Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

ЗВОРОТНА РОЗРОБКА ТА АНАЛІЗ ШКІДЛИВОГО ЗАБЕЗПЕЧЕННЯ

Лабораторна робота №5
Аналіз мережевих комунікацій

Виконала:
студентка 3 курсу
гр. ФБ-92
Шатковська Діана

Перевірив:
Якобчук Д.І.

Київ - 2021

Аналіз мережевих комунікацій

Мета роботи:

Отримати навички аналізу мережевих комунікацій ШПЗ.

Хід роботи

Завдання 1

Додайте INetSim у Cuckoo Sandbox. Проаналізуйте 3-5 зразків з theZoo.

Net-Worm.Win32.Kido

File *conficker*

Summary | Download | Resubmit sample | Download yara

Size	61.9KB
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
MD5	566119e4e5f4bda545b3b8af33c23698
SHA1	f00d3242a4761c55a532d642dd0631262d081af0
SHA256	523d40c69b0972ddeff0682fcb569e8a346cf10b2894479ab227bbb24e19846e
SHA512	Show SHA512
CRC32	AA5D3911
ssdeep	None
Yara	• UPX - (no description) • suspicious_packer_section - The packer/protector section names/keywords

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

- Yara rules detected for file (2 events)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- The executable is compressed using UPX (3 events)
- File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)
- File has been identified by 65 AntiVirus engines on VirusTotal as malicious (50 out of 65 events)

Ransomware.Cerber

File *cerber.exe*

Summary | Download | Resubmit sample | Download yara

Size	604.5KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8b6bc16fd137c09a08b02bbe1bb7d670
SHA1	c69a0f6c6f809c01db92ca658fcf1b643391a2b7
SHA256	e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678
SHA512	Show SHA512
CRC32	ED332B67
ssdeep	None
Yara	• DebuggerException__SetConsoleCtrl - (no description) • win_registry - Affect system registries • win_files_operation - Affect private profile

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

- Yara rules detected for file (3 events)
- Allocates read-write-execute memory (usually to unpack itself) (5 events)
- Queries for the computername (1 event)
- Command line console output was observed (1 event)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- One or more potentially interesting buffers were extracted, these generally contain injected code, configuration data, etc.
- Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (1 event)
- Executes one or more WMI queries (1 event)
- A process created a hidden window (2 events)

- Uses Windows utilities for basic Windows functionality (2 events)
- Raised Suricata alerts (1 event)
- Operates on local firewall's policies and settings (2 events)
- File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)
- File has been identified by 59 AntiVirus engines on VirusTotal as malicious (50 out of 59 events)

Ransomware.Rex

File *WTEpZSFwgb*

Summary

Download | Resubmit sample | Download yara

Size	7.3MB
Type	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, Go BuildID=fc5a3d09dbaf04f6ec0587eae8c207fe211c5530, stripped
MD5	5bd44a35094fe6f7794d895122ddfa62
SHA1	98172e49c3d5d70ffdcefd071f9762c58430a393
SHA256	762a4f2bf5ea4ff72fce674da1adf29f0b9357be18de4cd992d79198c56bb514
SHA512	Show SHA512
CRC32	F0DD41CB
ssdeep	None
Yara	• CrowdStrike_CSIT_18006_06 - Detects possible PHP-based webshells. The strings below are frequently used to obfuscate malicious webshell code. • shellcode - Matched shellcode byte patterns • network_smtp_raw - Communications smtp

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

- Yara rules detected for file (3 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)
- File has been identified by 35 AntiVirus engines on VirusTotal as malicious (35 events)

