

PCYB 23Z Projekt - Faza II: BLUE

Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych



27 marca 2024

Spis treści

1. Tematyka i zakres projektu	2
2. Wstępne rozpoznanie	2
3. Dalsze śledztwo	4
4. Identyfikacja skompromitowanego klienta	5
4.1. Numer IP	5
4.2. Nazwa hosta	6
4.3. Nazwa konta użytkownika	6
5. Złośliwe oprogramowanie	6
5.1. Działanie	6
5.2. Identyfikacja	6
5.3. MITRE ATTCK	7
6. Scenariusz ataku	7
7. Odpowiedzi	7
8. Podsumowanie	7
Parametry sprzętowe	7
Bibliografia	7

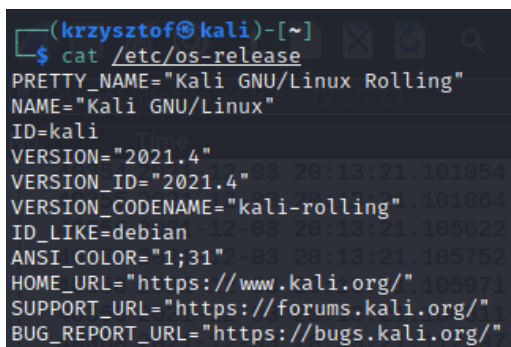
1. Tematyka i zakres projektu

Celem Fazy 2 gry projektowej jest przeprowadzenie analizy powłamaniowej, po incydencie, do którego doszło na maszynie z systemem operacyjnym Windows. Materiał badawczy stanowi plik z zapisem ruchu sieciowego (**faza2.22Z.red.pcap**) z zainfekowanego hosta. Zadanie będzie polegało na analizie tego zapisu, wykryciu i odtworzeniu przebiegu ataku.

Poniższa treść przedstawia nasz proces dedukcji - wszystkie odpowiedzi (i parametry sprzętowe) zostały podsumowane w zwięzłej formie na końcu sprawozdania.

2. Wstępne rozpoznanie

Zważywszy na prawdziwość analizowanych danych i potencjalną ich szkodliwość zdecydowaliśmy się wykonać maszynę wirtualną z systemem Kali Linux.



```
(krzysztof@kali)-[~]
$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2021.4"
VERSION_ID="2021.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```

Na maszynie tej uruchomiliśmy program **Wireshark** w wersji 3.4.9, który jest darmowym analizatorem protokołów sieciowych, umożliwiający analizę przechwyconego ruchu sieciowego. Pozwala on na monitorowanie i zrozumienie komunikacji między urządzeniami w sieci, umożliwia również identyfikację potencjalnych problemów.

Przydzielony nam plik **faza2.22Z.red.pcap** zawiera ok. 55 tysięcy pakietów. Postanowiliśmy sprawdzić jakie pliki jesteśmy w stanie wyeksportować za pomocą funkcji **File > Export Objects**, ponieważ pozwoliłoby to w łatwy sposób wykryć chociażby (potencjalnie zainfekowane) pliki pobrane przez użytkownika poprzez np.: protokół http.

Nasze zainteresowanie wzbudziła zakładka z plikami typu **IMF** (Internet Message Format), czyli format, w którym wiadomości tekstowe są przesyłane przez internet. IMF można wyobrazić sobie jako list w kopercie - zawiera nadawcę, odbiorców, temat i datę.

35

/ 61

35 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

0817fc094c9957461e379e2638e30d781b7015375aa12602bacc92303deefedb

Size52.01 KB

Last Analysis Date2 hours ago

EML

Fwd_email

email

Community Score

DETECTIONDETAILSCOMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.emotet/w97m

Threat categoriestrojan downloader

Family labelsemotet w97m

Security vendors' analysis

Do you want to automate checks?

Stwierdziliśmy, że może może być to dobry trop (w tym miejscu skonsultowaliśmy się z mentorką, która potwierdziła nasze przypuszczenia - idziemy w dobrym kierunku).

3. Dalsze śledztwo

Postanowiliśmy przejrzeć pozostałe maile. Wyróżniliśmy dwa adresy nadawcze:

1. *tenpo-kaihatsu@acoop-ks.co.jp*
2. *nobuyasu-takahashi@tachikawahouse.co.jp*

Maile wysłane z pierwszego adresu mają taką samą treść:

```

<html>
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8">
</head>
<body>
<br>
SCAN_1006384431078587279.zip<br>
Password: EGLFtF<br>
<br>
<br>
Thank you for your business - we appreciate it very much.<br>
<br>
<br>
Kunj Sharma<br>
kunj.sharma@opporajasthan.in<br>
<br>
<br>
<br>

```

Widzimy pewien plik **.zip** jak również hasło.

Wiadomości wysłane z drugiego adresu mają identyczną treść zachęcającą do zapoznania się z załączonym plikiem, natomiast zostały wysłane do różnych adresatów.

Najprawdopodobniej mamy do czynienia z szerzej zakrojoną kampanią phishingową.

4. Identyfikacja skompromitowanego klienta

4.1. Numer IP

W treści polecenia do 2 części projektu została informacja, że zainfekowane urządzenie działa pod kontrolą systemu operacyjnego **Windows**. Pierwszym co przyszło nam do głowy, było sprawdzenie pakietów **http**, ponieważ można w nich znaleźć informację o systemie operacyjnym klienta. Poniżej pierwszy zarejestrowany pakiet tego protokołu:

No.	Time	Source	Destination	Request Method	Protocol	Length
1743	2021-12-03 19:42:47.664570	10.12.3.66	104.21.29.80	GET	HTTP	245
1752	2021-12-03 19:42:47.785368	104.21.29.80	10.12.3.66		HTTP	60

▶ Frame 1743: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)

▶ Ethernet II, Src: Realtek_e7:81:3d (00:4f:49:e7:81:3d), Dst: Cisco_89:08:49 (00:30:b6:89:08:49)

▶ Destination: Cisco_89:08:49 (00:30:b6:89:08:49)

▶ Source: Realtek_e7:81:3d (00:4f:49:e7:81:3d)

Type: IPv4 (0x0800)

▶ Internet Protocol Version 4, Src: 10.12.3.66, Dst: 104.21.29.80

▶ Transmission Control Protocol, Src Port: 52414, Dst Port: 80, Seq: 1, Ack: 1, Len: 191

▶ Hypertext Transfer Protocol

▶ GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1\r\n

▶ [Expert Info (Chat/Sequence): GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1\r\n]

▶ [GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1\r\n]

▶ [Severity level: Chat]

▶ [Group: Sequence]

Request Method: GET

Request URI: /wp-content/plugins/sSTToaEwCG5VASw/

Request Version: HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1320\r\n

Host: gamaes.shop\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gamaes.shop/wp-content/plugins/sSTToaEwCG5VASw/]

[HTTP request 1/1]

[Response in frame: 1752]

Jak widać jest to żądanie wysłane z adresu **10.12.3.66**. Widzimy również, że system operacyjny klienta to Windows 10 lub 11. Następnie obserwujemy odpowiedź serwera, będącą jednoznaczną z załadowaniem witryny, której fragmenty kodu źródłowego zostały przedstawione poniżej:

```
<body>\n  <div id="cf-wrapper">\n    <div class="cf-alert cf-alert-error cf-cookie-error" id="cookie-alert" data-translate="enable_cookies">Please enable cookies.</div>\n    <div id="cf-error-details" class="cf-error-details-wrapper">\n      <div class="cf-wrapper cf-header cf-error-overview">\n        <h1 class="cf-text-error"><i class="cf-icon-exclamation-sign"></i> Warning: Suspected Phishing Site Ahead!</h1>\n        <h2 class="cf-subheadline">This link has been flagged as phishing. We suggest you avoid it.</h2>\n      </div><!-- /.header -->\n    </div>\n  </body>\n\n<h2>What is phishing?</h2>\n<p>This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.</p>\n<p>\n  <form action="/cdn-cgi/phish-bypass" method="GET">\n    <input type="hidden" name="u" value="/wp-content/plugins/sSTToaEwCG5VASw/">\n    <input type="hidden" name="atok" value="35d7f4bd3f8737ea3a4ca62f499fc4c9">\n    <button type="submit" class="cf-btn cf-btn-danger" data-translate="dismiss_and_enter">Dismiss this warning and enter site</button>\n  </form>\n
```

"This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source."

Widać wyraźnie, że vendor hostingu (w tym przypadku Cloudflare) ostrzega nas przed **phishingiem**. Na tej podstawie, jak również zauważając, że wszystkie wspomniane we wcześniejszych sekcjach maile zostały wysłane z tego samego adresu IP (**10.12.3.66**) doszliśmy do wniosku, iż wejście przez klienta na tę witrynę spowodowało zainfekowanie komputera. Najprawdopodobniej użytkownik kliknął w link przesłany mailem lub otworzył załącznik. Moment załadowania strony traktujemy jako czas rozpoczęcia aktywności przez złośliwe oprogramowanie:

```
1743 2021-12-03 19:42:47... 10.12.3.66 104.21.29.80 HTTP GET /wp-content/plugins/sSTToaEwCG5VASw/ HTTP/1.1
```

4.2. Nazwa hosta

Aby odnaleźć nazwę hosta wykorzystaliśmy funkcję szukania pakietów z konkretną wiadomością (**Edit > Find Packet**) w programie **Wireshark**. W oknie wyszukiwania wpisaliśmy frazę "**desktop-**", ponieważ domyślną nazwą hosta w systemach Windows 10 i 11 jest "**DESKTOP**" + 7 losowych wartości alfanumerycznych. 'Przeklikaliśmy' uzyskane wyniki - wszędzie powtarzała się nazwa "**DESKTOIIP-LU0ABV1**" - wnioskujemy, że jest to nazwa zainfekowanego urządzenia (jedyne z systemem Windows).

