

## ДОДАТОК А

### Головне меню розроблених програм

Після запуску розробленої програми BMP\_CHECK.py користувачу буде запропоновано вказати абсолютний або відносний шлях до файлу зображення (рисунок А.1).

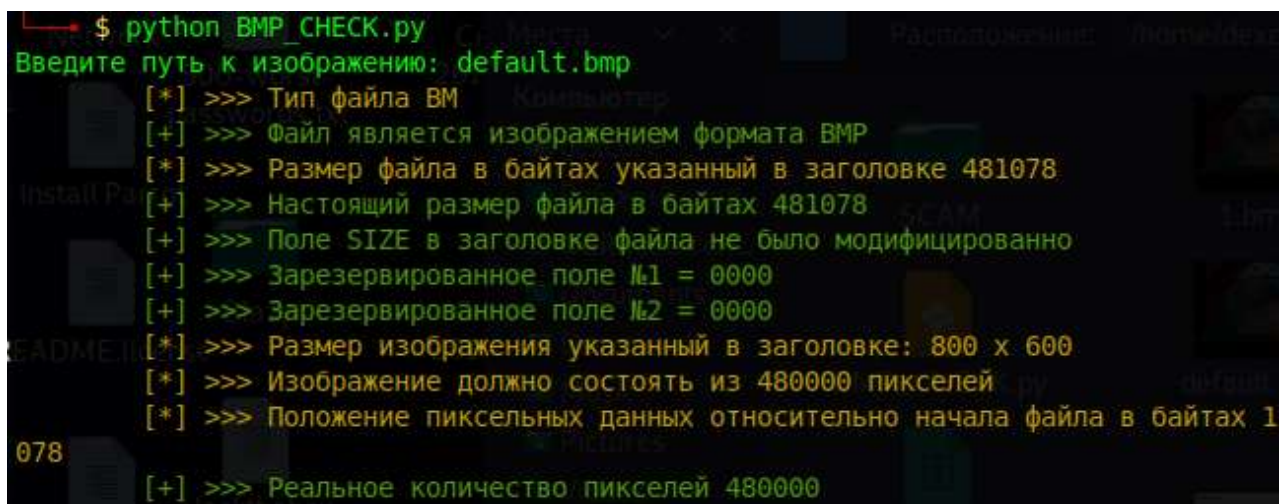


```
$ python BMP_CHECK.py
Введите путь к изображению: █
```

Рисунок А.1 – Запит шляху до файлу зображення

Після введення шляху, програма почне перевірку зображення за ключовими ознаками.

При перевірці оригінального зображення не буде виявлено жодних аномалій (рисунок А.2).



```
$ python BMP_CHECK.py
Введите путь к изображению: default.bmp
[*] >>> Тип файла ВМ
[+] >>> Файл является изображением формата BMP
[*] >>> Размер файла в байтах указанный в заголовке 481078
[+] >>> Настоящий размер файла в байтах 481078
[+] >>> Поле SIZE в заголовке файла не было модифицировано
[+] >>> Зарезервированное поле №1 = 0000
[+] >>> Зарезервированное поле №2 = 0000
[*] >>> Размер изображения указанный в заголовке: 800 x 600
[*] >>> Изображение должно состоять из 480000 пикселей
[*] >>> Положение пиксельных данных относительно начала файла в байтах 1078
[+] >>> Реальное количество пикселей 480000
```

Рисунок А.2 – Перевірка оригінального зображення

При перевірці інфікованого зображення виявлені аномалії за ключовими ознаками будуть виділені червоним кольором (рисунок А.3).

```

$ python BMP_CHECK.py
Введите путь к изображению: output.bmp
[*] >>> Тип файла BM
[+] >>> Файл является изображением формата BMP
[*] >>> Размер файла в байтах указанный в заголовке 123046121
[+] >>> Настоящий размер файла в байтах 481078
[!] >>> Поле SIZE в заголовке файла было модифицировано 123046121 != 481078
[!] >>> Зарезервированное поле M1 = effc
[!] >>> Зарезервированное поле M2 = ae4d
[*] >>> Размер изображения указанный в заголовке: 800 x 595
[*] >>> Изображение должно состоять из 476000 пикселей
[*] >>> Положение пиксельных данных относительно начала файла в байтах 1078
[!] >>> Реальное количество пикселей 480000 != 476000

```

Рисунок А.3 – Перевірка інфікованого зображення

Після запуску розробленої програми HID.py вона функціонує, як фоновий процес. Для коректної роботи програми необхідна наявність конфігураційного файлу (рисунок А.4).

```

HID.conf - Блокнот
Файл Правка Формат Вид Справка
#####
#                               HID                               #
# Программа для предотвращения HID-атак (Bad USB attack) #
#####

### Конфигурация пользователя ###
policy          =      "normal"
# Политика защиты -- Paranoid, Normal, Sneaky, LogOnly
password        =      "quack"
# (Только для уровня политики защиты Paranoid) Пароль - только нижний регистр
blacklist       =      "Command Prompt, Windows PowerShell" # Чёрный список программ

#### Дополнительные конфигурации ####
#Изменять значения по умолчанию необходимо только, если возникли ошибки в работе программы.
threshold       = 30      # Порог скорости между нажатиями клавиш в миллисекундах (по умолчанию: ~ 30
миллисекунд) | Все, что быстрее, считается подозрительным.
size            = 25      # Размер массива, который содержит историю скорости нажатия клавиш. (по
умлчанию: 25 нажатий клавиш).
randdrop        = 6       # Как часто нужно отбрасывать букву в скрытом режиме (по умолчанию: 6).
filename        = "log.txt" # Имя файла журнала.
allow_auto_type_software = True # Не блокировать программное обеспечение, такое как KeyPass или
LastPass, которое вводит нажатия клавиш через программное обеспечение. (По умолчанию: True).

```

Рисунок А.4 – Конфігураційний файл для програми HID.py

В даному файлі можна задати оду з чотирьох політик, що будуть використовуватися, пароль для розблокування вводу. Крім того можна задати

граничне значення швидкості, ім'я лог файлу, кількість символів, що будуть перервані у разі вибору політики “Sneaky”.

## ДОДАТОК Б

### Детальні результати сканування вірусних зразків різними антивірусними засобами

В цьому додатку наведені детальні результати сканування (рисунок Б.1-Б.6, Б.8-Б.9, Б.11-Б.12 та рисунок Б.14-Б.21). На всіх етапах використовувався один і той самий вірус. Спочатку був згенерований та просканований шелл-код в форматі raw у 2019 році (рисунок Б.1) та у 2020 (рисунок Б.2). Потім цей самий вірус був згенерований та перевірений в форматі exe 2019 рік (рисунок Б.3) та 2020 рік (рисунок Б.4). Була перевірена оригінальна програма PuTTY 2019 рік (рисунок Б.5) та 2020 рік (рисунок Б.6). Після цього був видалений цифровий підпис програми (рисунок Б.7) та проведене сканування у 2019 році (рисунок Б.8) та 2020 році (рисунок Б.9). Також була створена нова порожня секція в оригінальній програмі (рисунок Б.10) та проведена перевірка 2019 рік (рисунок Б.11) та 2020 рік (рисунок Б.12). Після цього в оригінальну PuTTY був впроваджений шелл-код за допомогою створення нової секції (рисунок Б.13), результати перевірки у 2019 році можна побачити на рисунку Б.14, та у 2020 році на рисунку Б.15. Також в оригінальну програму був впроваджений вірус з використанням code save, результати сканування 2019 року на рисунку Б.16, та 2020 року на рисунку Б.17. Після цього було проаналізоване оригінальне зображення 2019 рік (рисунок Б.18), 2020 рік (рисунок Б.19) та зображення з впровадженим вірусом 2019 рік (рисунок Б.20) та 2020 рік (рисунок Б.21).

66645f1a5214c778bd44c2fd43f384b19ecc82dd08e039e92e895de1d6ad565


341 B Size · 2019-04-02 15:54:18 UTC · 9 hours ago







21 / 59


21 engines detected this file

| DETECTION            | DETAILS                      | COMMUNITY                   |
|----------------------|------------------------------|-----------------------------|
| Ad-Aware             | Generic.PozemaA.79C48B57     | Trojan.Win32.Generic.4tc    |
| AhnLab-V3            | Bintraps/Shellcode           | Generic.PozemaA.79C48B57    |
| Avast                | Generic.PozemaA.79C48B57     | Win32.Sector-S [Trj]        |
| AVG                  | Win32.Sector-S [Trj]         | Generic.PozemaA.79C48B57    |
| ClamAV               | Win.Trojan.MSShellcode-7     | PowerShell.Downloader.26    |
| Emisoft              | Generic.PozemaA.79C48B57 [B] | Generic.PozemaA.79C48B57    |
| FireEye              | Generic.PozemaA.79C48B57     | Generic.PozemaA.79C48B57    |
| Kaspersky            | HEUR:Trojan.Win32.Generic    | Malware (M-Score=100)       |
| Microsoft            | Trojan:Win32/Melissa/ga?P    | Trojan.Dos.Shellcode.wsfvwj |
| Symantec             | Downloader                   | Win32.Trojan.Generic.Hnuu   |
| ZoneAlarm            | HEUR:Trojan.Win32.Generic    | Undetected                  |
| Avast-Mobile         | Undetected                   | Avira                       |
| Babable              | Undetected                   | Saidu                       |
| Bitav                | Undetected                   | CAT-QuickHeal               |
| CMC                  | Undetected                   | Comodo                      |
| Cyren                | Undetected                   | ESET-NOD32                  |
| F-Prot               | Undetected                   | F-Secure                    |
| Fortinet             | Undetected                   | Ikarus                      |
| Jiangmin             | Undetected                   | K7AntiVirus                 |
| K7GW                 | Undetected                   | Kingsoft                    |
| Malwarebytes         | Undetected                   | McAfee                      |
| McAfee-GW-Edition    | Undetected                   | Panda                       |
| Qihoo-360            | Undetected                   | Bitang                      |
| Sophos AV            | Undetected                   | SUPERAntiSpyware            |
| TACHYON              | Undetected                   | TheHacker                   |
| TotalDefense         | Undetected                   | TrendMicro                  |
| TrendMicro-HouseCall | Undetected                   | VBA32                       |
| VIPRE                | Undetected                   | VRebot                      |
| Yandex               | Undetected                   | Zillya                      |
| Zonar                | Undetected                   | Acronis                     |
| Alibaba              | Unable to process file type  | CrowdStrike Falcon          |
| Cybereason           | Unable to process file type  | Cylance                     |
| eGambit              | Unable to process file type  | Endgame                     |
| Palo Alto Networks   | Unable to process file type  | SentinelOne                 |
| Sophos ML            | Unable to process file type  | Symantec Mobile Insight     |
| Trapsim              | Unable to process file type  | Trustlook                   |
| Webroot              | Unable to process file type  |                             |

Рисунок Б.1 - Результат сканування шелл-код у форматі raw, що був згенерований за допомогою msfvenom 2019 рік