Встановимо INetSim:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install inetsim
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
inetsim is already the newest version (1.3.2+dfsg.1-1).
inetsim set to manually installed.
The following package was automatically installed and is no longer required:
  oracle-instantclient-basic
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1001 not upgraded.
```

Ізолюємо систему

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.132  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::20c:29ff:fe0a:fdcc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0a:fd:cc  txqueuelen 1000  (Ethernet)
        RX packets 1342628  bytes 1817377262 (1.6 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 487536  bytes 41638818 (39.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 506901  bytes 65104904 (62.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 506901  bytes 65104904 (62.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 down

┌──(kali㉿kali)-[~]
└─$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 506932  bytes 65115920 (62.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 506932  bytes 65115920 (62.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Піднімемо симуляцію за допомогою INetSim:

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim                                                          1 ×
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it ...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it ...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it ...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 45676) ===
Session ID:     45676
Listening on:   127.0.0.1
Real Date/Time: 2021-12-30 09:08:37
Fake Date/Time: 2021-12-30 09:08:37 (Delta: 0 seconds)
```

```
Forking services ...
 * dns_53_tcp_udp - started (PID 45680)
 * ident_113_tcp - started (PID 45693)
 * time_37_tcp - started (PID 45695)
 * irc_6667_tcp - started (PID 45690)
 * https_443_tcp - started (PID 45682)
 * daytime_13_tcp - started (PID 45697)
 * finger_79_tcp - started (PID 45692)
 * echo_7_udp - started (PID 45700)
 * daytime_13_udp - started (PID 45698)
 * syslog_514_udp - started (PID 45694)
 * ntp_123_udp - started (PID 45691)
 * time_37_udp - started (PID 45696)
 * echo_7_tcp - started (PID 45699)
 * discard_9_tcp - started (PID 45701)
 * http_80_tcp - started (PID 45681)
 * tftp_69_udp - started (PID 45689)
 * chargen_19_tcp - started (PID 45705)
 * pop3_110_tcp - started (PID 45685)
 * pop3s_995_tcp - started (PID 45686)
 * dummy_1_tcp - started (PID 45707)
 * smtps_465_tcp - started (PID 45684)
 * quotd_17_udp - started (PID 45704)
 * discard_9_udp - started (PID 45702)
 * quotd_17_tcp - started (PID 45703)
 * smtp_25_tcp - started (PID 45683)
 * ftp_21_tcp - started (PID 45687)
 * chargen_19_udp - started (PID 45706)
 * dummy_1_udp - started (PID 45708)
 * ftps_990_tcp - started (PID 45688)
 done.
Simulation running.
```

www.mozilla.org

Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Зупинимо симуляцію і переглянемо логи:

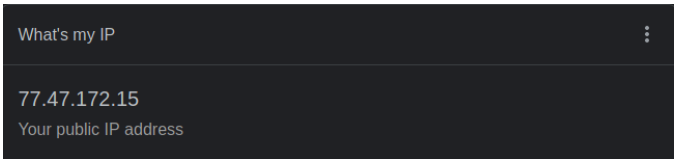
```
Simulation stopped.
 Report written to '/var/log/inetsim/report/report.45676.txt' (45 lines)
== INetSim main process stopped (PID 45676) ==
```

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/inetsim/report/report.45874.txt
== Report for session '45874' ==

Real start date            : 2021-12-30 09:13:25
Simulated start date       : 2021-12-30 09:13:25
Time difference on startup : none

