Analisis Forensik Jaringan terhadap Squirrelwaffle dengan Cobalt Strike: Menggunakan Metode NIST

Mohammad Farhan Asqolani*[1], Ridho Surya Kusuma[2]
[1,2] Department of Informatic, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
Email: [1]moh20220100063@sibermu.ac.id, [2]ridhosuryakusuma@sibermu.ac.id
*Corresponding Author

***Abstract*—Analisis forensik jaringan terhadap malware Squirrelwaffle yang menggunakan Cobalt Strike sebagai alat penyerangan telah dilakukan dengan mengacu pada kerangka kerja NIST. Penelitian ini bertujuan untuk mengidentifikasi tahapan serangan, teknik yang digunakan, serta artefak digital yang ditinggalkan oleh malware tersebut. Melalui analisis mendalam terhadap data jaringan, log sistem, dan file yang terinfeksi, penelitian ini berhasil mengungkap indikator kompromi (IoC) yang khas dari Squirrelwaffle dan Cobalt Strike. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan deteksi dan respons terhadap ancaman siber yang serupa.**

Kata kunci; Forensik Jaringan, Squirrelwaffle, Cobalt Strike, NIST SP 800-86, Analisis Malware.

I. PENDAHULUAN

Dalam lanskap ancaman siber yang terus berkembang, malware semakin canggih dan kompleks. Salah satu jenis malware yang sering digunakan oleh pelaku serangan siber adalah loader. Loader ini berfungsi sebagai pintu masuk bagi malware lain yang lebih berbahaya untuk menginfeksi sistem. Salah satu loader yang cukup populer dan berbahaya adalah Squirrelwaffle. Squirrelwaffle sering digunakan untuk mendistribusikan payload berbahaya seperti Cobalt Strike, sebuah kerangka kerja peretasan yang kuat dan fleksibel.

Penelitian ini bertujuan untuk menganalisis secara mendalam serangan siber yang melibatkan malware Squirrelwaffle dan Cobalt Strike. Dengan menggunakan metode NIST (National Institute of Standards and Technology) sebagai kerangka kerja, penelitian ini akan mengidentifikasi tahapan serangan, teknik yang digunakan, serta artefak digital yang ditinggalkan oleh malware tersebut. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan deteksi dan respons terhadap ancaman siber yang serupa.

Squirrelwaffle adalah sebuah loader malware yang dirancang untuk mendistribusikan payload berbahaya ke sistem yang terinfeksi. Malware ini sering digunakan sebagai tahap awal dalam serangan siber yang lebih besar. Setelah berhasil masuk ke dalam sistem, Squirrelwaffle akan mengunduh dan menjalankan payload tambahan, seperti Cobalt Strike.

Cobalt Strike adalah sebuah kerangka kerja peretasan yang populer di kalangan pelaku serangan siber. Alat ini menyediakan berbagai fitur yang memungkinkan penyerang untuk melakukan berbagai aktivitas jahat, seperti melakukan lateral movement, mengeksekusi perintah pada sistem yang terinfeksi, dan mencuri data sensitif. Kombinasi antara Squirrelwaffle dan Cobalt Strike membuat serangan siber menjadi lebih terorganisir dan sulit dilacak. Untuk melakukan analisis forensik jaringan terhadap serangan yang melibatkan Squirrelwaffle dan Cobalt Strike, penelitian ini akan mengadopsi metode NIST. NIST menyediakan kerangka kerja yang komprehensif untuk melakukan investigasi forensik. Kerangka kerja NIST meliputi beberapa tahapan yaitu Pengumpulan (Collection), Pemeriksaan (Examination), Analisis (Analysis), Pelaporan (Reporting). Dengan mengikuti langkah-langkah dalam kerangka kerja NIST, diharapkan penelitian ini dapat menghasilkan hasil yang akurat dan reliabel.

