
.010000B0:  B9 9B 7F 48.68 94 70 48.B9 9B 2F 48.F6 94
.010000C0:  B9 9B 10 48.4B 94 70 48.B9 9B 2E 48.7B 94
.010000D0:  B9 9B 2A 48.7B 94 70 48.52 69 63 68.7A 94
.010000E0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.010000F0:  50 45 00 00.4C 01 03 00.4C 96 D6 45.00 00 00 00  PE  L☺♥ Lû╓E
```

```
.0047B5F0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.0047D000:  00 C0 47 00.10 C0 47 00.A0 50 47 00.10 D0 47 00   └G ►└G áPG ►╨G
.0047D010:  00 00 00 00.00 00 00 00.45 6D 53 76.72 5F 4D 61          EmSvr_Ma
.0047D020:  69 6C 2E 44.4C 4C 00 00.00 00 53 65.6E 64 4D 73  il.DLL    SendMs
.0047D030:  67 00 00 28.D0 07 00 00.00 00 00 00.00 00 00 00  g  (╨•
.0047D040:  00 00 00 00.00 00 00 E8.97 07 00 2C.91 07 00 00         Φù• ,æ•
.0047D050:  00 00 00 00.00 00 00 00.00 00 00 08.9B 07 00 E4             ◘¢• Σ
.0047D060:  91 07 00 00.00 00 00 00.00 00 00 00.00 00 00 4E  æ•            N
```

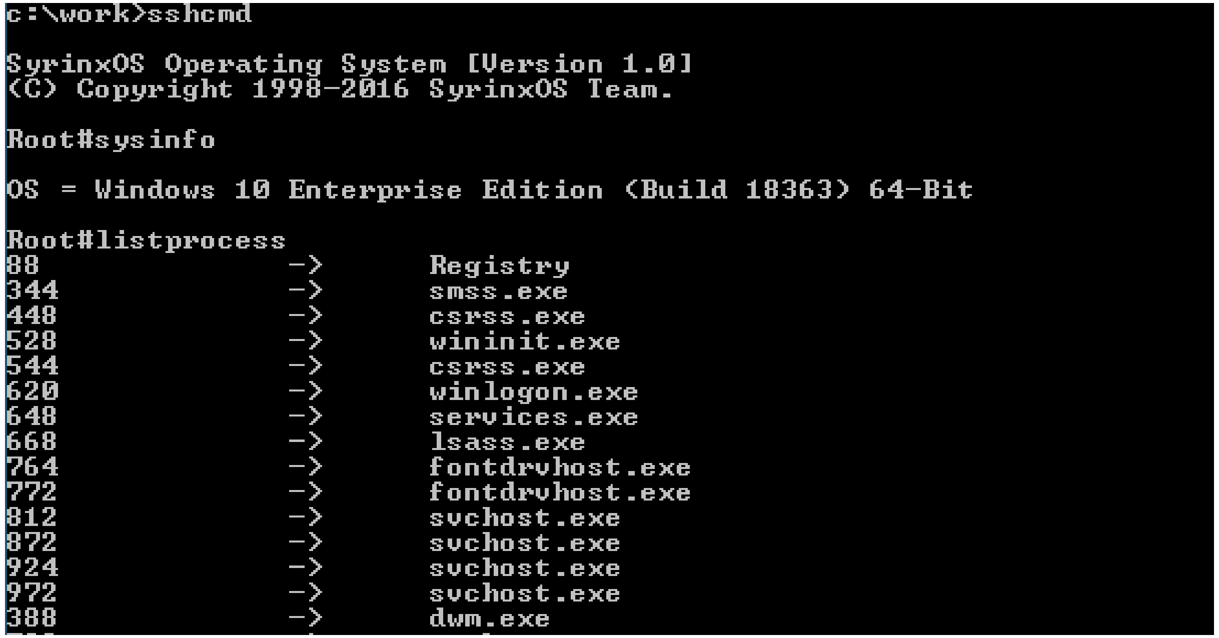
* md5 : f940d717a32ee34db39283deda9453f5

Tool – Sshcmd & SSHD

- Sshcmd (sshcmd.exe)

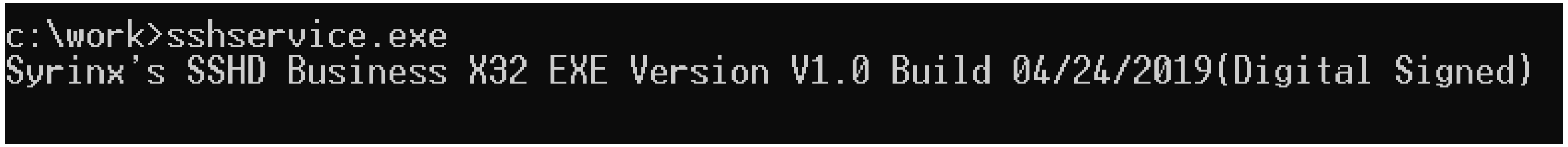
- First discovered in Nov 2019 (Created in 2016?)

 - Prints "SyrinxOS Operating System [Version 1.0] (c) Copyright 1998-2016 SyrinxOS Team."



```
c:\work>sshcmd

SyrinxOS Operating System [Version 1.0]
(C) Copyright 1998-2016 SyrinxOS Team.

Root#sysinfo

OS = Windows 10 Enterprise Edition (Build 18363) 64-Bit

Root#listprocess
88                  ->      Registry
344                 ->      smss.exe
448                 ->      csrss.exe
528                 ->      wininit.exe
544                 ->      csrss.exe
620                 ->      winlogon.exe
648                 ->      services.exe
668                 ->      lsass.exe
764                 ->      fontdrvhost.exe
772                 ->      fontdrvhost.exe
812                 ->      svchost.exe
872                 ->      svchost.exe
924                 ->      svchost.exe
972                 ->      svchost.exe
388                 ->      dwm.exe
```

-   SSHService.dll thought to create the file sshcmd.exe



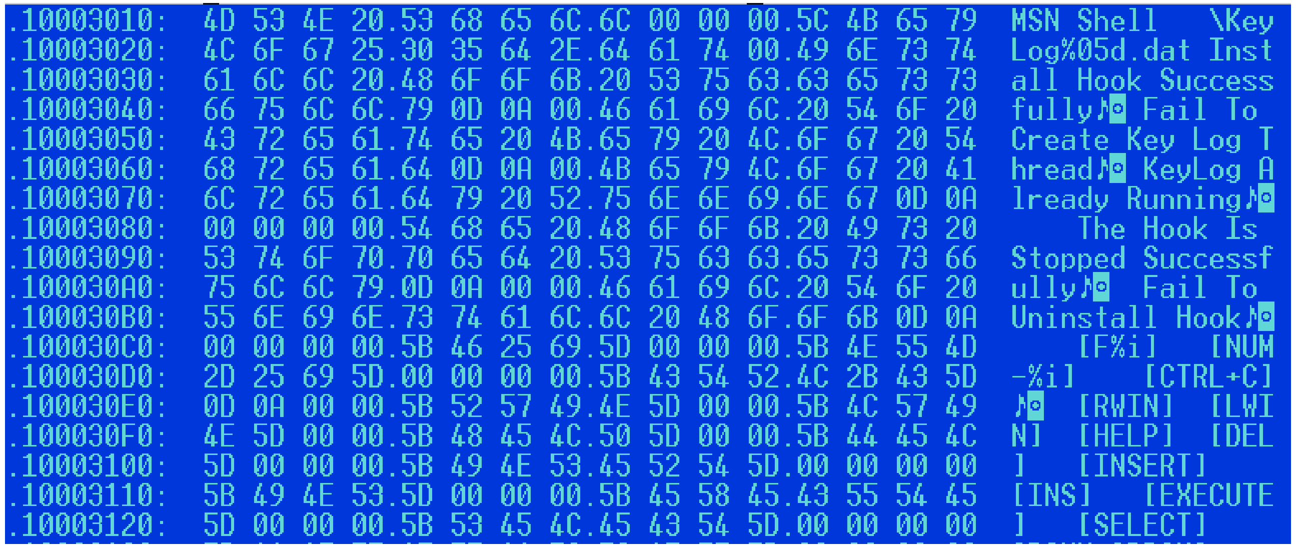
```
c:\work>sshservice.exe
Syrinx's SSHD Business X32 EXE Version V1.0 Build 04/24/2019(Digital Signed)
```

Tool - Keylogger

- Keylogger

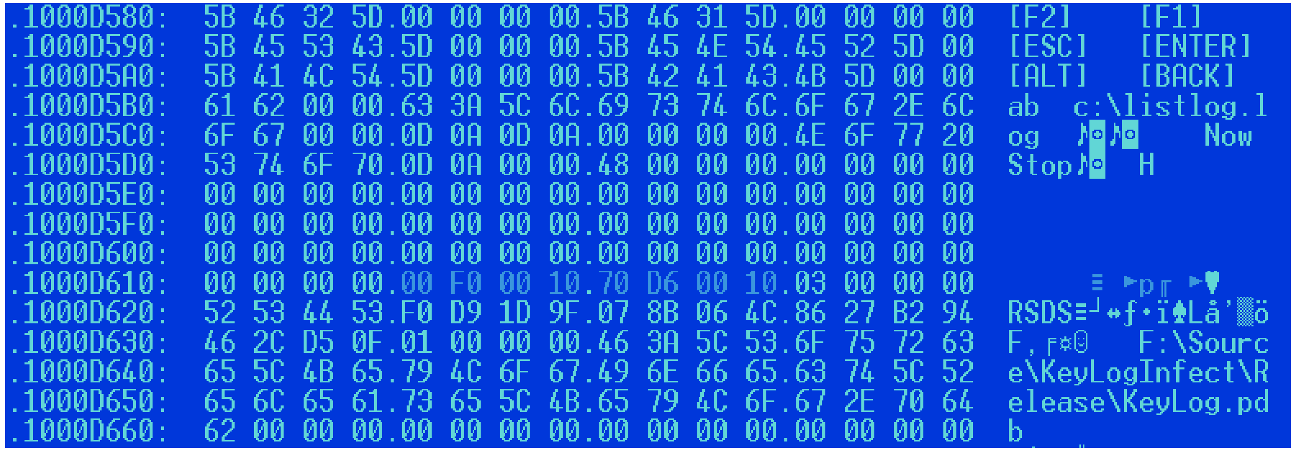
- Found in an infected system in March 2019

- RDPClient.dll (9,728 bytes)



