Journal of Cyber Health and Computer (JOCHAC)
Volume 3, Issue 1, August 2025
ISSN: 3031-4623, DOI: 10.64163/jochac.v3i1.48

Analisis Forensik Jaringan terhadap Infeksi Malware MetaStealer: Penerapan Metode SWGDE

Ruli Setiawan[1], Ridho Surya Kusuma[2]
[1, 2] Department of PJJ Informatic, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
Email: [1] Ruli20220100074@sibermu.ac.id, [2]ridhosuryakusuma@sibermu.ac.id

***Abstract*—Malware MetaStealer menjadi ancaman serius bagi keamanan siber. Malware ini memanfaatkan berbagai teknik untuk menginfeksi perangkat, seperti melalui email phishing, unduhan aplikasi palsu, atau eksploitasi kerentanan sistem. Setelah berhasil menginfeksi, MetaStealer akan secara diam-diam mengumpulkan data sensitif korban dan mengirimkannya ke server pelaku serangan. Akibatnya, korban dapat mengalami pencurian identitas, penipuan finansial, dan gangguan operasional bisnis. Penelitian ini bertujuan melakukan analisis forensik jaringan terhadap infeksi MetaStealer menggunakan metode Scientific Working Group on Digital Evidence (SWGDE), fokus pada identifikasi pola serangan, mekanisme penyebaran, dan dampaknya. Metodologi mengikuti kerangka kerja SWGDE dengan empat tahap: Persiapan, Pengumpulan Data, Analisis, dan Pelaporan, menggunakan alat seperti Wireshark, Any Run, dan Virustotal. Kesimpulannya, metode SWGDE terbukti efektif dalam analisis forensik MetaStealer, menyediakan kerangka kerja sistematis yang meningkatkan deteksi dan analisis ancaman sophisticated, serta dapat menjadi dasar pengembangan prosedur standar untuk analisis forensik malware kompleks, dengan penelitian lanjutan diperlukan untuk adaptasi terhadap evolusi malware dan teknik anti-forensik.**

Keywords—Forensik Jaringan; Malware MetaStealer; SWGDE; Analisis Keamanan Siber; Digital Forensics

I. INTRODUCTION

Dalam era digital yang semakin berkembang, ancaman keamanan siber, termasuk infeksi malware, menjadi isu yang semakin mendesak. Salah satu malware yang baru-baru ini menarik perhatian adalah MetaStealer, jenis malware yang dirancang untuk mencuri informasi sensitif dari perangkat korban. MetaStealer dapat menyebabkan kerugian finansial dan reputasi yang signifikan bagi individu maupun organisasi.. Penanganan insiden yang melibatkan malware ini memerlukan pendekatan yang sistematis dan terstruktur, terutama dalam konteks analisis forensik jaringan. Analisis forensik jaringan merupakan disiplin ilmu yang berfokus pada pengumpulan, analisis, dan pelaporan bukti digital yang diperoleh dari jaringan komputer, yang sangat penting dalam mengidentifikasi dan memahami serangan siber

Metode SWGDE (Scientific Working Group on Digital Evidence) merupakan salah satu pendekatan yang dapat diterapkan dalam analisis forensik jaringan untuk mengatasi infeksi malware seperti MetaStealer. Metode ini menyediakan kerangka kerja yang komprehensif untuk pengumpulan dan analisis bukti digital, yang mencakup tahapan mulai dari persiapan, penanganan insiden, pengumpulan data, hingga analisis dan pelaporan hasil. Dengan menerapkan metode ini, penyelidik dapat memastikan bahwa semua langkah diambil untuk menjaga integritas bukti dan menghasilkan laporan yang akurat dan dapat dipertanggungjawabkan di pengadilan.

Dalam konteks ini, penting untuk memahami bahwa analisis forensik jaringan tidak hanya melibatkan teknik pengumpulan data, tetapi juga memerlukan pemahaman mendalam tentang perilaku malware dan cara kerjanya dalam jaringan. Penelitian sebelumnya menunjukkan bahwa malware seperti MetaStealer dapat beroperasi dengan cara yang sangat tersembunyi, sehingga memerlukan teknik analisis yang canggih untuk mendeteksi dan mengidentifikasi jejaknya dalam sistem. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi penerapan metode SWGDE dalam analisis forensik jaringan terhadap infeksi malware MetaStealer, dengan harapan dapat memberikan kontribusi signifikan terhadap praktik forensik digital yang lebih baik dan lebih efektif.

Lebih lanjut, penelitian ini juga akan membahas tantangan yang dihadapi dalam analisis forensik jaringan, termasuk masalah terkait dengan pengumpulan dan preservasi bukti, serta pentingnya kolaborasi antara berbagai pihak dalam menangani insiden keamanan siber. Dengan memahami tantangan ini, diharapkan dapat ditemukan solusi yang lebih baik untuk meningkatkan efektivitas analisis forensik dalam menghadapi ancaman malware yang terus berkembang. Penelitian ini diharapkan dapat memberikan wawasan baru dan rekomendasi praktis bagi para profesional di bidang keamanan siber dan forensik digital dalam menangani infeksi malware yang kompleks seperti MetaStealer.

Dalam rangka mencapai tujuan tersebut, penelitian ini akan menggunakan pendekatan kualitatif dengan analisis studi kasus yang mendalam, serta mengintegrasikan berbagai sumber data dan literatur yang relevan. Dengan demikian, diharapkan hasil dari penelitian ini tidak hanya bermanfaat bagi akademisi, tetapi juga bagi praktisi di lapangan yang terlibat dalam investigasi dan penanganan insiden keamanan siber. Melalui pendekatan yang sistematis dan berbasis bukti, penelitian ini bertujuan untuk memberikan kontribusi yang berarti dalam pengembangan ilmu forensik digital, khususnya dalam konteks analisis forensik jaringan terhadap infeksi malware.