68645f1e5214c78bd44c2f043f35ab19eccb2dd0f08e039692e895de1d9ad565





29  
/ 61

🚫 29 engines detected this file

68645f1e5214c78bd44c2f043f35ab19eccb2dd0f08e039692e895de1d9ad565  
shd

341.00 KB    2020-11-12 16:22:48 UTC  
a trawler's age

| DETECTION                | DETAILS   | COMMUNITY  |
|--------------------------|---|--|
| Ad-Aware                 | <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857       | AvastLab <span style="color: red;">🚫</span> Trojan.Win32.Camerix.46                      |
| AhnLab-V3                | <span style="color: red;">🚫</span> Win32/Downloader               | ALYac <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857                        |
| Antiy-AVL                | <span style="color: red;">🚫</span> Trojan.Win32.RozonaA           | Avast <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857                        |
| Avast                    | <span style="color: red;">🚫</span> Win32/Sworn1-5 [Trj]           | AVG <span style="color: red;">🚫</span> Win32/Sworn1-5 [Trj]                              |
| BitDefender              | <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857       | ClamAV <span style="color: red;">🚫</span> Win32/Trojan.MSDNHackcode-7                    |
| DrWeb                    | <span style="color: red;">🚫</span> PowerSploit.Down.Loader.36     | Emisoft <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857 (B)                  |
| eScan                    | <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857       | ESET-NOD32 <span style="color: red;">🚫</span> Win32/Rozona.A#E                           |
| FireEye                  | <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857       | Fortinet <span style="color: red;">🚫</span> DataRozona.A#E#T                             |
| GData                    | <span style="color: red;">🚫</span> Generic.RozonaA.79C4d857       | Ikarus <span style="color: red;">🚫</span> Trojan.Win32.Antiexpenter                      |
| Kaspersky                | <span style="color: red;">🚫</span> Trojan.Win32.Shellcode         | MAX <span style="color: red;">🚫</span> Malware (AI Score=100)                            |
| Microsoft                | <span style="color: red;">🚫</span> Trojan.Win32.Meterpreter.gen#E | NANO-Antivirus <span style="color: red;">🚫</span> Trojan.Dos.Shellcode.mw#nsj            |
| Qhoo-360                 | <span style="color: red;">🚫</span> Win32/Trojan.sdl               | Sophos AV <span style="color: red;">🚫</span> ATK/Shellcode-A                             |
| Sophos ML                | <span style="color: red;">🚫</span> ATK/Shellcode-A                | Symantec <span style="color: red;">🚫</span> Downloader                                   |
| Tencent                  | <span style="color: red;">🚫</span> Win32/Trojan.Generic.Hack      | Tencent <span style="color: red;">🚫</span> Trojan.AntiSecurp565#T                        |
| ZonaAlarm by Check-Point | <span style="color: red;">🚫</span> Trojan.Win32.Shellcode         | Avira (HO Cloud) <span style="color: green;">✅</span> Undetected                         |
| Baidu                    | <span style="color: green;">✅</span> Undetected                   | BitDefender Theta <span style="color: green;">✅</span> Undetected                        |
| Bkav                     | <span style="color: green;">✅</span> Undetected                   | CAT-QuickHeal <span style="color: green;">✅</span> Undetected                            |
| CMC                      | <span style="color: green;">✅</span> Undetected                   | Comodo <span style="color: green;">✅</span> Undetected                                   |
| Cyren                    | <span style="color: green;">✅</span> Undetected                   | Cyren <span style="color: green;">✅</span> Undetected                                    |
| F-Secure                 | <span style="color: green;">✅</span> Undetected                   | Grisoft <span style="color: green;">✅</span> Undetected                                  |
| Jiangmin                 | <span style="color: green;">✅</span> Undetected                   | K7AntiVirus <span style="color: green;">✅</span> Undetected                              |
| K7PW                     | <span style="color: green;">✅</span> Undetected                   | Kingsoft <span style="color: green;">✅</span> Undetected                                 |
| MaxSecure                | <span style="color: green;">✅</span> Undetected                   | MaxSecure <span style="color: green;">✅</span> Undetected                                |
| McAfee                   | <span style="color: green;">✅</span> Undetected                   | McAfee-GW-Edition <span style="color: green;">✅</span> Undetected                        |
| Panda                    | <span style="color: green;">✅</span> Undetected                   | Panda <span style="color: green;">✅</span> Undetected                                    |
| Sangfor Engine Zero      | <span style="color: green;">✅</span> Undetected                   | SUPERAntiSpyware <span style="color: green;">✅</span> Undetected                         |
| TACHYON                  | <span style="color: green;">✅</span> Undetected                   | TrendMicro <span style="color: green;">✅</span> Undetected                               |
| TrendMicro-HouseCall     | <span style="color: green;">✅</span> Undetected                   | YBAll <span style="color: green;">✅</span> Undetected                                    |
| ViPINE                   | <span style="color: green;">✅</span> Undetected                   | Villabot <span style="color: green;">✅</span> Undetected                                 |
| Virva                    | <span style="color: green;">✅</span> Undetected                   | Zoner <span style="color: green;">✅</span> Undetected                                    |
| Avast                    | <span style="color: grey;">⚠️</span> Unable to process file type  | Alibaba <span style="color: grey;">⚠️</span> Unable to process file type                 |
| SecureAge APEX           | <span style="color: grey;">⚠️</span> Unable to process file type  | Avast-Mobile <span style="color: grey;">⚠️</span> Unable to process file type            |
| CrowdStrike Falcon       | <span style="color: grey;">⚠️</span> Unable to process file type  | Cybereason <span style="color: grey;">⚠️</span> Unable to process file type              |
| Cylance                  | <span style="color: grey;">⚠️</span> Unable to process file type  | eScanBit <span style="color: grey;">⚠️</span> Unable to process file type                |
| Elastic                  | <span style="color: grey;">⚠️</span> Unable to process file type  | Palo Alto Networks <span style="color: grey;">⚠️</span> Unable to process file type      |
| SentinelOne (Static ML)  | <span style="color: grey;">⚠️</span> Unable to process file type  | Symantec Mobile insight <span style="color: grey;">⚠️</span> Unable to process file type |
| Trojanix                 | <span style="color: grey;">⚠️</span> Unable to process file type  | Trustlook <span style="color: grey;">⚠️</span> Unable to process file type               |
| Webroot                  | <span style="color: grey;">⚠️</span> Unable to process file type  |  |

Рисунок Б.2 - Результат сканування шелл-код у форматі raw, що був згенерований за допомогою msfvenom 2020 рік

381aff5e567104b85f3c64fd929626f66980f88172ce54947f21bd117f71557b

53 engines detected this file

72.07 KB Size | 2019-04-02 13:30:41 UTC a moment ago

381aff5e567104b85f3c64fd929626f66980f88172ce54947f21bd117f71557b

72.07 KB Size | 2019-04-02 13:30:41 UTC a moment ago

EXE

| DETECTION            | DETAILS                            | COMMUNITY                         |
|----------------------|------------------------------------|-----------------------------------|
| Acronis              | Suspicious                         | Trojan.CryptZ.Gen                 |
| AegisLab             | Heuristic Win32.BDF.31c            | Trojan.Win32.Shell.R1883          |
| Alibaba              | Trojan.Win32/Melanger.gen@518a     | Trojan.CryptZ.Gen                 |
| Avast                | Trojan.CryptZ.Gen                  | Win32-SpPatch (Win)               |
| AVG                  | Win32-SpPatch (Win)                | TR/Crypt.EPACK.Gen2               |
| BitDefender          | Trojan.CryptZ.Gen                  | Win32.Fam/VT.Boron/Ho.Trojan      |
| CAT-QuickHeal        | Trojan.Swroot.A                    | Win.Trojan.MSShellcode.F          |
| Comodo               | Trojan.Win32/Rozema.A@4webp        | Win/malicious_confidence_100% (D) |
| Cybereason           | Malicious.Shellcode                | Unsafe                            |
| Cyren                | Win32/Swroot.A.gen/Eldorado        | Trojan.Swroot.1                   |
| eGambit              | Trojan.Generic                     | Trojan.CryptZ.Gen (8)             |
| Endgame              | Malicious (high Confidence)        | Trojan.CryptZ.Gen                 |
| ESET-NOD32           | A Variant Of Win32/Rozema.ED       | Win32/Swroot.A.gen/Eldorado       |
| F-Secure             | Trojan.TR/Crypt.EPACK.Gen2         | Generic.mg.38369553d5c0bee        |
| Fortinet             | Win32/Swroot.C/tr                  | Trojan.CryptZ.Gen                 |
| Ikarus               | Trojan.Win32.Swroot                | Trojan ( 004c4811 )               |
| K7GW                 | Trojan ( 004c4811 )                | Packed.Win32.BDF.a                |
| MAX                  | Malware (ai Score=88)              | Swroot.1                          |
| McAfee-QW-Edition    | BehavesLike.Win32.Swroot.H         | Trojan.Win32/Melanger.gen.C       |
| NANO-Antivirus       | Trojan.Win32.Shellcode.avehwa      | HEUR/HQVM20.1.4178.Malware.Gen    |
| Rising               | Trojan.Rozema@80/NQ100% (RDM+ s... | DFI - Malicious.PE                |
| Sophos AV            | Mal/EncPk-FZ                       | Heuristic                         |
| SUPERAntiSpyware     | Trojan.Backdoor.Prisontry          | Packed.Generic.347                |
| Trapmine             | Malicious (high ml score)          | BKDR_SWROTF.SM                    |
| TrendMicro-HouseCall | BKDR_SWROTF.SM                     | Trojan.Win32/Etcob.Gen            |
| Webroot              | Trojan.Win32/Swroot.A              | Trojan.Rozema.Gen.1               |
| ZoneAlarm            | Packed.Win32.BDF.a                 | Undetected                        |
| Avast-Mobile         | Undetected                         | Undetected                        |
| Baidu                | Undetected                         | Undetected                        |
| Jiangmin             | Undetected                         | Undetected                        |
| Malwarebytes         | Undetected                         | Undetected                        |
| Panda                | Undetected                         | Undetected                        |
| Tencent              | Undetected                         | Undetected                        |
| TotalDefense         | Undetected                         | Undetected                        |
| VBA32                | Undetected                         | Undetected                        |
| Zoner                | Undetected                         | Undetected                        |
|                      |                                    | Symantec Mobile Insight           |

Рисунок Б.3 - Результат сканування шелл-код у форматі ехе, що був згенерований за допомогою msfvenom 2019 рік

381a1fe667104b85f1c64f9296286909f88172ae54947021bd11771557b

63 engines detected this file

381a1fe667104b85f1c64f9296286909f88172ae54947021bd11771557b.exe  
72.07 KB  
2020-11-13 16:33 UTC  
3 minutes ago

Community score

STATUS: **malicious** | **passed**

| DETECTION                | DETAILS | RELATIONS                           | BEHAVIOR | COMMUNITY               |                                      |
|--------------------------|---------|-------------------------------------|----------|-------------------------|--------------------------------------|
| Acronis                  |         | ⚠️ Suspicious                       |          | Ad-Aware                | ⚠️ Trojan.Crypt2.Gen                 |
| Aegix Lab                |         | ⚠️ Hacktool.Win32.SDF-3c            |          | AhnLab-V3               | ⚠️ Trojan.Win32.Shell.HQ83           |
| Alibaba                  |         | ⚠️ Trojan.Win32/Meterpreter.SDF     |          | ALYac                   | ⚠️ Trojan.Crypt2.Gen                 |
| Antiy-AVL                |         | ⚠️ Trojan/Packed.Win32.SDF          |          | Secunia APEX            | ⚠️ Malicious                         |
| Avast                    |         | ⚠️ Trojan.Crypt2.Gen                |          | Avast                   | ⚠️ Win32.Shellch [Worm]              |
| AVG                      |         | ⚠️ Win32.SelfPact [Worm]            |          | Avira Pro Cloud         | ⚠️ TR/Pack.HQ.Ce12                   |
| BitDefender              |         | ⚠️ Trojan.Crypt2.Gen                |          | BitDefender Theta       | ⚠️ Gen/HijackBot-34634.exe/Win32/Cop |
| Bkav                     |         | ⚠️ Win32.FamV1.Rover/Hic.Trojan     |          | CAT-QuickHeal           | ⚠️ Trojan.Swroot.A                   |
| CamScanner               |         | ⚠️ Win32.Trojan.MSDWebcode-7        |          | Comodo                  | ⚠️ Troj/Worm.Win32.Mozilla.AB4jvdw   |
| CrowdStrike Falcon       |         | ⚠️ Win/Malicious_confidence_100%_W0 |          | Cyberason               | ⚠️ MW/Cloud.Softest                  |
| Cyren                    |         | ⚠️ Win32/Swroot.A.gen/Sdorado       |          | Cyren                   | ⚠️ Malicious (score: 100)            |
| eScan                    |         | ⚠️ Trojan.Generic                   |          | DrWeb                   | ⚠️ Trojan.Swroot.1                   |
| Emisoft                  |         | ⚠️ Trojan.Crypt2.Gen (B)            |          | EsScan                  | ⚠️ Trojan.Crypt2.Gen                 |
| ESET-NOD32               |         | ⚠️ A Variant Of Win32/Rovena.ED     |          | F-Secure                | ⚠️ Trojan/TR/Pack.HQ.Ce12            |
| FireEye                  |         | ⚠️ Generic.mg.3d3e5d33b0b0e4ee      |          | Fortinet                | ⚠️ Win32.Generic.AC.C1hr             |
| GData                    |         | ⚠️ Trojan.Crypt2.Gen                |          | Grisoft                 | ⚠️ Trojan.Win32.Swroot.A.v32         |
| Ikarus                   |         | ⚠️ Trojan.Win32.Swroot              |          | K7AntiVirus             | ⚠️ Trojan (204c8f81)                 |
| K7GW                     |         | ⚠️ Trojan (204c8f81)                |          | Kaspersky               | ⚠️ HEUR:Trojan.Win32.Generic         |
| Malwarebytes             |         | ⚠️ Trojan.Firmware                  |          | MAX                     | ⚠️ Malware (ai Score=100)            |
| MaxSecure                |         | ⚠️ Trojan/Malware.300783.suagen     |          | McAfee                  | ⚠️ Swroot.1                          |
| McAfee-GW-Edison         |         | ⚠️ BehaviorLike.Win32.Swroot.H      |          | Microsoft               | ⚠️ Trojan.Win32/Meterpreter.gen.C    |
| NANO-Antivirus           |         | ⚠️ Trojan.Win32.Shellcode.exe/Win32 |          | Palo Alto Networks      | ⚠️ Generic.HI                        |
| Panda                    |         | ⚠️ Trj/GdSte.A                      |          | Qihoo-360               | ⚠️ Win32/Trojan.Shr                  |
| Rising                   |         | ⚠️ HackTool.Swroot.H4AT7 [CLASSIC]  |          | Sangfor Engine Zero     | ⚠️ Malware                           |
| SentinelOne (Static ML)  |         | ⚠️ Static AI - Malicious PE         |          | Sophos AV               | ⚠️ ATK/SH-12                         |
| Sophos ML                |         | ⚠️ MAL/Generis-II + ATK/SH-12       |          | SUPERAntiSpyware        | ⚠️ Trojan.Backdoor.Shell             |
| Symantec                 |         | ⚠️ Packed.Generic.347               |          | Tencent                 | ⚠️ Win32/Trojan.Generic.Liga         |
| TrendMicro               |         | ⚠️ BDR_SWRORT.SM                    |          | TrendMicro-HomeCall     | ⚠️ BDR_SWRORT.SM                     |
| VIPRE                    |         | ⚠️ Trojan.Win32/Swroot.B (s)        |          | VirusBolt               | ⚠️ Trojan.Win32.Shell.Ce12           |
| Webroot                  |         | ⚠️ Trojan.Win32/Swroot.A            |          | Tencent                 | ⚠️ Trojan.Firmware.Gen.1             |
| ZoneAlarm by Check-Point |         | ⚠️ HEUR:Trojan.Win32.Generic        |          | Baidu                   | ⚠️ Undetected                        |
| CMC                      |         | ⚠️ Undetected                       |          | Jiangmin                | ⚠️ Undetected                        |
| Kingsoft                 |         | ⚠️ Undetected                       |          | TACHYON                 | ⚠️ Undetected                        |
| TotalDefense             |         | ⚠️ Undetected                       |          | VBA32                   | ⚠️ Undetected                        |
| Zillya                   |         | ⚠️ Undetected                       |          | Zoner                   | ⚠️ Undetected                        |
| Avast-Mobile             |         | ⚠️ Unable to process file type      |          | Symantec Mobile Insight | ⚠️ Unable to process file type       |
| TrojanFire               |         | ⚠️ Unable to process file type      |          | Trustlook               | ⚠️ Unable to process file type       |