```
.10003010:  4D 53 4E 20.53 68 65 6C.6C 00 00 00.5C 4B 65 79  MSN Shell   \Key
.10003020:  4C 6F 67 25.30 35 64 2E.64 61 74 00.49 6E 73 74  Log%05d.dat Inst
.10003030:  61 6C 6C 20.48 6F 6F 6B.20 53 75 63.63 65 73 73  all Hook Success
.10003040:  66 75 6C 6C.79 0D 0A 00.46 61 69 6C.20 54 6F 20  fully♪◙ Fail To
.10003050:  43 72 65 61.74 65 20 4B.65 79 20 4C.6F 67 20 54  Create Key Log T
.10003060:  68 72 65 61.64 0D 0A 00.4B 65 79 4C.6F 67 20 41  hread♪◙ KeyLog A
.10003070:  6C 72 65 61.64 79 20 52.75 6E 6E 69.6E 67 0D 0A  lready Running♪◙
.10003080:  00 00 00 00.54 68 65 20.48 6F 6F 6B.20 49 73 20      The Hook Is
.10003090:  53 74 6F 70.70 65 64 20.53 75 63 63.65 73 73 66  Stopped Successf
.100030A0:  75 6C 6C 79.0D 0A 00 00.46 61 69 6C.20 54 6F 20  ully♪◙  Fail To
.100030B0:  55 6E 69 6E.73 74 61 6C.6C 20 48 6F.6F 6B 0D 0A  Uninstall Hook♪◙
.100030C0:  00 00 00 00.5B 46 25 69.5D 00 00 00.5B 4E 55 4D      [F%i]   [NUM
.100030D0:  2D 25 69 5D.00 00 00 00.5B 43 54 52.4C 2B 43 5D  -%i]    [CTRL+C]
.100030E0:  0D 0A 00 00.5B 52 57 49.4E 5D 00 00.5B 4C 57 49  ♪◙  [RWIN]  [LWI
.100030F0:  4E 5D 00 00.5B 48 45 4C.50 5D 00 00.5B 44 45 4C  N]  [HELP]  [DEL
.10003100:  5D 00 00 00.5B 49 4E 53.45 52 54 5D.00 00 00 00  ]   [INSERT]
.10003110:  5B 49 4E 53.5D 00 00 00.5B 45 58 45.43 55 54 45  [INS]   [EXECUTE
.10003120:  5D 00 00 00.5B 53 45 4C.45 43 54 5D.00 00 00 00  ]   [SELECT]
```

- KeyLog.dll (62,464 bytes): F:₩Source₩KeyLogInfect₩Release₩KeyLog.pdb'

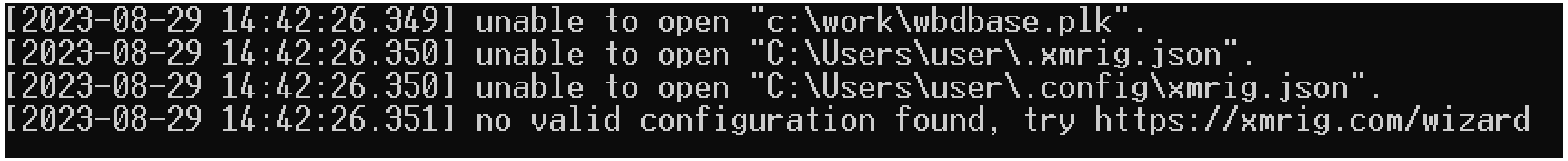


```
.1000D580:  5B 46 32 5D.00 00 00 00.5B 46 31 5D.00 00 00 00  [F2]    [F1]
.1000D590:  5B 45 53 43.5D 00 00 00.5B 45 4E 54.45 52 5D 00  [ESC]   [ENTER]
.1000D5A0:  5B 41 4C 54.5D 00 00 00.5B 42 41 43.4B 5D 00 00  [ALT]   [BACK]
.1000D5B0:  61 62 00 00.63 3A 5C 6C.69 73 74 6C.6F 67 2E 6C  ab  c:\listlog.l
.1000D5C0:  6F 67 00 00.0D 0A 0D 0A.00 00 00 00.4E 6F 77 20  og  ♪◙♪◙    Now
.1000D5D0:  53 74 6F 70.0D 0A 00 00.48 00 00 00.00 00 00 00  Stop♪◙  H
.1000D5E0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.1000D5F0:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.1000D600:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.1000D610:  00 00 00 00.00 F0 00 10.70 D6 00 10.03 00 00 00       ≡ ►p╓ ►♥
.1000D620:  52 53 44 53.F0 D9 1D 9F.07 8B 06 4C.86 27 B2 94  RSDS≡┘↔ƒ•ï♠Lå'▓ö
.1000D630:  46 2C D5 0F.01 00 00 00.46 3A 5C 53.6F 75 72 63  F,╒☼☺   F:\Sourc
.1000D640:  65 5C 4B 65.79 4C 6F 67.49 6E 66 65.63 74 5C 52  e\KeyLogInfect\R
.1000D650:  65 6C 65 61.73 65 5C 4B.65 79 4C 6F.67 2E 70 64  elease\KeyLog.pd
.1000D660:  62 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00  b
```

* md5 : 359f09a1313e79aebf93bf3109e7afd9, 06961fa526d26403f1d894fdf45346a5

Miner

- Miner
  - Found in some systems after 2021
  - Requires the additional files wbdbase.plk and .xmrig.json to run

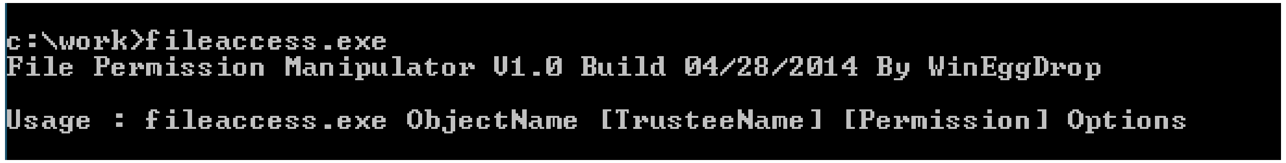


```
[2023-08-29 14:42:26.349] unable to open "c:\work\wbdbase.plk".
[2023-08-29 14:42:26.350] unable to open "C:\Users\user\.xmrig.json".
[2023-08-29 14:42:26.350] unable to open "C:\Users\user\.config\xmrig.json".
[2023-08-29 14:42:26.351] no valid configuration found, try https://xmrig.com/wizard
```

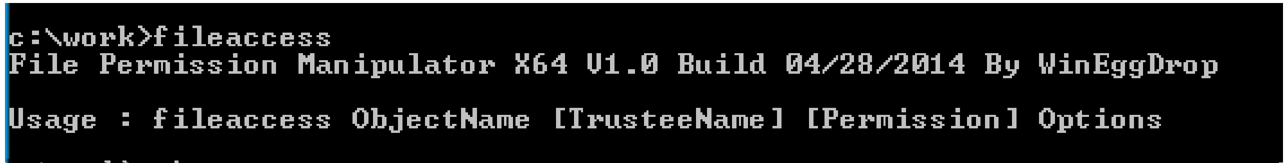
* md5 : 5bfc7795c4e7bfff983854d09586d821

Other Tools

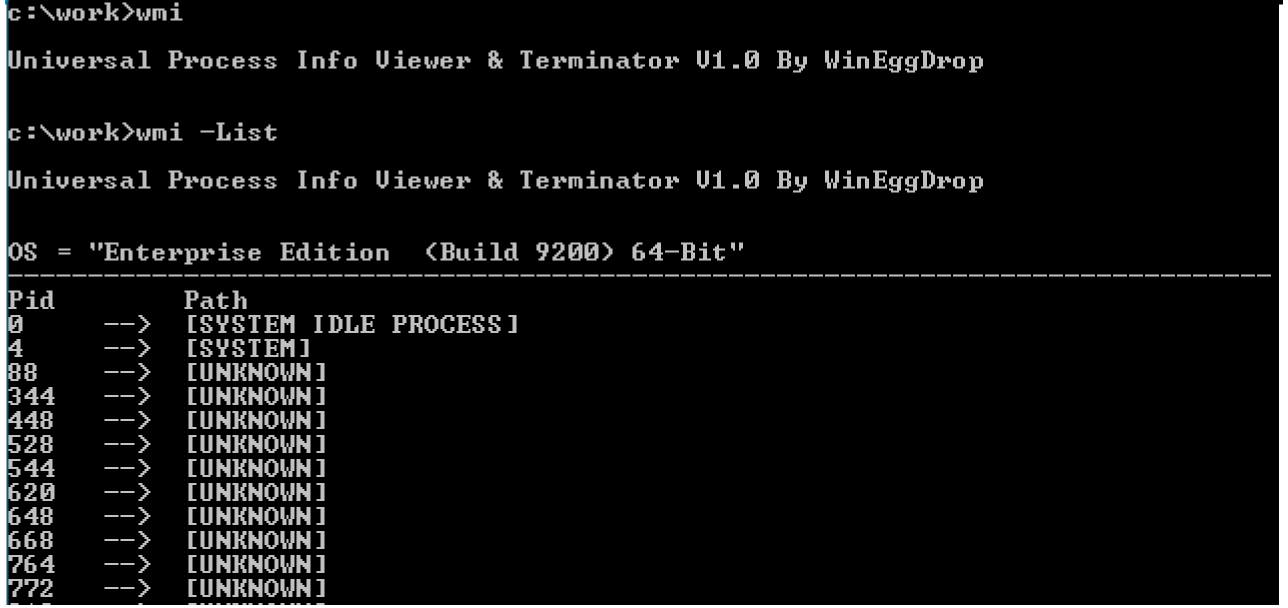
- Various tools
  - File permission, process information, service information, IPC scanner, log deletion



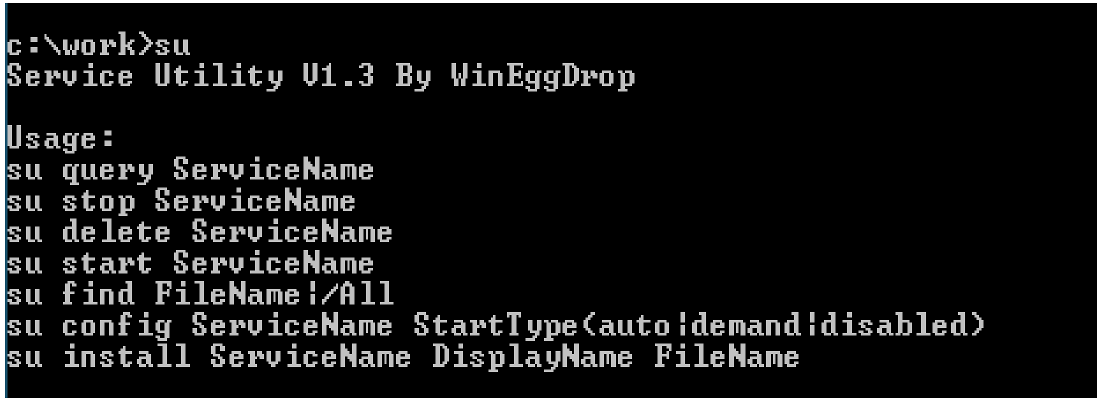
```
c:\work>fileaccess.exe
File Permission Manipulator V1.0 Build 04/28/2014 By WinEggDrop