II. TINJAUAN LITERATUR

A. PHISING

Ada banyak jenis dan ragam kejahatan dunia maya, termasuk phishing. Phishing merupakan metode mencoba mendapatkan informasi seperti nama pengguna, kata sandi,

dan informasi kartu kredit dengan berpura-pura menjadi perusahaan komunikasi elektronik yang sah. Posting dari situs web terkenal, situs penjualan, pemroses pembayaran online, atau administrator TI sering kali digunakan untuk menarik perhatian yang tidak menaruh curiga. Informasi ini kemudian digunakan oleh penjahat untuk mengakses akun pengguna, menarik dana dari akun tersebut atau mentransfernya ke penjahat, atau melakukan pembelian online menggunakan kartu kredit orang lain.[1]

B. CRACKING

Kejahatan yang dilakukan oleh cracking ataupun cracker salah satunya ialah Phising karena kejahatan ini tujuannya untuk menguntungkan diri sendiri dan tentunya merugikan pihak lain jika menjadi korban dari cyber crime dalam bentuk phising ini. Dalam ruang lingkup keamanan komputer, phising adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya atau legitimate organization dan biasanya berkomunikasi secara elektronik. Phising ini juga biasanya ditujukan kepada pengguna online banking, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna online lainnya. [2]

C. CYBER CRIME

Cyber Crime dalam bentuk phising saat ini di Indonesia dimungkinkan dapat dikenakan Pasal 35 jo Pasal 51 ayat (1) karena phising merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. Cyber crime dalam bentuk phising ini juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) karena phising juga melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang dimana link tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku. [2]

D. HACKER

Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelijen asing (foreign intelligence service), kekecewaan (disaffected employees), investigasi jurnalis (investigative journalist), organisasi ekstremis (extremist organization), aktivitas para hacker (hacktivist), dan kelompok kejahatan terorganisir (organized crime groups).Hacker adalah seseorang atau sekelompok orang yang memberikan sumbangan yang bermanfaat terhadap dunia jaringan internet, sistem operasi, serta memberikan bantuan untuk dunia internet dan komputer. Pekerjaan hacker juga dapat dikategorikan sebagai seseorang yang mencari kelemahan dari suatu sistem dan memberikan ide untuk menutup celah atau kelemahan yang terdapat dalam sistem tersebut.[3]

E. ARTIFICIAL INTELLIGENCE CYBER SECURITY

Artificial Intelligence dalam Cyber Security bermanfaat karena meningkatkan cara profesional keamanan menyelidiki, menganalisis, dan memahami kejahatan siber. Hal ini melengkapi teknologi keamanan siber yang digunakan bisnis untuk melawan penjahat siber dan membantu menjaga keamanan tim dan pelanggan dari bisnis itu sendiri. Di sisi lain, kecerdasan buatan juga bisa sangat bermanfaat. Meskipun tidak berguna di semua aplikasi, teknologi ini juga dapat berfungsi sebagai gudang senjata bagi penjahat dunia maya yang menggunakan teknologi ini untuk menyempurnakan dan meningkatkan serangan siber mereka.[4]

F. MALWARE

Malware adalah perangkat lunak berbahaya yang dikembangkan untuk mengganggu operasi komputer untuk mengumpulkan kredensial pengguna dan mendapatkan akses ke informasi pribadinya. Dalam beberapa kasus, malware dapat menggunakan kredensial yang diperoleh untuk menyamar sebagai pengguna dan mengirim pesan menular ke teman online pengguna. Koobface adalah malware pertama yang berhasil disebarkan melalui sosial media seperti Facebook, MySpace, dan Twitter. Pada infeksi, Koobface mencoba mengumpulkan informasi login. Penelitian dari Bromium dari Februari tahun 2019 menemukan bahwa satu dari lima organisasi telah terinfeksi malware yang didistribusikan melalui platform media sosial. Yang lebih mengkhawatirkan adalah fakta bahwa 12 persen dari organisasi yang terinfeksi tersebut mengalami pelanggaran data sebagai akibatnya (Mcguire, 2019) Alasan lain mengapa platform media sosial menjadi cara yang efektif untuk mendistribusikan malware adalah kenyataan bahwa ada lebih banyak metode pengiriman untuk kode berbahaya seperti malvertising, tautan dan gambar bersama, plugin, dan media digital. Berbagi konten dan bahkan profil secara konstan mendorong penyebaran malware lebih jauh. [5]

III. METODE PENELITIAN

Metodologi penelitian ini dirancang untuk menganalisis infeksi malware MetaStealer melalui pendekatan forensik jaringan dengan menggunakan metode Scientific Working Group on Digital Evidence (SWGDE). Metode SWGDE memberikan kerangka kerja yang sistematis dan terstruktur untuk pengumpulan, analisis, dan pelaporan bukti digital. Proses ini terdiri dari beberapa tahap yang saling terkait, yang akan dijelaskan secara rinci yang dapat dilihat pada Gambar 1. Adapaun penjelasan tahap pada flowchart sebagai berikut

A. Persiapan

Tahap pertama dalam metodologi ini adalah persiapan, yang mencakup perencanaan dan pengorganisasian sumber daya yang diperlukan untuk analisis. Pada tahap ini, tim forensik harus mengidentifikasi tujuan penelitian, menentukan jenis bukti yang akan dikumpulkan, serta merencanakan alat dan teknik yang akan digunakan dalam proses analisis. Persiapan juga melibatkan pelatihan anggota tim mengenai prosedur SWGDE dan pemahaman mendalam tentang malware MetaStealer dan karakteristiknya.

