VB 2024

The Mask Has Been Unmasked Again

Georgy Kucherin
Marc Rivero Lopez
Kaspersky GReAT

The World of APTs

DarkHotel

APT31

Equation

Winnti

APT35

The Mask

Turla

Lazarus

APT29

APT28

Sofacy

Regin

The World of APTs

DarkHotel

APT31

Equation

Winnti

APT35

Turla

The Mask

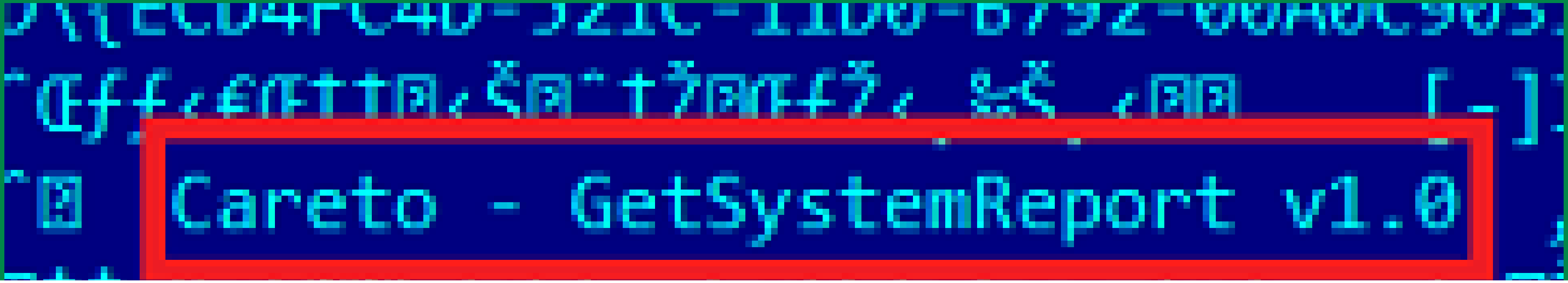
Lazarus

APT29

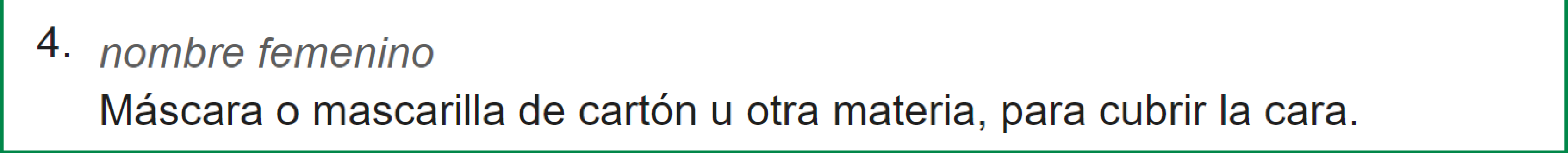
Sofacy

Regin

This APT speaks Spanish!

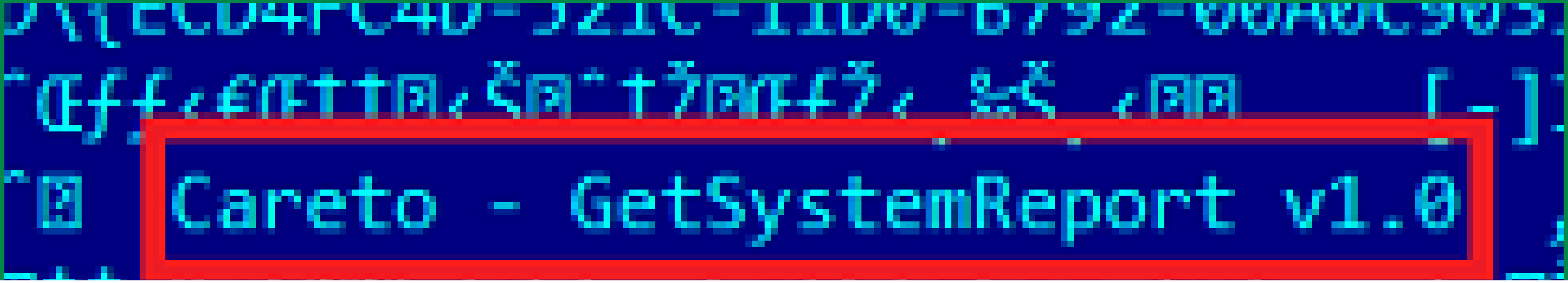


```
Careto - GetSystemReport v1.0
```



4. *nombre femenino*
   Máscara o mascarilla de cartón u otra materia, para cubrir la cara.

This APT speaks Spanish!



```
Careto - GetSystemReport v1.0
```

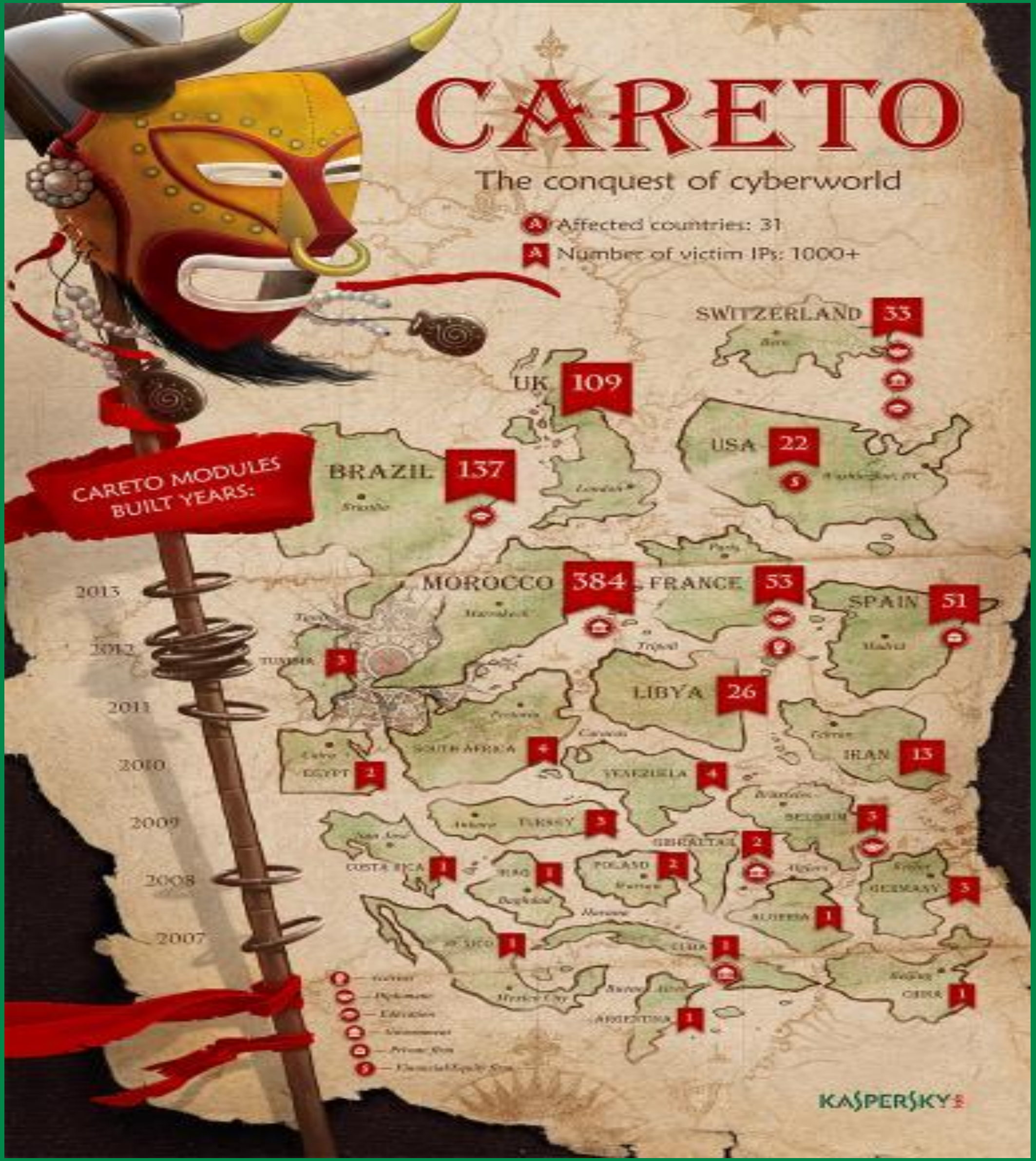
4. *nombre femenino*

   Máscara o mascarilla de cartón u otra materia, para cubrir la cara.

4 . *female name*

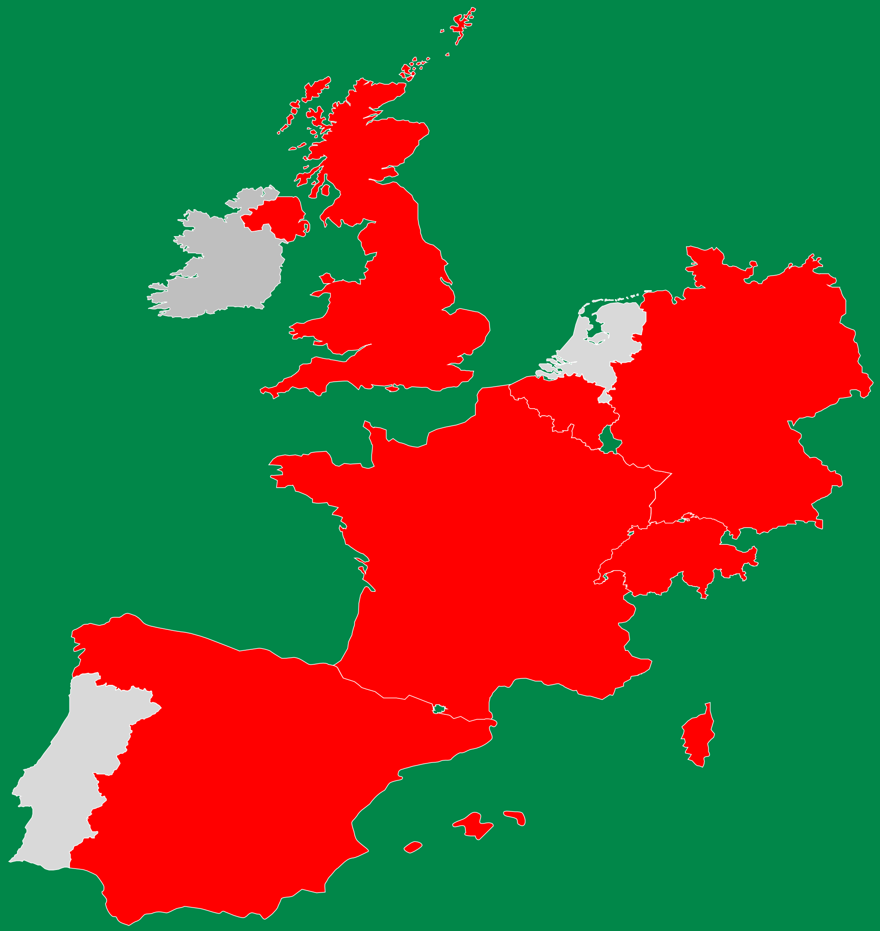
   Mask or face covering made of cardboard or other material, to cover the face.