Usage : fileaccess.exe ObjectName [TrusteeName] [Permission] Options
```



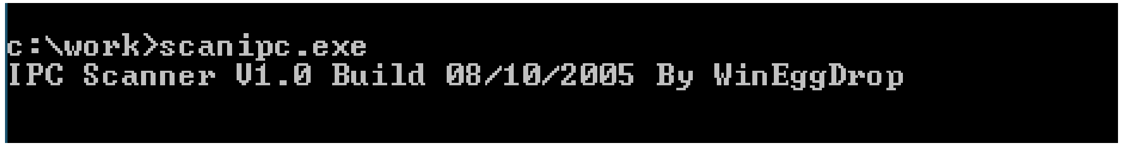
```
c:\work>fileaccess
File Permission Manipulator X64 V1.0 Build 04/28/2014 By WinEggDrop

Usage : fileaccess ObjectName [TrusteeName] [Permission] Options
```



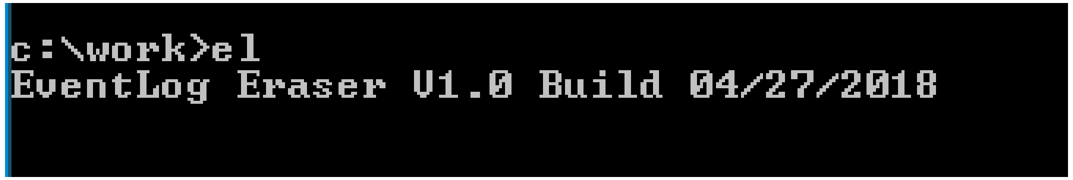
```
c:\work>wmi

Universal Process Info Viewer & Terminator V1.0 By WinEggDrop


c:\work>wmi -List

Universal Process Info Viewer & Terminator V1.0 By WinEggDrop


OS = "Enterprise Edition  (Build 9200) 64-Bit"
-------------------------------------------------------------------------------
Pid        Path
0     -->  [SYSTEM IDLE PROCESS]
4     -->  [SYSTEM]
88    -->  [UNKNOWN]
344   -->  [UNKNOWN]
448   -->  [UNKNOWN]
528   -->  [UNKNOWN]
544   -->  [UNKNOWN]
620   -->  [UNKNOWN]
648   -->  [UNKNOWN]
668   -->  [UNKNOWN]
764   -->  [UNKNOWN]
772   -->  [UNKNOWN]
```



```
c:\work>su
Service Utility V1.3 By WinEggDrop

Usage:
su query ServiceName
su stop ServiceName
su delete ServiceName
su start ServiceName
su find FileName¦/All
su config ServiceName StartType(auto¦demand¦disabled)
su install ServiceName DisplayName FileName
```



