Wojskowa Akademia Techniczna

Sprawozdanie z zadania projektowego

Przedmiot: Oprogramowanie niepożądane i analiza kodu

Weronika Raczyńska

WCY19KC1S1

Spis treści

1. Cel projektu 3
2. Opis programu 3
   2.1. Nazwa i funkcje 3
   2.2. Pochodzenie programu 3
3. Opis działania 4
4. Instalacja 4
5. Wykrywalność programu 4
6. Zapewnienie bezpieczeństwa osoby atakującej 6
7. Spełnione wymagania 6
8. Podsumowanie 8

1. Cel projektu

Celem projektu było wykonanie narzędzia typu APT (Advanced Persistent Threat) spełniającego funkcje keyloggera. Powinien to być kod wykonywalny osadzany trwale na określonym komputerze, zdolny do skrytego śledzenia działania operatorów i dostępu do niektórych zasobów informacyjnych oraz do wyprowadzania informacji skrycie z zapewnieniem bezpieczeństwa lokalizacji i tożsamości odbiorcy informacji.

2. Opis programu

2.1. Nazwa i funkcje

W ramach realizacji zadania projektowego został napisany kod w Pythonie, a następnie zamieniony na plik wykonywalny o nazwie services.exe. Wykonany program posiada funkcje keyloggera, który rejestruje wciskane klawisze przez użytkownika.

W kodzie została zawarta funkcja modyfikująca rejestr systemu w celu dodania programu do autostartu, dzięki czemu program podejmuje działanie automatycznie po wznowieniu pracy komputera.

Program wyprowadza informację o wciśniętych klawiszach przez użytkownika za pomocą poczty. Raporty wysyłane są do atakującego co 20 sekund tylko w czasie aktywności ofiary. Za każdym razem przesyłany zostaje nowy raport, a logi nie są zapisywane na komputerze ofiary.

2.2. Pochodzenie programu

Program został napisany na podstawie artykułu, którego autorem jest Abdou Rockikz. Artykuł opisuje sposób wykonania prostego keyloggera rejestrującego wciśnięte klawisze z klawiatury i wysyłającego raporty przez email lub zapisującego logi na komputerze. Zawarta została także instrukcja zamiany kodu na plik wykonywalny. Artykuł znajduje się na stronie: https://www.thepythoncode.com/article/write-a-keylogger-python.

Kod został zmodyfikowany i wzbogacony o funkcję pozwalającą na dodanie programu do autostartu: https://www.geeksforgeeks.org/autorun-a-python-script-on-windows-startup/. W finalnej wersji programu została uwzględniona tylko możliwość wysyłania raportów przez email, bez zapisywania logów na komputerze ofiary.

3. Opis działania

Program po instalacji na komputerze ofiary działa w tle i nie sygnalizuje w żaden sposób swojej obecności podczas pracy. W programie zawarta jest funkcja która rejestruje zdarzenie za każdym razem, kiedy użytkownik puści klawisz na klawiaturze. Każdy wpisany znak jest dodawany do zmiennej, której wartość wysyłana jest co 20 sekund do osoby atakującej w ramach raportu przez email. Po wysłaniu raportu wartość zmiennej jest usuwana. Po restarcie komputera program wznawia swoje działanie, dzięki dodaniu go do autostartu.

4. Instalacja

W celu umieszczenia programu na komputerze ofiary można poprzez email wysłać plik lub link do programu znajdującego się na tymczasowym dysku internetowym np.: https://www.mediafire.com/. W celu nakłonienia ofiary do pobrania pliku należy użyć socjotechniki . Atakujący może podszyć się pod znajomego lub osobę z działu IT firmy, w której pracuje ofiara. Po pobraniu programu wystarczy, że ofiara uruchomi plik services.exe. Od tej pory program będzie działał w tle na komputerze użytkownika, a raporty będą wysyłane na adres email atakującego.

Program można zmodyfikować zmieniając czas co jaki wysyłane są raporty. Domyślnie ustawiony adres email na który wysyłane są raporty znajduje się na poczcie outlook. W przypadku chęci zmiany adresu należy także zmienić server SMTP w funkcji sendmail oraz sprawdzić jaki port obsługuje wybrana poczta.