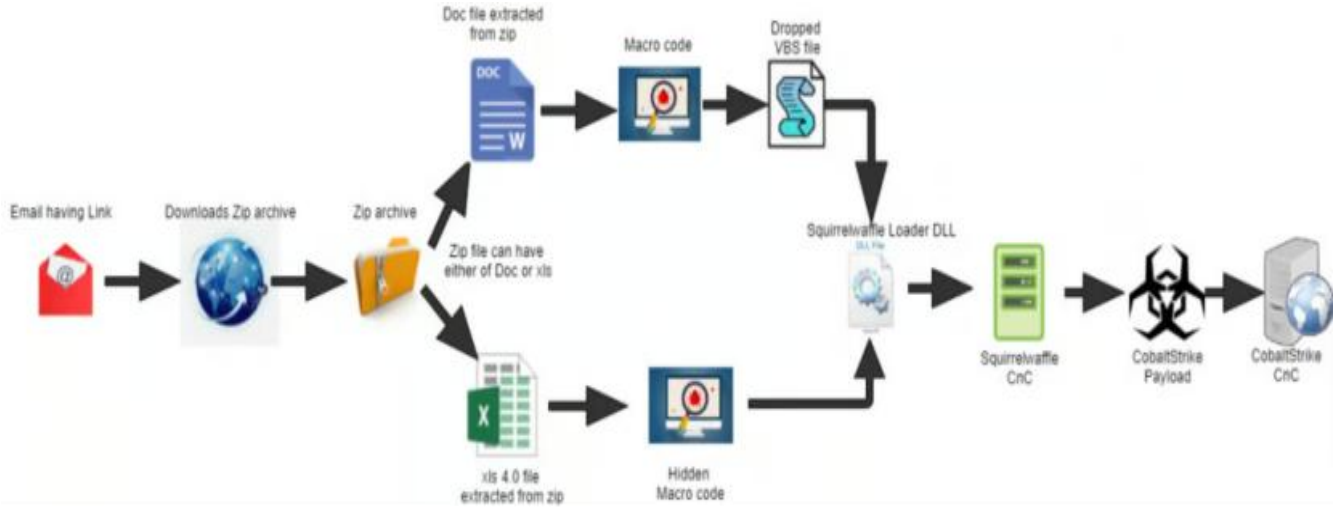
II. TUJUAN LITERATUR

Squirrelwaffle adalah salah satu jenis malware yang pertama kali muncul pada tahun 2021 dan sering digunakan sebagai pemuat (loader) untuk mengunduh serta mengeksekusi muatan berbahaya lainnya seperti Cobalt Strike. Malware ini biasanya didistribusikan melalui kampanye email phishing dengan lampiran dokumen berbahaya atau tautan yang mengarahkan ke unduhan berbahaya (Huntress Labs, 2021). Studi oleh McAfee (2022) menunjukkan bahwa Squirrelwaffle memanfaatkan taktik seperti spoofing email dan eksploitasi makro Microsoft Office untuk menyusup ke sistem target. Selain itu, malware ini menggunakan infrastruktur command and control (C2) yang fleksibel untuk berkomunikasi dengan server penyerang. Untuk *Squirrelwaffle Attack-chain* bisa dilihat pada Gambar 1.

Beberapa penelitian menunjukkan bahwa Squirrelwaffle sering bertindak sebagai tahap awal dalam serangan siber yang melibatkan Cobalt Strike. Setelah berhasil menginfeksi target, Squirrelwaffle mengunduh dan menjalankan beacon Cobalt Strike untuk memungkinkan kendali jarak jauh oleh penyerang (Talos Intelligence, 2022). Analisis dari Unit 42 Palo Alto Networks (2023) mengonfirmasi bahwa kombinasi Squirrelwaffle dan Cobalt Strike banyak digunakan dalam serangan ransomware serta pencurian data. Berikut *tools* dan teknologi yang digunakan dalam penelitian ini.