B. Pengumpulan Data

Pengumpulan data adalah tahap krusial dalam metodologi SWGDE. Pada tahap ini, tim forensik harus mengumpulkan semua bukti digital yang relevan dari jaringan yang

terpengaruh. Ini termasuk log jaringan, paket data, dan informasi konfigurasi perangkat. Penggunaan alat seperti Wireshark untuk sniffing paket dan Snort untuk analisis log sangat dianjurkan. Tim juga harus memastikan bahwa semua data yang dikumpulkan disimpan dengan aman dan dalam format yang dapat dipertanggungjawabkan.

C. Preservasi Bukti

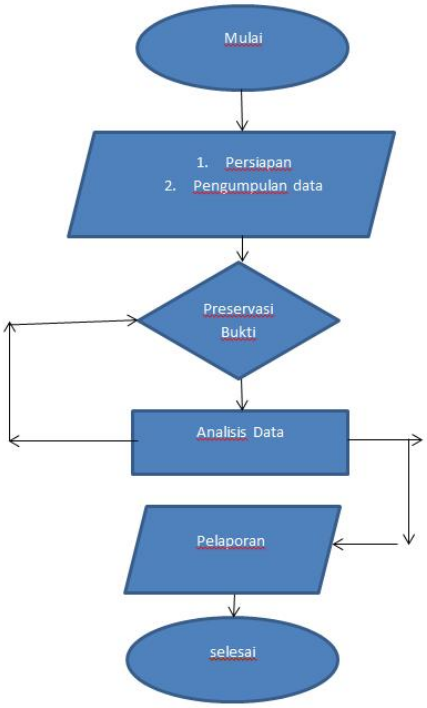
Setelah data dikumpulkan, langkah selanjutnya adalah preservasi bukti. Ini melibatkan pembuatan salinan bit-by-bit dari data yang dikumpulkan untuk memastikan bahwa bukti asli tetap utuh dan tidak terpengaruh oleh analisis yang dilakukan. Proses ini harus dilakukan dengan menggunakan teknik yang sesuai untuk menjaga integritas bukti. Penggunaan checksum dan hash function sangat penting untuk memastikan bahwa data yang disalin tidak mengalami perubahan.

D. Analisis Data

Tahap analisis data adalah inti dari metodologi ini. Pada tahap ini, tim forensik akan menganalisis data yang telah dikumpulkan untuk mengidentifikasi pola dan tanda-tanda yang menunjukkan adanya infeksi malware MetaStealer. Teknik analisis yang digunakan dapat mencakup analisis log, analisis trafik jaringan, dan penggunaan alat forensik digital untuk mendalami lebih lanjut. Tim juga harus mempertimbangkan untuk melakukan analisis terhadap artefak yang mungkin ditinggalkan oleh malware dalam sistem.

E. Pelaporan

Setelah analisis selesai, tim forensik harus menyusun laporan yang mendokumentasikan semua temuan dan proses yang telah dilakukan. Laporan ini harus mencakup deskripsi rinci tentang metode yang digunakan, bukti yang ditemukan, dan kesimpulan yang diambil dari analisis. Laporan harus disusun dengan cara yang dapat dipahami oleh pihak non-teknis dan harus siap untuk disajikan di pengadilan jika diperlukan. Kejelasan dan ketepatan informasi dalam laporan sangat penting untuk mendukung validitas temuan.



Gambar 1. Flowchat

IV. HASIL DAN PEMBAHASAN

Analisis malware MetaStealer akan dilakukan secara bertahap. Tahap awal akan fokus pada identifikasi varian dan karakteristik umum malware. Selanjutnya, analisis statis akan dilakukan untuk memahami struktur kode dan fungsi-fungsi utama. Analisis dinamis akan memberikan gambaran yang lebih jelas tentang perilaku malware saat berjalan. Terakhir, analisis jaringan akan dilakukan untuk mengidentifikasi komunikasi malware dengan server C&C. Dengan menggabungkan hasil dari berbagai tahapan analisis, kita dapat menyusun laporan yang komprehensif tentang ancaman yang ditimbulkan oleh malware MetaStealer.

A. Persiapan

Tahap pertama dalam metodologi ini adalah persiapan, yang mencakup perencanaan dan pengorganisasian sumber daya yang diperlukan untuk analisis

1. Alat

- PC OS Kali Linux
- Aplikasi Wiresark
- Virus Total https://www.virustotal.com/gui/home/upload\
- Any run https://app.any.run/

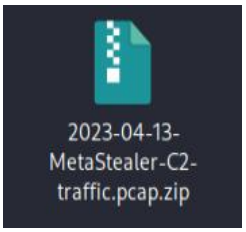
2. Bahan

- Malware MetaStealer https://www.malware-traffic-analysis.net/2023/04/13/index.html

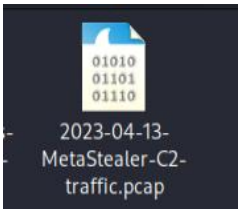
B. Pengumpulan Data

Penggunaan alat Wireshark untuk sniffing paket dan Snort untuk analisis log, menggunakan Any Run dan Virus Total untuk menganalisa maslware.