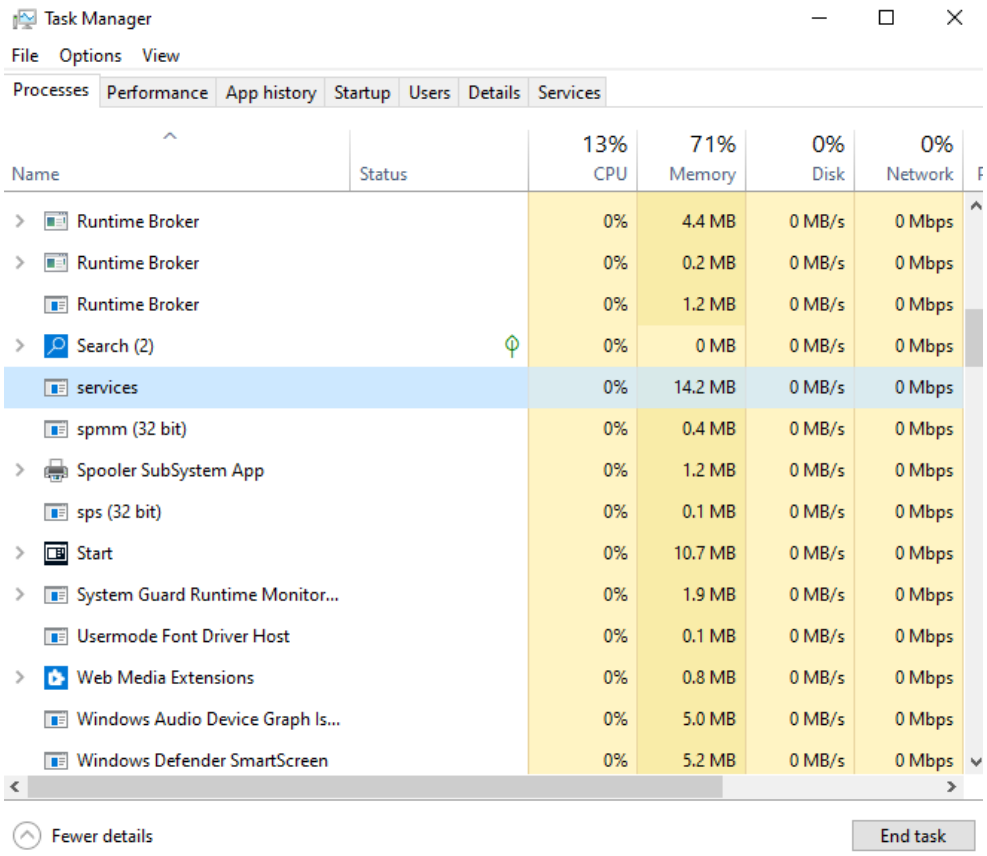
W przypadku wybrania poczty gmail należy włączyć uwierzytelnienie dwuskładnikowe znajdujące się pod zakładką „Logowanie w Google”. W celu zachowania anonimowości należy użyć numeru telefonu wymaganego do weryfikacji umieszczonego na jednej ze stron, gdzie dostępne są tymczasowe numery telefonu, np. https://quackr.io/. Następnie w zakładce „Hasła do aplikacji” należy dodać nową aplikację poprzez wybranie „Innej opcji” i wygenerować kod. Podany kod należy podmienić pod hasło do poczty w kodzie programu.

5. Wykrywalność programu

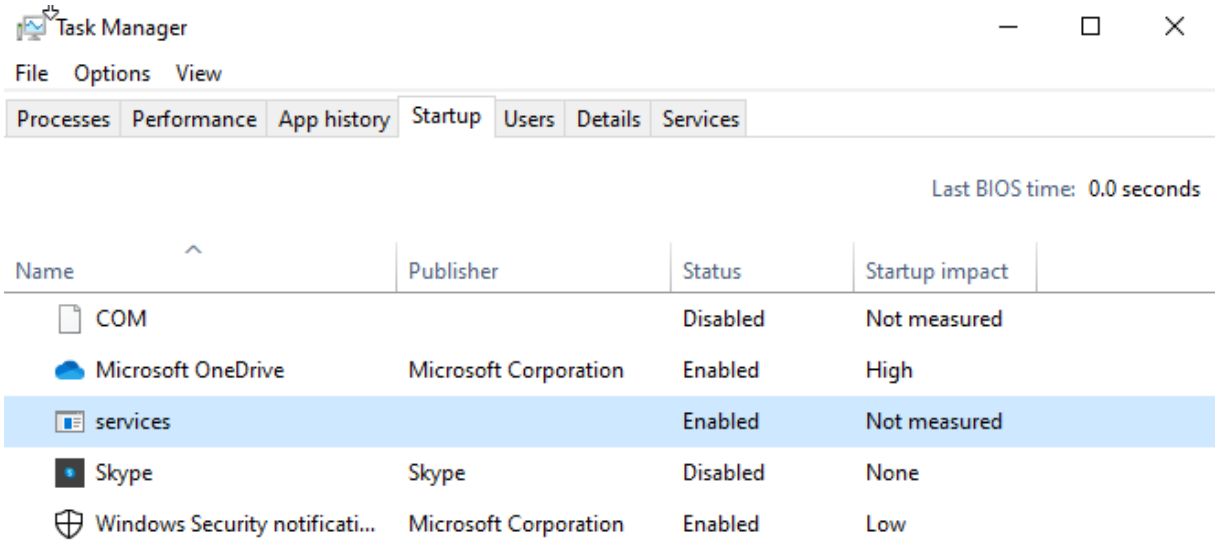
Program nie sygnalizuje swojej obecności w czasie działania, lecz nadal jest widoczny w Menedżerze Zadań w zakładce „Procesy” oraz „Uruchamianie”. W celu utrudnienia wykrywalności programu została ustawiona nazwa services.exe, która podszywa się pod proces systemowy o takiej samej nazwie. Dodatkowo ikona programu została zmieniona w

programie ResourceHacker. Dzięki tym zabiegom program nie wygląda podejrzanie i jest trudny do wykrycia dla ofiary.