1) Wireshark

Wireshark adalah sebuah network protocol analyzer yang digunakan untuk menangkap dan menganalisis lalu lintas jaringan secara real time. Aplikasi ini memungkinkan pengguna untuk melihat data yang mengalir melalui jaringan dalam bentuk paket-paket yang dapat diperiksa secara mendetail. Wireshark sering digunakan oleh administrator jaringan, analis keamanan, dan peneliti forensik untuk mendeteksi masalah jaringan, memeriksa serangan siber, serta memahami bagaimana data dikirim dan diterima. Wireshark mendukung berbagai protokol jaringan seperti TCP, UDP, HTTP, HTTPS, DNS, dan banyak lagi



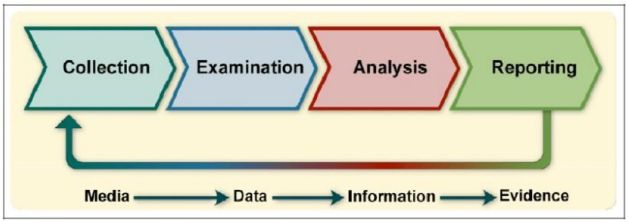
Gambar 1. Squirrelwaffle Attack-chain

2) VirusTotal

VirusTotal adalah layanan berbasis web yang memungkinkan pengguna untuk menganalisis file dan URL guna mendeteksi kemungkinan ancaman keamanan seperti virus, malware, trojan, dan phishing. Layanan ini bekerja dengan mengunggah file atau memasukkan URL ke dalam sistemnya, kemudian VirusTotal akan memeriksa menggunakan berbagai mesin antivirus dan alat deteksi keamanan dari berbagai vendor. VirusTotal juga memberikan informasi tentang tingkat kepercayaan file atau situs web berdasarkan analisis komunitas dan database keamanan. Layanan ini sering digunakan oleh peneliti keamanan, analis malware, dan administrator IT untuk memverifikasi keamanan file atau situs sebelum digunakan.

III. METODE PENELITIAN

Penelitian ini menggunakan metode Digital Forensics Investigation Framework berdasarkan standar yang dikembangkan oleh National Institute of Standards and Technology (NIST). Metode ini terdiri dari beberapa tahapan yang sistematis dalam melakukan investigasi digital forensik guna memperoleh, menganalisis, dan menyajikan bukti digital secara valid dan sah. Adapun metode NIST memiliki 4 tahapan utama yaitu:



Gambar 2. Digital Forensik Flowchart

A. Collection (Pengumpulan Data)

Pada tahap ini, data digital yang relevan dikumpulkan dari berbagai sumber. Dalam penelitian ini, data diperoleh dari situs Malware Traffic Analysis, khususnya dari halaman malware-traffic-analysis.net yang menyediakan rekaman lalu lintas jaringan dari serangan malware. Data yang dikumpulkan di arsip tanggal 21-09-2021 dengan judul SQUIRRELWAFFLE LOADER WITH COBALT STRIKE meliputi:

a) **2021-09-21-IOCs-for-Squirrelwaffle-Loader-and-Cobalt Strike.txt.zip** yaitu file berisi Indicators of Compromise (IOCs) Daftar domain, IP, hash file, dan URL yang terkait dengan Squirrelwaffle Loader dan Cobalt Strike.

b) **2021-09-21-Squirrelwaffle-Loader-with-Cobalt-Strike.pcap.zip** yaitu file Paket jaringan (PCAP files) yang mencatat komunikasi antara sistem yang terinfeksi dan server berbahaya.

c) **2021-09-21-Squirrelwaffle-Loader-malware-and-artifacts.zip** yaitu Artefak malware yang ditemukan dalam lalu lintas jaringan atau file yang diunduh selama serangan berlangsung.

B. Examination (Pemeriksaan)

Tahap ini melibatkan proses penyaringan dan identifikasi data yang relevan dengan kasus. Pemeriksaan dilakukan dengan:

a) Analisis paket jaringan untuk mengidentifikasi lalu lintas mencurigakan yang mengarah ke unduhan malware.

b) Pemeriksaan file eksekusi untuk menentukan apakah file tertentu berisi kode berbahaya atau skrip yang mencurigakan.
c) Analisis hashing (MD5, SHA-1) guna memverifikasi integritas data dan membandingkannya dengan database malware yang sudah dikenal.
d) Eksaminasi header email atau metadata URL untuk memahami bagaimana malware dikirimkan ke targetnya.