Рисунок Б.4 - Результат сканування шелл-код у форматі exe, що був згенерований за допомогою msfvenom 2020 рік

fc7a687c2d828fd71199e59fa68bd55be20852d6c492d655b4991a3ea2dca2

1 / 71

One engine detected this file

fc7a687c2d828fd71199e59fa68bd55be20852d6c492d655b4991a3ea2dca2  
PuTTY Portable  
Size: 1.38 MB  
2019-04-02 13:37:58 UTC  
4 months ago

EXE

Community Note

DETECTION DETAILS BEHAVIOR COMMUNITY

|                      |  |                         |                                  |
|----------------------|--|-------------------------|----------------------------------|
| Rising               | Malware Heuristic.ML26(87%) (AI-LITE k...) | Acronis                 | Undetected                       |
| Ad-Aware             | Undetected                                 | AegisLab                | Undetected                       |
| AhoLab-V3            | Undetected                                 | Alibaba                 | Undetected                       |
| ALYac                | Undetected                                 | Antiy-AVL               | Undetected                       |
| Arcabit              | Undetected                                 | Avast                   | Undetected                       |
| Avast-Mobile         | Undetected                                 | AVG                     | Undetected                       |
| Avira                | Undetected                                 | Babable                 | Undetected                       |
| Baidu                | Undetected                                 | BitDefender             | Undetected                       |
| Bkav                 | Undetected                                 | CAT-QuickHeal           | Undetected                       |
| ClamAV               | Undetected                                 | CMC                     | Undetected                       |
| Comodo               | Undetected                                 | CrowdStrike Falcon      | Undetected                       |
| Cybereason           | Undetected                                 | Cylance                 | Undetected                       |
| Cyren                | Undetected                                 | DrWeb                   | Undetected                       |
| eGambit              | Undetected                                 | Emisoft                 | Undetected                       |
| Endgame              | Undetected                                 | eScan                   | Undetected                       |
| ESET-NOD32           | Undetected                                 | F-Prot                  | Undetected                       |
| F-Secure             | Undetected                                 | FireEye                 | Undetected                       |
| Fortinet             | Undetected                                 | GData                   | Undetected                       |
| Ikarus               | Undetected                                 | Jiangmin                | Undetected                       |
| K7AntiVirus          | Undetected                                 | K7GW                    | Undetected                       |
| Kaspersky            | Undetected                                 | Kingsoft                | Undetected                       |
| Malwarebytes         | Undetected                                 | MAX                     | Undetected                       |
| McAfee               | Undetected                                 | McAfee-GW-Edition       | Undetected                       |
| Microsoft            | Undetected                                 | NANO-Antivirus          | Undetected                       |
| Palo Alto Networks   | Undetected                                 | Panda                   | Undetected                       |
| Qihoo-360            | Undetected                                 | SentinelOne             | Undetected                       |
| Sophos AV            | Undetected                                 | Sophos ML               | Undetected                       |
| SUPERAntiSpyware     | Undetected                                 | Symantec                | Undetected                       |
| TACHYON              | Undetected                                 | Tencent                 | Undetected                       |
| TheHacker            | Undetected                                 | TotalDefense            | Undetected                       |
| Trapsine             | Undetected                                 | TrendMicro              | Undetected                       |
| TrendMicro-HouseCall | Undetected                                 | Trustlook               | Undetected                       |
| VBA32                | Undetected                                 | ViRobot                 | Undetected                       |
| Webroot              | Undetected                                 | Yandex                  | Undetected                       |
| Zillya               | Undetected                                 | ZoneAlarm               | Undetected                       |
| Zoner                | Undetected                                 | Symantec Mobile Insight | Undetected. AI-powered file type |

Рисунок Б.5 - Результат сканування оригінального PuTTY 2019 рік

Ac7a687c2d828871100e59f6af02b555be20852d6c492d955b4891a3ba2dca2

1  
172

One engine detected this file

fu7a687c2d828871100e59f6af02b555be20852d6c492d955b4891a3ba2dca2  
PuTTY Portable  
1.38 MB  
2020-10-13 16:34:29 UTC  
a moment ago  
EXE

Connect Scan

UNSAFE SIGNATURE Risk Severity (none) Signed

| DETECTION                | DETAILS                     | BEHAVIOR                | COMMUNITY                   |
|--------------------------|-----------------------------|-------------------------|-----------------------------|
| Tandex                   | Trojan.Gen/Aesgrf480G5IA    | Acronis                 | Undetected                  |
| Ad-Aware                 | Undetected                  | AegisLab                | Undetected                  |
| AhnLab-V3                | Undetected                  | Alibaba                 | Undetected                  |
| ALYac                    | Undetected                  | Avily-WL                | Undetected                  |
| SecureAge APEX           | Undetected                  | Avast                   | Undetected                  |
| Avast                    | Undetected                  | AVG                     | Undetected                  |
| Avira (no cloud)         | Undetected                  | Baidu                   | Undetected                  |
| BitDefender              | Undetected                  | BitDefender Theta       | Undetected                  |
| Bkav                     | Undetected                  | CAT-QuackHeal           | Undetected                  |
| CcmAV                    | Undetected                  | CMC                     | Undetected                  |
| Comodo                   | Undetected                  | CrowdStrike Falcon      | Undetected                  |
| Cybereason               | Undetected                  | Cyence                  | Undetected                  |
| Cynet                    | Undetected                  | Cyren                   | Undetected                  |
| DrWeb                    | Undetected                  | eGambit                 | Undetected                  |
| Elastic                  | Undetected                  | Emisoft                 | Undetected                  |
| eScan                    | Undetected                  | ESET-NOD32              | Undetected                  |
| F-Secure                 | Undetected                  | FireEye                 | Undetected                  |
| Fortinet                 | Undetected                  | GDData                  | Undetected                  |
| Geldmifft                | Undetected                  | Ikarus                  | Undetected                  |
| Jiangmin                 | Undetected                  | ITAVirVirus             | Undetected                  |
| K7GW                     | Undetected                  | Kaspersky               | Undetected                  |
| Kingsoft                 | Undetected                  | McAfeeBytes             | Undetected                  |
| MAX                      | Undetected                  | MaxSecure               | Undetected                  |
| McAfee                   | Undetected                  | McAfee-GW-Edition       | Undetected                  |
| Microsoft                | Undetected                  | MSNG-Antivirus          | Undetected                  |
| Palo Alto Networks       | Undetected                  | Panda                   | Undetected                  |
| Qihoo-360                | Undetected                  | Shang                   | Undetected                  |
| Sangfor Engine Zero      | Undetected                  | SentinelOne (Static ML) | Undetected                  |
| Sophos AV                | Undetected                  | Sophos ML               | Undetected                  |
| SOPHOS Antispyware       | Undetected                  | Symantec                | Undetected                  |
| TACHYON                  | Undetected                  | Tencent                 | Undetected                  |
| TotalDefense             | Undetected                  | TrendMicro              | Undetected                  |
| TrendMicro-HouseCall     | Undetected                  | VBA32                   | Undetected                  |
| VHE                      | Undetected                  | Virusok                 | Undetected                  |
| Webroot                  | Undetected                  | Zillya                  | Undetected                  |
| ZonaAlarm by Check Point | Undetected                  | Zoner                   | Undetected                  |
| Avast-Mobile             | Unable to process file type | Symantec Mobile Insight | Unable to process file type |
| ThreatSense              | Unable to process file type | Trustlook               | Unable to process file type |

Рисунок Б.6 - Результат сканування оригінального PuTTY 2020 рік



35d93763121ced7391ef11b680f8520771209d38593a5d66089338f64b2fc2a

3 engines detected this file

35d93763121ced7391ef11b680f8520771209d38593a5d66089338f64b2fc2a  
PuTTY Portable  
Size: 1.35 MB | 2019-04-02 13:38:56 UTC | a month ago  
EXE

| DETECTION               | DETAILS                                      | COMMUNITY            |                             |
|-------------------------|--|----------------------|-----------------------------|
| Blav                    | HW32.Patched                                 | McAfee-OW-Edition    | Behaved.Like.Wizard.Dropper |
| BitDefender             | MALWARE.HAZARD.ML.NET.PC (A-LITE)            | Acroria              | Undetected                  |
| BitDefender             | Undetected                                   | AegisLab             | Undetected                  |
| BitDefender             | Undetected                                   | Alibaba              | Undetected                  |
| BitDefender             | Undetected                                   | Anti-VXL             | Undetected                  |
| BitDefender             | Undetected                                   | Avast                | Undetected                  |
| BitDefender             | Undetected                                   | AVG                  | Undetected                  |
| BitDefender             | Undetected                                   | Bababab              | Undetected                  |
| BitDefender             | Undetected                                   | BitDefender          | Undetected                  |
| BitDefender             | Undetected                                   | ClamAV               | Undetected                  |
| BitDefender             | Undetected                                   | Comodo               | Undetected                  |
| BitDefender             | Undetected                                   | Cybereason           | Undetected                  |
| BitDefender             | Undetected                                   | Cyren                | Undetected                  |
| BitDefender             | Undetected                                   | eGambit              | Undetected                  |
| BitDefender             | Undetected                                   | Endgame              | Undetected                  |
| BitDefender             | Undetected                                   | ESET-NOD32           | Undetected                  |
| BitDefender             | Undetected                                   | F-Secure             | Undetected                  |
| BitDefender             | Undetected                                   | Fortinet             | Undetected                  |
| BitDefender             | Undetected                                   | Ikarus               | Undetected                  |
| BitDefender             | Undetected                                   | KTAntiVirus          | Undetected                  |
| BitDefender             | Undetected                                   | Kaspersky            | Undetected                  |
| BitDefender             | Undetected                                   | Malwarebytes         | Undetected                  |
| BitDefender             | Undetected                                   | McAfee               | Undetected                  |
| BitDefender             | Undetected                                   | NANO-Antivirus       | Undetected                  |
| BitDefender             | Undetected                                   | Panda                | Undetected                  |
| BitDefender             | Undetected                                   | SentinelOne          | Undetected                  |
| BitDefender             | Undetected                                   | Sophos ML            | Undetected                  |
| BitDefender             | Undetected                                   | Symantec             | Undetected                  |
| BitDefender             | Undetected                                   | Tencent              | Undetected                  |
| BitDefender             | Undetected                                   | Trapmine             | Undetected                  |
| BitDefender             | Undetected                                   | TrendMicro-HouseCall | Undetected                  |
| BitDefender             | Undetected                                   | VBA32                | Undetected                  |
| BitDefender             | Undetected                                   | Webroot              | Undetected                  |
| BitDefender             | Undetected                                   | Zillya               | Undetected                  |
| BitDefender             | Undetected                                   | Zoner                | Undetected                  |
| Symantec Mobile Insight | Unable to connect to Symantec Mobile Insight |                      |                             |

Рисунок Б.8 - Результат сканування оригінального PuTTY з видаленим цифровим підписом 2019 рік

fc7a687c2d828d77f99e079e488d55e20852d6c492a955e4901a3ea23ca2

1  
172

One engine detected this file

fc7a687c2d828d77f99e079e488d55e20852d6c492a955e4901a3ea23ca2  
PuTTY Portable  
1.38 MB  
Size  
2020-11-13 16:34:29 UTC  
a moment ago  
EXE