Uruchomiony program services.exe w Menadżerze Zadań:



Program services.exe widoczny w zakładce „Uruchamianie”:



6. Zapewnienie bezpieczeństwa osoby atakującej

Osoba atakująca nie powinna zostać wykryta, dlatego do wszystkich działań związanych z przesyłaniem programu i odbieraniem raportów zalecane jest użycie wirtualnej sieci komputerowej Tor, która pozwoli na ochronę tożsamości i działalności w sieci przed analizą ruchu. Zalecanym działaniem jest również korzystanie z publicznych sieci WIFI.

Założenie adresu email, używanego do otrzymywania raportów, nie wymaga podawania prawdziwych danych osobowych, a numer telefonu potrzebny do weryfikacji można wybrać ze strony udostępniającej tymczasowe numery. Dzięki tym działaniom można uchronić prywatność atakującego .

7. Spełnione wymagania

Poniżej zostały wymienione wymagania zadania projektowego, które spełnia wykonywany program.

A. Kod powinien być instalowany bez świadomości operatora:

a. Przez intruza o uprawnieniach administratora

b. Nieświadomie przez operatora o uprawnieniach administratora

c. Nieświadomie przez operatora bez uprawnień administratora

Program może być instalowany zarówno przez nieświadomego użytkownika, który pobierze program z emaila lub w najłatwiejszym przypadku przez samego intruza. Instalacja nie wymaga wprowadzenia danych administratora.

B. Kod powinien przetrwać wyłączenie/restart komputera – podjąć działanie automatycznie po wznowieniu pracy komputera.

W programie znajduje się funkcja, która umieszcza go w autostarcie, dzięki czemu program działa przy każdym włączeniu komputera przez ofiarę.

C. Kod powinien być przeznaczony do wykorzystania w stacjach roboczych (PC) z systemem Windows nie wcześniejszym niż Windows 7. Systemem „minimalnym" jest Windows 7 Pro z 2009 roku bez aktualizacji.

a. Na „minimalnym" komputerze

b. Na laboratoryjnym Windows 10 bez nowych aktualizacji

c. Na Windows 7 zaktualizowanym

d. Na Windows 10

Program został przetestowany i działa na wszystkich wymienionych wyżej systemach.

D. Kod powinien być możliwie trudny do wykrycia

a. Przez nieuważnego/naiwnego (zwiedzionego) operatora

b. Bez sygnalizacji po restarcie

c. Bez żadnej sygnalizacji obecności podczas pracy

d. Niewidoczny w menedżerze zadań

Program nie sygnalizuje swojej obecności w żaden sposób. Nieuważny operator nie jest w stanie go wykryć. W menedżerze zadań podszywa się pod proces systemowy o nazwie services.exe.

E. Kod powinien mieć funkcje keyloggera

a. Powinien rejestrować wciskane klawisze

Program jest prostym keyloggerem rejestrującym klawisze wciskane przez użytkownika.

F. Kod powinien funkcjonować podczas sesji operatora

a. Jednego wybranego operatora

Program funkcjonuje tylko na koncie jednego operatora u którego został zainstalowany.

H. Kod powinien wyprowadzać informacje

b. Pocztą

Informacje wyprowadzane są przez program tylko poprzez pocztę.

I. Wysyłanie informacji powinno być możliwie słabo rozpoznawalne

a. Dla operatora

Operator nie jest w stanie wykryć wyprowadzania informacji.

J. Sposób przekazywania informacji powinien zapewnić, że odbiorca wyprowadzanej informacji pozostanie anonimowy i nielokalizowalny [oraz że nadawca informacji wysyłanej do ofiary pozostanie anonimowy i nielokalizowalny]

a. Dla zwykłego operatora

b. Dla specjalisty-pracownika SOC (Security Operation Center)

c. Dla organów ścigania – państwowych

Dzięki użyciu sieci Tor oraz publicznych sieci WIFI atakujący nie zostanie zlokalizowany. Używanie tymczasowych adresów email z fałszywymi danymi osobowymi oraz tymczasowych numerów telefonu udostępnionych publicznie zapewni atakującemu anonimowość.

8. Podsumowanie

Program stworzony w ramach projektu realizuje podstawowe funkcje keyloggera oraz spełnia minimalne wymagania zawarte w zadaniu projektowym, a także kilka dodatkowych.

Napisanie kodu programu pozwoliło na zapoznanie się z możliwościami wytwarzania oprogramowania niepożądanego od strony praktycznej. Projekt umożliwił poznanie sposobów w jaki atakujący rozsyłają złośliwe pliki do nieświadomych ofiar oraz pozwolił na zgłębienie się w sposoby w jaki osoby atakujące mogą zachować swoją anonimowość podczas ataku.