C. Analysis (Analisis)

Pada tahap ini, data yang telah diperiksa dianalisis untuk menemukan hubungan antara bukti digital yang ditemukan. Analisis meliputi:

a) Rekonstruksi aktivitas pengguna untuk memahami bagaimana serangan dimulai dan bagaimana malware menyebar dalam sistem.
b) Identifikasi command and control (C2) server untuk mengetahui komunikasi antara perangkat yang terinfeksi dan server penyerang.
c) Analisis malware behavior dengan mengeksekusi sampel malware dalam lingkungan yang terkendali (sandbox) guna memahami cara kerjanya.
d) Korelasi log dan timeline analysis untuk menentukan urutan kejadian yang mengarah ke infeksi malware.

D. Reporting (Pelaporan)

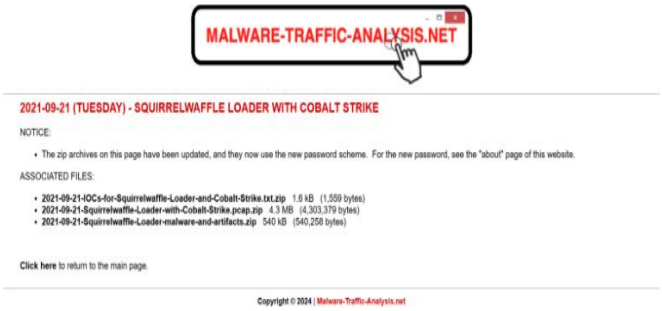
Tahap akhir dalam metode NIST adalah penyusunan laporan hasil investigasi yang mencakup:

a) Deskripsi kasus berdasarkan analisis data yang dikumpulkan.
b) Dokumentasi temuan teknis, seperti sumber infeksi, alamat IP berbahaya, dan teknik eksploitasi yang digunakan.
c) Visualisasi lalu lintas jaringan yang menunjukkan komunikasi antara malware dan server penyerang.
d) Kesimpulan dan rekomendasi untuk mitigasi serta tindakan pencegahan agar kejadian serupa tidak terjadi di masa depan.

IV. HASIL PEMBAHASAN

A. COLLECTION (Pengumpulan Data)

Berdasarkan analisis di malware-traffic-analysis.net, khususnya pada tanggal 21 September 2021, penelitian ini berhasil mengumpulkan sejumlah artefak digital. Pengumpulan data ini menggunakan metodologi NIST. Artefak-artefak yang terkumpul tersebut ditampilkan pada gambar berikut.

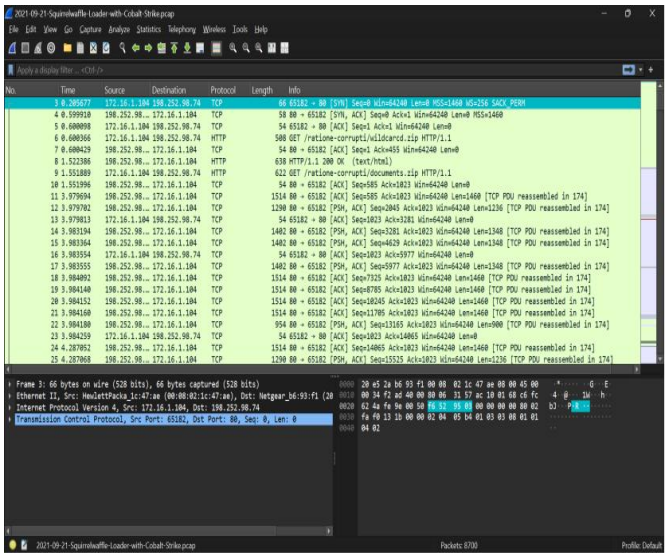


Gambar 3. Sumber Data

Artefak-artefak yang dapat ditemukan adalah:

a) **2021-09-21-IOCs-for-Squirrelwaffle-Loader-and-Cob alt Strike.txt.zip** yaitu berisi Indicators of Compromise (IOCs) Daftar domain, IP, hash file, dan URL yang terkait dengan Squirrelwaffle Loader dan Cobalt Strike.
b) **2021-09-21-Squirrelwaffle-Loader-with-Cobalt-Strik e.pcap.zip** yaitu file Paket jaringan (PCAP files) yang mencatat komunikasi antara sistem yang terinfeksi dan server berbahaya.
c) **2021-09-21-Squirrelwaffle-Loader-malware-and-artif acts.zip** yaitu Artefak malware yang ditemukan dalam lalu lintas jaringan atau file yang diunduh selama serangan berlangsung.

Jika dibuka pada Wireshark file PCAP terlihat seperti gambar dibawah:


Gambar 4. File PCAP pada Wireshark

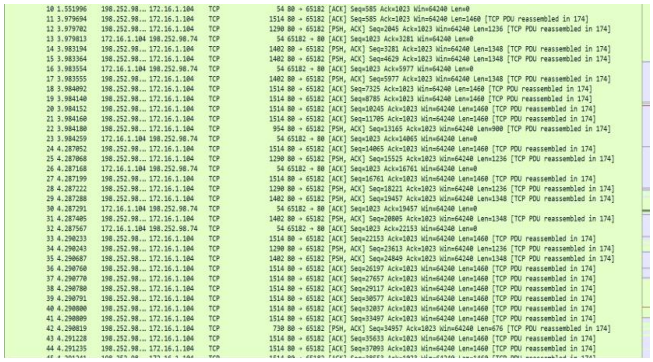
Ini mengindikasikan bahwa file pcap ini kemungkinan besar berisi informasi atau bukti terkait dengan aktivitas malware Squirrelwaffle dan Cobalt Strike.

Kolom Info pada baris 6 dan 9: Menunjukkan adanya komunikasi HTTP yang mencurigakan, yaitu GET/ratione-corrupti/documents.zip HTTP/1.1 adalah permintaan untuk mengunduh file wildcard.zip dan documents.zip dari server. Nama file dan direktori yang tidak biasa (ratione-corrupti) bisa menjadi indikasi bahwa ini adalah bagian dari serangan atau aktivitas mencurigakan.

Baris 11, 12, 14, 15, 17, 18, 19, 20, 21, 24, 25: Menunjukkan adanya fragmentasi TCP (TCP segment reassembly). Hal ini bisa jadi upaya untuk menyembunyikan payload atau untuk menghindari deteksi. Perhatikan kata-kata seperti "[TCP PDU reassembled in 174]" yang mengindikasikan paket-paket TCP yang disusun ulang.

B. EXAMINATION (Pemeriksaan)

Pada Proses pemeriksaan ini lebih berfokus pada log lalu lintas jaringan, seperti terlihat pada gambar di bawah:



Gambar 5. Log lalu lintas jaringan

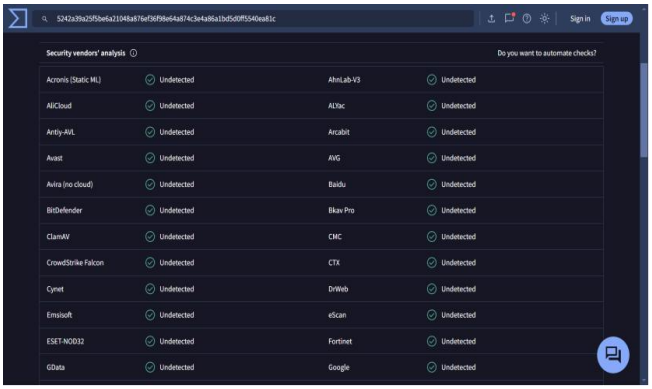
Dalam file pcap "2021-09-21-Squirrelwaffle-Loader-with-Cobalt Strike.pcap " yang dibuka melalui Wireshark, ditemukan aktivitas yang sangat mencurigakan dan mengindikasikan adanya infeksi malware. Baris-baris log menampilkan komunikasi jaringan yang tidak biasa, dimulai dengan serangkaian paket TCP yang terfragmentasi. Paket paket ini, dengan nomor urut 11, 12, 14, 15, dan seterusnya, menunjukkan upaya untuk menyusun ulang data yang kemungkinan besar sengaja dipecah-pecah untuk menghindari deteksi. Pola fragmentasi ini sangat mirip dengan taktik yang sering digunakan oleh malware untuk menyembunyikan payload berbahaya.