DETECTION DETAILS BEHAVIOR COMMUNITY 1

| Vendor                   | Detection                       | Category                | Status                          |
|--------------------------|---------------------------------|-------------------------|---------------------------------|
| Trend Micro              | Trojan.Gen/Acgr/fv64Og5IA       | Acronis                 | Undetected                      |
| Ad-Aware                 | Undetected                      | Avast!Lab               | Undetected                      |
| AhnLab-V3                | Undetected                      | Alibaba                 | Undetected                      |
| Avast                    | Undetected                      | Antiy-AVL               | Undetected                      |
| SecureAge APEX           | Undetected                      | Arcabit                 | Undetected                      |
| Avast                    | Undetected                      | AVG                     | Undetected                      |
| Avira (no cloud)         | Undetected                      | Baidu                   | Undetected                      |
| BitDefender              | Undetected                      | BitDefenderTheta        | Undetected                      |
| Bkav                     | Undetected                      | CAT-QuickHeal           | Undetected                      |
| ClamAV                   | Undetected                      | CMC                     | Undetected                      |
| Comodo                   | Undetected                      | CrowdStrike Falcon      | Undetected                      |
| Cybereason               | Undetected                      | Cyren                   | Undetected                      |
| Cyren                    | Undetected                      | Cyren                   | Undetected                      |
| DrWeb                    | Undetected                      | eGambit                 | Undetected                      |
| Elastic                  | Undetected                      | Emisoft                 | Undetected                      |
| eScan                    | Undetected                      | ESET-NOD32              | Undetected                      |
| F-Secure                 | Undetected                      | FireEye                 | Undetected                      |
| Fortinet                 | Undetected                      | GGIA                    | Undetected                      |
| Gridinsoft               | Undetected                      | Ikarus                  | Undetected                      |
| Jiangmin                 | Undetected                      | ITAVI-Virus             | Undetected                      |
| K7GW                     | Undetected                      | Kaspersky               | Undetected                      |
| Kingsoft                 | Undetected                      | Malwarebytes            | Undetected                      |
| MAX                      | Undetected                      | MaxSecure               | Undetected                      |
| McAfee                   | Undetected                      | McAfee-GW-Edition       | Undetected                      |
| Microsoft                | Undetected                      | MAND-Antivirus          | Undetected                      |
| Palo Alto Networks       | Undetected                      | Panda                   | Undetected                      |
| Qihoo-360                | Undetected                      | Rising                  | Undetected                      |
| Sangfor Engine Zero      | Undetected                      | SentinelOne (Static ML) | Undetected                      |
| Sophos AV                | Undetected                      | Sophos ML               | Undetected                      |
| SUPERAntiSpyware         | Undetected                      | Symantec                | Undetected                      |
| TACHYON                  | Undetected                      | Tencent                 | Undetected                      |
| TotalDefense             | Undetected                      | TrendMicro              | Undetected                      |
| TrendMicro-HouseCall     | Undetected                      | VBA32                   | Undetected                      |
| VHE                      | Undetected                      | Virusit                 | Undetected                      |
| Webroot                  | Undetected                      | Zillya                  | Undetected                      |
| ZonaAlarm by Check Point | Undetected                      | Zoner                   | Undetected                      |
| Avast-Mobile             | Unable to process the signature | Symantec Mobile Insight | Unable to process the signature |
| Truprise                 | Unable to process the signature | Truebot                 | Unable to process the signature |

Рисунок Б.9 - Результат сканування оригінального PuTTY з видаленим цифровим підписом 2020 рік

```
!- $ backdoor-factory -f PuTTY.exe -s user_supplied_shellcode_threaded -U section -a -Z -o PuTTY+section0.exe
Author: Joshua Pitts
Email: the.midnite.runr[-at ]gmail<d o-t>com
Twitter: @midnite_runr
IRC: freenode.net #BDFactory

Version: 3.4.2

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Creating Code Cave
- Adding a new section to the exe/dll for shellcode injection
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File PuTTY+section0.exe is in the 'backdoored' directory
```

Рисунок Б.10 – Створення нової порожньої секції в оригінальному PuTTY

30 / 61

30 engines detected this file

Bb6d84d88ffedce6a5b4834d9840128f4c4630fb3b75b8bd07bf366a8d3883e  
PuTTY.exe (2019-04-04)

1.36 MB Size | 2019-04-04 12:19:49 UTC | 1 minute ago

EXE

| DETECTION               | DETAILS                           | COMMUNITY          |                                       |
|-------------------------|-----------------------------------|--------------------|---------------------------------------|
| AegisLab                | 1 Trojan.Win32.Patched.BSQ        | Avast              | 1 Win32:SaiCode                       |
| AVG                     | 1 Win32:SaiCode                   | Avira              | 1 TR/Patched.sai                      |
| Bkav                    | 1 HW32-Packed                     | ClamAV             | 1 Win.Trojan.BDFactory-6              |
| Comodo                  | 1 Troj/Win32-Fixers.A@hwjwp       | CrowdStrike Falcon | 1 WinMalicious_confidence_100%_01     |
| CyLance                 | 1 Unsafe                          | Cyren              | 1 Win32/Serwit.C                      |
| DrWeb                   | 1 Trojan.Serwit.1                 | eGambit            | 1 PE_HowToInstallSig                  |
| Endgame                 | 1 Malicious (moderate Confidence) | ESET-NOD32         | 1 A Variant Of Win32/Fixers.ACO.gen   |
| F-Secure                | 1 Trojan.TR/Patched.sai           | FireEye            | 1 Genem.ng.124288a162084e2            |
| Fortinet                | 1 W32/Serwit.C@                   | Kaspersky          | 1 HEUR:Trojan.Win32.Genem-            |
| McAfee                  | 1 BDF/Shellcode!D4288A16208       | McAfee-GW-Edison   | 1 BehavesLike.Win32.Dropper.tr        |
| Microsoft               | 1 Trojan/Win32/Serwit.A           | NANO-Antivirus     | 1 Virus.Win32.Gen.come                |
| Qihoo-360               | 1 HEUR/QVM19.1-4C80/Malware.Gen   | Rising             | 1 Trojan/Ransom860.N3457% (RDM+ori... |
| SentinelOne             | 1 DR - Malicious PE               | Sophos AV          | 1 Mal/Serwit.C                        |
| Symantec                | 1 Metaspeter                      | VIPRE              | 1 Trojan.Win32/Serwit.B (x)           |
| Yandex                  | 1 Win32/Serwit.Gen.2              | ZoneAlarm          | 1 HEUR:Trojan.Win32.Genem-            |
| Acronis                 | 1 Undetected                      | Ad-Aware           | 1 Undetected                          |
| AhnLab-V3               | 1 Undetected                      | Alibaba            | 1 Undetected                          |
| ALYac                   | 1 Undetected                      | Antiy-AVL          | 1 Undetected                          |
| Avast                   | 1 Undetected                      | Avast-Mobile       | 1 Undetected                          |
| Babable                 | 1 Undetected                      | Baidu              | 1 Undetected                          |
| BitDefender             | 1 Undetected                      | CAT-QuickHeal      | 1 Undetected                          |
| CMC                     | 1 Undetected                      | Cybereason         | 1 Undetected                          |
| Emisoft                 | 1 Undetected                      | eScan              | 1 Undetected                          |
| GData                   | 1 Undetected                      | Jiangmin           | 1 Undetected                          |
| ITAntivirus             | 1 Undetected                      | K7GW               | 1 Undetected                          |
| Kingsoft                | 1 Undetected                      | Malwarebytes       | 1 Undetected                          |
| MAX                     | 1 Undetected                      | Palo Alto Networks | 1 Undetected                          |
| Panda                   | 1 Undetected                      | Sophos ML          | 1 Undetected                          |
| SUPERAntiSpyware        | 1 Undetected                      | TACHYON            | 1 Undetected                          |
| Tencent                 | 1 Undetected                      | TheHacker          | 1 Undetected                          |
| TotalDefense            | 1 Undetected                      | Trigmine           | 1 Undetected                          |
| TrendMicro              | 1 Undetected                      | Trustlook          | 1 Undetected                          |
| YBA32                   | 1 Undetected                      | VIRobot            | 1 Undetected                          |
| Webroot                 | 1 Undetected                      | Zoner              | 1 Undetected                          |
| Symantec Mobile Insight | 1 Undetected                      |                    |                                       |

Рисунок Б.11 - Результат сканування оригінального PuTTY новою порожньою секцією 2019 рік



```

$ backdoor-factory -f PuTTY.exe -s user_supplied_shellcode_threaded -U section -a -o PuTTY+section.exe -Z
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Creating Code Cave
- Adding a new section to the exe/dll for shellcode injection
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
File PuTTY+section.exe is in the 'backdoored' directory

```

Author: Joshua Pitts  
 Email: SQL | the.midnite.runr[-at ]gmail<d o-t>com  
 Twitter: her@midnite\_runr  
 IRC: ypass@freenode.net #BDFactory

Version: 3.4.2

Рисунок Б.13 – Впровадження вірусу в нову порожню секцію

32  
70

32 engines detected this file

gycb704cb22f404ca79017f7c8f7dd21bf0f8232414801f84d10ca707b92657  
PuTTY.exe@bamae

1.08 MB  
Size

2019-04-02 14:15:33 UTC  
2 minutes ago

EXE

| DETECTION               | DETAILS                        | COMMUNITY          |                                      |
|-------------------------|--------------------------------|--------------------|--------------------------------------|
| AngisLab                | Trojan.Win32.Patched.BBQ       | Avast              | Win32-SolCode                        |
| AVG                     | Win32-SolCode                  | Avira              | TR/Patched.any                       |
| Bkav                    | HW32.Patched                   | ClimAV             | Win.Trojan.BDFactory-6               |
| Comodo                  | TrojWare.Win32.Foxera.A@4jddj  | CrowdStrike Falcon | Win/malicious_confidence_100% (D)    |
| Cyance                  | Ursafe                         | Cyren              | W32/Swarot.C                         |
| DrWeb                   | Trojan.Swarot.I                | eGambit            | PE.Haus.IrvakidSig                   |
| Endgame                 | Malicious (malware Confidense) | ESET-NOD32         | A Variant Of Win32/Foxera.ACD.gen    |
| F-Prot                  | W32/Swarot.C                   | F-Secure           | Trojan.TR.Patched.any                |
| FireEye                 | Generic.mg.226537ab0f6ec       | Fortinet           | W32/Swarot.Ctr                       |
| Ikarus                  | Trojan.Win32.Swarot            | Kaspersky          | HEUR.Trojan.Win32.Genens             |
| McAfee                  | BDF/Shellcode2F2F83DF/AIIF     | McAfee-GW-Edition  | BehavesLike.Win32.Virus.tr           |
| Microsoft               | Trojan/Win32/Swarot.A          | NANO-Antivirus     | Virus.Win32.Gen.ccmw                 |
| Qihoo-360               | HEUR/QVM19.1.41801/Malware.Gen | Rising             | Trojan.Genens/B.C2/NOM7% (FDM)-cm... |
| SentinelOne             | DFI - Malicious PE             | Sophos AV          | Mal/Swarot.C                         |
| Symantec                | Metasploit                     | Yandex             | Win32.Swarot.Gen.2                   |
| Zillya                  | Backdoor.Genens.Win32.3294     | ZoneAlarm          | HEUR.Trojan.Win32.Genens             |
| Acronis                 | Undetected                     | Ad-Aware           | Undetected                           |
| AhnLab-V3               | Undetected                     | Alibaba            | Undetected                           |
| ALYac                   | Undetected                     | Antiy-AVL          | Undetected                           |
| Arcabit                 | Undetected                     | Avast-Mobile       | Undetected                           |
| Babable                 | Undetected                     | Baidu              | Undetected                           |
| BitDefender             | Undetected                     | CAT-QuickHeal      | Undetected                           |
| CMC                     | Undetected                     | Cybereason         | Undetected                           |
| Emisoft                 | Undetected                     | eScan              | Undetected                           |
| GData                   | Undetected                     | Jiangmin           | Undetected                           |
| K7AntiVirus             | Undetected                     | K7GW               | Undetected                           |
| Kingsoft                | Undetected                     | Malwarebytes       | Undetected                           |
| MAX                     | Undetected                     | Palo Alto Networks | Undetected                           |
| Panda                   | Undetected                     | Sophos ML          | Undetected                           |
| SUPERAntiSpyware        | Undetected                     | TACHYON            | Undetected                           |
| Tencent                 | Undetected                     | TheInfoSec         | Undetected                           |
| TotalDefense            | Undetected                     | Trapmine           | Undetected                           |
| TrendMicro-HouseCall    | Undetected                     | Trustlook          | Undetected                           |
| VBA32                   | Undetected                     | ViRobot            | Undetected                           |
| Webroot                 | Undetected                     | Zoner              | Undetected                           |
| Symantec Mobile Insight | Search for previous file type  |                    |                                      |