2021-12-30 09:13:34  First simulated date in log file
2021-12-30 09:13:34  DNS connection, type: A, class: IN, requested name: canarytokens.org
2021-12-30 09:13:34  DNS connection, type: AAAA, class: IN, requested name: canarytokens.org
2021-12-30 09:13:40  DNS connection, type: A, class: IN, requested name: www.wikipedia.org
2021-12-30 09:13:40  DNS connection, type: AAAA, class: IN, requested name: www.wikipedia.org
2021-12-30 09:13:44  DNS connection, type: A, class: IN, requested name: support.mozilla.org
2021-12-30 09:13:44  DNS connection, type: AAAA, class: IN, requested name: support.mozilla.org
2021-12-30 09:13:53  HTTPS connection, method: GET, URL: https://www.wikipedia.org/, file name: /var/lib/inetsim/http/fak
efiles/sample.html
2021-12-30 09:13:53  DNS connection, type: A, class: IN, requested name: www.wikipedia.org
2021-12-30 09:13:53  DNS connection, type: AAAA, class: IN, requested name: www.wikipedia.org
2021-12-30 09:13:53  Last simulated date in log file
```

Завдання 2

Розгорніть OpenVPN, робота за протоколом TCP. На стороні клієнта встановіть з’єднання з OpenVPN сервером через HTTP проксі.

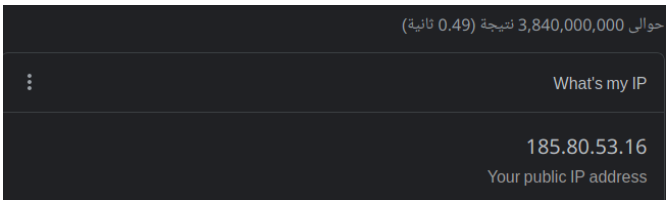
Моя зовнішня айпі-адреса до встановлення VPN:




```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat Netherlands_freeopenvpn_tcp.ovpn
################################
# FreeOpenVPN.Org config file #
# https://www.freeopenvpn.org #
################################

setenv UV_ID c57b5a462a0945a1be2231545434163c
setenv UV_NAME guarded-refuge-8353
client
dev tun
dev-type tun
remote nl1.freeopenvpn.org 443 tcp-client
nobind
persist-tun
cipher AES-128-CBC
auth SHA1
verb 2
mute 3
push-peer-info
ping 10
ping-restart 60
hand-window 70
server-poll-timeout 4
reneg-sec 2592000
sndbuf 393216
rcvbuf 393216
max-routes 1000
remote-cert-tls server
comp-lzo no
auth-user-pass
key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIFcTCCA1mgAwIBAgIIdO1gfGEKRc4wDQYJKoZIhvcNAQELBQAwRjEhMB8GA1UE
CgwYNWUxMWM5ZTRjNDdiMjE2NzUxOWU5ZWY2MSEwHwYDVQQDDBg1ZTExYzllNGM0
N2IyMTY3NTE5ZTlmMDMwHhcNMjAwMTA1MTEzNTAyWhcNMzAwMTA0MTEzNTAyWjBG
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn --config Netherlands_freeopenvpn_tcp.ovpn
2021-12-30 09:38:59 DEPRECATED OPTION: --max-routes option ignored.The number of routes is unlimited as of OpenVPN 2.4. T
his option will be removed in a future version, please remove it from your configuration.
2021-12-30 09:38:59 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-G
CM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change -
-cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2021-12-30 09:38:59 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] bu
ilt on May 14 2021
2021-12-30 09:38:59 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
🔐 Enter Auth Username: freeopenvpn
🔐 Enter Auth Password: *********
2021-12-30 09:39:34 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-30 09:39:34 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-30 09:39:34 TCP/UDP: Preserving recently used remote address: [AF_INET]185.80.53.16:443
2021-12-30 09:39:34 Attempting to establish TCP connection with [AF_INET]185.80.53.16:443 [nonblock]
2021-12-30 09:39:34 TCP connection established with [AF_INET]185.80.53.16:443
2021-12-30 09:39:34 TCP_CLIENT link local: (not bound)
2021-12-30 09:39:34 TCP_CLIENT link remote: [AF_INET]185.80.53.16:443
2021-12-30 09:39:34 VERIFY OK: depth=1, O=5e11c9e4c47b2167519e9ef6, CN=5e11c9e4c47b2167519e9f03
2021-12-30 09:39:34 VERIFY KU OK
2021-12-30 09:39:34 Validating certificate extended key usage
2021-12-30 09:39:34 NOTE: --mute triggered...
2021-12-30 09:39:34 4 variation(s) on previous 3 message(s) suppressed by --mute
2021-12-30 09:39:34 [5e11c9e6c47b2167519e9f07] Peer Connection Initiated with [AF_INET]185.80.53.16:443
2021-12-30 09:39:41 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2021-12-30 09:39:41 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-30 09:39:41 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2021-12-30 09:39:41 NOTE: --mute triggered...
2021-12-30 09:39:41 1 variation(s) on previous 3 message(s) suppressed by --mute
2021-12-30 09:39:41 TUN/TAP device tun0 opened
2021-12-30 09:39:41 net_iface_mtu_set: mtu 1500 for tun0
2021-12-30 09:39:41 net_iface_up: set tun0 up
2021-12-30 09:39:41 net_addr_v4_add: 192.168.245.240/24 dev tun0
2021-12-30 09:39:41 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent t
his
2021-12-30 09:39:41 Initialization Sequence Completed
```

Адреса при ввімкненому VPN:



Завдання 3

Додайте сертифікат CA mitmproxy у список довірених на клієнті.

Завдання 4

Розробіть застосунок, що емулює (sinkhole) сервер керування