Selanjutnya, perhatian tertuju pada baris 10, di mana terlihat paket TCP dengan flag ACK. Meskipun terlihat normal, paket ini menjadi janggal ketika dilihat bersamaan dengan fragmentasi TCP sebelumnya. Ini mengisyaratkan bahwa ada data penting yang sedang dinegosiasikan atau dikirimkan secara tersembunyi. Kecurigaan semakin bertambah ketika melihat baris-baris berikutnya, di mana pola fragmentasi TCP terus berlanjut dengan berbagai ukuran paket dan flag yang berbeda. Hal ini mengindikasikan adanya upaya yang terus-menerus untuk menyusun kembali sesuatu yang tersembunyi.

Tidak hanya itu, kejanggalan juga ditemukan pada baris 42, di mana terlihat paket dengan flag PSH dan ACK. Flag PSH (Push) menandakan bahwa data harus segera disampaikan ke aplikasi penerima. Kombinasi dengan ACK (Acknowledgement) menunjukkan bahwa data telah diterima dan diakui. Namun, yang lebih mencurigakan adalah ukuran paket ini yang relatif kecil dibandingkan dengan paket-paket terfragmentasi sebelumnya. Ini menimbulkan dugaan bahwa data yang "didorong" ini mungkin merupakan perintah atau instruksi tersembunyi dari command and control server malware.

C. ANALYSIS (Analisis)

Berdasarkan analisis aktivitas HTTP, ditemukan permintaan untuk mengunduh dua file mencurigakan, /ratione-corrupti/wildcarcd.zip dan /ratione-corrupti/documents.zip. Nama file dan direktori yang tidak biasa ini mengindikasikan potensi aktivitas berbahaya. Selain itu, terjadi fragmentasi TCP yang signifikan, di mana beberapa paket TCP perlu disusun ulang, yang mungkin merupakan upaya untuk menyembunyikan payload atau menghindari deteksi. Analisis lebih lanjut mengungkapkan bahwa nama file pcap mengandung kata-kata "Squirrelwaffle" dan "Cobalt Strike", yang merupakan indikator kuat adanya aktivitas malware. Squirrelwaffle adalah jenis malware yang sering digunakan untuk menyebarkan payload berbahaya, termasuk Cobalt Strike, yang merupakan framework penetrasi yang sering digunakan oleh penyerang untuk post-exploitation. Terakhir, string "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36 Edg/93.0.961.52" terdeteksi dalam detail paket data. Meskipun ini adalah user agent yang umum, namun tetap perlu diperhatikan jika ada anomali lain yang ditemukan.



Gambar 6. Hasil pemeriksaan file

File yang mencurigakan ini telah melewati serangkaian pengujian ketat oleh berbagai vendor keamanan terkemuka. Mayoritas, termasuk Avast, AVG, BitDefender, ESET-NOD32, dan Fortinet, menyatakan file tersebut tidak terdeteksi atau tidak berbahaya. Namun, satu vendor, AhnLab, memberikan peringatan dengan tanda seru berwarna merah, menandakan adanya potensi ancaman. Meskipun demikian, tanpa rincian lebih lanjut mengenai jenis atau tingkat keparahan virus yang terdeteksi oleh AhnLab.