A bit of history



- **First seen:** 2007
- **Discovered:** 2014
- **Victims:** government, diplomatic, energy sectors, activists

A bit of history

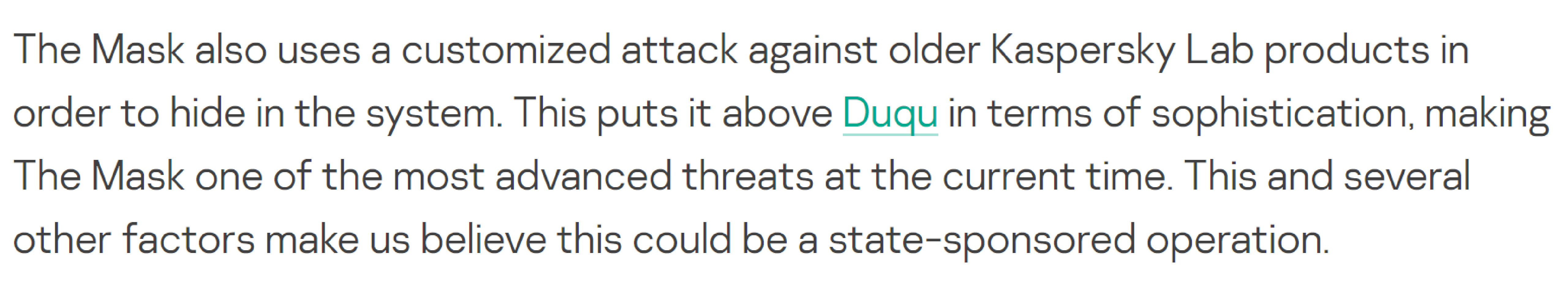


Targeted countries In Western Europe

Notable regions affected:

- Europe (but not Ireland!)
- Latin America
- Middle East

A bit of history

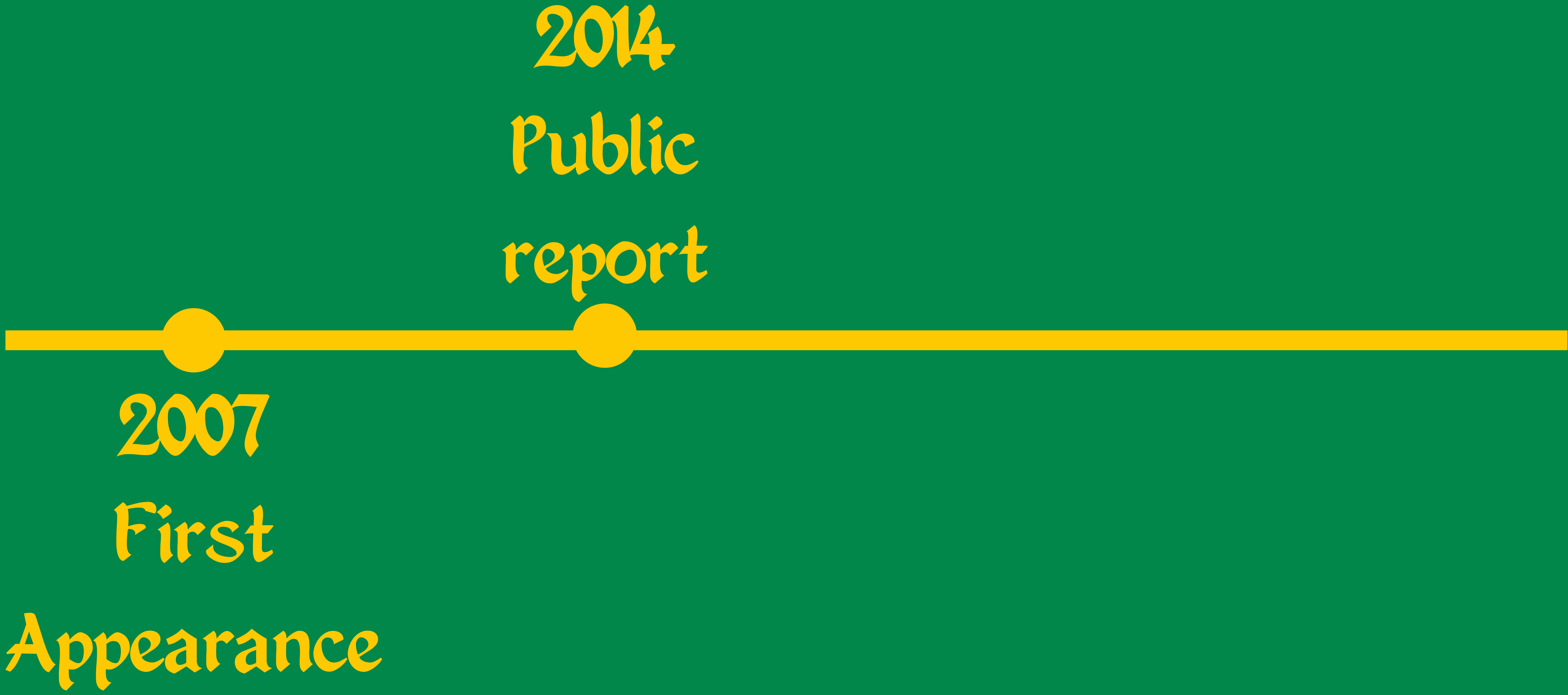


The Mask also uses a customized attack against older Kaspersky Lab products in order to hide in the system. This puts it above Duqu in terms of sophistication, making The Mask one of the most advanced threats at the current time. This and several other factors make us believe this could be a state-sponsored operation.

Very sophisticated!