1. Bahan Utama



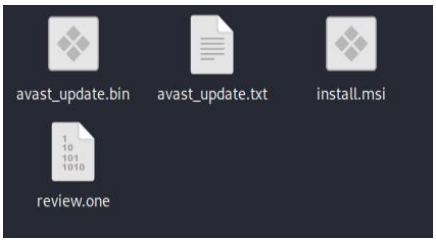
Gambar 2. Data **Malware MetaStealer (di dapat dari web https://www.malware-traffic-analysis.net/2023/04/13/index.html)**



Gambar 3. Data **Malware MetaStealer yang sudah terunzip**

2. Bahan Tambahan

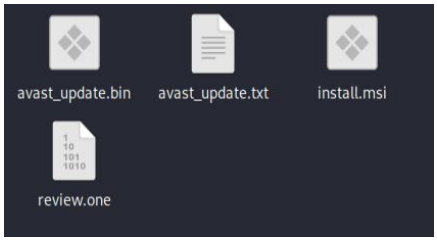
Gambar 4. Data **Malware MetaStealer Tambahan dalam bentuk zip (di dapat dari web** https://www.malware-traffic-analysis.net/2023/04/13/index.html)



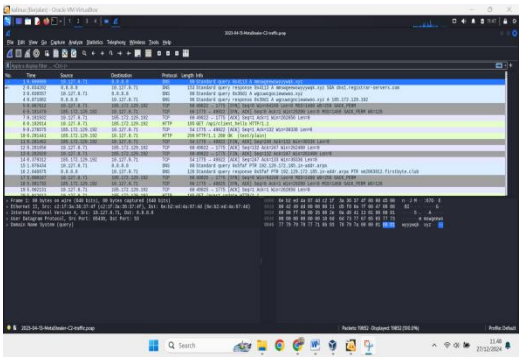
Gambar 5. Data **Malware MetaStealer Tambahan ketika berada dalam proses infeksi Malware ke Komputer**

3. Analisis Malware dengan Menggunakan Aplikasi Wireshark

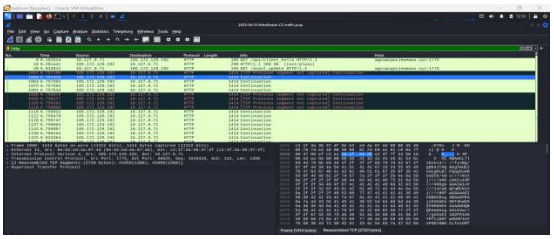
Gambar 6. Bahan Utama



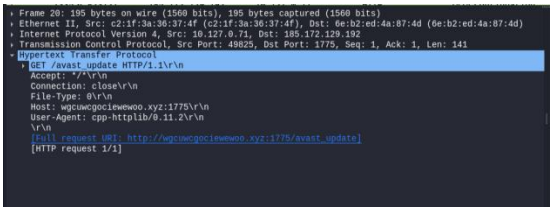
Gambar 7. Data Tambahan



Gambar 8. Penggunaan Aplikasi Wireshark untuk identifikasi Data Malware MetaStealer yang sudah terunzip

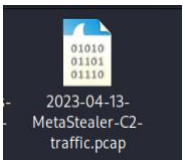


Gambar 9. Proses analisis



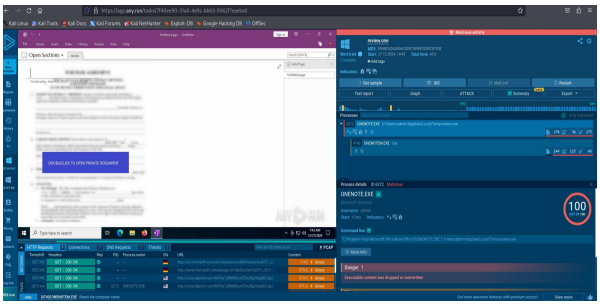
Gambar 10. Link Dicurigai

4. Analisis Malware dengan Menggunakan Aplikasi Any Run

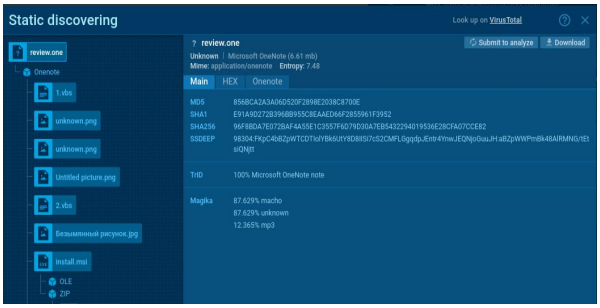


Gambar 11. Bahan Utama

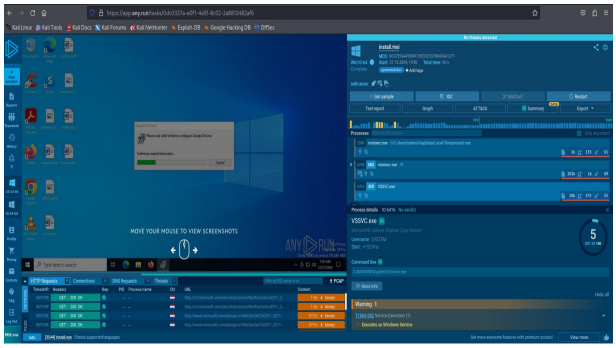
Gambar 12. Data Tambahan



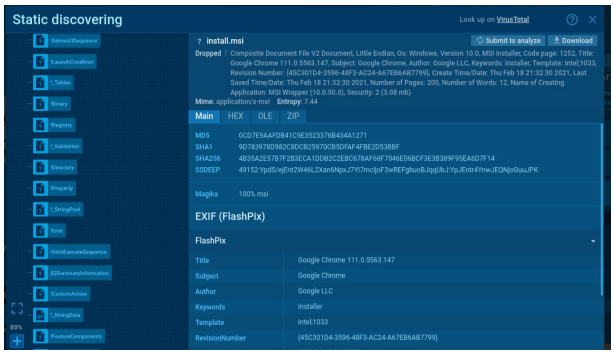
Gambar 13. Penggunaan Aplikasi Any Run untuk identifikasi File review.one (1)