D. REPORTING (Pelaporan)

File pcap ini dengan jelas menunjukkan adanya aktivitas berbahaya yang terkait dengan malware. Fragmentasi TCP yang signifikan menjadi indikator kuat adanya upaya penyembunyian payload berbahaya. Pola fragmentasi yang kompleks ini melibatkan serangkaian

paket dengan berbagai ukuran dan flag TCP yang tidak biasa, mengisyaratkan adanya komunikasi tersembunyi dengan command and control server malware. Komunikasi ini kemungkinan besar digunakan untuk mengirimkan perintah, menerima instruksi, atau mentransfer data curian.

Analisis lebih lanjut mengungkapkan adanya permintaan HTTP GET yang mencurigakan, yang mengarahpada pengunduhan file bernama "wildcarcd". File ini sangat mungkin merupakan komponen berbahaya dari malware. Nama "wildcarcd" sendiri terdengar mencurigakan dan tidak umum, sehingga memperkuat dugaan bahwa file ini berbahaya. Kemungkinan besar, file ini berisi payload berbahaya yang akan dieksekusi pada sistem yang terinfeksi.

V. KESIMPULAN

Analisis lalu lintas jaringan menggunakan metode NIST menunjukkan adanya aktivitas mencurigakan yang melibatkan indikator-indikator "Malicious" atau "Malware". File pcap yang dianalisis memperlihatkan adanya fragmentasi TCP yang signifikan. Teknik ini umum digunakan untuk menyembunyikan payload berbahaya, mempersulit deteksi oleh sistem keamanan konvensional. Pola fragmentasi yang kompleks, bersamaan dengan ukuran paket yang tidak biasa dan kombinasi flag TCP yang mencurigakan (PSH, ACK), mengindikasikan adanya komunikasi tersembunyi. Komunikasi ini diduga kuat menuju command and control server yang berpotensi berbahaya.

Lebih lanjut, beberapa anomali ditemukan dalam urutan dan waktu antar paket, menimbulkan pertanyaan tentang integritas dan asal-usul data. Beberapa paket menunjukkan adanya retransmission atau pengiriman ulang, yang bisa jadi merupakan indikasi masalah jaringan atau upaya untuk memastikan data berbahaya terkirim dengan sukses. Selain itu, ditemukan adanya paket-paket dengan ukuran sangat kecil yang dikirimkan setelah serangkaian paket terfragmentasi. Ini mengisyaratkan kemungkinan adanya instruksi atau perintah tersembunyi yang disisipkan di antara lalu lintas yang tampak normal.

Secara keseluruhan, temuan ini mengindikasikan adanya ancaman keamanan yang perlu diselidiki lebih lanjut. Meskipun jenis dan tujuan pasti dari aktivitas ini belum dapat ditentukan dengan pasti, indikator indikator yang ditemukan sangat mengkhawatirkan. Investigasi lebih lanjut diperlukan untuk mengungkap payload yang tersembunyi, mengidentifikasi command and control server, dan menentukan tingkat kerusakan yang mungkin ditimbulkan. Langkah-langkah mitigasi yang tepat harus segera diambil untuk melindungi sistem dari potensi serangan siber.

REFERENCES

[1] Casey, E. (2011). Digital Forensics and Cyber Crime. Elsevier.
[2] Huntress Labs. (2021). Analysis of Squirrelwaffle Malware Campaigns.
[3] McAfee. (2022). Threat Report: Squirrelwaffle and Emerging Malware Trends.
[4] Mandiant. (2022). Understanding the Use of Cobalt Strike in Cyber Attacks.
[5] Talos Intelligence. (2022). Cyber Threat Analysis: Squirrelwaffle and Cobalt Strike.
[6] Unit 42 Palo Alto Networks. (2023). Ransomware Threat Report.
[7] NIST SP 800-86. (2006). Guide to Integrating Forensic Techniques into Incident Response.
[8] VirusTotal. (2023). Threat Intelligence and Malware Detection Services.
[9] Orebaugh, A., Ramirez, G., & Beale, J. (2006). Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress.
[10] SANS Institute. (2023). Advanced Network Forensics and Analysis.