- Advanced malware
- Custom rootkits
- Vulnerabilities in Kaspersky solutions

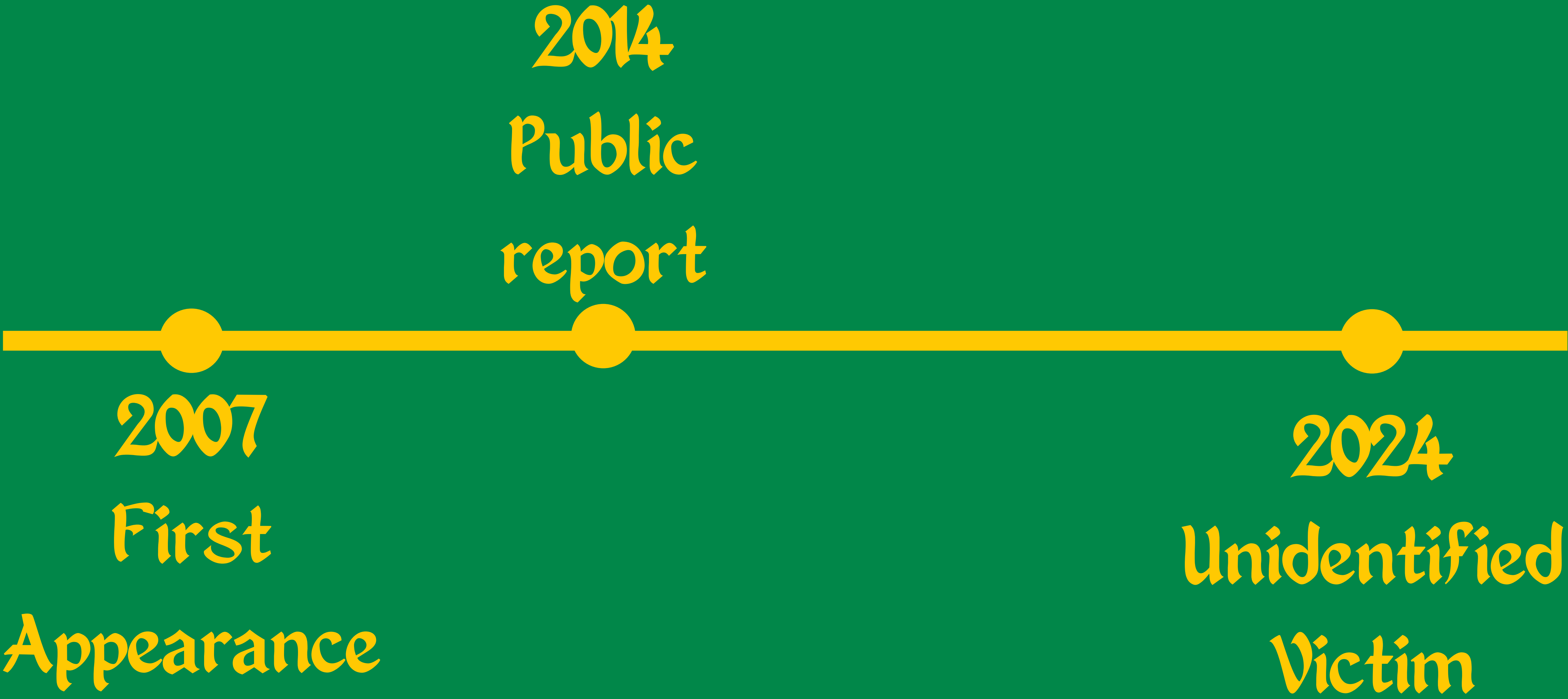
The great comeback



2014
Public
report

2007
First
Appearance

The great comeback

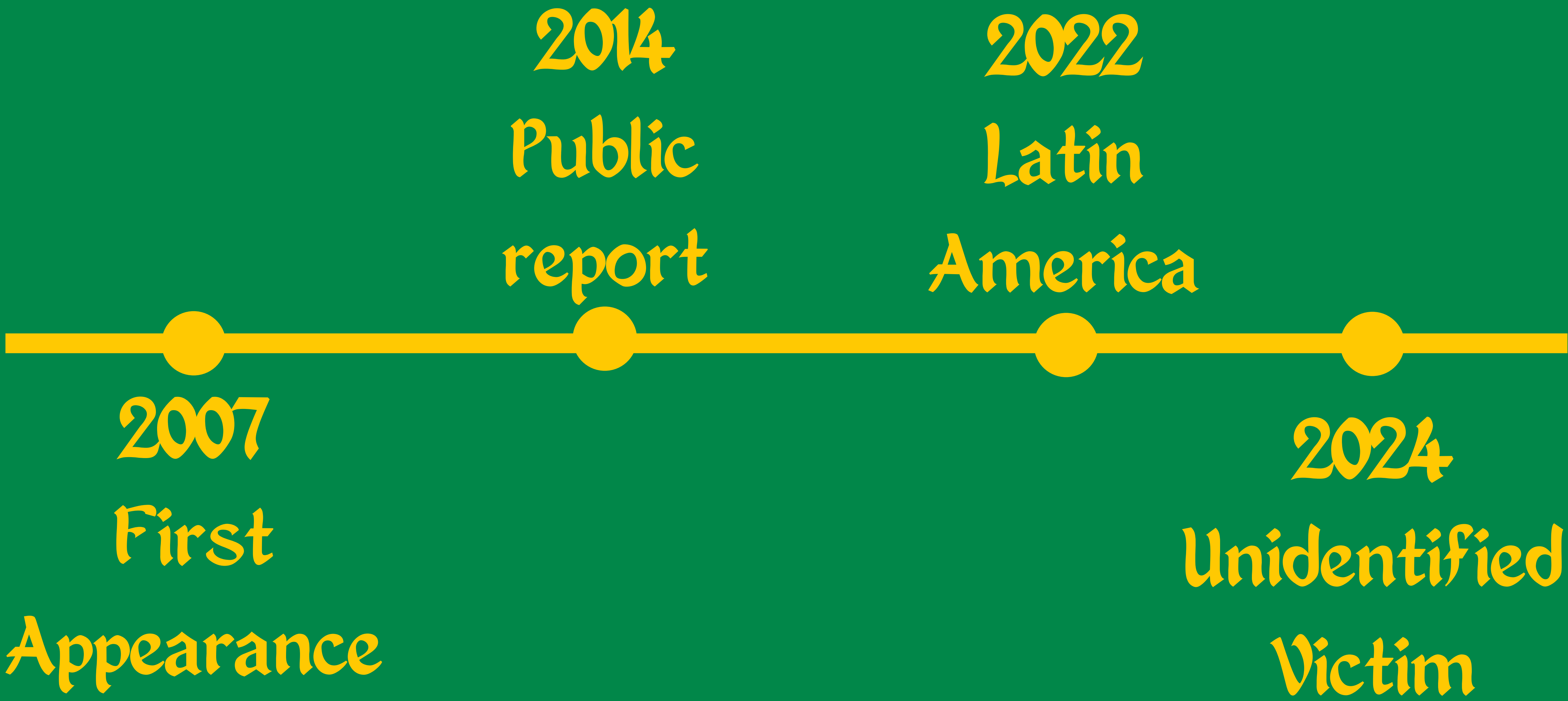


2014
Public
report

2007
First
Appearance

2024
Unidentified
Victim

The great comeback



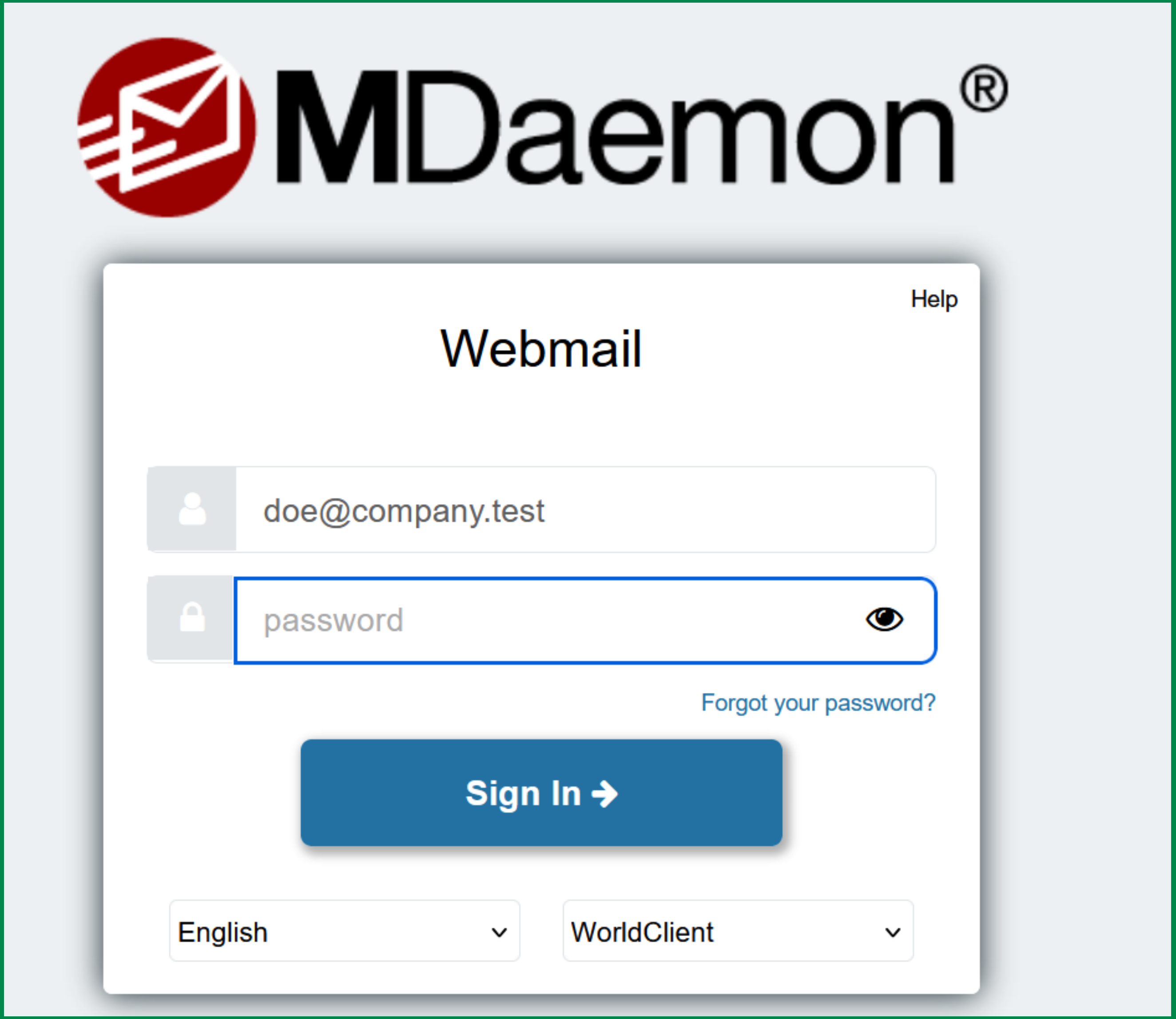
2007
First
Appearance

2014
Public
report

2022
Latin
America

2024
Unidentified
Victim

Internet-facing email server



MDaemon®

Help

Webmail

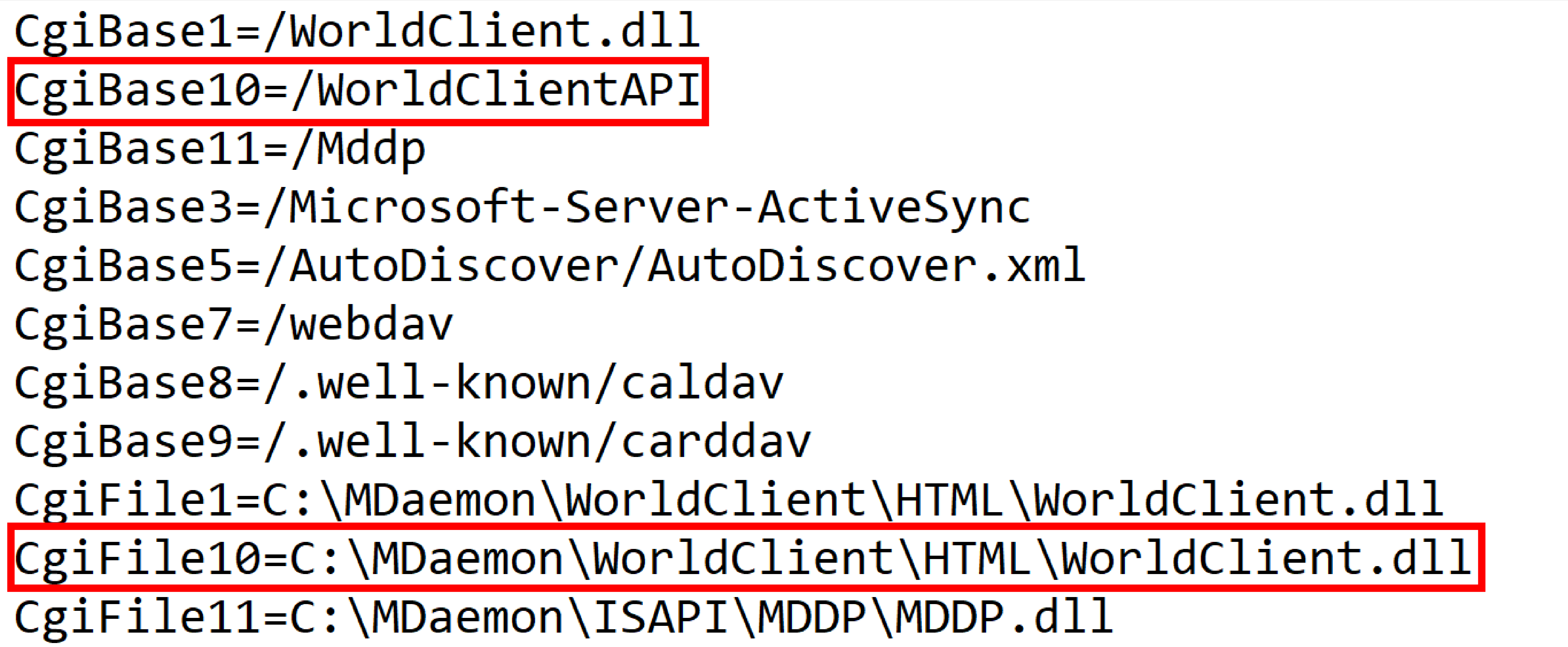
doe@company.test

password

Extension configuration

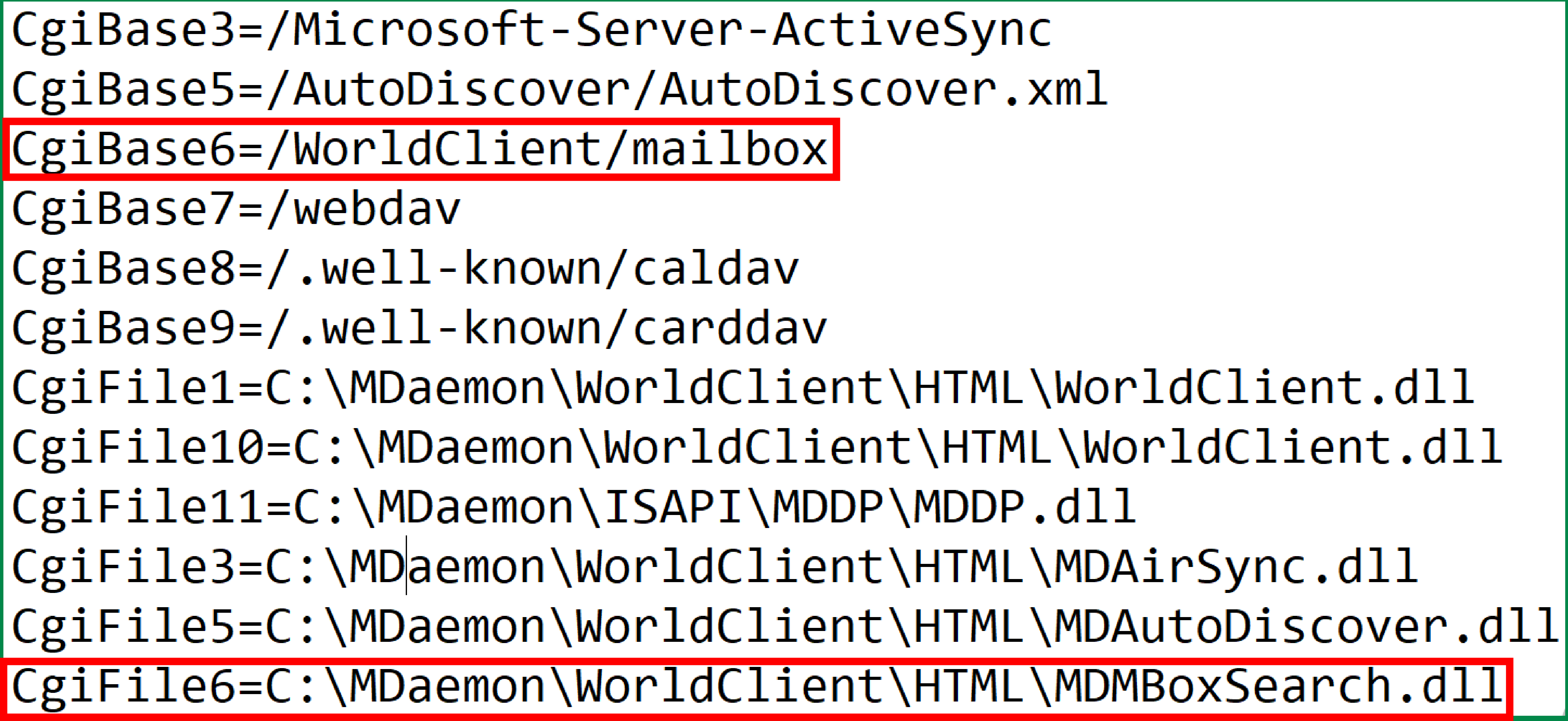
```
CgiBase1=/WorldClient.dll
CgiBase10=/WorldClientAPI
CgiBase11=/Mddp
CgiBase3=/Microsoft-Server-ActiveSync
CgiBase5=/AutoDiscover/AutoDiscover.xml
CgiBase7=/webdav
CgiBase8=/.well-known/caldav
CgiBase9=/.well-known/carddav
CgiFile1=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile10=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile11=C:\MDaemon\ISAPI\MDDP\MDDP.dll