Рисунок Б.14 - Результат сканування PuTTY з вірусом, впровадженим в нову порожню секцію 2019 рік

e64b13ec806263863ca06e13d90c30274f9b30f112b9436492b6d0c26335

31 / 72

21 engines detected this file

e64b13ec806263863ca06e13d90c30274f9b30f112b9436492b6d0c26335  
PuTTY-section.exe

1.99 MB Size  
2020-10-18 16:46:20 UTC  
5 minutes ago

Upload

Similarity Score

| DETECTION                | DETAILS                          | BEHAVIOR                | COMMUNITY                           |
|--------------------------|----------------------------------|-------------------------|-------------------------------------|
| SecureAge APEX           | 1 Malicious                      | Avast                   | 1 Win32/PrefPolV(C)/ppl             |
| AVG                      | 1 Win32/PrefPolV(C)/ppl          | Avira (no cloud)        | 1 TR/FatcheJaej                     |
| BitDefender              | 1 Win32/DetectVM.malware         | ClamAV                  | 1 Win.Trojan.BDFactory-r            |
| Comodo                   | 1 Trojan.Win32.Hrozna.A@Majesty  | CrowdStrike Falcon      | 1 Win/malicious_confidence_80%_001  |
| Cybereason               | 1 Unsafe                         | Cyren                   | 1 W32/Sworn.C                       |
| DrWeb                    | 1 Trojan.Sworn.C                 | ESET-NOD32              | 1 A Variant Of Win32/Ruzona.ACD.gen |
| F-Secure                 | 1 Trojan.TR/FatcheJaej           | FireEye                 | 1 Generous.c88d9d2b4b161            |
| Fortinet                 | 1 W32/Sworn.C@r                  | Ikarus                  | 1 Trojan.Win32.Sworn                |
| Kaspersky                | 1 HEUR:Trojan.Win32.Denserv      | McAfee                  | 1 RDP/StealCode/CRDPof32FF          |
| McAfee-GW-Edison         | 1 Behavior-like.Win32.Droppers   | Microsoft               | 1 Trojan.Win32.Sworn.A              |
| MAX Antivirus            | 1 Virus.Win32.Gen.zmrv           | Qihoo-360               | 1 HEUR/GVWYIY-3308 Malware.Gen      |
| BitDefender              | 1 HackTool.Suexec.1447 (CLASDIO) | SentinelOne (Static ML) | 1 Malware AI - Malicious PE         |
| Sophos AV                | 1 Mal/Sworn-C                    | Sophos ML               | 1 Mal/Sworn-C                       |
| Symantec                 | 1 Metaspinter                    | VIRRE                   | 1 Trojan.Win32.Sworn.Bivl           |
| Yandex                   | 1 Win32/Suexec1.Gen.2            | Zillya                  | 1 Backdoor.Generic.Win32.3254       |
| ZonaAlarm by Check Point | 1 HEUR:Trojan.Win32.Denserv      | Acronis                 | Undetected                          |
| Ad-Aware                 | Undetected                       | Avast                   | Undetected                          |
| AlmLab-V3                | Undetected                       | Avira                   | Undetected                          |
| AVeas                    | Undetected                       | Avira-ASC               | Undetected                          |
| Avast                    | Undetected                       | Baidu                   | Undetected                          |
| BitDefender              | Undetected                       | BitDefenderThreat       | Undetected                          |
| BitDefender              | Undetected                       | CMC                     | Undetected                          |
| Cybereason               | Undetected                       | Cyren                   | Undetected                          |
| eGambit                  | Undetected                       | Elatio                  | Undetected                          |
| Emisoft                  | Undetected                       | eScan                   | Undetected                          |
| EQoats                   | Undetected                       | Gridinsoft              | Undetected                          |
| Jiangmin                 | Undetected                       | K7AntiVirus             | Undetected                          |
| K7GW                     | Undetected                       | Kingsoft                | Undetected                          |
| Malwarebytes             | Undetected                       | MAX                     | Undetected                          |
| MaxSecure                | Undetected                       | Palo Alto Networks      | Undetected                          |
| Panda                    | Undetected                       | Sangfor Engine Zero     | Undetected                          |
| SUPERAntiSpyware         | Undetected                       | TACHYON                 | Undetected                          |
| Tencent                  | Undetected                       | TotalDefense            | Undetected                          |
| TrendMicro               | Undetected                       | TrendMicro-HouseCall    | Undetected                          |
| VBA32                    | Undetected                       | VirusBot                | Undetected                          |
| Webroot                  | Undetected                       | Zoner                   | Undetected                          |
| Avast-Mobile             | Unable to process the report     | Symantec Mobile Insight | Unable to process the report        |
| Tragosec                 | Unable to process the report     | TruSight                | Unable to process the report        |

Рисунок Б.15 - Результат сканування PuTTY з вірусом, впровадженим в нову порожню секцію 2020 рік

9 engines detected this file

1.38 MB Size 2019-04-02 16:00:07 UTC 4 minutes ago

File ID: f79ec1c1803976bac8d6d0d6aa20b19711f4bebafaa72586dc20d0d90fd96735

File Name: PuTTY.exe

Community Score: 71

| DETECTION               | DETAILS                          | COMMUNITY |
|-------------------------|----------------------------------|-----------|
| AgisLab                 | Trojan.Win32.Patchet.B5Q         | 9         |
| CrowdStrike Falcon      | Win/malicious_confidence_60% (3) | 9         |
| eGambit                 | PE_heur.InvalidSig               | 9         |
| Microsoft               | Trojan.Win32.Sweet.A             | 9         |
| Symantec                | Meterpreter                      | 9         |
| Ad-Aware                | Undetected                       | 9         |
| Alibaba                 | Undetected                       | 9         |
| Avast-Mobile            | Undetected                       | 9         |
| Avast                   | Undetected                       | 9         |
| AVG                     | Undetected                       | 9         |
| Babable                 | Undetected                       | 9         |
| BitDefender             | Undetected                       | 9         |
| ClamAV                  | Undetected                       | 9         |
| Comodo                  | Undetected                       | 9         |
| Cyren                   | Undetected                       | 9         |
| Emisoft                 | Undetected                       | 9         |
| eScan                   | Undetected                       | 9         |
| F-Prot                  | Undetected                       | 9         |
| FireEye                 | Undetected                       | 9         |
| GData                   | Undetected                       | 9         |
| K7AntiVirus             | Undetected                       | 9         |
| Kaspersky               | Undetected                       | 9         |
| Malwarebytes            | Undetected                       | 9         |
| McAfee                  | Undetected                       | 9         |
| NANO-Antivirus          | Undetected                       | 9         |
| Panda                   | Undetected                       | 9         |
| SentinelOne             | Undetected                       | 9         |
| Sophos ML               | Undetected                       | 9         |
| TACHYON                 | Undetected                       | 9         |
| TheHacker               | Undetected                       | 9         |
| Trapsine                | Undetected                       | 9         |
| TrendMicro-HouseCall    | Undetected                       | 9         |
| VBA32                   | Undetected                       | 9         |
| Webroot                 | Undetected                       | 9         |
| Zillya                  | Undetected                       | 9         |
| Zoner                   | Undetected                       | 9         |
| Bear                    | HW32.Packard                     | 9         |
| Cylance                 | Unsafe                           | 9         |
| Ikarus                  | Trojan.Win32.Sweet               | 9         |
| Rising                  | HackTool.Sweet11.8477 (CLASSIC)  | 9         |
| Aronis                  | Undetected                       | 9         |
| AhnLab-V3               | Undetected                       | 9         |
| ALYac                   | Undetected                       | 9         |
| Arcabit                 | Undetected                       | 9         |
| Avast-Mobile            | Undetected                       | 9         |
| Avira                   | Undetected                       | 9         |
| Baidu                   | Undetected                       | 9         |
| CAT-QuickHeal           | Undetected                       | 9         |
| CMC                     | Undetected                       | 9         |
| Cybereason              | Undetected                       | 9         |
| DrWeb                   | Undetected                       | 9         |
| Endgame                 | Undetected                       | 9         |
| ESET-NOD32              | Undetected                       | 9         |
| F-Secure                | Undetected                       | 9         |
| Fortinet                | Undetected                       | 9         |
| Jiangmin                | Undetected                       | 9         |
| K7GW                    | Undetected                       | 9         |
| Kingshot                | Undetected                       | 9         |
| MAX                     | Undetected                       | 9         |
| McAfee-GW-Edition       | Undetected                       | 9         |
| Palo Alto Networks      | Undetected                       | 9         |
| Qihoo-360               | Undetected                       | 9         |
| Sophos AV               | Undetected                       | 9         |
| SUPERAntiSpyware        | Undetected                       | 9         |
| Tencent                 | Undetected                       | 9         |
| TotalDefense            | Undetected                       | 9         |
| TrendMicro              | Undetected                       | 9         |
| Trustlook               | Undetected                       | 9         |
| ViRobot                 | Undetected                       | 9         |
| Yandex                  | Undetected                       | 9         |
| ZoneAlarm               | Undetected                       | 9         |
| Symantec Mobile Insight | Undetected                       | 9         |

Рисунок Б.16 - Результат сканування PuTTY з вірусом впровадженим в code save 2019 рік

179e1c1803976bac8a6d038aa20b19711f4bea8ab72686ac20d0d00090735

18 / 72

18 engines detected this file

179e1c1803976bac8a6d038aa20b19711f4bea8ab72686ac20d0d00090735  
PuTTY Portable

1.88 MB Size 2020-11-13 16:54:33 UTC a moment ago

EXE

Download signature View history View comments Report

| DETECTION                | DETAILS                        | BEHAVIOR                | COMMUNITY                      |
|--------------------------|--------------------------------|-------------------------|--------------------------------|
| Alibaba                  | Trojan.Win32/Servot.48521cd0   | SecureAge APEX          | Malware                        |
| Avast                    | Win32/Malware-gen              | AVG                     | Win32/Malware-gen              |
| CrowdStrike Falcon       | WinMalicious_confidence_00%_RW | eGambit                 | PE.HeuristicSig                |
| Kaspersky                | Trojan.Win32/Servot            | AVASTVirus              | Malware (OO4GdRT1)             |
| K7GW                     | Malware (OO4GdRT1)             | McAfee                  | Antimalware (OO4GdRT1)         |
| McAfee-GW-Edison         | Artemis                        | Microsoft               | Trojan.Win32/Servot.A          |
| PaloAlto Networks        | Generic.M                      | Rang                    | Heuristic (OO4GdRT1) (CLASSIC) |
| Sophos AV                | MalGeneric-5                   | Sophos ML               | MalGeneric-5                   |
| Symantec                 | Metasploit                     | Tencent                 | Trojan.Gen/Mal/HVNR0gSA        |
| Avira                    | Undetected                     | Ad-Aware                | Undetected                     |
| AvgLabs                  | Undetected                     | AviLab-V3               | Undetected                     |
| ALYac                    | Undetected                     | Avira-AM                | Undetected                     |
| Avast                    | Undetected                     | Avira (no cloud)        | Undetected                     |
| Baidu                    | Undetected                     | BitDefender             | Undetected                     |
| BitDefender Theta        | Undetected                     | BitDefender             | Undetected                     |
| CAT-QuickHeal            | Undetected                     | ClamAV                  | Undetected                     |
| CMC                      | Undetected                     | Comodo                  | Undetected                     |
| Cybereason               | Undetected                     | Cybereason              | Undetected                     |
| Cyren                    | Undetected                     | Cyren                   | Undetected                     |
| DrWeb                    | Undetected                     | DrWeb                   | Undetected                     |
| Emsisoft                 | Undetected                     | eScan                   | Undetected                     |
| ESET-NOD32               | Undetected                     | F-Secure                | Undetected                     |
| FireEye                  | Undetected                     | Fortinet                | Undetected                     |
| GData                    | Undetected                     | Grisoft                 | Undetected                     |
| Janminer                 | Undetected                     | Kaspersky               | Undetected                     |
| Kingsoft                 | Undetected                     | Kingsoft                | Undetected                     |
| MAX                      | Undetected                     | MaxSecure               | Undetected                     |
| NANO-Antivirus           | Undetected                     | Panda                   | Undetected                     |
| Qihoo-360                | Undetected                     | Sangfor Engine Zero     | Undetected                     |
| SentinelOne (State ML)   | Undetected                     | SUPERAntiSpyware        | Undetected                     |
| TACHYON                  | Undetected                     | Tencent                 | Undetected                     |
| TotalDefense             | Undetected                     | TrendMicro              | Undetected                     |
| TrendMicro-HouseCall     | Undetected                     | YBASIC                  | Undetected                     |
| VPRE                     | Undetected                     | VirusShare              | Undetected                     |
| Webroot                  | Undetected                     | Webroot                 | Undetected                     |
| ZoneAlarm by Check Point | Undetected                     | Zoner                   | Undetected                     |
| Avast-Mobile             | Unable to process file type    | Symantec Mobile Insight | Unable to process file type    |
| Truprise                 | Unable to process file type    | Trustlook               | Unable to process file type    |

Рисунок Б.17 - Результат сканування PuTTY з вірусом впровадженим в code save 2020 рік

f11ade584dec73fe35d67d17ea8a6a50abfd629f3f5dbc72c5c4d8d6a8a438
Search
Share
Sign in


0
7.5k
No engines detected this file
Refresh
Share

f11ade584dec73fe35d67d17ea8a6a50abfd629f3f5dbc72c5c4d8d6a8a438
default.png
488.8 KB
2019-04-02 16:16:44 UTC
6 months ago
BPM