```
c:\work>scanipc.exe
IPC Scanner V1.0 Build 08/10/2005 By WinEggDrop
```



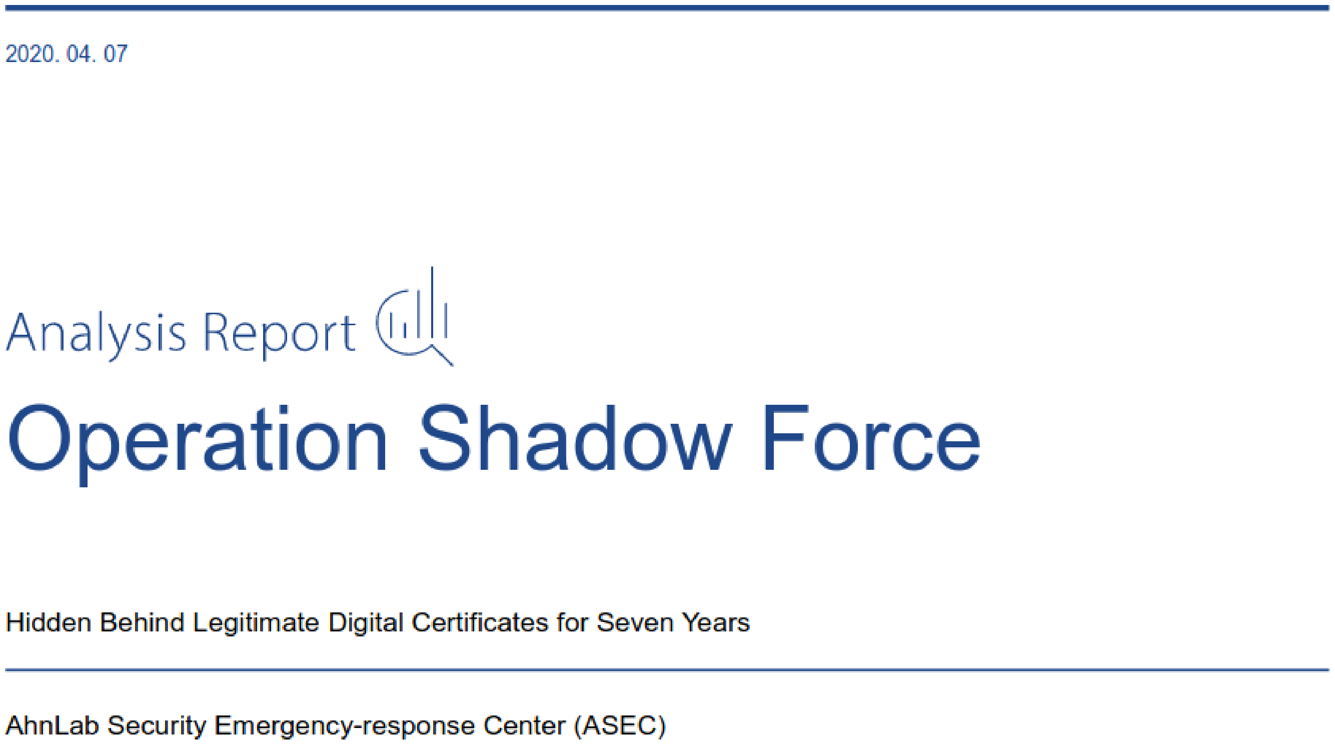
```
c:\work>el
EventLog Eraser V1.0 Build 04/27/2018
```

5
Maggie (WIP19)

Shadow Force Report

- Operation Shadow Force

 - Published in 2020 and 2022 in Korea



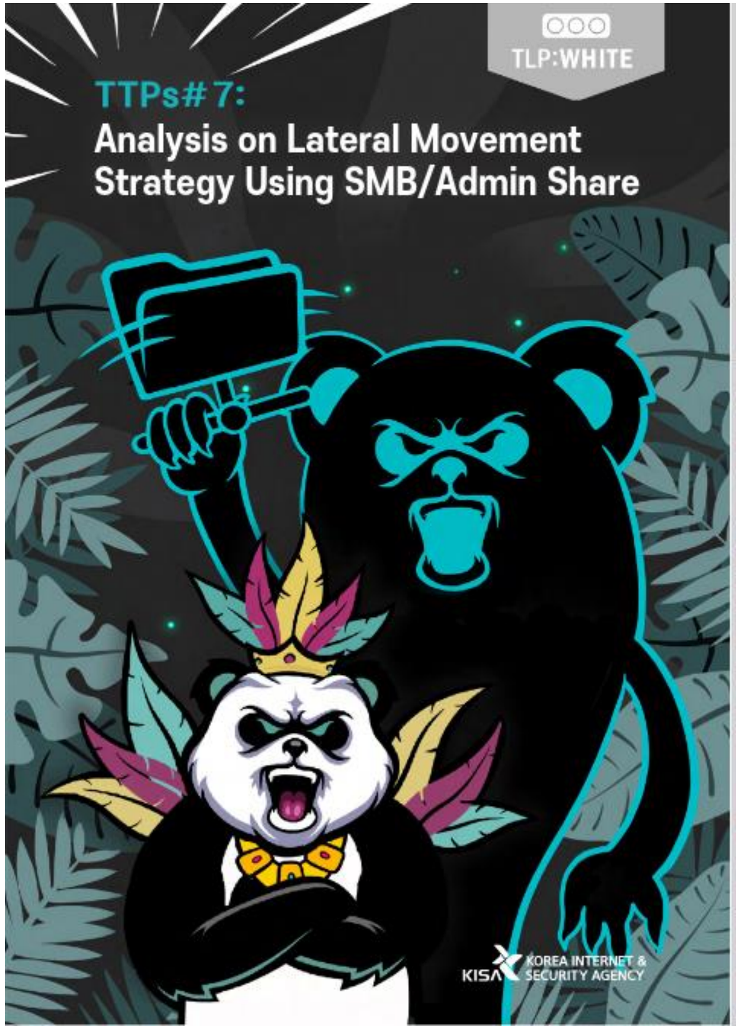
2020. 04. 07

Analysis Report

Operation Shadow Force

Hidden Behind Legitimate Digital Certificates for Seven Years

AhnLab Security Emergency-response Center (ASEC)



TLP:WHITE

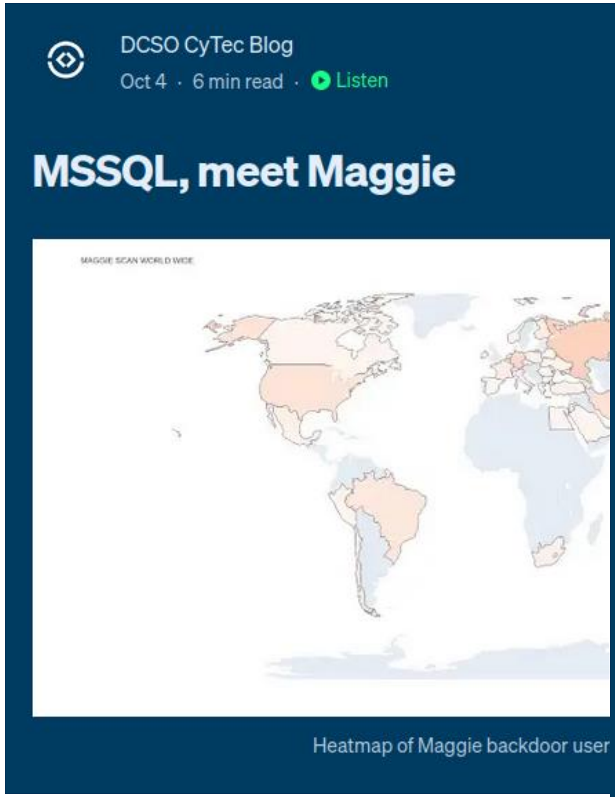
TTPs#7:

Analysis on Lateral Movement Strategy Using SMB/Admin Share

* Source: https://download.ahnlab.com/global/brochure/[Analysis_Report]Operation_Shadow_Force.pdf , https://www.boho.or.kr/en/bbs/view.do?searchCnd=&bbsId=B0001041&searchWrd=&menuNo=205083&pageIndex=1&categoryCode=&nttId=66921

WIP19 - Maggie

- Maggie
  - Infects MS-SQL servers
  - High infection rates in Asian regions including Korea

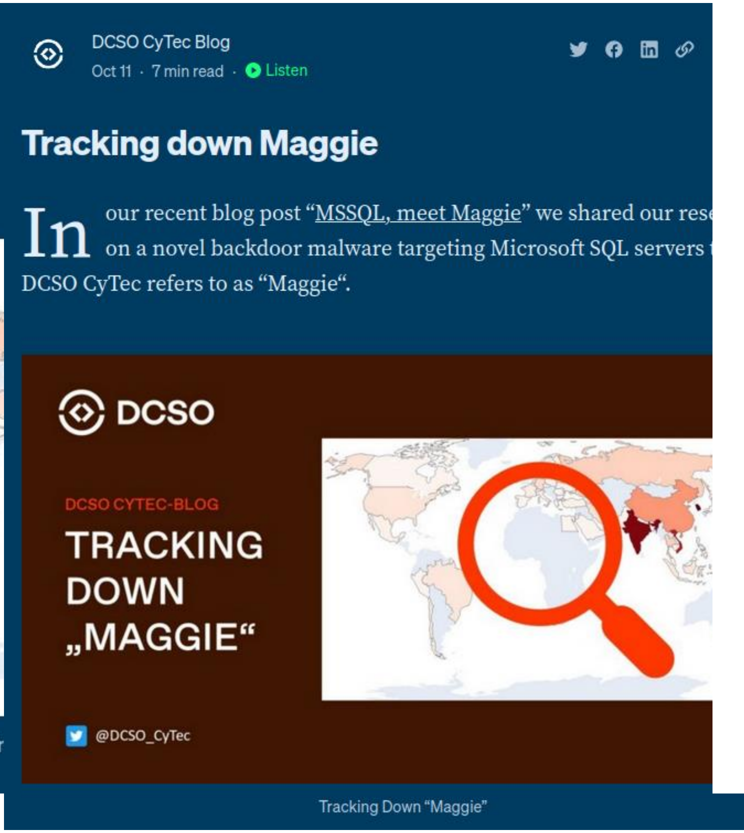


DCSO CyTec Blog

Oct 4 · 6 min read · Listen

MSSQL, meet Maggie

Heatmap of Maggie backdoor user



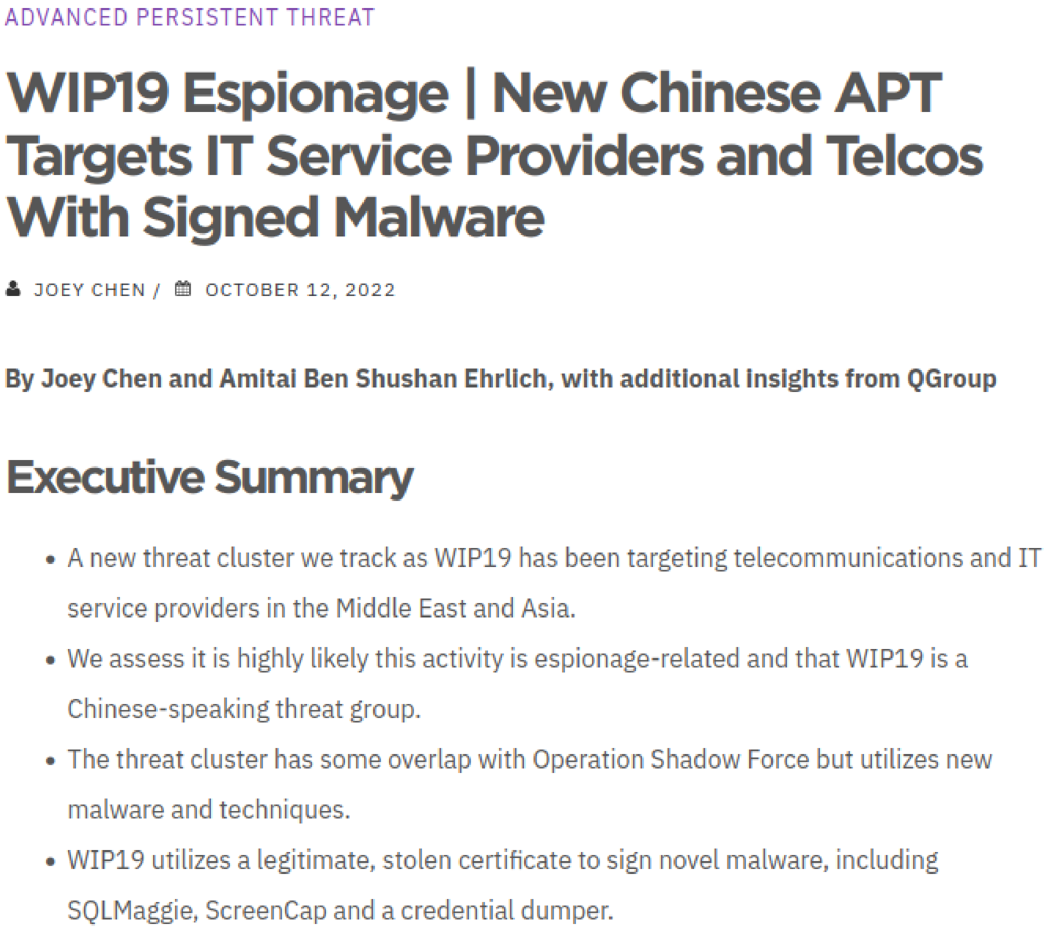
DCSO CyTec Blog

Oct 11 · 7 min read · Listen

Tracking down Maggie

In our recent blog post "MSSQL, meet Maggie" we shared our rese on a novel backdoor malware targeting Microsoft SQL servers t DCSO CyTec refers to as "Maggie".

Tracking Down "Maggie"



ADVANCED PERSISTENT THREAT

WIP19 Espionage | New Chinese APT Targets IT Service Providers and Telcos With Signed Malware

JOEY CHEN / OCTOBER 12, 2022

By Joey Chen and Amitai Ben Shushan Ehrlich, with additional insights from QGroup

Executive Summary

- A new threat cluster we track as WIP19 has been targeting telecommunications and IT service providers in the Middle East and Asia.
- We assess it is highly likely this activity is espionage-related and that WIP19 is a Chinese-speaking threat group.
- The threat cluster has some overlap with Operation Shadow Force but utilizes new malware and techniques.
- WIP19 utilizes a legitimate, stolen certificate to sign novel malware, including SQLMaggie, ScreenCap and a credential dumper.

* Source: https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01 , https://medium.com/@DCSO_CyTec/tracking-down-maggie-4d889872513d , https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/

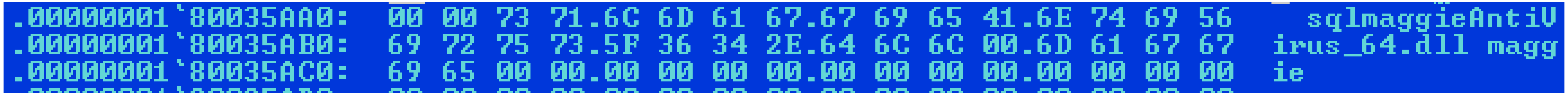
Maggie (SQL Extended Procedure, MSSQL Procedure)

- Maggie

 - Detected since March 2020

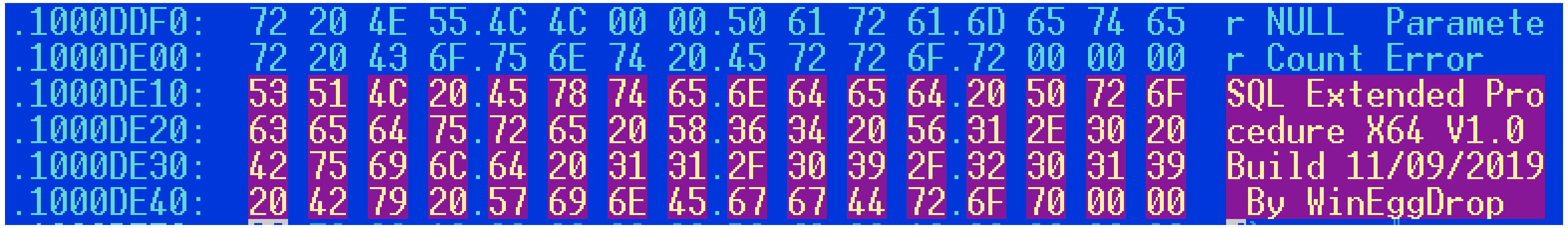
- File names: ExtendedProcedure.dll, infectsocks.dll, mpfter.cat, mssql32.log, **NTUser.dat**, ReadMe.txt, sql.dat, sql_ep.dll, sql_exp64.dll, sqlext.pnf, sqlmaggieAntivirus_64.dll, xp_examples.dll, xp_exampleX64.dll, etc.

  - Export functions: Maggie, sql_ep_door, xp_example



```
.00000001`80035AA0:  00 00 73 71.6C 6D 61 67.67 69 65 41.6E 74 69 56    sqlmaggieAntiV
.00000001`80035AB0:  69 72 75 73.5F 36 34 2E.64 6C 6C 00.6D 61 67 67   irus_64.dll magg
.00000001`80035AC0:  69 65 00 00.00 00 00 00.00 00 00 00.00 00 00 00   ie
```

- Some early version of variants include the string "SQL Extended Procedure X64 V1.0 Build 11/09/2019 By WinEggDrop"