```

Extension configuration



```
CgiBase1=/WorldClient.dll
CgiBase10=/WorldClientAPI
CgiBase11=/Mddp
CgiBase3=/Microsoft-Server-ActiveSync
CgiBase5=/AutoDiscover/AutoDiscover.xml
CgiBase7=/webdav
CgiBase8=/.well-known/caldav
CgiBase9=/.well-known/carddav
CgiFile1=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile10=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile11=C:\MDaemon\ISAPI\MDDP\MDDP.dll
```

A sneaky modification



```
CgiBase3=/Microsoft-Server-ActiveSync
CgiBase5=/AutoDiscover/AutoDiscover.xml
CgiBase6=/WorldClient/mailbox
CgiBase7=/webdav
CgiBase8=/.well-known/caldav
CgiBase9=/.well-known/carddav
CgiFile1=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile10=C:\MDaemon\WorldClient\HTML\WorldClient.dll
CgiFile11=C:\MDaemon\ISAPI\MDDP\MDDP.dll
CgiFile3=C:\MDaemon\WorldClient\HTML\MDAirSync.dll
CgiFile5=C:\MDaemon\WorldClient\HTML\MDAutoDiscover.dll
CgiFile6=C:\MDaemon\WorldClient\HTML\MDMBoxSearch.dll
```