Community
Vote

| DETECTION               | DETAILS                     | COMMUNITY                   |
|-------------------------|-----------------------------|-----------------------------|
| Ad-Aware                | Undetected                  | Undetected                  |
| AhnLab-V3               | Undetected                  | Undetected                  |
| Andy-AVL                | Undetected                  | Undetected                  |
| Avast                   | Undetected                  | Undetected                  |
| AVG                     | Undetected                  | Undetected                  |
| Babable                 | Undetected                  | Undetected                  |
| BitDefender             | Undetected                  | Undetected                  |
| CAT-QuickHeal           | Undetected                  | Undetected                  |
| CMC                     | Undetected                  | Undetected                  |
| Cyren                   | Undetected                  | Undetected                  |
| Emisoft                 | Undetected                  | Undetected                  |
| ESET-NOD32              | Undetected                  | Undetected                  |
| F-Secure                | Undetected                  | Undetected                  |
| Fortinet                | Undetected                  | Undetected                  |
| Ikarus                  | Undetected                  | Undetected                  |
| K7AntiVirus             | Undetected                  | Undetected                  |
| Kaspersky               | Undetected                  | Undetected                  |
| Malwarebytes            | Undetected                  | Undetected                  |
| McAfee                  | Undetected                  | Undetected                  |
| Microsoft               | Undetected                  | Undetected                  |
| Panda                   | Undetected                  | Undetected                  |
| Rising                  | Undetected                  | Undetected                  |
| SUPERAntiSpyware        | Undetected                  | Undetected                  |
| TACHYON                 | Undetected                  | Undetected                  |
| TheHacker               | Undetected                  | Undetected                  |
| TrendMicro-HouseCall    | Undetected                  | Undetected                  |
| VIPRE                   | Undetected                  | Undetected                  |
| Yandex                  | Undetected                  | Undetected                  |
| ZoneAlarm               | Undetected                  | Undetected                  |
| Acronis                 | Unable to process file type | Unable to process file type |
| CrowdStrike Falcon      | Unable to process file type | Unable to process file type |
| eGambit                 | Unable to process file type | Unable to process file type |
| Palo Alto Networks      | Unable to process file type | Unable to process file type |
| Sophos ML               | Unable to process file type | Unable to process file type |
| Trapsine                | Unable to process file type | Unable to process file type |
| Webroot                 | Unable to process file type | Unable to process file type |
| AngisLab                | Undetected                  | Undetected                  |
| ALYac                   | Undetected                  | Undetected                  |
| Arcabit                 | Undetected                  | Undetected                  |
| Avast-Mobile            | Undetected                  | Undetected                  |
| Avira                   | Undetected                  | Undetected                  |
| Beidu                   | Undetected                  | Undetected                  |
| Bkav                    | Undetected                  | Undetected                  |
| ClamAV                  | Undetected                  | Undetected                  |
| Comodo                  | Undetected                  | Undetected                  |
| DrWeb                   | Undetected                  | Undetected                  |
| eScan                   | Undetected                  | Undetected                  |
| F-Prot                  | Undetected                  | Undetected                  |
| FireEye                 | Undetected                  | Undetected                  |
| GDData                  | Undetected                  | Undetected                  |
| Jiangmin                | Undetected                  | Undetected                  |
| K7GW                    | Undetected                  | Undetected                  |
| Kingsoft                | Undetected                  | Undetected                  |
| MAX                     | Undetected                  | Undetected                  |
| McAfee-GW-Edition       | Undetected                  | Undetected                  |
| NANO-Antivirus          | Undetected                  | Undetected                  |
| Qihoo-360               | Undetected                  | Undetected                  |
| Sophos AV               | Undetected                  | Undetected                  |
| Symantec                | Undetected                  | Undetected                  |
| Tencent                 | Undetected                  | Undetected                  |
| TrendMicro              | Undetected                  | Undetected                  |
| VBA32                   | Undetected                  | Undetected                  |
| ViRobot                 | Undetected                  | Undetected                  |
| Zillya                  | Undetected                  | Undetected                  |
| Zoner                   | Undetected                  | Undetected                  |
| Alibaba                 | Unable to process file type | Unable to process file type |
| Cybereason              | Unable to process file type | Unable to process file type |
| Endgame                 | Unable to process file type | Unable to process file type |
| SentinelOne             | Unable to process file type | Unable to process file type |
| Symantec Mobile Insight | Unable to process file type | Unable to process file type |
| Trustlook               | Unable to process file type | Unable to process file type |

Рисунок Б.18 - Результат сканування оригінального зображення 2019 рік


f11ade584dec731e35d67d17eebaafa950af631620c315dbc72c5c4db36a9438
400.81 KB
2020-11-13 17:00:49 UTC
4 moment ago

No engines detected this file

default.png

Community

| DETECTION               | DETAILS                     | COMMUNITY                |
|-------------------------|-----------------------------|--------------------------|
| Ad-Aware                | Undetected                  | AvastLab                 |
| ArcLab-V3               | Undetected                  | ALYac                    |
| Antiy-AVL               | Undetected                  | Arcabit                  |
| Avast                   | Undetected                  | AVG                      |
| Avira (no cloud)        | Undetected                  | Baidu                    |
| BitDefender             | Undetected                  | BitDefender Theta        |
| Bear                    | Undetected                  | CAT-QuickHeal            |
| ClamAV                  | Undetected                  | CMC                      |
| Comodo                  | Undetected                  | Cyren                    |
| Cyren                   | Undetected                  | DrWeb                    |
| Emisoft                 | Undetected                  | eScan                    |
| EST-NOD32               | Undetected                  | F-Secure                 |
| FireEye                 | Undetected                  | Fortinet                 |
| GData                   | Undetected                  | Gridinsoft               |
| Ikarus                  | Undetected                  | Jiangmin                 |
| K7AntiVirus             | Undetected                  | K7GW                     |
| Kaspersky               | Undetected                  | Kingsoft                 |
| McAfeeBots              | Undetected                  | MAX                      |
| McAfee                  | Undetected                  | McAfee                   |
| McAfee-GW-Edgemon       | Undetected                  | Microsoft                |
| NANO-Antivirus          | Undetected                  | Panda                    |
| Qipco 360               | Undetected                  | Qipco                    |
| Sangfor Engine Zero     | Undetected                  | Sophos AV                |
| Sophos ML               | Undetected                  | SUPERAntiSpyware         |
| Symantec                | Undetected                  | TACHYON                  |
| Tencent                 | Undetected                  | TrendMicro               |
| TrendMicro              | Undetected                  | TrendMicro-HouseCall     |
| VBA32                   | Undetected                  | VIRRE                    |
| VirusBot                | Undetected                  | ViRobot                  |
| Zillya                  | Undetected                  | ZoneAlarm by Check Point |
| Zona                    | Undetected                  | Axentis                  |
| AVeasys                 | Unable to process file type | SecunAge APEX            |
| Avast-Mobile            | Unable to process file type | CrowdStrike Falcon       |
| Cybereason              | Unable to process file type | Cylance                  |
| eGambit                 | Unable to process file type | Elastic                  |
| Palo Alto Networks      | Unable to process file type | SentinelOne (Static ML)  |
| Symantec Mobile insight | Unable to process file type | Trapsone                 |
| Trustlook               | Unable to process file type | Webroot                  |

Рисунок Б.19 - Результат сканування оригінального зображення 2020 рік

14b3b37aa01c41c81c67454720b74219bf3a9749e4be0f413a53607d1cc8ca03

0 / 25

**No engines detected this file**

14b3b37aa01c41c81c67454720b74219bf3a9749e4be0f413a53607d1cc8ca03  
subject.sha256  
(SHA256)

468 KB  
Size


2019-04-02 18:19:51 UTC  
a moment ago


SPPM

Community Score

| DETECTION               | DETAILS                     | COMMUNITY                   |
|-------------------------|-----------------------------|-----------------------------|
| Ad-Aware                | Undetected                  | Undetected                  |
| AhnLab-V3               | Undetected                  | Undetected                  |
| Ardy-AVL                | Undetected                  | Undetected                  |
| Avast                   | Undetected                  | Undetected                  |
| AVG                     | Undetected                  | Undetected                  |
| Bababie                 | Undetected                  | Undetected                  |
| BitDefender             | Undetected                  | Undetected                  |
| CAT-QuickHeal           | Undetected                  | Undetected                  |
| CMC                     | Undetected                  | Undetected                  |
| Cyren                   | Undetected                  | Undetected                  |
| Emisoft                 | Undetected                  | Undetected                  |
| ESET-NOD32              | Undetected                  | Undetected                  |
| F-Secure                | Undetected                  | Undetected                  |
| Fortinet                | Undetected                  | Undetected                  |
| Ikarus                  | Undetected                  | Undetected                  |
| K7AntiVirus             | Undetected                  | Undetected                  |
| Kaspersky               | Undetected                  | Undetected                  |
| Malwarebytes            | Undetected                  | Undetected                  |
| McAfee                  | Undetected                  | Undetected                  |
| Microsoft               | Undetected                  | Undetected                  |
| Panda                   | Undetected                  | Undetected                  |
| Rising                  | Undetected                  | Undetected                  |
| SUPERAntiSpyware        | Undetected                  | Undetected                  |
| TACHYON                 | Undetected                  | Undetected                  |
| TheHacker               | Undetected                  | Undetected                  |
| TrendMicro              | Undetected                  | Undetected                  |
| VBA32                   | Undetected                  | Undetected                  |
| VIRobot                 | Undetected                  | Undetected                  |
| Zillya                  | Undetected                  | Undetected                  |
| Zoner                   | Undetected                  | Undetected                  |
| Alibaba                 | Unable to process file type | Unable to process file type |
| Cyberason               | Unable to process file type | Unable to process file type |
| eGambit                 | Unable to process file type | Unable to process file type |
| Palo Alto Networks      | Unable to process file type | Unable to process file type |
| Sophos ML               | Unable to process file type | Unable to process file type |
| Trapsite                | Unable to process file type | Unable to process file type |
| Webroot                 | Unable to process file type | Unable to process file type |
| Acronis                 | Unable to process file type | Unable to process file type |
| CrowdStrike Falcon      | Unable to process file type | Unable to process file type |
| Cylance                 | Unable to process file type | Unable to process file type |
| Endgame                 | Unable to process file type | Unable to process file type |
| SentinelOne             | Unable to process file type | Unable to process file type |
| Symantec Mobile Insight | Unable to process file type | Unable to process file type |
| Trustlook               | Unable to process file type | Unable to process file type |

Рисунок Б.20 - Результат сканування зображення з прихованим вірусом 2019 рік


f11ade5640cc73fe35e07d17eab6af650af639e20d3f5bc72c5c4d6d6a8438
Search
Share
Grid
Chat
Sign in
Sign up


No engines detected this file

f11ade5640cc73fe35e07d17eab6af650af639e20d3f5bc72c5c4d6d6a8438
469.80 KB
2020-11-13 17:00:49 UTC
Output.png
Download

Community Score
powered by

| DETECTION               | DETAILS                     | COMMUNITY  |
|-------------------------|-----------------------------|--|
| Ad-Aware                | Undetected                  | AegisLab  Undetected                                 |
| AhnLab-V3               | Undetected                  | ALYac  Undetected                                    |
| Antiy-AVL               | Undetected                  | Arcabit  Undetected                                  |
| Avast                   | Undetected                  | AVG  Undetected                                      |
| Avira (no cloud)        | Undetected                  | Baidu  Undetected                                    |
| BitDefender             | Undetected                  | BitDefender Theta  Undetected                        |
| Bkav                    | Undetected                  | CAT-Quacknet  Undetected                             |
| ClimAV                  | Undetected                  | CMC  Undetected                                      |
| Comodo                  | Undetected                  | Cynet  Undetected                                    |
| Cyren                   | Undetected                  | D-Wells  Undetected                                  |
| Emisoft                 | Undetected                  | eScan  Undetected                                    |
| ESET-NOD32              | Undetected                  | F-Secure  Undetected                                 |
| FireEye                 | Undetected                  | Fortinet  Undetected                                 |
| GData                   | Undetected                  | Gridinsoft  Undetected                               |
| Avast                   | Undetected                  | Jiangmin  Undetected                                 |
| KTAntiVirus             | Undetected                  | K7GW  Undetected                                     |
| Kaspersky               | Undetected                  | Kingsoft  Undetected                                 |
| McAfee/bytes            | Undetected                  | MAX  Undetected                                      |
| MaxSecure               | Undetected                  | McAfee  Undetected                                   |
| McAfee-QW-Edison        | Undetected                  | Microsoft  Undetected                                |
| NANO-Antivirus          | Undetected                  | Panda  Undetected                                    |
| Qhoo-360                | Undetected                  | Rising  Undetected                                   |
| Singlar Engine Zero     | Undetected                  | Sophos AV  Undetected                                |
| Sophos ML               | Undetected                  | SUPERAntiSpyware  Undetected                         |
| Symantec                | Undetected                  | TACHYON  Undetected                                  |
| Tencent                 | Undetected                  | TotalDefense  Undetected                             |
| TrendMicro              | Undetected                  | TrendMicro-HouseCall  Undetected                     |
| VBA32                   | Undetected                  | VPRE  Undetected                                     |
| VRobot                  | Undetected                  | Yandex  Undetected                                   |
| Zillya                  | Undetected                  | ZoneAlarm by Check Point  Undetected                 |
| Zoner                   | Undetected                  | Acrone  Unable to process file type                  |
| Alibaba                 | Unable to process file type | SecureAge APEX  Unable to process file type          |
| Avast-Mobile            | Unable to process file type | CrowdStrike Falcon  Unable to process file type      |
| Cybereason              | Unable to process file type | Cylance  Unable to process file type                 |
| eGambit                 | Unable to process file type | Elastic  Unable to process file type                 |
| Foxit-Alpha Networks    | Unable to process file type | SentinelOne (Static ML)  Unable to process file type |
| Symantec Mobile Insight | Unable to process file type | Trapsense  Unable to process file type               |
| Trustlook               | Unable to process file type | Webroot  Unable to process file type                 |