```
┌──(kali㉿kali)-[~/lab5]
└─$ python3 server.py                                                    1 ✗
Client connected succesfully    IP: ('127.0.0.1', 58302)
Data received.
Disconnected.
```

```
┌──(kali㉿kali)-[~/lab5]
└─$ python3 client.py
Connection: Success!
Data sent..
Disconnected.
```

server.py

```
import socket

server = socket.socket()
server_ip = socket.gethostbyname(socket.gethostname())

server.bind((server_ip, 12284))
server.listen(1)
client, client_ip = server.accept()

mes = client.recv(1024).decode()
print("{}\tIP: {}".format(mes, client_ip))

with open("/home/kali/lab5/connection_data.txt", 'wb') as file:
    data = client.recv(2058)
    file.write(data)
    print("Data received.")

client.close()
print("Disconnected.")
```

client.py

```
import socket
import os
import subprocess

client = socket.socket()
client_ip = socket.gethostbyname(socket.gethostname())

client.connect((client_ip, 12284))

print('Connection: Success!')

client.send('Client connected succesfully'.encode())
```

```
if os.name == 'posix':
    info = (subprocess.getoutput('lscpu')).encode()
    client.send(info)
    print('Data sent..')

client.close()
print('Disconnected.')
```

отримані дані у файлі connection_data.txt:

```
┌──(kali㉿kali)-[~/lab5]
└─$ cat connection_data.txt
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Address sizes:                   40 bits physical, 48 bits virtual
Byte Order:                      Little Endian
CPU(s):                          4
On-line CPU(s) list:             0-3
Vendor ID:                       AuthenticAMD
Model name:                      AMD Ryzen 5 4600HSS with Radeon Graphics
CPU family:                      23
Model:                           96
Thread(s) per core:              1
Core(s) per socket:              2
Socket(s):                       2
Stepping:                        1
BogoMIPS:                        5988.75
Flags:                           fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxs
r sse sse2 ht syscall nx mmxext fxsr_opt rdtscp lm constant_tsc rep_good nopl tsc_reliable nonstop_tsc cpuid extd_apicid
 pni pclmulqdq ssse3 fma cx16 sse4_1 sse4_2 movbe popcnt aes xsave avx hypervisor lahf_lm extapic abm sse4a misalignsse
3dnowprefetch osvw ssbd vmmcall arat overflow_recov succor
Hypervisor vendor:               VMware
Virtualization type:             full
L1d cache:                       128 KiB (4 instances)
L1i cache:                       128 KiB (4 instances)
L2 cache:                        2 MiB (4 instances)
L3 cache:                        32 MiB (4 instances)
NUMA node(s):                    1
NUMA node0 CPU(s):               0-3
Vulnerability Itlb multihit:     Not affected
Vulnerability L1tf:              Not affected
Vulnerability Mds:               Not affected
Vulnerability Meltdown:          Not affected
Vulnerability Spec store bypass: Mitigation; Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1:        Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2:        Mitigation; Full AMD retpoline, STIBP disabled, RSB filling
Vulnerability Srbds:             Not affected
Vulnerability Tsx async abort:   Not affected
```