```
.1000DDF0:  72 20 4E 55.4C 4C 00 00.50 61 72 61.6D 65 74 65  r NULL  Paramete
.1000DE00:  72 20 43 6F.75 6E 74 20.45 72 72 6F.72 00 00 00  r Count Error
.1000DE10:  53 51 4C 20.45 78 74 65.6E 64 65 64.20 50 72 6F  SQL Extended Pro
.1000DE20:  63 65 64 75.72 65 20 58.36 34 20 56.31 2E 30 20  cedure X64 V1.0
.1000DE30:  42 75 69 6C.64 20 31 31.2F 30 39 2F.32 30 31 39  Build 11/09/2019
.1000DE40:  20 42 79 20.57 69 6E 45.67 67 44 72.6F 70 00 00   By WinEggDrop
```

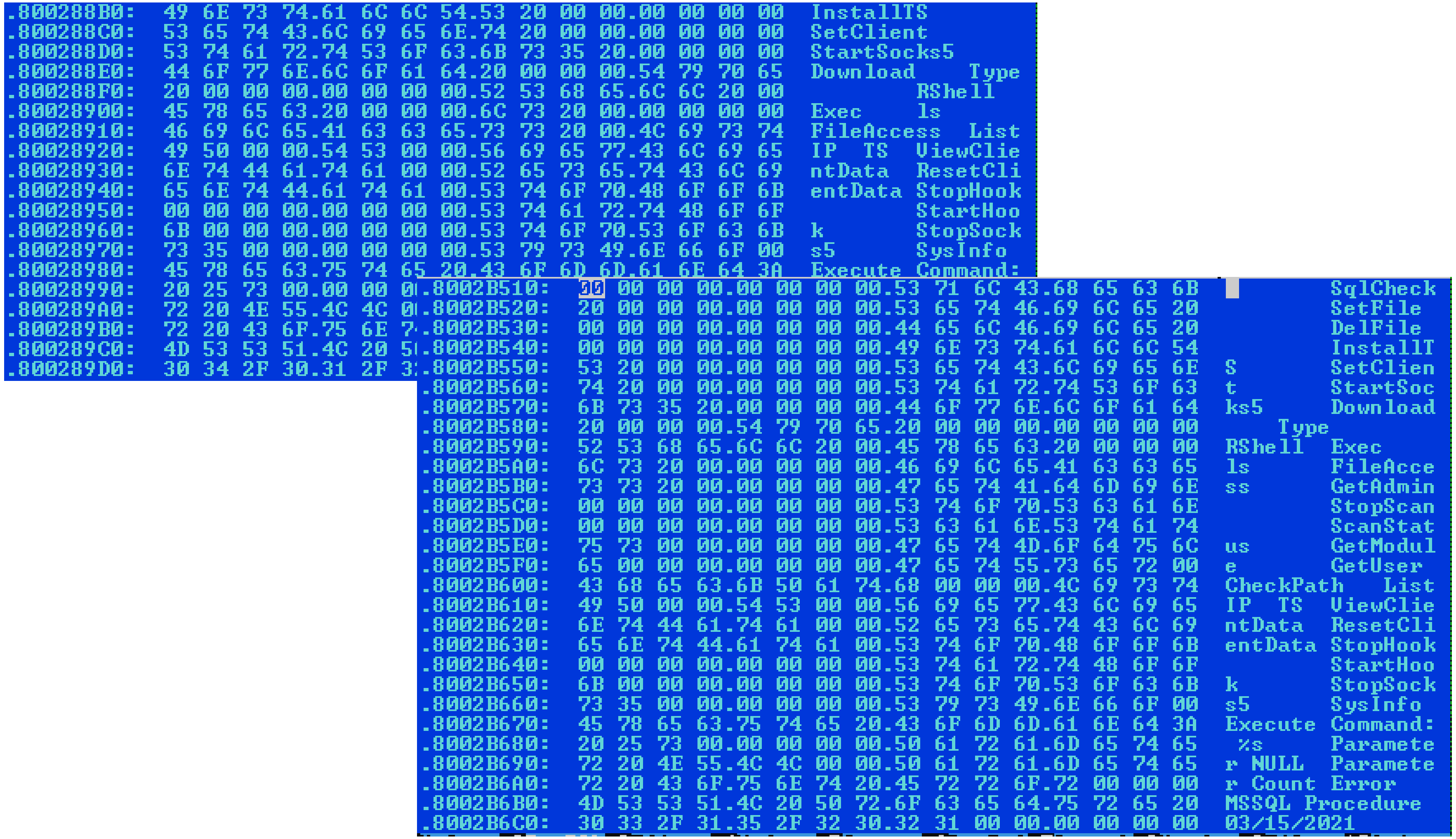
 - Includes the string "MSSQL Procedure" after 2020

 - Extended Stored Procedure (ESP) type used in SQL servers -> Loaded in SQL servers and can be controlled with SQL queries (no C2)

 - Some variants discovered after April 2022 are signed with the certificate of a Korean software developer.

Maggie (SQL Extended Procedure, MSSQL Procedure)

- Major commands (still being added)
  - File management (properties, deletion, execution)
  - Reverse Shell
  - Download
  - SOCKS5 server
  - SQL Server
  - System information
  - TermServ



```
.800288B0:  49 6E 73 74.61 6C 6C 54.53 20 00 00.00 00 00 00  InstallTS
.800288C0:  53 65 74 43.6C 69 65 6E.74 20 00 00.00 00 00 00  SetClient
.800288D0:  53 74 61 72.74 53 6F 63.6B 73 35 20.00 00 00 00  StartSocks5
.800288E0:  44 6F 77 6E.6C 6F 61 64.20 00 00 00.54 79 70 65  Download    Type
.800288F0:  20 00 00 00.00 00 00 00.52 53 68 65.6C 6C 20 00              RShell
.80028900:  45 78 65 63.20 00 00 00.6C 73 20 00.00 00 00 00  Exec        ls
.80028910:  46 69 6C 65.41 63 63 65.73 73 20 00.4C 69 73 74  FileAccess  List
.80028920:  49 50 00 00.54 53 00 00.56 69 65 77.43 6C 69 65  IP  TS      ViewClie
.80028930:  6E 74 44 61.74 61 00 00.52 65 73 65.74 43 6C 69  ntData      ResetCli
.80028940:  65 6E 74 44.61 74 61 00.53 74 6F 70.48 6F 6F 6B  entData     StopHook
.80028950:  00 00 00 00.00 00 00 00.53 74 61 72.74 48 6F 6F              StartHoo
.80028960:  6B 00 00 00.00 00 00 00.53 74 6F 70.53 6F 63 6B  k           StopSock
.80028970:  73 35 00 00.00 00 00 00.53 79 73 49.6E 66 6F 00  s5          SysInfo
.80028980:  45 78 65 63.75 74 65 20.43 6F 6D 6D.61 6E 64 3A  Execute     Command:
.80028990:  20 25 73 00.00 00 0
.800289A0:  72 20 4E 55.4C 4C 0
.800289B0:  72 20 43 6F.75 6E 7
.800289C0:  4D 53 53 51.4C 20 5
.800289D0:  30 34 2F 30.31 2F 3
```

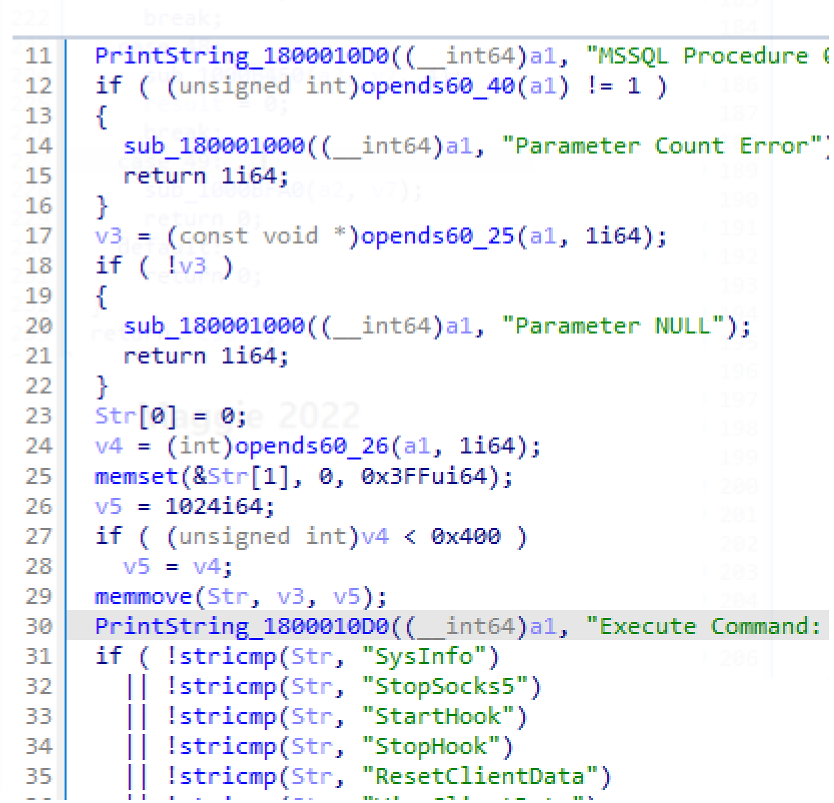
```
.8002B510:  00 00 00 00.00 00 00 00.53 71 6C 43.68 65 63 6B              SqlCheck
.8002B520:  20 00 00 00.00 00 00 00.53 65 74 46.69 6C 65 20              SetFile
.8002B530:  00 00 00 00.00 00 00 00.44 65 6C 46.69 6C 65 20              DelFile
.8002B540:  00 00 00 00.00 00 00 00.49 6E 73 74.61 6C 6C 54              InstallT
.8002B550:  53 20 00 00.00 00 00 00.53 65 74 43.6C 69 65 6E  S           SetClien
.8002B560:  74 20 00 00.00 00 00 00.53 74 61 72.74 53 6F 63  t           StartSoc
.8002B570:  6B 73 35 20.00 00 00 00.44 6F 77 6E.6C 6F 61 64  ks5         Download
.8002B580:  20 00 00 00.54 79 70 65.20 00 00 00.00 00 00 00      Type
.8002B590:  52 53 68 65.6C 6C 20 00.45 78 65 63.20 00 00 00  RShell      Exec
.8002B5A0:  6C 73 20 00.00 00 00 00.46 69 6C 65.41 63 63 65  ls          FileAcce
.8002B5B0:  73 73 20 00.00 00 00 00.47 65 74 41.64 6D 69 6E  ss          GetAdmin
.8002B5C0:  00 00 00 00.00 00 00 00.53 74 6F 70.53 63 61 6E              StopScan
.8002B5D0:  00 00 00 00.00 00 00 00.53 63 61 6E.53 74 61 74              ScanStat
.8002B5E0:  75 73 00 00.00 00 00 00.47 65 74 4D.6F 64 75 6C  us          GetModul
.8002B5F0:  65 00 00 00.00 00 00 00.47 65 74 55.73 65 72 00  e           GetUser
.8002B600:  43 68 65 63.6B 50 61 74.68 00 00 00.4C 69 73 74  CheckPath   List
.8002B610:  49 50 00 00.54 53 00 00.56 69 65 77.43 6C 69 65  IP  TS      ViewClie
.8002B620:  6E 74 44 61.74 61 00 00.52 65 73 65.74 43 6C 69  ntData      ResetCli
.8002B630:  65 6E 74 44.61 74 61 00.53 74 6F 70.48 6F 6F 6B  entData     StopHook
.8002B640:  00 00 00 00.00 00 00 00.53 74 61 72.74 48 6F 6F              StartHoo
.8002B650:  6B 00 00 00.00 00 00 00.53 74 6F 70.53 6F 63 6B  k           StopSock
.8002B660:  73 35 00 00.00 00 00 00.53 79 73 49.6E 66 6F 00  s5          SysInfo
.8002B670:  45 78 65 63.75 74 65 20.43 6F 6D 6D.61 6E 64 3A  Execute     Command:
.8002B680:  20 25 73 00.00 00 00 00.50 61 72 61.6D 65 74 65   %s         Paramete
.8002B690:  72 20 4E 55.4C 4C 00 00.50 61 72 61.6D 65 74 65  r NULL      Paramete
.8002B6A0:  72 20 43 6F.75 6E 74 20.45 72 72 6F.72 00 00 00  r Count     Error
.8002B6B0:  4D 53 53 51.4C 20 50 72.6F 63 65 64.75 72 65 20  MSSQL Procedure
.8002B6C0:  30 33 2F 31.35 2F 32 30.32 31 00 00.00 00 00 00  03/15/2021
```

* Source: https://gist.github.com/usualsuspect/6667dc0053bb51e78a4594fe6185a4a5#file-commands-txt

Maggie (SQL Extended Procedure, MSSQL Procedure)

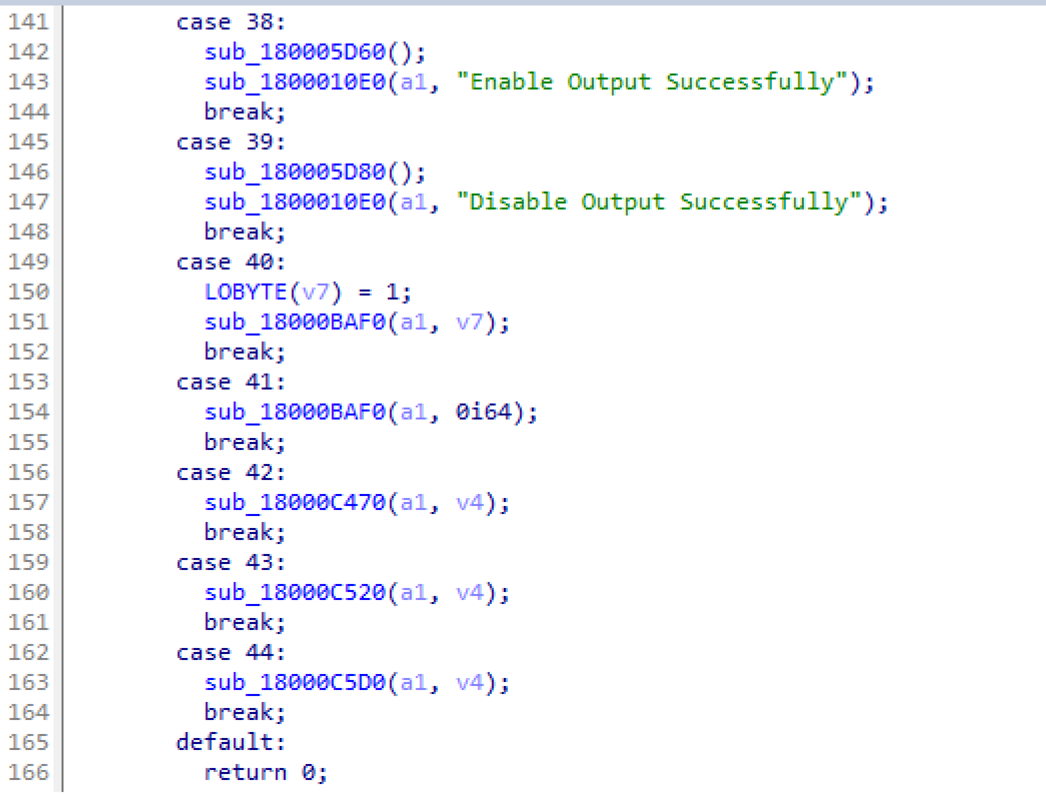
- Commands are still being added

  - 57 commands in 2023



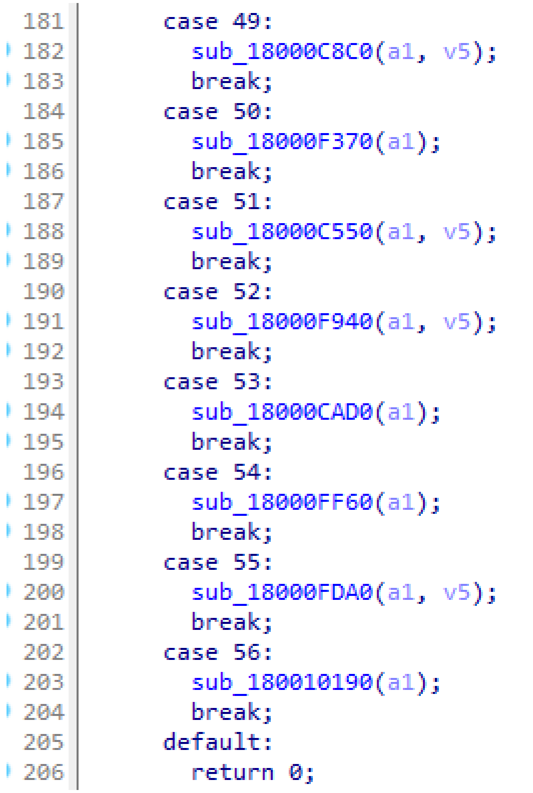
```
PrintString_1800010D0((__int64)a1, "MSSQL Procedure (
if ( (unsigned int)opends60_40(a1) != 1 )
{
  sub_180001000((__int64)a1, "Parameter Count Error")
  return 1i64;
}
v3 = (const void *)opends60_25(a1, 1i64);
if ( !v3 )
{
  sub_180001000((__int64)a1, "Parameter NULL");
  return 1i64;
}
Str[0] = 0;
v4 = (int)opends60_26(a1, 1i64);
memset(&Str[1], 0, 0x3FFui64);
v5 = 1024i64;
if ( (unsigned int)v4 < 0x400 )
  v5 = v4;
memmove(Str, v3, v5);
PrintString_1800010D0((__int64)a1, "Execute Command:
if ( !stricmp(Str, "SysInfo")
  || !stricmp(Str, "StopSocks5")
  || !stricmp(Str, "StartHook")
  || !stricmp(Str, "StopHook")
  || !stricmp(Str, "ResetClientData")
```

Maggie (2020-2021)