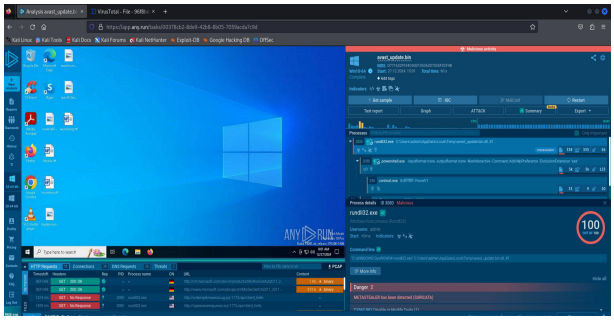
Gambar 14. Penggunaan Aplikasi Any Run untuk identifikasi File review.one (2)



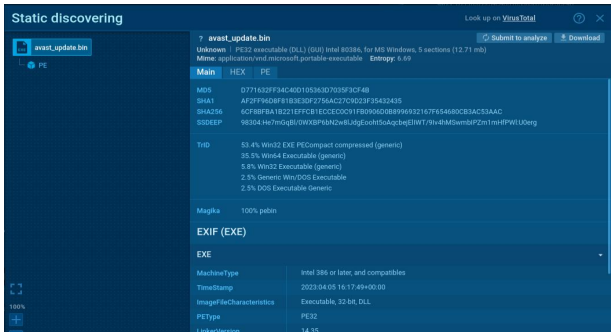
Gambar 15. Penggunaan Aplikasi Any Run untuk identifikasi File install.msi (1)



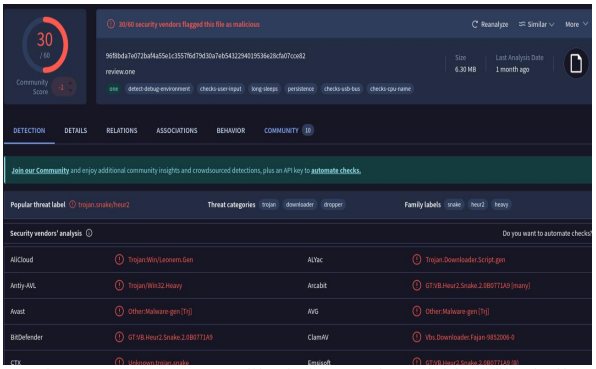
Gambar 16. Penggunaan Aplikasi Any Run untuk identifikasi File install.msi (2)



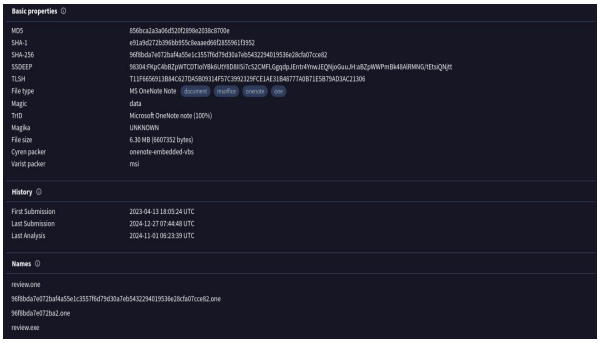
Gambar 17. Penggunaan Aplikasi Any Run untuk identifikasi File avast_update.bin (1)



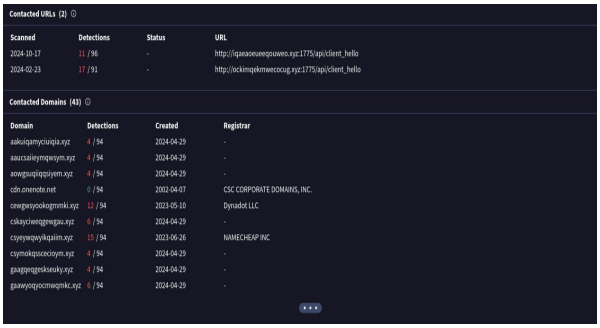
Gambar 18. Penggunaan Aplikasi Any Run untuk identifikasi File avast_update.bin (2)



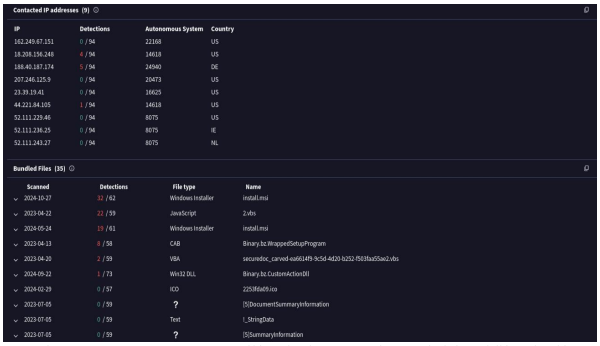
Gambar 19. Penggunaan Aplikasi virus total untuk identifikasi File review.one (1)



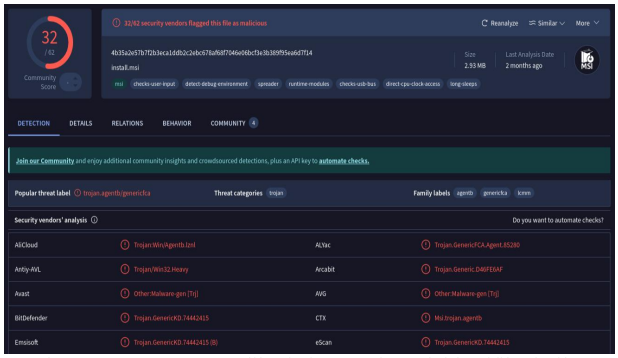
Gambar 20. Penggunaan Aplikasi virus total untuk identifikasi File review.one (2)