Activities performed

SAM Stealing

```
reg save \\<IP>\hklm\sam c:\windows\temp\msarp.tmp
```

Copying documents

```
copy "\\<IP>\<document>" %Temp%\pkcskes082022.tmp
```

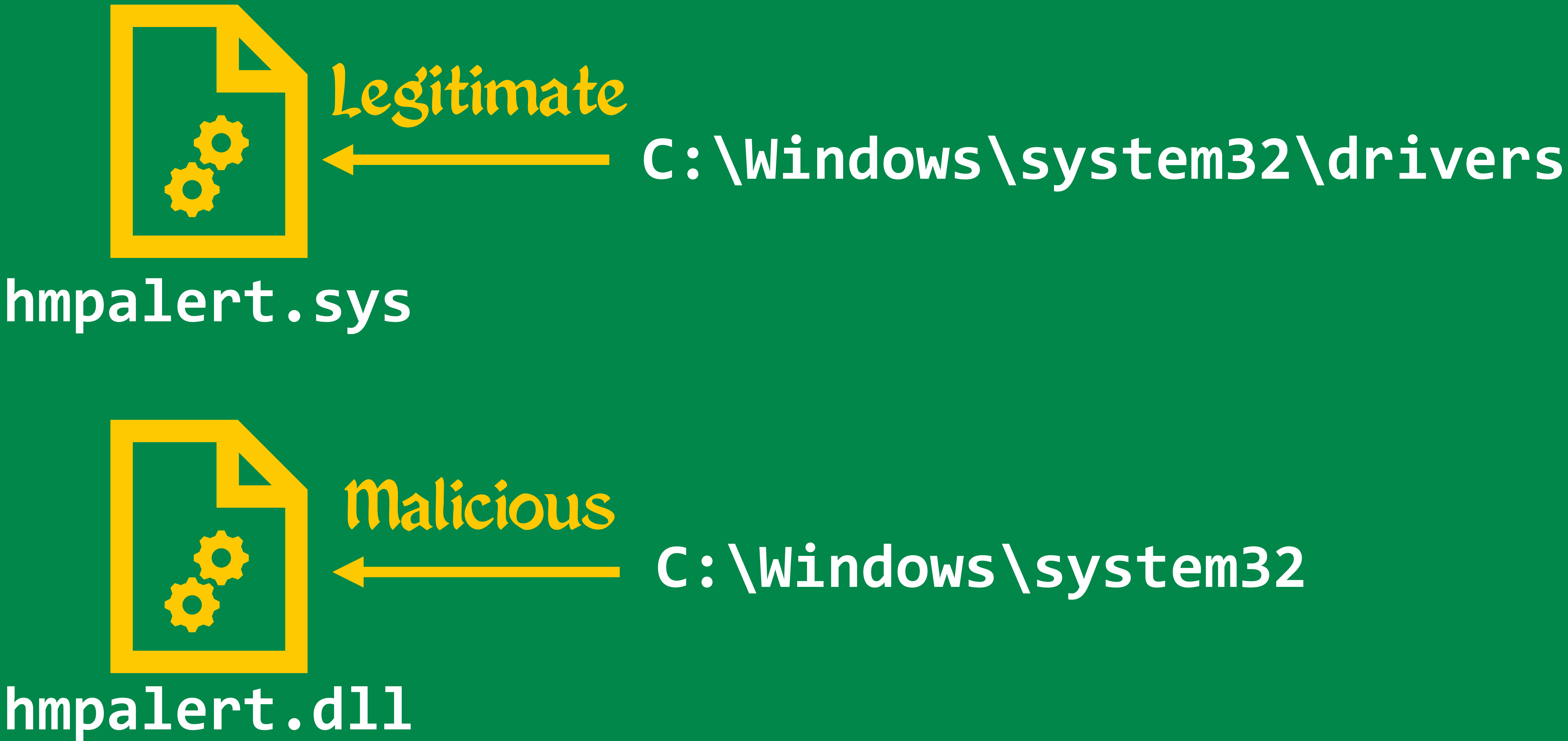
Activities performed

Legitimate

C:\Windows\system32\drivers

hmpalert.sys

Activities performed



Legitimate

C:\Windows\system32\drivers

hmpalert.sys

Malicious

C:\Windows\system32

hmpalert.dll

Activities performed

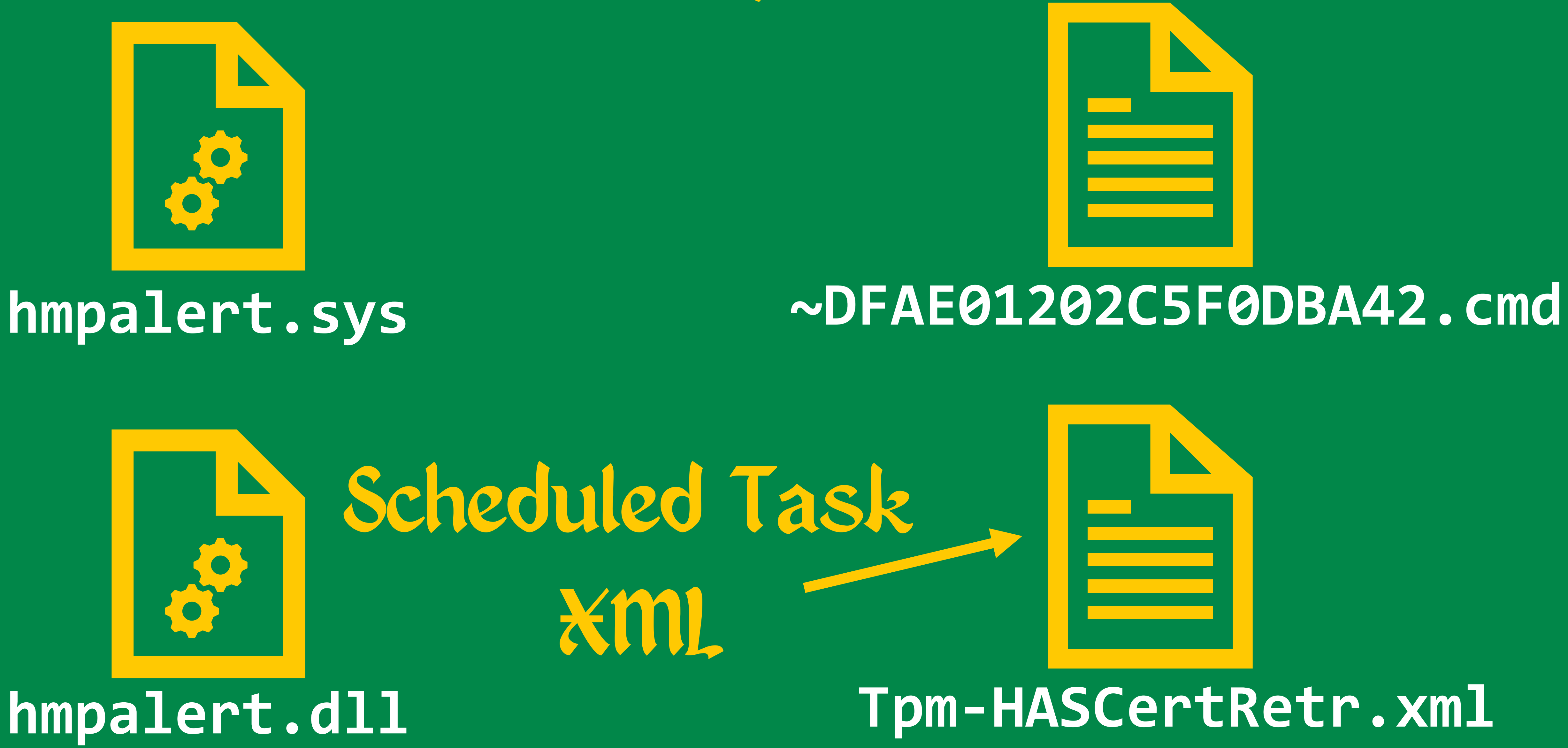
hmpalert.sys

~DFAE01202C5F0DBA42.cmd

hmpalert.dll

Tpm-HASCertRetr.xml

Activities performed



hmpalert.sys

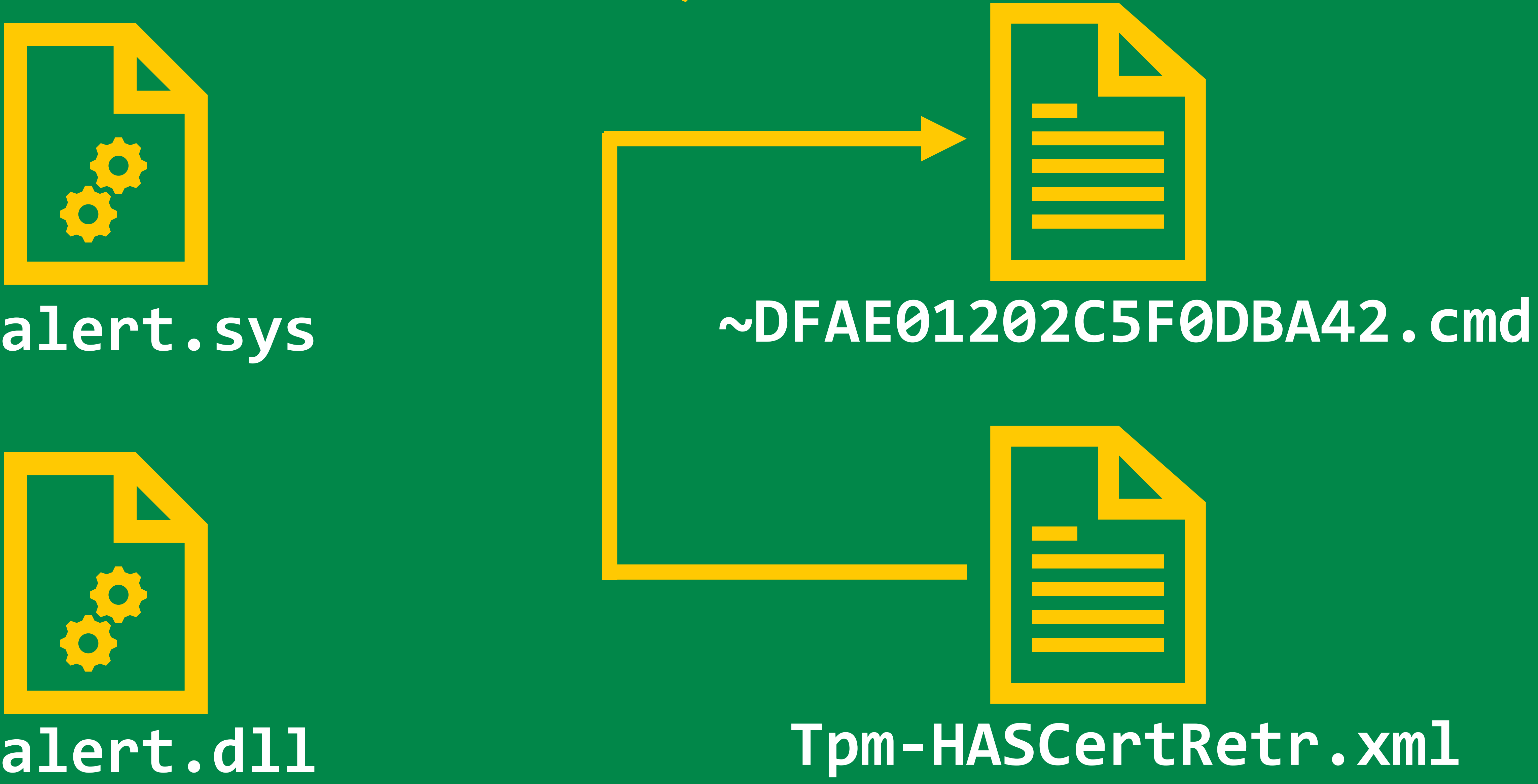
~DFAE01202C5F0DBA42.cmd

hmpalert.dll

Scheduled Task XML

Tpm-HASCertRetr.xml

Activities performed



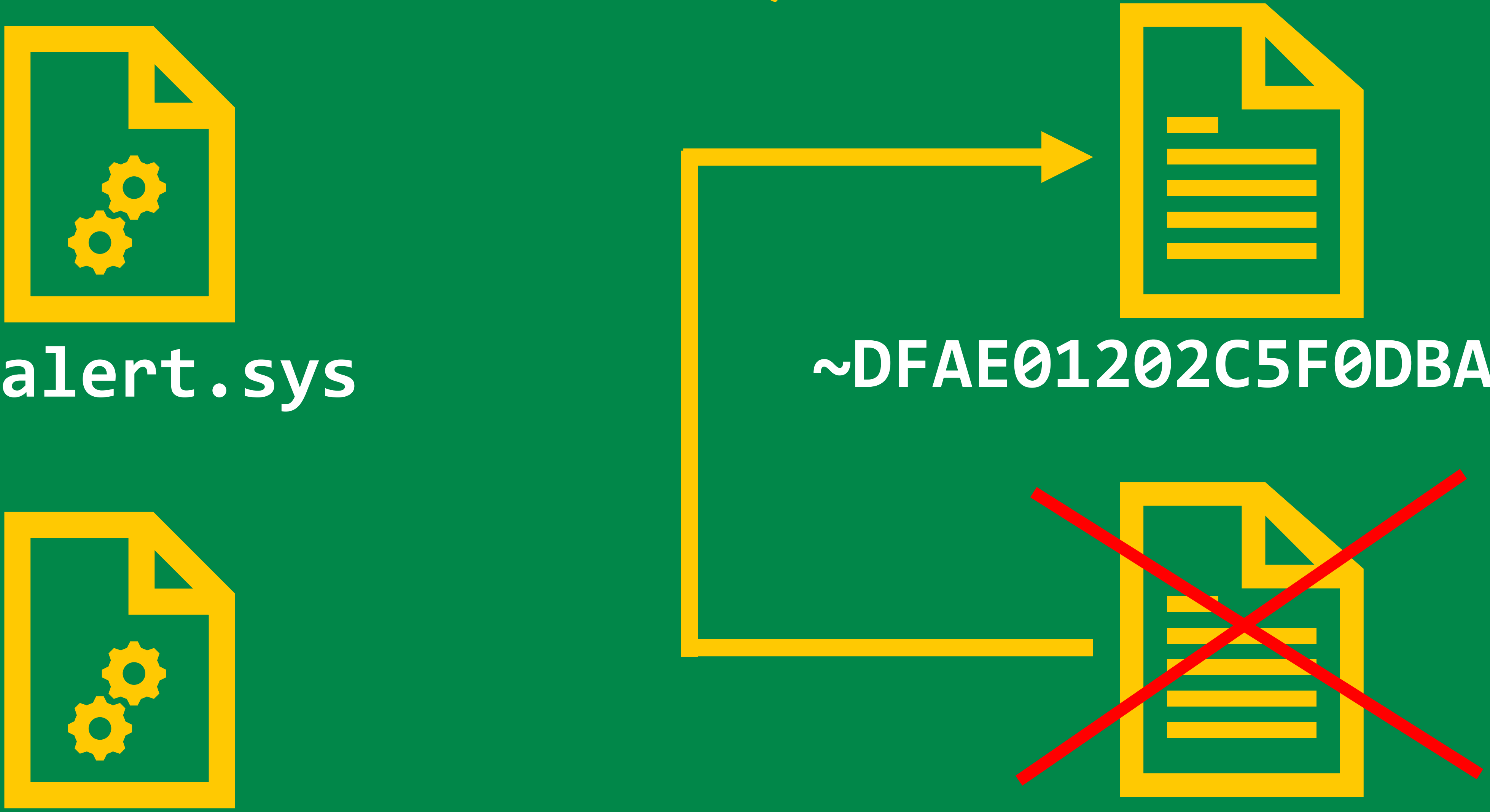
hmpalert.sys

hmpalert.dll

~DFAE01202C5F0DBA42.cmd

Tpm-HASCertRetr.xml

Activities performed



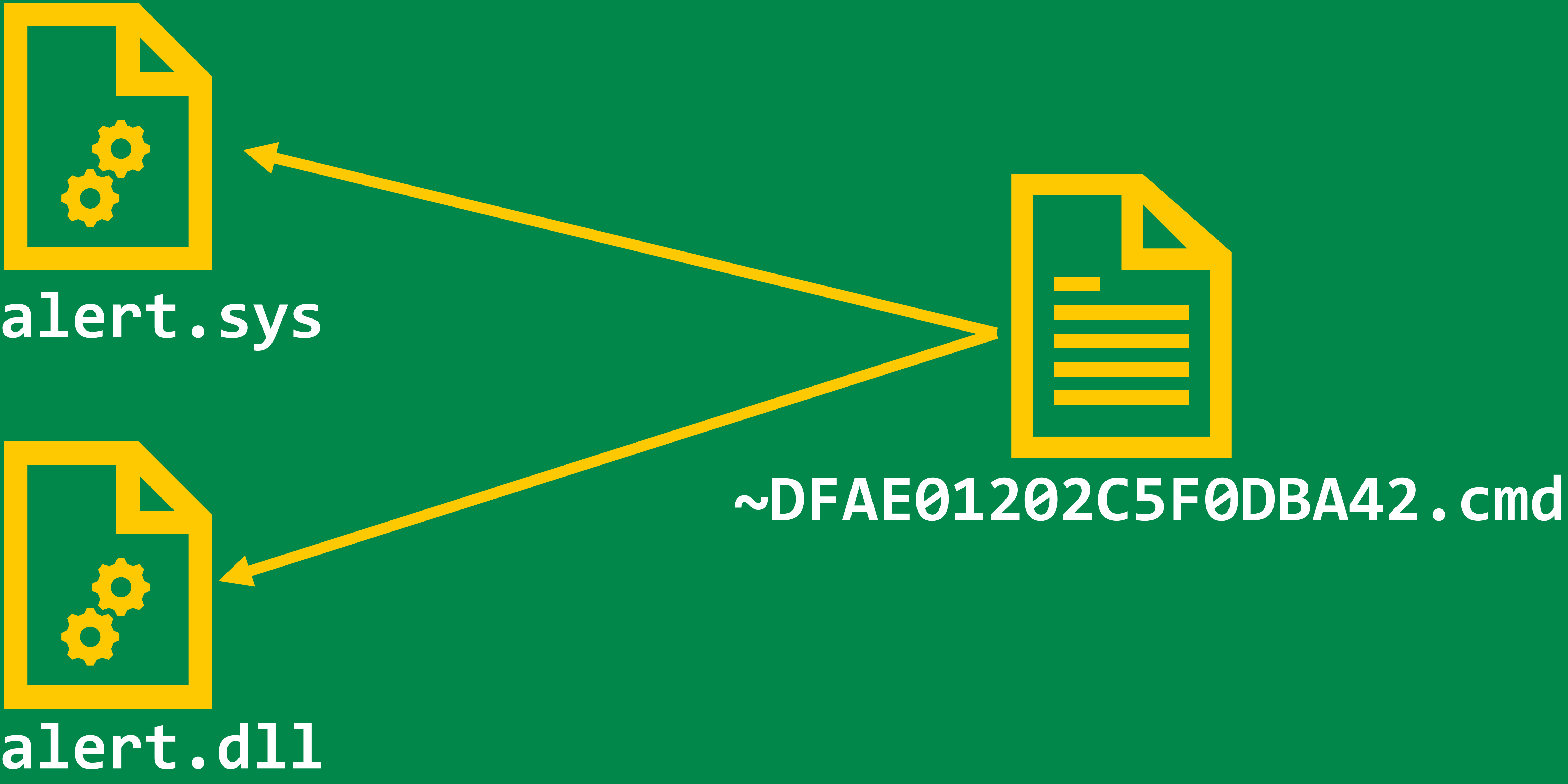
hmpalert.sys

hmpalert.dll