Рисунок Б.21 - Результат сканування зображення з прихованим вірусом 2020

рiк

## ДОДАТОК В

## Детальна інформація про оригінальне зображення

The screenshot shows the VirusShare interface for a file named 'default.bmp'. The file is 488.8 KB and was submitted on 2019-04-02 16:16:44 UTC. The interface includes a 'DETECTION' tab showing 'No engines detected this file' and a 'DETAILS' tab with the following information:

| Basic Properties |   | History          |                     |
|------------------|---|------------------|---------------------|
| MD5              | a8D3e2cef9d45bba66527a696dd75d2                                   | First Submission | 2019-04-02 16:16:44 |
| SHA-1            | 4ad7bb1aa4cb7050ee8042495a1ace4c6d6dcd                            | Last Submission  | 2019-04-02 16:16:44 |
| SHA-256          | f11ade584dec73fe35d67d17ea8ea6a50abf6de29f3f5dbc72c5c4d8d6a8a438  | Last Analysis    | 2019-04-02 16:16:44 |
| SSDEEP           | 3072-KA7AnAPYgLiDzVgV3qdzq7TqAEGKCNnCa4xJEH077udKwUQRYo11E6od177X | Names            |                     |
| File type        | BMP   | default.bmp      |                     |
| Image            | PC bitmap, Windows 3.x format, 800 x 600 x 8                      |                  |                     |
| File size        | 488.8 KB (481078 bytes)   |                  |                     |

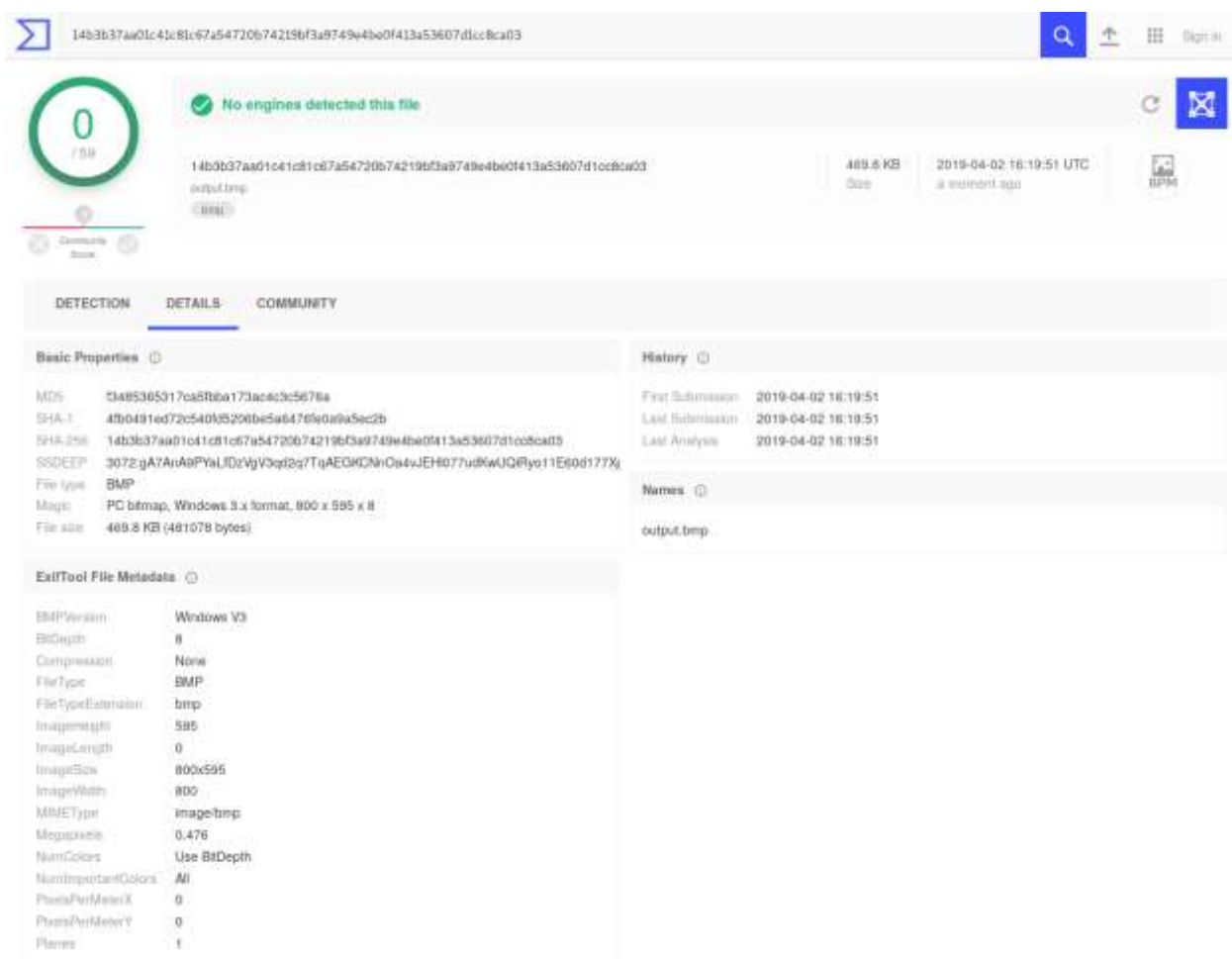
  

| ExifTool File Metadata |              |
|------------------------|--------------|
| BMPVersion             | Windows V3   |
| BitDepth               | 8            |
| Compression            | None         |
| FileType               | BMP          |
| FileTypeExtension      | bmp          |
| ImageHeight            | 600          |
| ImageLength            | 0            |
| ImageSize              | 800x600      |
| ImageWidth             | 800          |
| MMEType                | image/bmp    |
| Megapixels             | 0.48         |
| NumColors              | Use BitDepth |
| NumImportantColors     | All          |
| PixelsPerMeterX        | 0            |
| PixelsPerMeterY        | 0            |
| Planes                 | 1            |

Рисунок В.1 - Детальна інформація про оригінальне зображення

## ДОДАТОК Г

## Детальна інформація про інфіковане зображення



14b3b37aa01c41c81c67a54720b74219b3a9749e4be0f413a53607d1cc8ca03

0 / 50

No engines detected this file

14b3b37aa01c41c81c67a54720b74219b3a9749e4be0f413a53607d1cc8ca03

output.bmp

489.8 KB  
Size

2019-04-02 16:19:51 UTC  
a moment ago

BPM

Community

DETECTION DETAILS COMMUNITY

Basic Properties

|           |   |
|-----------|---|
| MD5       | 0485365317ca5f8be173aac03c5678a                                 |
| SHA-1     | 4fb0491ed72c540f95296be5a647690a9a5ec2b                         |
| SHA-256   | 14b3b37aa01c41c81c67a54720b74219b3a9749e4be0f413a53607d1cc8ca03 |
| SSDEEP    | 3072:gAYArA9PYaLIDzVgV3q2g7TqAEGKCN+Oa4wEH077u8WJQRyo11E60d177X |
| File type | BMP   |
| Magic     | PC bitmap, Windows 3.x format, 800 x 595 x 8                    |
| File size | 489.8 KB (481078 bytes)   |

History

|                  |                     |
|------------------|---------------------|
| First Submission | 2019-04-02 16:19:51 |
| Last Submission  | 2019-04-02 16:19:51 |
| Last Analysis    | 2019-04-02 16:19:51 |

Names

output.bmp

Exitool File Metadata

|                    |              |
|--------------------|--------------|
| BMP Version        | Windows V3   |
| BitDepth           | 8            |
| Compression        | None         |
| FileType           | BMP          |
| FileTypeExtension  | bmp          |
| ImageHeight        | 595          |
| ImageLength        | 0            |
| ImageSize          | 800x595      |
| ImageWidth         | 800          |
| MIMEType           | image/bmp    |
| MetaPixel          | 0.476        |
| NumColors          | Use BitDepth |
| NumImportantColors | All          |
| PixelsPerMeterX    | 0            |
| PixelsPerMeterY    | 0            |
| Planes             | 1            |

Рисунок Г.1 - Детальна інформація про інфіковане зображення

## ДОДАТОК Д

## Код програми BMP\_ЧЕКС.ру

```

# -*- coding: utf-8 -*-
import os
import struct
import random
import time

def print_msg(msg): #Выводит сообщения и вспомогательную информацию
    print "\t\033[32m[+] >>> %s\033[00m" % msg

def print_error(error): #Выводит сообщения об ошибке во время работы модулей
    print "\t\033[91m[!] >>> %s\033[00m" % error

def print_info(info): #Выводит сообщения и вспомогательную информацию
    print "\t\033[33m[*] >>> %s\033[00m" % info

#convert string to hex
def toHex(s):
    lst = []
    for ch in s:
        hv = hex(ord(ch)).replace('0x', '')
        if len(hv) == 1:
            hv = '0'+hv
        lst.append(hv)

    return reduce(lambda x,y:x+y, lst)

image = {}

def Check(vars):
    data, size = get_file_data(vars) #Открытие файла для чтения
    if data:
        header, data = parse_image(data) #Считывание данных из изображения
        image["header"] = header #Заголовок файла
        image["data"] = data #Все остальное

    print_info("Тип файла %s " % header[0:2])
    if header[0:2] == "BM":
        print_msg("Файл является изображением формата BMP")
    else:
        print_error("Файл не является изображением формата BMP")
        exit()

```

```

print_info("Размер файла в байтах указанный в заголовке %d" % struct.unpack("<i",
header[2:6])[0])
print_msg("Настоящий размер файла в байтах %d" % size)
if struct.unpack("<i", header[2:6])[0] == size:
    print_msg("Поле SIZE в заголовке файла не было модифицировано")
else:
    print_error("Поле SIZE в заголовке файла было модифицировано %d != %d" %
(struct.unpack("<i", header[2:6])[0], size))

HexRES1 = toHex(header[6:8])
HexRES2 = toHex(header[8:10])
if HexRES1 == "0000":
    print_msg("Зарезервированное поле №1 = %s" % HexRES1)
else:
    print_error("Зарезервированное поле №1 = %s" % HexRES1)

if HexRES2 == "0000":
    print_msg("Зарезервированное поле №2 = %s" % HexRES2)
else:
    print_error("Зарезервированное поле №2 = %s" % HexRES2)

image["width"] = header[18:22] #Ширина изображения в пикселях
image["height"] = header[22:26] #Высота изображения в пикселях

width = struct.unpack("<i", header[18:22])[0]
#Распаковывает строку в формат int и получает значение ширины в пикселях
#< означает, что порядок цифр little-endian (от младшего к старшему или обратный)
#i означает, что тип int
height = struct.unpack("<i", image["height"])[0]
print_info("Размер изображения указанный в заголовке: %d x %d" % (width, height))
print_info("Изображение должно состоять из %d пикселей" % (width * height))
PixSTART = struct.unpack("<i", header[10:14])[0]
print_info("Положение пиксельных данных относительно начала файла в байтах %d" %
PixSTART)
Pixel = len(data[PixSTART:]) + 26
if Pixel == width * height:
    print_msg("Реальное количество пикселей %d " % Pixel)
else:
    print_error("Реальное количество пикселей %d != %d" % (Pixel, width * height))

def get_file_data(vars):
    data = ""
    path = os.getcwd()
    if os.path.exists(vars): #Проверка существования файла (относительный путь)
        data = open(vars, "rb").read()
        size = os.path.getsize(vars)
    elif os.path.exists(path + "/" + vars): #Проверка существования файла (полное указание пути)
        data = open(path + "/" + vars, "rb").read()
        size = os.path.getsize(path + "/" + vars)

```

```
if data == "":
    print_error("Файл %s не найден" % vars)
    return False
return data, size

def parse_image(data): #Получение данных из изображения
    header = data[:26] #Считывание заголовка (первые 26 символов)
    data = data[(len(data) - 26) * -1:] #Считываются все оставшиеся символы
    return header, data

FileIn = raw_input("Введите путь к изображению: ")
#FileIn = "2.bmp"
Check(FileIn)
```

## ДОДАТОК И

### Слайди презентації

Міністерство освіти і науки України  
Харківський національний університет радіоелектроніки  
Кафедра «Безпеки інформаційних і комунікаційних систем»

### **Методи виявлення та протидії НІД-атакам у зображеннях формату BMP**

Автор:  
студент гр. БІКСм -19 -1  
Гриньов Р.С.  
Керівник:  
к.т.н. Сєверінов О.В.

Рисунок И.1 – Слайд презентації № 1

Мета роботи – розробка методів протидії НІД-атакам та виявлення вірусів у графічних файлах формату BMP.

Об'єкт дослідження – методи подолання засобів захисту, що використовують НІД-атаки та файли зображень для приховування вірусів.