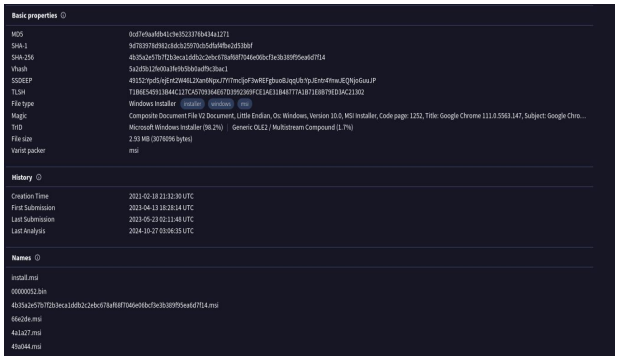
Gambar 21. Penggunaan Aplikasi virus total untuk identifikasi File review.one (3)



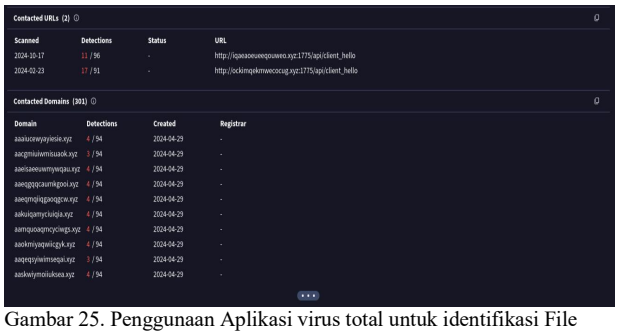
Gambar 22. Penggunaan Aplikasi virus total untuk identifikasi File review.one (4)



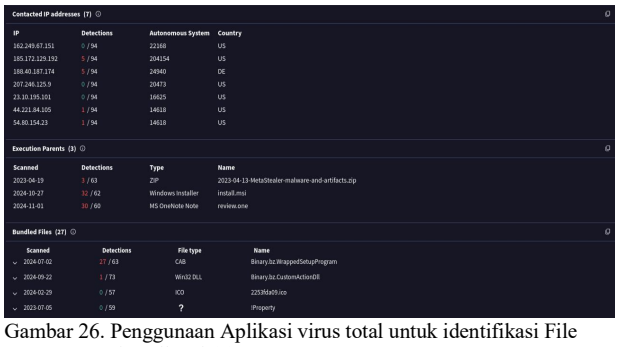
Gambar 23. Penggunaan Aplikasi virus total untuk identifikasi File install.msi (1)



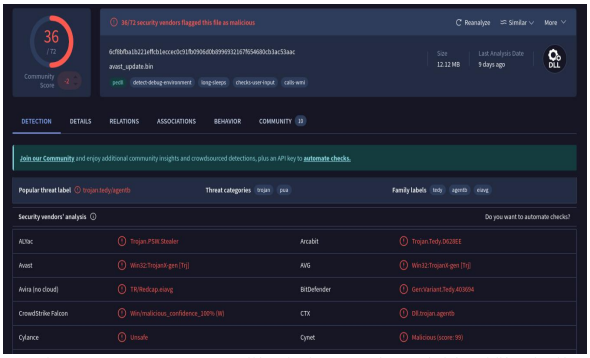
Gambar 24. Penggunaan Aplikasi virus total untuk identifikasi File install.msi (2)



Gambar 25. Penggunaan Aplikasi virus total untuk identifikasi File install.msi (3)

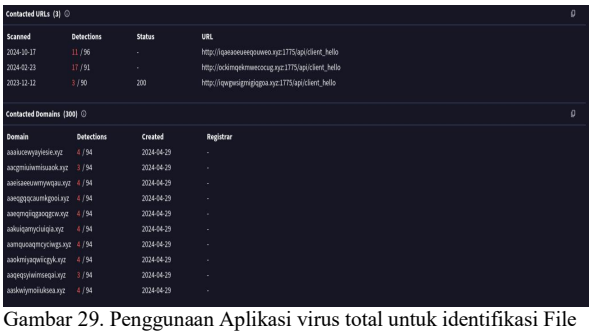


Gambar 26. Penggunaan Aplikasi virus total untuk identifikasi File install.msi (4)

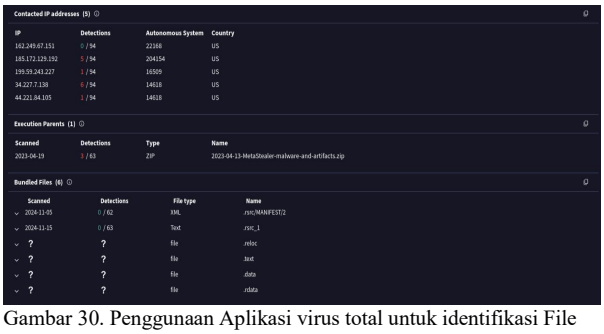


Gambar 27. Penggunaan Aplikasi virus total untuk identifikasi File avast_update.bin (1)

Gambar 28. Penggunaan Aplikasi virus total untuk identifikasi File avast_update.bin (2)



Gambar 29. Penggunaan Aplikasi virus total untuk identifikasi File avast_update.bin (3)

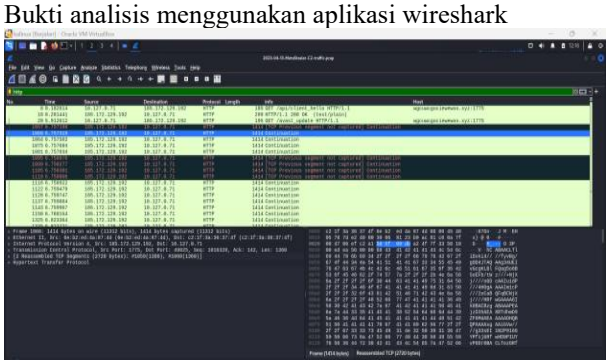


Gambar 30. Penggunaan Aplikasi virus total untuk identifikasi File avast_update.bin (4)

C. Preservasi Bukti

Setelah data dikumpulkan, langkah selanjutnya adalah Preservasi bukti digital. Preservasi bukti digital merupakan langkah yang sangat penting dalam proses forensik digital. Dengan menerapkan teknik preservasi yang tepat, kita dapat memastikan bahwa bukti digital tetap utuh dan dapat dipercaya sebagai bukti hukum.