```
case 38:
  sub_180005D60();
  sub_1800010E0(a1, "Enable Output Successfully");
  break;
case 39:
  sub_180005D80();
  sub_1800010E0(a1, "Disable Output Successfully");
  break;
case 40:
  LOBYTE(v7) = 1;
  sub_18000BAF0(a1, v7);
  break;
case 41:
  sub_18000BAF0(a1, 0i64);
  break;
case 42:
  sub_18000C470(a1, v4);
  break;
case 43:
  sub_18000C520(a1, v4);
  break;
case 44:
  sub_18000C5D0(a1, v4);
  break;
default:
  return 0;
```

Maggie (2022)

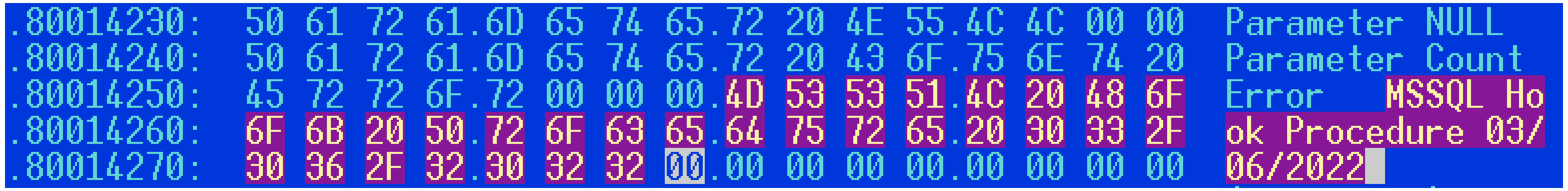


```
case 49:
  sub_18000C8C0(a1, v5);
  break;
case 50:
  sub_18000F370(a1);
  break;
case 51:
  sub_18000C550(a1, v5);
  break;
case 52:
  sub_18000F940(a1, v5);
  break;
case 53:
  sub_18000CAD0(a1);
  break;
case 54:
  sub_18000FF60(a1);
  break;
case 55:
  sub_18000FDA0(a1, v5);
  break;
case 56:
  sub_180010190(a1);
  break;
default:
  return 0;
```

Maggie (2023)

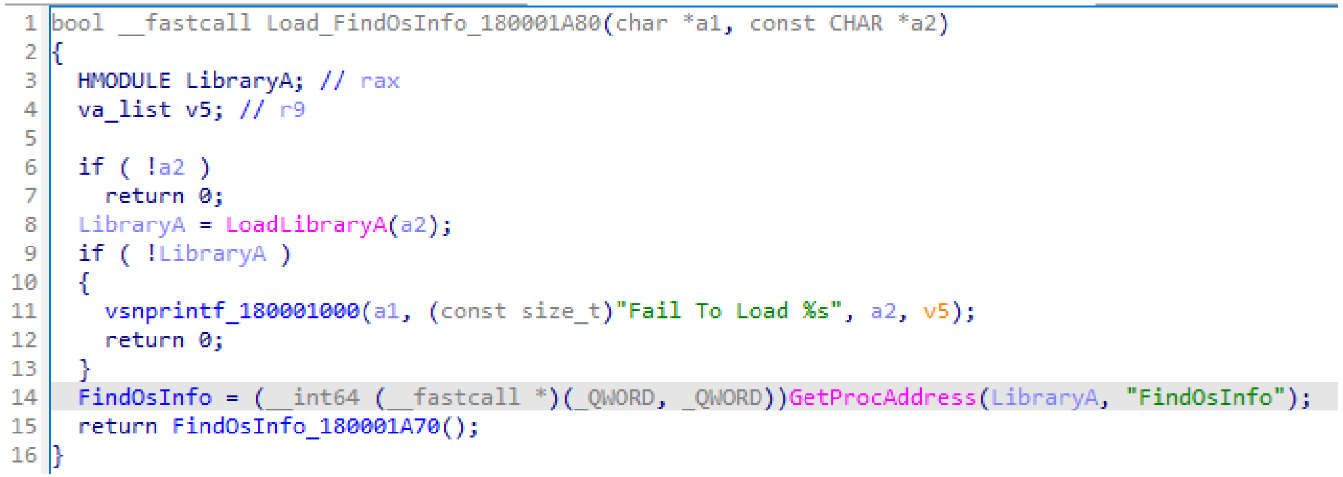
Maggie (MSSQL Hook Procedure)

- Maggie (MSSQL Hook Procedure)
  - Similar to Maggie
  - Includes "MSSQL Hook Procedure"