~DFAE01202C5F0DBA42.cmd

Tpm-HASCertRetr.xml

Activities performed



hmpalert.sys

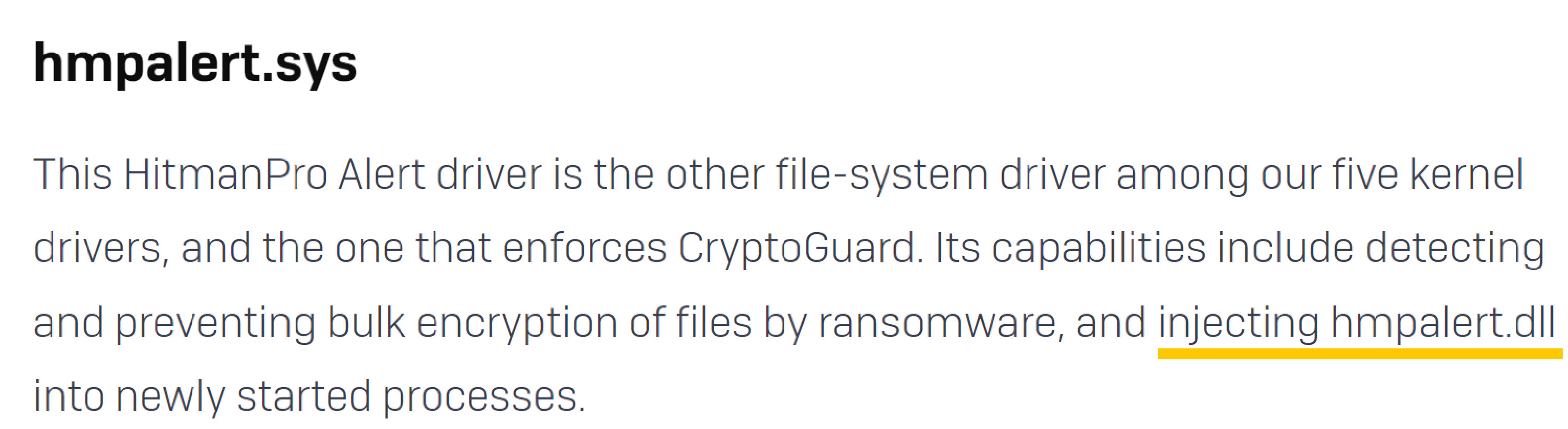
hmpalert.dll

~DFAE01202C5F0DBA42.cmd

Installing a driver

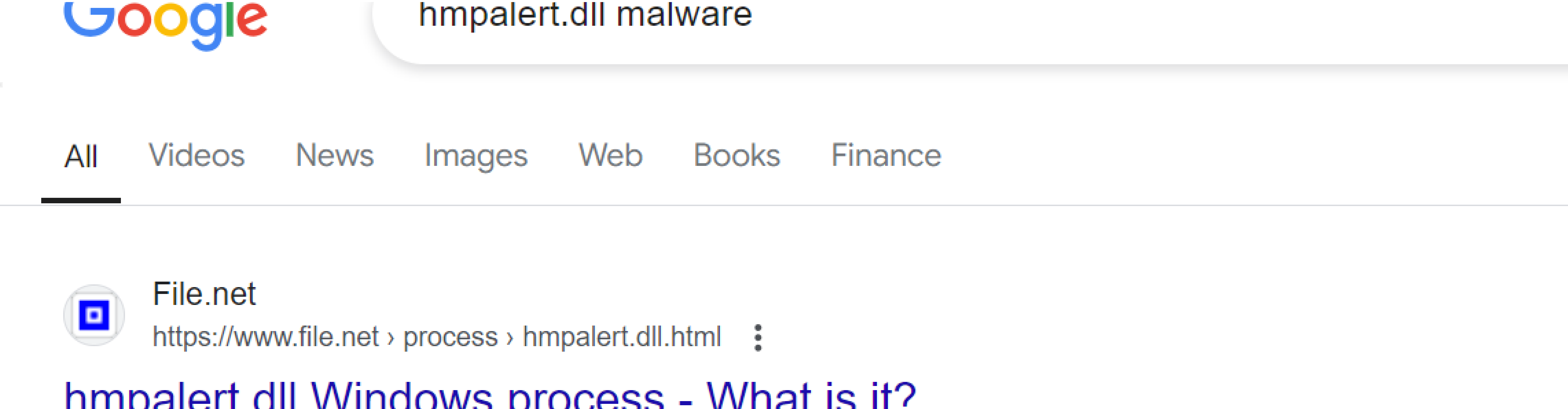
```
reg add
HKLM\SYSTEM\CurrentControlSet\Services\hmpalert
reg add
HKLM\SYSTEM\CurrentControlSet\Services\hmpalert\
Instances

. . .

sc create hmpalert binPath=
c:\windows\system32\drivers\hmpalert.sys type=
kernel start= system
```

Attackers using an antivirus?



hmpalert.sys

This HitmanPro Alert driver is the other file-system driver among our five kernel drivers, and the one that enforces CryptoGuard. Its capabilities include detecting and preventing bulk encryption of files by ransomware, and injecting hmpalert.dll into newly started processes.



hmpalert.dll malware

File.net

https://www.file.net › process › hmpalert.dll.html

hmpalert.dll Windows process - What is it?

This is **not** a vulnerability!