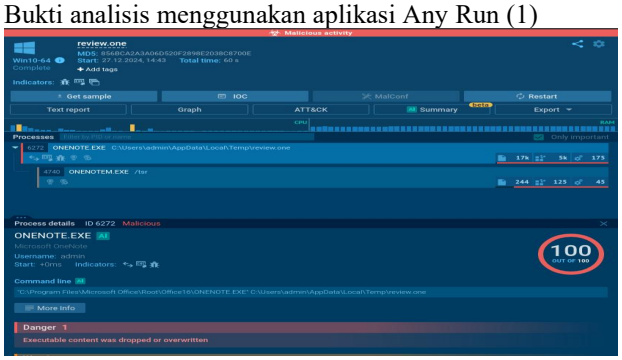
1. Bukti analisis menggunakan aplikasi wireshark



Gambar 31. Bukti analisis menggunakan aplikasi wireshark

Gambar diatas menampilkan potongan data jaringan yang biasanya terlihat di dalam sebuah packet capture atau log server. Tabel ini menyajikan informasi dasar tentang beberapa paket data yang tertangkap. Data ini menunjukkan bahwa pengguna dengan alamat IP 10.127.0.71 sedang mencoba mengakses sebuah situs web

2. Bukti analisis menggunakan aplikasi Any Run (1)



Gambar 32. Bukti analisis menggunakan aplikasi Any Run (1)

Analisis aktivitas di direktori cache dalam tugas ini menunjukkan adanya penggunaan yang umum oleh aplikasi sah seperti Microsoft OneNote untuk menyimpan data. proses menunjukkan bahwa aplikasi OneNote diluncurkan dengan argumen baris perintah tertentu dan serta mengubah beberapa file di direktori cache

3. Bukti analisis menggunakan aplikasi Any Run (2)

Gambar 33. Bukti analisis menggunakan aplikasi Any Run (2)

Proses yang disediakan menunjukkan serangkaian peristiwa proses yang terjadi selama eksekusi program. Program yang sedang dieksekusi adalah "C:\Users\admin\AppData\Local\Temp\MW-12c1c855-a5d4-411e-bb0c-bf00059d00c5\files\install.exe".Pohon proses mencakup informasi tentang eksekusi berbagai file dan proses, seperti "C:\Windows\Installer\MSIA183.tmp", "C:\Windows\Installer\139fed.msi", dan "C:\System Volume Information\SPP\metadata-2"

4. Bukti analisis menggunakan aplikasi Any Run (3)

Gambar 34. Bukti analisis menggunakan aplikasi Any Run (3)

Proses menunjukkan rangkaian aktivitas yang mencurigakan, meliputi eksekusi rundll32.exe, pembuatan dan eksekusi skrip PowerShell, serta permintaan terhadap berkas CRL.

5. Bukti analisis menggunakan aplikasi Virus Total (1)

Gambar 35. Bukti analisis menggunakan aplikasi Virus Total (1)

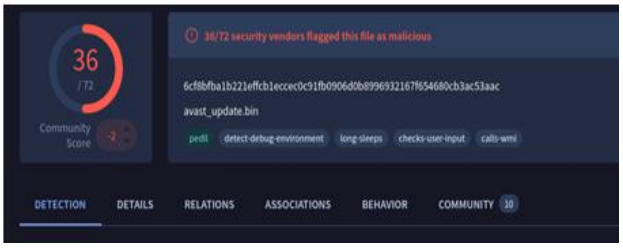
File review.one dengan hash 3a4fb21e7c2553a4e3574d3a7625424154d252c73ec0e2 telah terdeteksi sebagai malware oleh setidaknya 30 vendor keamanan. Hal ini menunjukkan bahwa file tersebut sangat mungkin merupakan ancaman serius bagi sistem komputer.

6. Bukti analisis menggunakan aplikasi Virus Total (2)

Gambar 36. Bukti analisis menggunakan aplikasi Virus Total (2)

File dengan nama "install.msi" dan hash 4b35a2e57b7f2b3eca1ddb2c2ebc67af68f7046e06bcf3e3b389954667114
telah dikategorikan sebagai malware oleh 32 dari 62 vendor keamanan. Hal ini menunjukkan bahwa file tersebut sangat mungkin merupakan ancaman serius bagi sistem komputer.

7. Bukti analisis menggunakan aplikasi Virus Total (1)



Gambar 37. Bukti analisis menggunakan aplikasi Virus Total (1)

File dengan nama "avast_update.bin" dan hash 6cfbfba1b221effc0eccc91f0300adeb996932167f5466db0cb51aaac telah dikategorikan sebagai malware oleh 36 dari 72 vendor keamanan. Ini adalah indikasi yang sangat kuat bahwa file tersebut merupakan ancaman serius bagi sistem komputer.

D. Analisis Data

Tahap analisis data adalah inti dari metodologi ini. Pada tahap ini, tim forensik akan menganalisis data yang telah dikumpulkan untuk mengidentifikasi pola dan tanda-tanda yang menunjukkan adanya infeksi malware.