```
▼ Option: (12) Host Name
  Length: 15
  Host Name: DESKTOP-LU0ABV1
```

4.3. Nazwa konta użytkownika

Mamy do czynienia z systemem **Windows**, więc dane uwierzytelniające, dotyczące tożsamości są zarządzane przez **AD** (Active Directory). By odnaleźć poszukiwane informacje, zdecydowaliśmy się przejrzeć pakiety protokołu **Kerberos** (jest to protokół bezpieczeństwa komputerowego, który umożliwia bezpieczną autentykację użytkowników w sieciach komputerowych.)

kerberos					
No.	Time	Source	Destination	Protocol	CNameString
349	2021-12-03 19:42:09.116976	10.12.3.3	10.12.3.66	DCERPC	
3122	2021-12-03 19:43:09.873709	10.12.3.3	10.12.3.66	DCERPC	
4902	2021-12-03 19:47:27.500215	10.12.3.3	10.12.3.66	DCERPC	
395	2021-12-03 19:42:09.181757	10.12.3.3	10.12.3.66	KRB5	darin.figueroa
232	2021-12-03 19:42:08.918139	10.12.3.66	10.12.3.3	KRB5	darin.figueroa
234	2021-12-03 19:42:08.919743	10.12.3.3	10.12.3.66	KRB5	darin.figueroa
341	2021-12-03 19:42:09.115939	10.12.3.3	10.12.3.66	KRB5	darin.figueroa

Naszym oczom ukazała się nazwa konta użytkownika w formacie *imię.nazwisko*: **darin.figueroa**.

5. Złośliwe oprogramowanie

5.1. Działanie

Złośliwe oprogramowanie propaguje się poprzez złośliwe załączniki (np.: **.xlsm** lub **.zip**, co wynika z analizy zawartości maila w serwisie **virustotal**, zamieszczonej w jednej ze wcześniejszej sekcji) w poczcie elektronicznej. Po zainfekowaniu urządzenia, zostają z niego rozesłane kolejne maile phishingowe.

5.2. Identyfikacja

Typem złośliwego oprogramowania, które działa zgodnie z opisanym scenariuszem, jest zazwyczaj trojan phishingowy. Trojan phishingowy są programami, które wydają się nieszkodliwe lub korzystne, ale w rzeczywistości zawierają złośliwe funkcje. W przypadku rozsyłania phishingowych maili po infekcji, może to również być

klasyfikowane jako malware typu botnet, gdzie zainfekowane urządzenie staje się częścią zdalnie sterowanego botnetu do przeprowadzania ataków, w tym kampanii phishingowych.

5.3. MITRE ATTCK

ID Phishing: Spearphishing Attachment - **T1566.001**

6. Scenariusz ataku

1. Zainfekowanie systemu - najprawdopodobniej użytkownik otworzył załącznik przesłany w mailu phishingowym
2. rozpoczęcie pracy przez złośliwe oprogramowanie
3. rozesłanie kolejnych 'zakażonych' maili z zainfekowanego urządzenia

7. Odpowiedzi

1. **10.12.3.66**
2. **DESKTOIIP-LU0ABV1**
3. **darin.figueroa**
4. **2021-12-03 19:42:47** [rok-miesiąc-dzień godzina:minuty:sekundy]
5. **phishing-trojan** lub malware typu **botnet**
6. [patrz sekcja wyżej]

8. Podsumowanie

Dany był plik **.pcap** (packet capture) i informacja o systemie operacyjnym zainfekowanego urządzenia (Windows). Zadaniem było przeanalizowanie ów pliku z pomocą wybranych narzędzi i udzielenie odpowiedzi na pytania - a zatem analiza powłamaniowa. Wykorzystaliśmy analizator Wireshark i z jego pomocą odpowiedzieliśmy na wszystkie pytania związane z przeprowadzonym atakiem, cały proces został udokumentowany w niniejszym raporcie. Na podstawie tego zadania zostało nam uzmysłowione jak ważne jest zachowanie ostrożności w sieci oraz jak łatwo jest zainfekować urządzenie nieświadomego użytkownika.

Parametry sprzętowe

Komputer stacjonarny z procesorem Intel Core i5-8400, kartą graficzną Palit GeForce GTX 1060 Super JetStream 6GB i 8GB pamięci RAM, system Windows 11, oprogramowanie Oracle VM VirtualBox.

Bibliografia

1. <https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/>