Malware in three processes

`winlogon.exe`

Running payloads

Malware in three processes

winlogon.exe

Running payloads

dwm.exe

Screenshotting

Malware in three processes

`winlogon.exe`

Running payloads

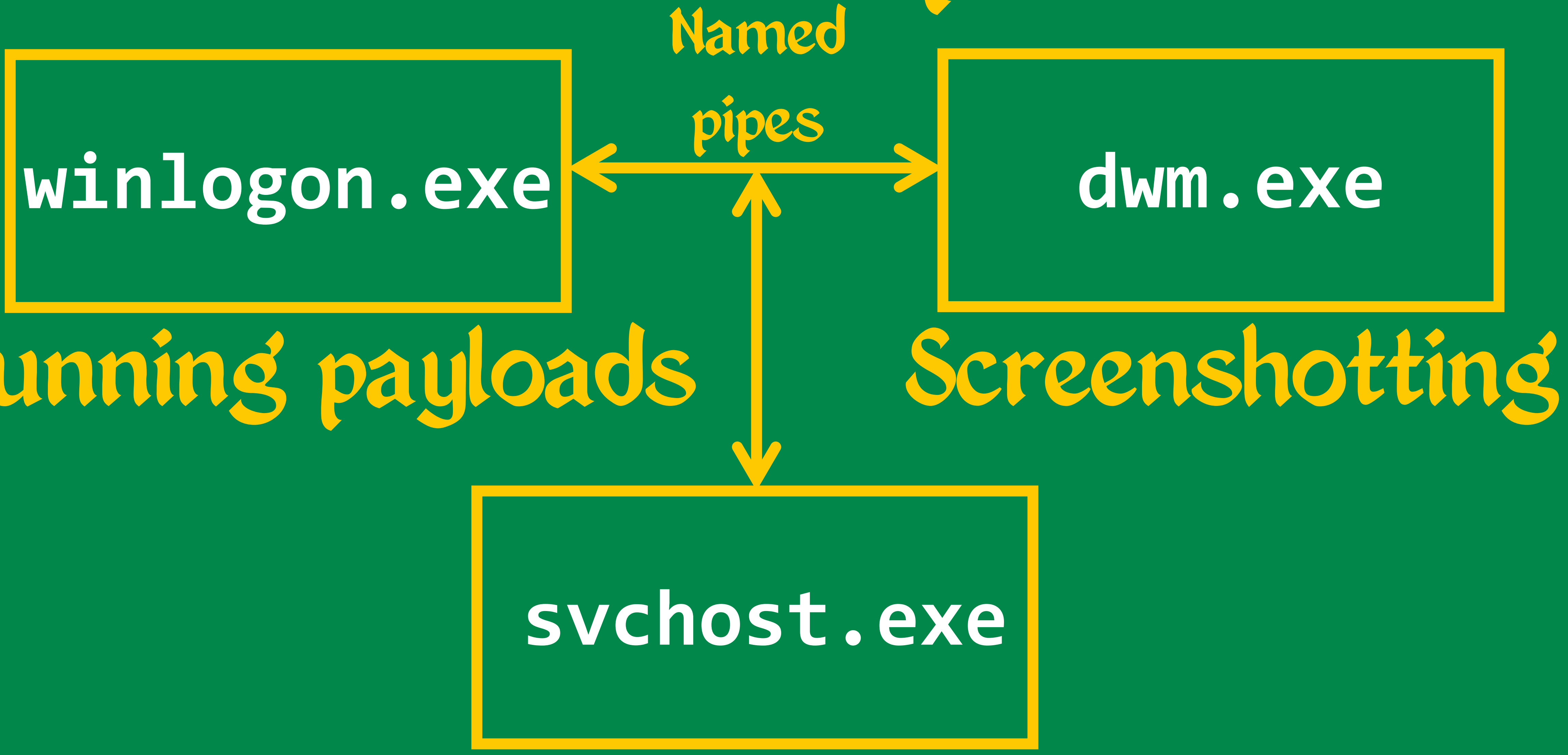
`dwm.exe`

Screenshotting

`svchost.exe`

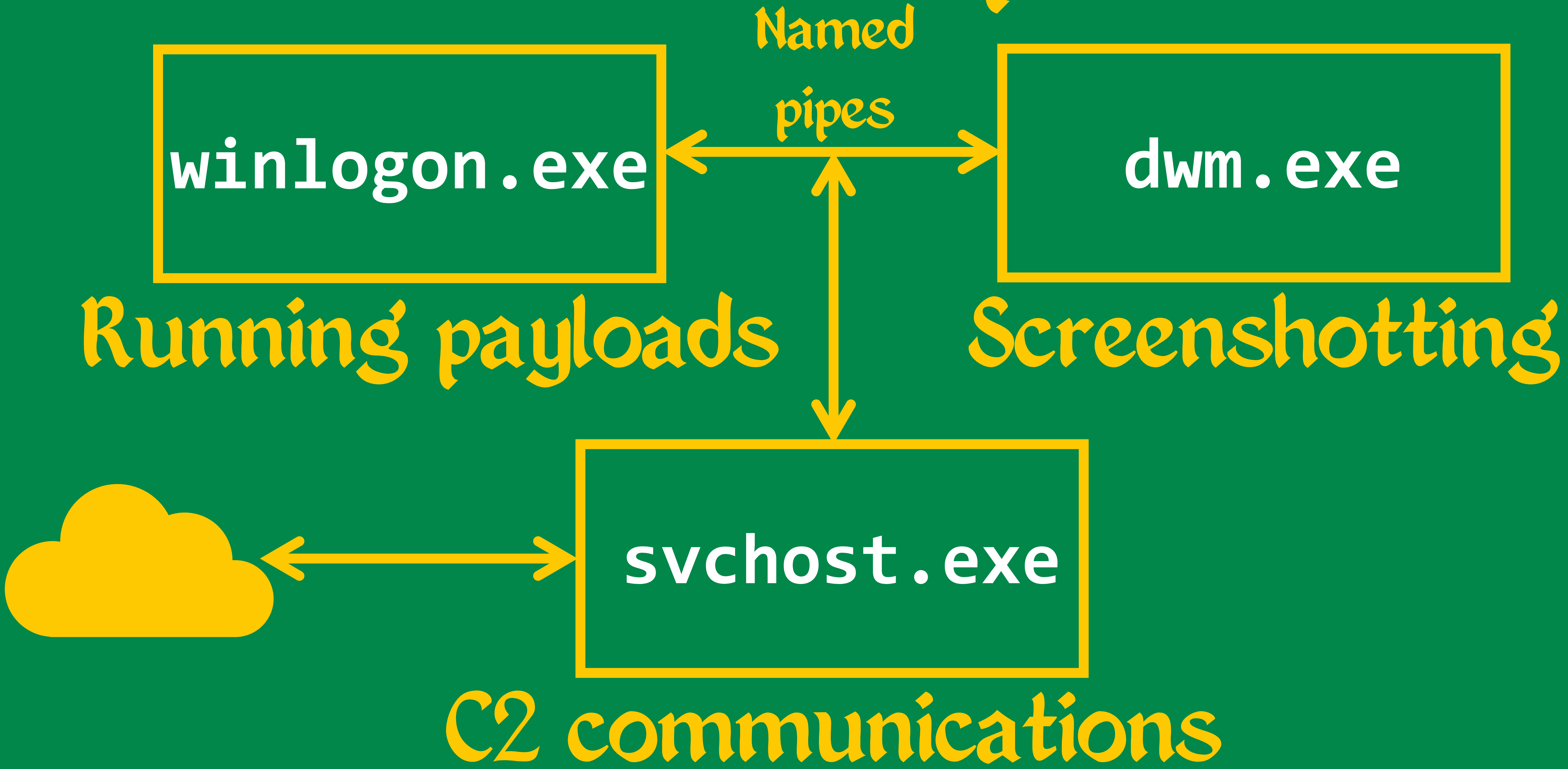
C2 communications

Malware in three processes



C2 communications

Malware in three processes



Named pipes

winlogon.exe

dwm.exe

svchost.exe

Running payloads

Screenshotting

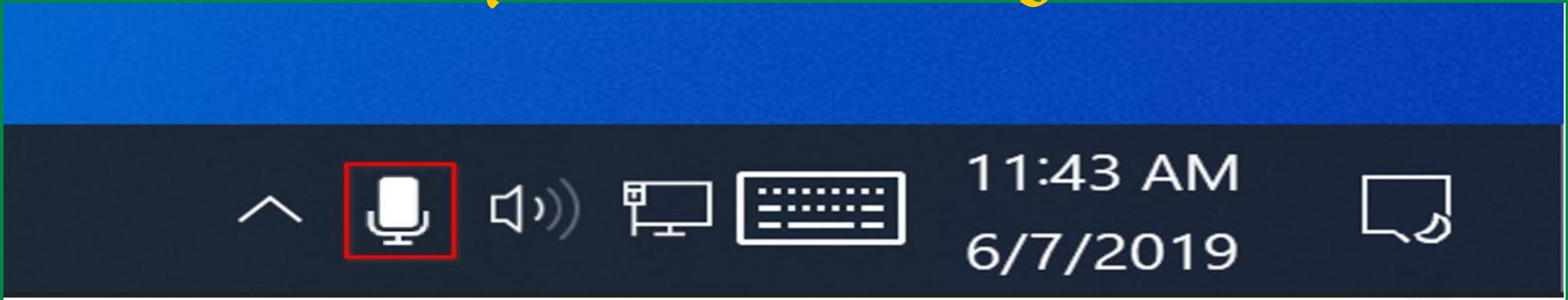
C2 communications

Microphone recording

Windows 10: hook Shell_NotifyIconW to prevent icon display

Windows 11: patch OnMicCapabilityUsageChanged via PDB file parsing

Exfiltration: via Dropbox with an API key



File stealing

Hi! I’m Baymax, the file stealing superhero!`

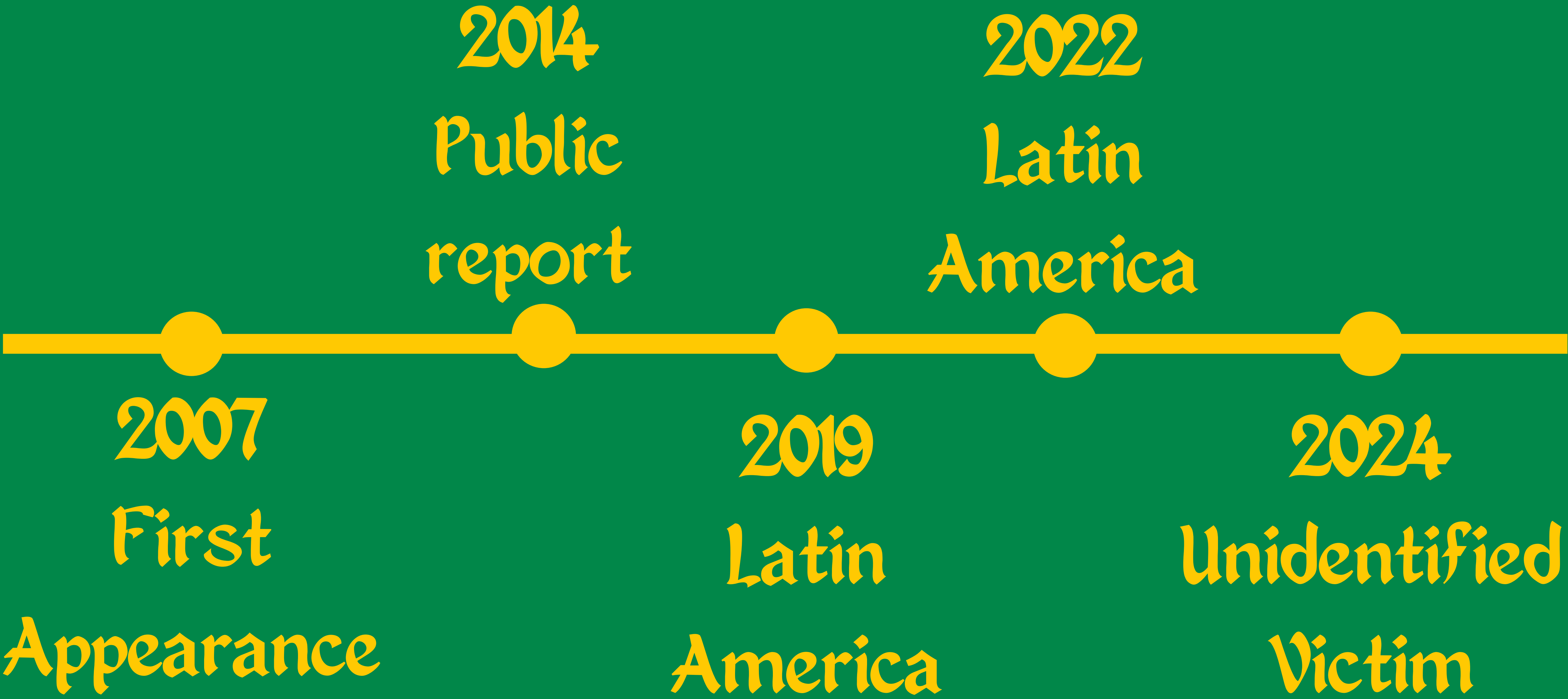
PDB Path:

`D:\GIT\Baymax\x64\Release\Baymax.pdb`

Targeted Data:

Cookies, data from messengers, confidential documents