1. Analisis review.one
   a. MD5 : 856BCA2A3A06D520F2898E2038C8700E
   b. Aktifitas:
      - Konten yang dapat dieksekusi telah dijatuhkan atau ditimpa.
      - Membuat file di root drive system
      - Membaca nama komputer
      - Membaca kunci registri Microsoft Office
      - Mengirim pesan debugging
      - Memeriksa bahasa yang didukung
   c. Kesimpulan:
      Analisis review.one menunjukkan perilaku yang sangat mencurigakan, termasuk memodifikasi file sistem, mengumpulkan informasi sistem, dan berkomunikasi dengan server eksternal.
2. Analisis install.msi
   a. MD5 : 0CD7E9AAFDB41C9E3523376B434A1271
   b. Aktifitas:
      - Membongkar berkas CAB
      - Dieksekusi sebagai Layanan Windows
      - Membaca pengaturan keamanan Internet Explorer
      - Memeriksa bahasa yang didukung
      - Membaca GUID mesin dari registri
      - Mengelola titik pemulihan sistem
      - Membuat file dalam direktori sementara
      - Dokumen yang dibuat secara otomatis
      - onten yang dapat dieksekusi telah dihapus atau ditimpa
      - Membaca nama komputer
      - Proses memeriksa pengaturan lokasi komputer
   c. Kesimpulan:
      Analisis Install.msi menunjukkan perilaku aktivitas mencurigakan, seperti mengubah pengaturan sistem, mengakses data sensitif, dan bahkan merusak file-file penting. Akibatnya, kinerja komputer Anda bisa menurun, data pribadi Anda bisa terancam, dan sistem Anda bisa menjadi tidak stabil.
3. Analisis avast_update.bin
   a. MD5 : D771632FF34C40D105363D7035F3CF4B
   b. Aktifitas:
      - Menambahkan ekstensi ke daftar pengecualian Windows Defender
      - METASTEALER telah terdeteksi (SURICATA)
      - Skrip menambahkan ekstensi pengecualian ke Windows Defender
      - Proses menyembunyikan perintah interaktif dari pengguna
      - Memulai POWERSHELL.EXE untuk menjalankan perintah
      - Terhubung ke port yang tidak biasa
      - Menjalankan aplikasi yang mogok
      - Memeriksa apakah ada kunci dalam kamus opsi (POWERSHELL)
      - Proses menggunakan file yang diunduh
      - Memeriksa informasi server proxy
      - Membaca pengaturan kebijakan perangkat lunak
   c. Kesimpulan:
      Analisis avast_update.bin menunjukkan kemampuan untuk melakukan berbagai aktivitas berbahaya, termasuk manipulasi sistem operasi, pengumpulan informasi sensitif, dan penyebaran diri. Aktivitas-aktivitas ini mengindikasikan adanya ancaman serius terhadap integritas data, privasi pengguna, dan ketersediaan layanan.

E. Pelaporan

Setelah analisis selesai, tim forensik harus menyusun laporan yang mendokumentasikan semua temuan dan proses yang telah dilakukan. Laporan analisis forensik ini disusun untuk memberikan gambaran menyeluruh mengenai hasil investigasi terhadap insiden infeksi malware Meta Stealer. Analisis ini bertujuan untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital yang relevan guna mendukung proses pengambilan keputusan.

Dari hasil pengumpulan data dan analisis data menggunakan aplikasi wireshark,Any Run serta Virus total, menunjukan bahwa menunjukkan adanya aktivitas jaringan yang cukup tinggi. Banyak paket data yang terkirim dan diterima, dengan berbagai tujuan dan protokol. penggunaan protokol HTTP, yang umumnya digunakan untuk

mengakses halaman web. Ini bisa menandakan aktivitas browsing atau pengunduhan file dari internet.

File review.one menunjukkan perilaku yang sangat mencurigakan, termasuk memodifikasi file sistem, mengumpulkan informasi sistem, dan berkomunikasi dengan server eksternal.Sedangkan File Install.msi menunjukkan perilaku aktivitas mencurigakan, seperti mengubah pengaturan sistem, mengakses data sensitif, dan bahkan merusak file-file penting. Akibatnya, kinerja komputer Anda bisa menurun, data pribadi Anda bisa terancam, dan sistem Anda bisa menjadi tidak stabil.

Pada Hasil analisis File avast_update.bin menunjukkan adanya infeksi malware Meta Stealer. Malware ini telah berhasil mengeksekusi beberapa tindakan berbahaya, termasuk menambahkan ekstensi ke daftar pengecualian Windows Defender untuk menghindari deteksi, menjalankan skrip untuk mengotomatiskan tugas jahat, dan menggunakan PowerShell untuk menjalankan perintah dengan hak akses yang tinggi. Selain itu, malware ini juga terdeteksi berkomunikasi dengan server eksternal melalui port yang tidak biasa, mengindikasikan adanya aktivitas peretasan.

REFERENCES

[1] Purnama Sari and Tata Sutabri, 'Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari', Jurnal Digital Teknologi Informasi, 6.1 (2023), p. 29, doi:10.32502/digital.v6i1.5620.

[2] A A I Ferrary, S Hartini, and P Purwaningsih, 'Kajian Hukum Terhadap Tindak Pidana Cyber Phising Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading …', Yustisi, 10.2 (2023),pp.1–12<https://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/view/14314%0Ahttps://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/download/14314/4490>.

[3] Mohd Yusuf Dm, Addermi, and Jasmine Lim, 'Kejahatan Phising Dalam Dunia Cyber Crime Dan Sistem Hukum Di Indonesia', Jurnal Pendidikan Dan Konseling, 4.5 (2022), pp. 8018–23.

[4] Lim Jong Su and Binastya Anggara Sekti, 'Implementasi Artificial Intelligence Dalam Meningkatkan Cyber Security : Analisis Ancaman Dan Pencegahan', pp. 199–203.

[5] Leona Elsa N and others, 'Information Security Awareness and Privacy Protection Behavior in Using Social Media', Seminar Nasional Teknologi Dan Sistem Informasi 2021, 101.November (2021), pp. 101–9.