Предметом дослідження є – процес впровадження вірусів в зображення та подолання засобів захисту з використанням НІД-атак.

Рисунок И.2 – Слайд презентації № 2

### **Часткові задачі дослідження**

- 1 Аналіз різноманітності та особливостей комп'ютерних вірусів
- 2 Аналіз способів та методів розповсюдження вірусів
- 3 Аналіз сучасних засобів захисту від комп'ютерних вірусів та вторгнень
- 4 Аналіз особливостей НІД-атак та атак, що використовують файли зображень формату BMP
- 5 Розробка методів протидії НІД-атакам та виявлення вірусів у графічних файлах формату BMP
- 6 Аналіз результатів випробувань

3

Рисунок И.3 – Слайд презентації № 3

### **Класифікація комп'ютерних вірусів**

Комп'ютерні віруси можна класифікувати за наступними ознаками:

- 1 За деструктивним впливом
- 2 За способом зараження
- 3 За середовищем існування
- 4 За особливостями алгоритму

4

Рисунок И.4 – Слайд презентації № 4

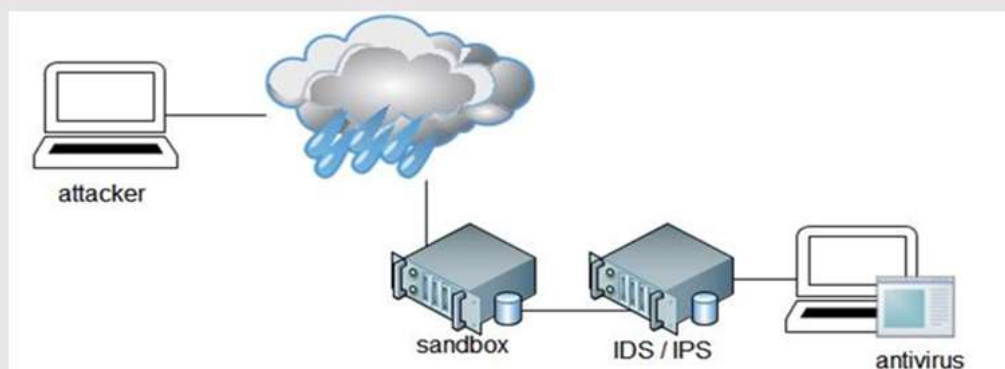
## Способи розповсюдження вірусів

- 1 Претекстінг
- 2 Фішинг
- 3 Послуга за послугу
- 4 Дорожнє яблуко
- 5 Зворотня соціальна інженерія
- 6 Неліцензійне програмне забезпечення

5

Рисунок И.5 – Слайд презентації № 5

## СУЧАСНІ ЗАСОБИ ЗАХИСТУ



Візуалізація шляху вірусу до цільового комп'ютера

6

Рисунок И.6 – Слайд презентації № 6

## ДОСЛІДЖЕННЯ ФОРМАТУ BMP

Розглянемо формат зображень BMP. Кожен файл цього формату має:

- заголовок файлу,
- заголовок зображення,
- растрові данні,
- карту кольорів (крім зображень з 24-бітним кольором).

7

Рисунок И.7 – Слайд презентації № 7

| Зміщення | Розмір<br>(байт) | Ім'я       | Опис  |
|----------|------------------|------------|---|
| 0        | 2                | Type       | Сигнатура формату. Використовується для ідентифікації формату. Має бути 4D42(hex)/424D(hex) (little-endian/big-endian). Після приведення до системи ASCII-символів має вигляд "BM". |
| 2        | 4                | Size       | Розмір файлу в байтах.  |
| 6        | 2                | Reserved 1 | Зарезервоване поле має містити 0.   |
| 8        | 2                | Reserved 2 | Зарезервоване поле має містити 0.   |
| 10       | 4                | OffsetBits | Положення піксельних даних відносно початку файлу (в байтах).   |

Рисунок И.8 – Слайд презентації № 8

| Зміщення | Розмір<br>(байт) | Ім'я          | Опис   |
|----------|------------------|---------------|--|
| 14       | 4                | Size          | Довжина заголовку.   |
| 18       | 4                | Width         | Ширина зображення в пікселях.  |
| 22       | 4                | Height        | Висота зображення в пікселях.  |
| 26       | 2                | Planes        | Кількість площин.  |
| 28       | 2                | BitCount      | Глибина кольору, біт на піксель (1, 4, 8, 24).   |
| 30       | 4                | Compression   | Тип компресії (0 – відсутня, 1 – RLE-8, 2 – RLE-4).                                      |
| 34       | 4                | SizeImage     | Розмір зображення, байт (включно з доповненням).   |
| 38       | 4                | XpelsPerMeter | Горизонтальна роздільна здатність, пікселів на метр.                                     |
| 42       | 4                | YpelsPerMeter | Вертикальна роздільна здатність, пікселів на метр.                                       |
| 46       | 4                | ColorsUsed    | Число кольорів, що використовується (0 – максимально можливе для даної глибини кольору). |
| 50       | 4                | ColorTable    | Кількість основних кольорів.   |

Рисунок И.9 – Слайд презентації № 9

## МЕТОДИ ПРОТИДІЇ

- перевірка зарезервованих полів;
- перевірка поля “Size” в заголовку файлу;
- отримання з заголовку зображення даних, що вказують на горизонтальну та вертикальну кількість пікселів;
- крім того можна використовувати методи, що дозволяють знаходити аномалії у зображеннях.

Рисунок И.10 – Слайд презентації № 10

```

$ python BMP_CHECK.py
Введите путь к изображению: output.bmp
[*] >>> Тип файла BM
[+] >>> Файл является изображением формата BMP
[*] >>> Размер файла в байтах указанный в заголовке 123046121
[+] >>> Настоящий размер файла в байтах 481078
[!] >>> Поле SIZE в заголовке файла было модифицировано 123046121 != 481078
[!] >>> Зарезервированное поле №1 = effc
[!] >>> Зарезервированное поле №2 = ae4d
[*] >>> Размер изображения указанный в заголовке: 800 x 595
[*] >>> Изображение должно состоять из 476000 пикселей
[*] >>> Положение пиксельных данных относительно начала файла в байтах 1078
[!] >>> Реальное количество пикселей 480000 != 476000

```

11

Рисунок И.11 – Слайд презентації № 11

## HID-АТАКИ

HID, або Human Interface Device – тип комп’ютерного пристрою, який взаємодіє безпосередньо з людиною. Найбільш часто приймає від оператора вхідні дані і надає йому вихідні дані. Найпоширеніші типи HID-пристрої – це клавіатура, маніпулятор “миша” і джойстики.

12

Рисунок И.12 – Слайд презентації № 12



13

Рисунок И.13 – Слайд презентації № 13

## ІСНУЮЧІ ПРИСТРОЇ ДЛЯ ПРОВЕДЕННЯ НІД-АТАК



USB Rubber  
Ducky



Bash bunny



USBHarpoon та  
O.MG Cable

14

Рисунок И.14 – Слайд презентації № 14

# МЕТОДИ ПРОТИДІЇ

- заборона на встановлення з'ємних пристроїв;
- використовувати список довірених пристроїв;
- заборона фізичного доступу до USB-портів;
- найбільш вдалим та ефективним є використання евристичних методів для виявлення і блокування НІД-атак.

Рисунок И.15 – Слайд презентації № 15

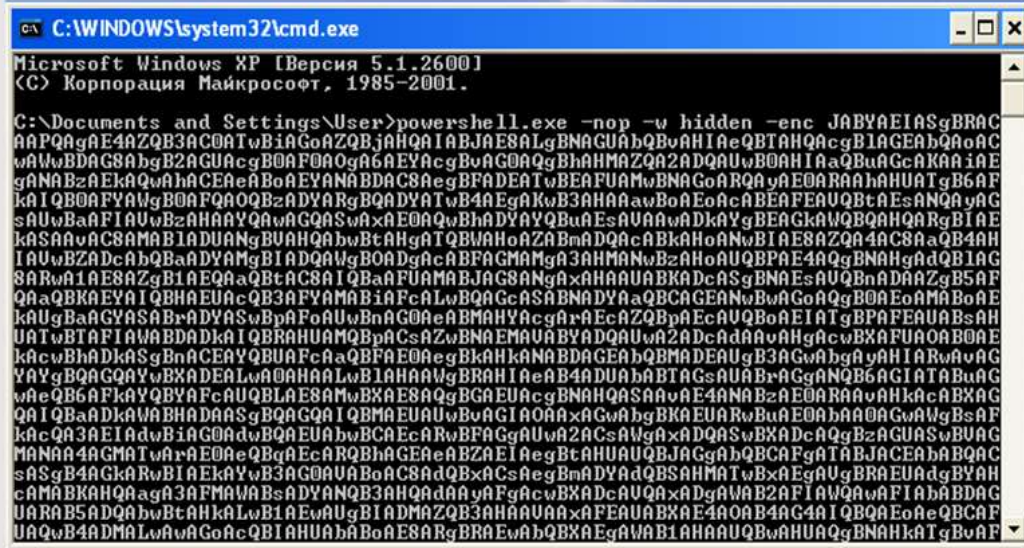
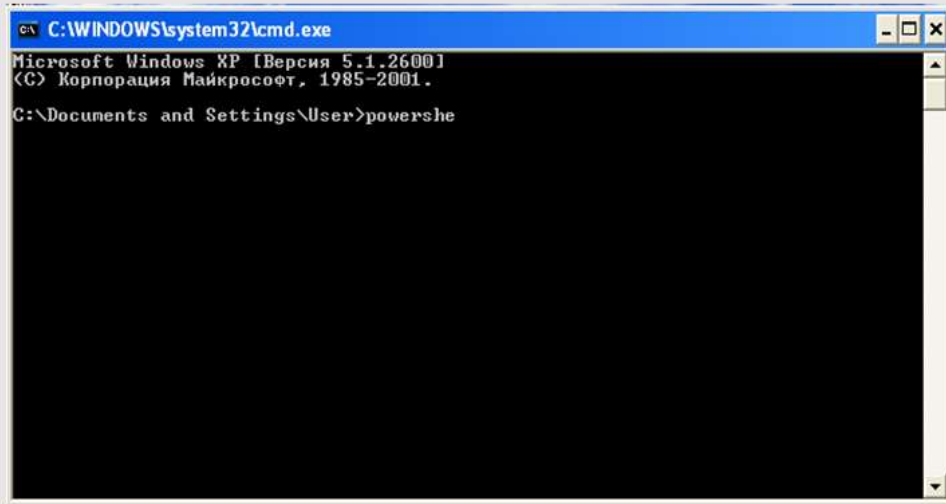
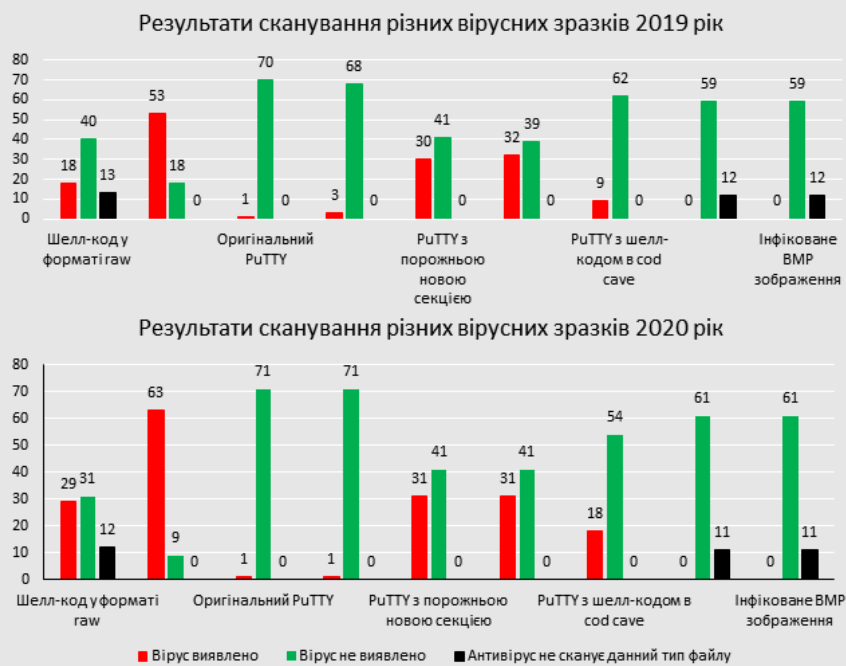


Рисунок И.16 – Слайд презентації № 16



17

Рисунок И.17 – Слайд презентації № 17



18

Рисунок И.18 – Слайд презентації № 18

## Висновки

В рамках дипломної роботи були розроблені методи протидії HID-атакам та виявлення вірусів у графічних файлах формату BMP. В роботі були проаналізовані:

- різних типів комп'ютерних вірусів, способів їх розповсюдження та подолання засобів захисту;
- сучасних засобів захисту від комп'ютерних вірусів та вторгнень;
- особливості файлів формату BMP;
- особливості HID-атак;
- існуючих пристроїв для проведення HID-атак;
- розроблена програма та проаналізовані результати.

Рисунок И.19 – Слайд презентації № 19