```
.80014230:  50 61 72 61.6D 65 74 65.72 20 4E 55.4C 4C 00 00  Parameter NULL
.80014240:  50 61 72 61.6D 65 74 65.72 20 43 6F.75 6E 74 20  Parameter Count
.80014250:  45 72 72 6F.72 00 00 00.4D 53 53 51.4C 20 48 6F  Error   MSSQL Ho
.80014260:  6F 6B 20 50.72 6F 63 65.64 75 72 65.20 30 33 2F  ok Procedure 03/
.80014270:  30 36 2F 32.30 32 32 00.00 00 00 00.00 00 00 00  06/2022
```

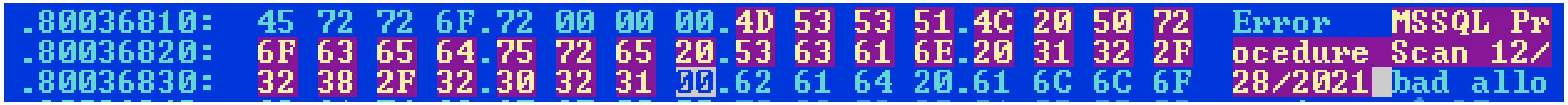
  - Export: sql_hook
  - Versions after Mar 2023 load and call osinfo.dll!FindOsInfo



```
bool __fastcall Load_FindOsInfo_180001A80(char *a1, const CHAR *a2)
{
  HMODULE LibraryA; // rax
  va_list v5; // r9

  if ( !a2 )
    return 0;
  LibraryA = LoadLibraryA(a2);
  if ( !LibraryA )
  {
    vsnprintf_180001000(a1, (const size_t)"Fail To Load %s", a2, v5);
    return 0;
  }
  FindOsInfo = (__int64 (__fastcall *)(_QWORD, _QWORD))GetProcAddress(LibraryA, "FindOsInfo");
  return FindOsInfo_180001A70();
}
```

MSSQL Procedure Scan

- MSSQL Procedure Scan
  - Includes the string "MSSQL Procedure Scan"

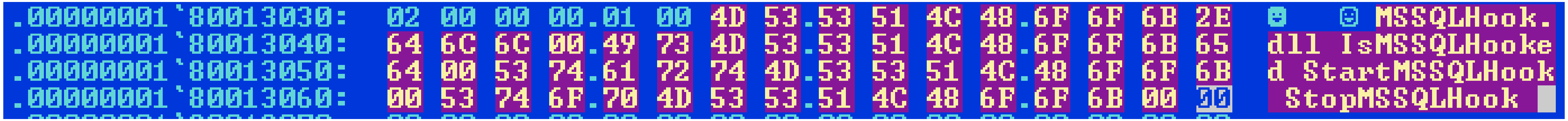