The great comeback



2007
First
Appearance

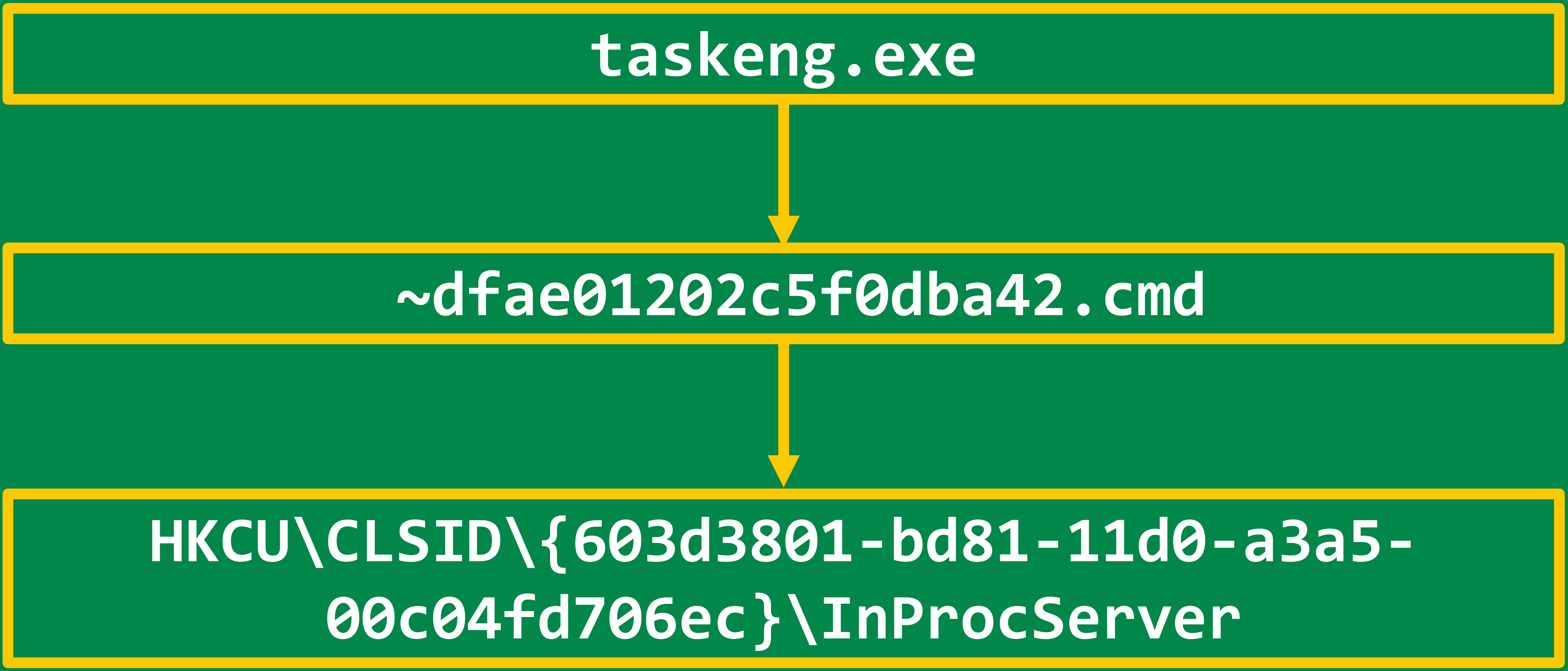
2014
Public
report

2019
Latin
America

2022
Latin
America

2024
Unidentified
Victim

2019 version



taskeng.exe

~dfae01202c5f0dba42.cmd

HKCU\CLSID\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\InProcServer

2019 version: plugins

```
38568efd

b6df77b6

5ca54969

8d82f0fa

82b79b83
```

2019 version: plugins

38568efd	ConfigMgr.dll
b6df77b6	Storage.dll
5ca54969	FileFilter.dll
8d82f0fa	KeybFilter.dll
82b79b83	Comm.dll

Attribution

2022-2024: `~DFAE01202C5F0DBA42.cmd`

2019: `~DFAE01202C5F0DBA42.cmd`

2007-2013: `~DF01AC74D8BE15EE01.tmp`

2007-2013 module names	2019 module names (cracked)
FileFlt	FileFilter
Storage	Storage
Config	ConfigMgr

Should have been more creative with names!

Conclusions

Antivirus tools turned into malware for persistence!

Multiple persistence techniques: registry, DLL sideloading

Cloud storages used for exfiltration

These smaller APTs need more research!