```
.80036810:  45 72 72 6F.72 00 00 00.4D 53 53 51.4C 20 50 72  Error   MSSQL Pr
.80036820:  6F 63 65 64.75 72 65 20.53 63 61 6E.20 31 32 2F  ocedure Scan 12/
.80036830:  32 38 2F 32.30 32 31 00.62 61 64 20.61 6C 6C 6F  28/2021 bad allo
```

  - Scanning features: SynScan, SqlScan, IOCPScan, SysScanAll, IOCPScanAll
  - Scans, then uploads the file Success.dat to the FTP server.
  - Session name is MelodyFTP

HookSQL (Proxy)

- MSSQLLHook
  - Uses Detour to hook certain APIs: AcceptEx, setsockopt, CreateIoCompletionPort
  - IsMSSQLHooked, StartMSSQLHook, StopMSSQLHook
  - Proxy



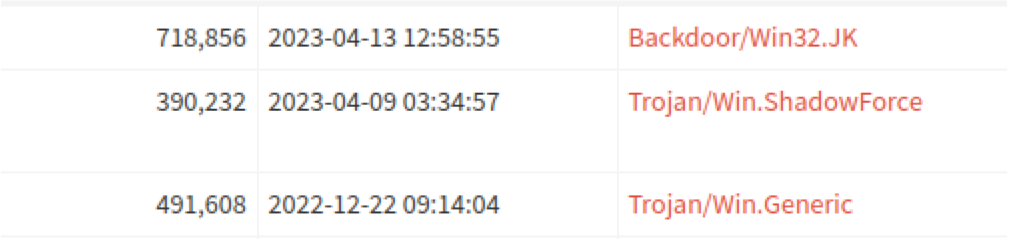
```
.00000001`80013030:  02 00 00 00.01 00 4D 53.53 51 4C 48.6F 6F 6B 2E  ☻   ☺ MSSQLHook.
.00000001`80013040:  64 6C 6C 00.49 73 4D 53.53 51 4C 48.6F 6F 6B 65  dll IsMSSQLHooke
.00000001`80013050:  64 00 53 74.61 72 74 4D.53 53 51 4C.48 6F 6F 6B  d StartMSSQLHook
.00000001`80013060:  00 53 74 6F.70 4D 53 53.51 4C 48 6F.6F 6B 00 00   StopMSSQLHook
```

Leaked Certificate

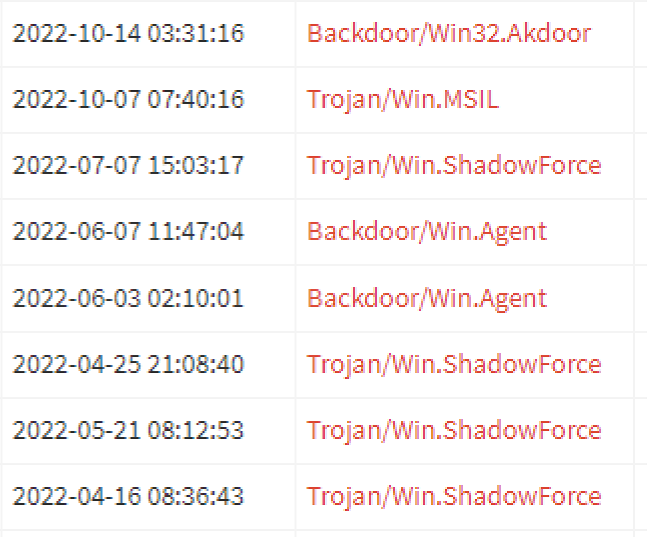
- DEEPSoft

 - Used to sign files from April 16, 2022 - April 2023

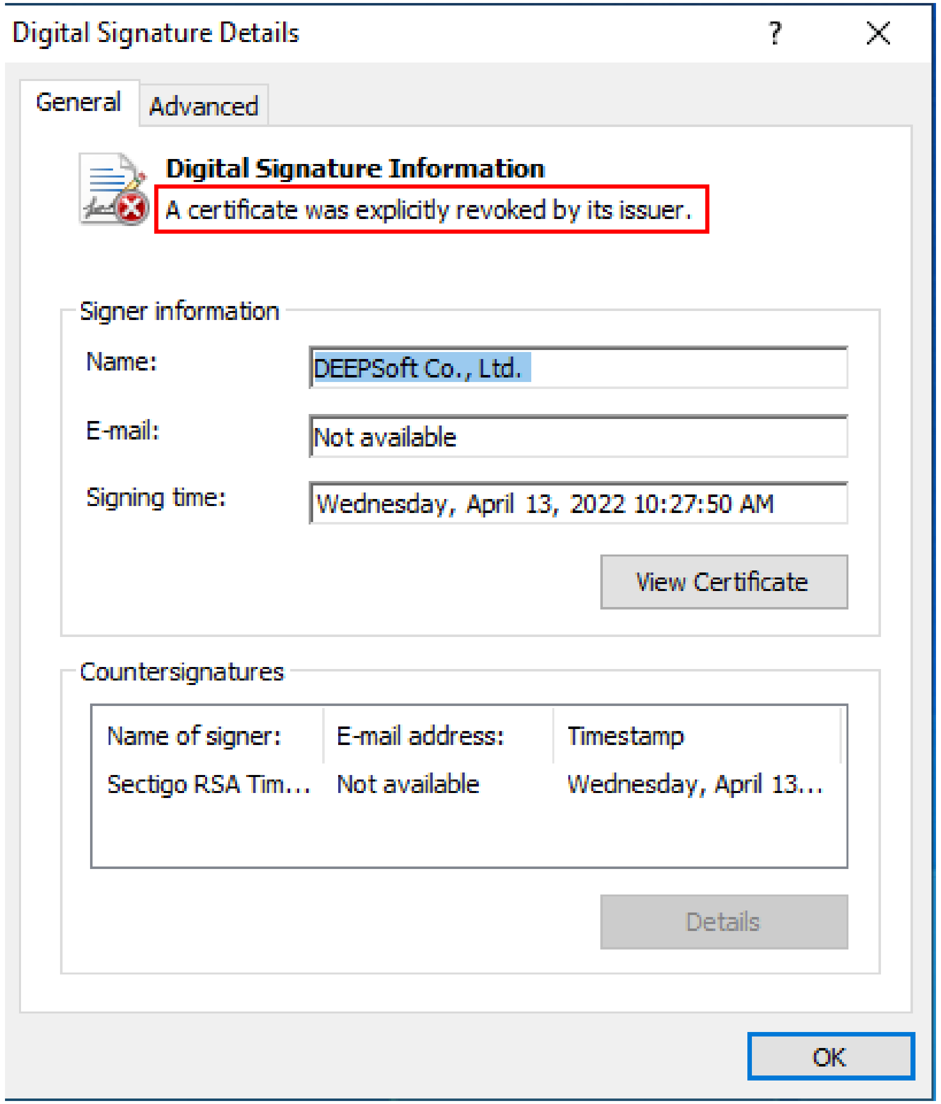
 - 10 out of 63 were found to be malware



718,856	2023-04-13 12:58:55	Backdoor/Win32.JK
390,232	2023-04-09 03:34:57	Trojan/Win.ShadowForce
491,608	2022-12-22 09:14:04	Trojan/Win.Generic



2022-10-14 03:31:16	Backdoor/Win32.Akdoor
2022-10-07 07:40:16	Trojan/Win.MSIL
2022-07-07 15:03:17	Trojan/Win.ShadowForce
2022-06-07 11:47:04	Backdoor/Win.Agent
2022-06-03 02:10:01	Backdoor/Win.Agent
2022-04-25 21:08:40	Trojan/Win.ShadowForce
2022-05-21 08:12:53	Trojan/Win.ShadowForce
2022-04-16 08:36:43	Trojan/Win.ShadowForce



Digital Signature Information

A certificate was explicitly revoked by its issuer.

Signer information

Name: DEEPSoft Co., Ltd.

E-mail: Not available

Signing time: Wednesday, April 13, 2022 10:27:50 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Sectigo RSA Tim...	Not available	Wednesday, April 13...

6
Attribution

Malware Authors

Melody

- Wgdrop

Syrinx

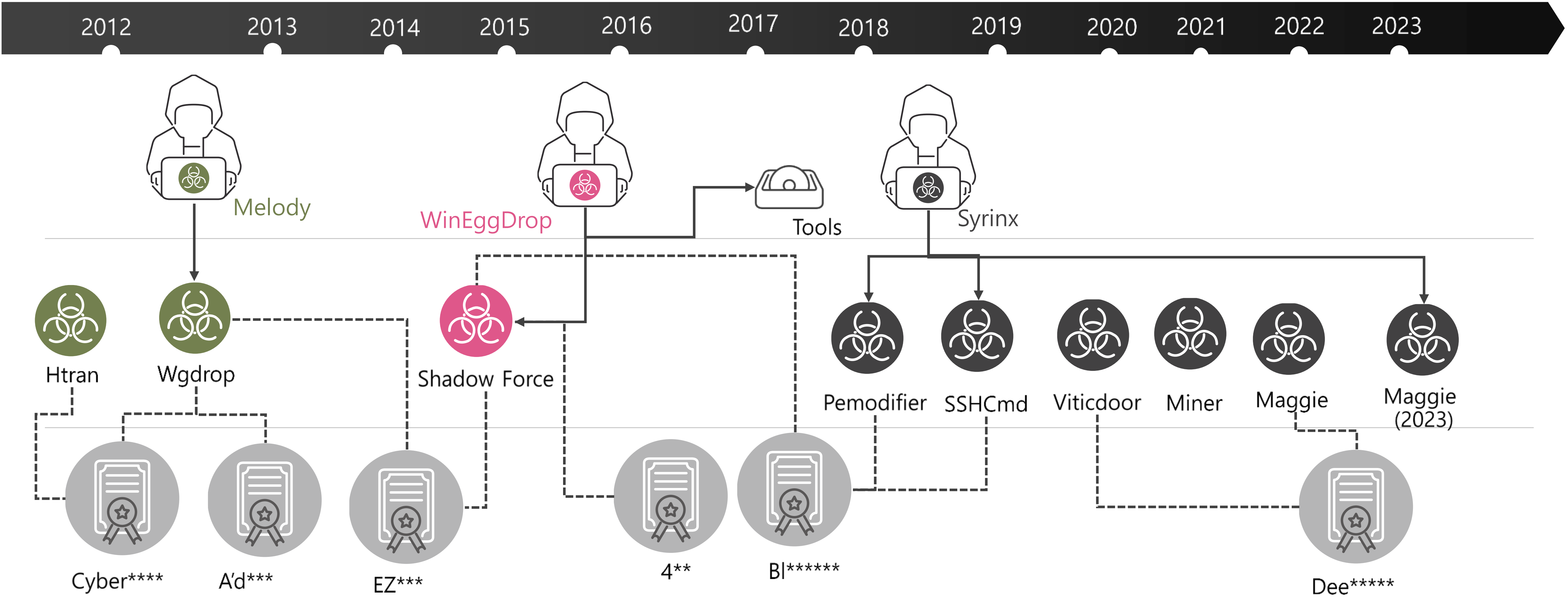
- Pemodifier
- sshcmd, SSHD
- Maggie (2023)

WinEggDrop

- Pemodifier
- Shadowforce
- Maggie (2019)
- Tools

Connections

Malware + Certificate + Writer



Relationship Between Shadow Force and Maggie

- Shadow Force and Maggie

 - Usually targets MS-SQL servers

 - Shadow Force and Maggie's codes are similar

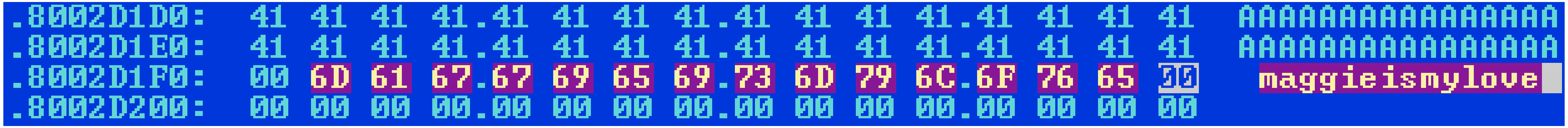
 - Shadow Force has been in use until Mar 2020 Afterward, shifted to using Maggie

 - Same author - WinEggDrop, Syrinx

 - The same tools and file names used by the Shadow Force group were used in attacks with Maggie

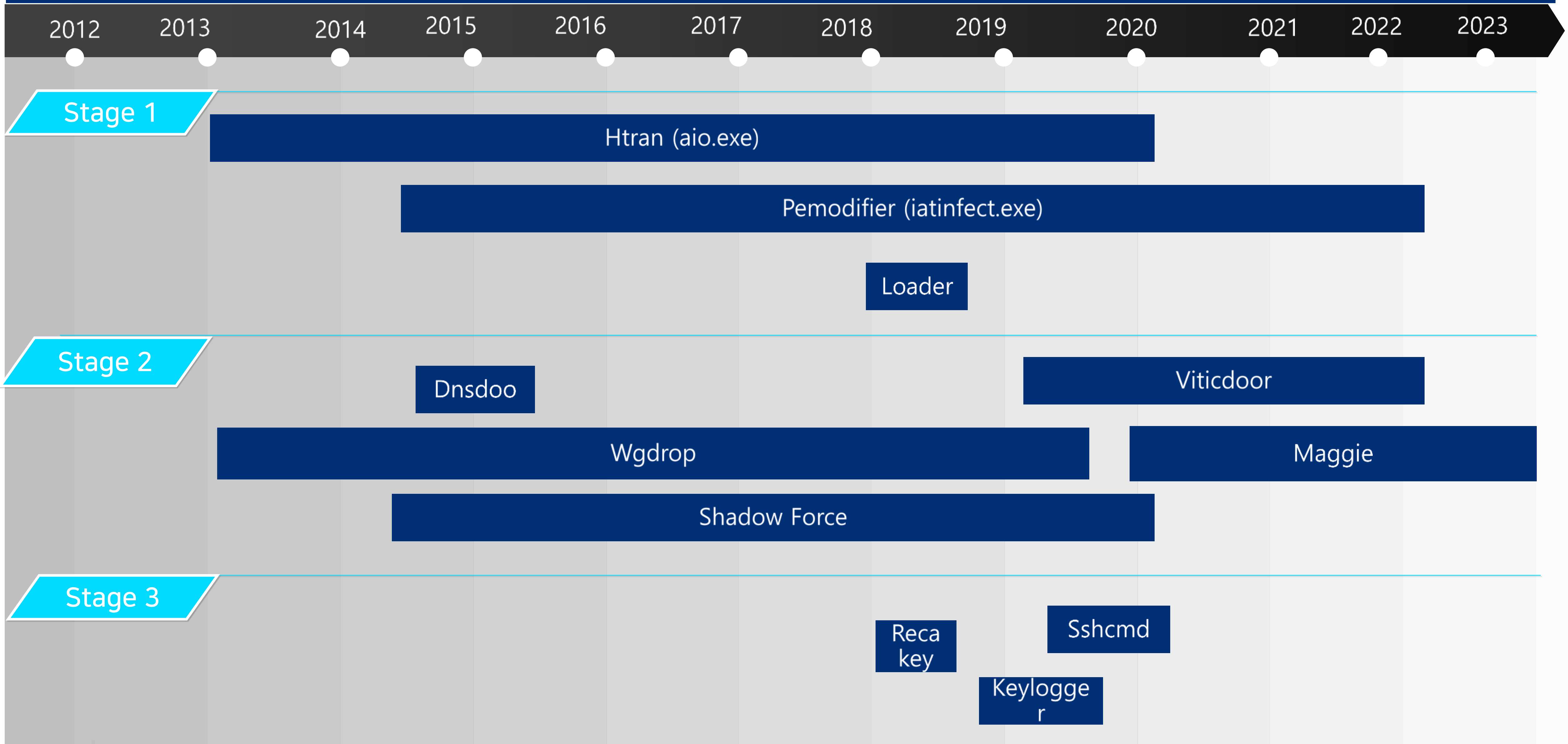
 - Conclusive evidence (?): Found in a Shadow Force variant (md5: dd3232e2924ae6a11c393c27713d5873) discovered in Mar 2020

The string "maggieismylove"



```
.8002D1D0:  41 41 41 41.41 41 41 41.41 41 41 41.41 41 41 41   AAAAAAAAAAAAAAAA
.8002D1E0:  41 41 41 41.41 41 41 41.41 41 41 41.41 41 41 41   AAAAAAAAAAAAAAAA
.8002D1F0:  00 6D 61 67.67 69 65 69.73 6D 79 6C.6F 76 65 00    maggieismylove
.8002D200:  00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
```

Shadow Force Group = Operation Shadow Force + Maggie



2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

Stage 1

Htran (aio.exe)

Pemodifier (iatinfect.exe)

Loader

Stage 2

Dnsdoo

Viticdoor

Wgdrop

Maggie

Shadow Force

Stage 3

Reca key

Sshcmd

Keylogge r

7
Conclusion

AhnLab

Takeaways

- Shadow Force Group (Operation Shadow Force)
  - Mainly active in Korea from 2013 - present (2023)
  - Authors : Melody, Syrinx, WinEggDrop
  - No clear attack vector identified (SQL server vulnerability suspected)
  - Malware signed with forged (4NB, CyberLink, PandoraTV) and leaked (A'digm, blueside, EZNIX) digital certificates
  - Consists of PE modifier, backdoor, keylogger, and tools
  - Process: Server intrusion via unidentified routes -> Downloads additional malware with Htran (aio.exe) -> Patches certain EXE files with Pemodifier (iatinfect.exe) -> Loads a malicious DLL when patched EXE is run -> Installs coin miner (after 2021)
- Maggie
  - Attacks MS-SQL servers (exact attack vectors are not known)
  - Infected MS-SQL servers in the Asia-Pacific region including Korea and Japan
  - Close resemblance to the Shadow Force Group including the coding style, author names, file names, and the use of the same tools
- Questions
  - What is their specific attack vector, and is only South Korea targeted? Why is there no information?

Contact

Thank you for your attention!

CHA Minseok (Jacky)

- minseok.cha@ahnlab.com
- mstoned7@gmail.com
- 𝕏 @mstoned7

LEE Jaejin

- jaejin.lee@ahnlab.com

KIM Junseok

- junseok.kim@ahnlab.com

Reference

- Shadow Force Uses DLL Hijacking, Targets South Korean Company (https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company)
- MSSQL, meet Maggie (https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01)
- Tracking down Maggie (https://medium.com/@DCSO_CyTec/tracking-down-maggie-4d889872513d)
- WIP19 Espionage | New Chinese APT Targets IT Service Providers and Telcos With Signed Malware (https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/)

More security, More freedom

AhnLab