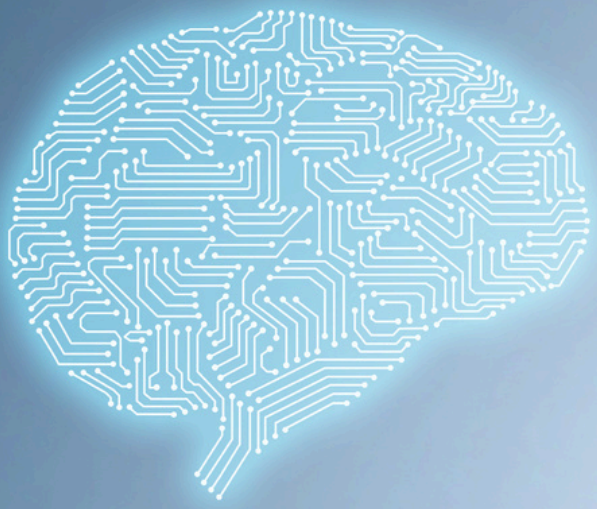
MAGAZINE PUNGGAWA

VOLUME 3.0



ARTIFICIAL INTELLIGENCE

Integrasi Ollama dan AnythingLLM

Keamanan Siber : AI Chatbot

Patching The Human Vulnerability

RansomHub : The Rising Star

TOP 5 CVE Kuartal 3 2024

PUNGGAWA cybersecurity

Tentang Kami

PUNGGAWA merupakan istilah dari kebudayaan Indonesia yang mengacu pada sosok pemimpin atau figur berwibawa yang terkenal akan kepemimpinannya, tanggung jawab, dan arahan dalam suatu komunitas. Istilah ini melambangkan dedikasi terhadap keunggulan kepemimpinan, praktik etik, atribut kekuatan, kearifan, dan kepercayaan, serta sikap pelindung terhadap mereka yang berada dalam lingkup pengawasannya.

Kami Merupakan PUNGGAWA

Tim PUNGGAWA didirikan pada tahun 2018 dan mulai memberikan layanan kepada pelanggan pada tahun 2019, dengan memulai dari layanan uji penetrasi. Kami telah berhasil merealisasikan dan menembus pasar keamanan siber di Indonesia. Dalam kemitraan dengan klien, kami menyediakan solusi dan layanan keamanan siber yang dirancang untuk meningkatkan postur keamanan secara komprehensif, menutup celah, dan memantau kerentanan secara berkelanjutan melalui operasi dan dukungan yang persisten dengan mengimplementasikan identifikasi, perlindungan, deteksi, respons, dan pemulihan.

Visi

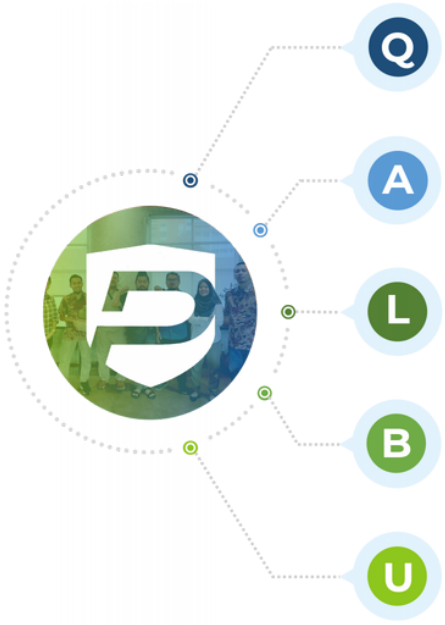
Menjadi Mitra Pilihan dalam Kemampuan Keamanan Siber sebagai Kontribusi Utama dalam Mewujudkan Dunia yang Lebih Aman bagi Transformasi Digital.

Misi

Mengantarkan Hasil yang Berhasil, dimana pada akhirnya, dedikasi kami terhadap proses dan tenaga ahli kami akan mengarah pada solusi yang mengantarkan hasil yang berhasil bagi klien kami.
Membangun Budaya Pembelajaran dan Kesadaran, kami berkomitmen untuk terus membangun budaya pembelajaran dan kesadaran di dalam tim kami.
Berbagi dan Berkolaborasi dengan Komunitas, kami beroperasi secara kolaboratif sebagai mitra dan tim, baik dalam organisasi maupun dalam komunitas yang lebih luas.

Nilai Inti Kami

Di PUNGGAWA, kami mengejar tujuan dan kesuksesan, dengan pemahaman bahwa satu akan membawa pada yang lain. Nilai inti kami membina budaya yang mendukung respons yang cepat dan berkualitas tinggi, sikap proaktif, pembelajaran dan kepemimpinan yang berkelanjutan, pemecahan masalah yang inovatif, dan kesatuan yang kokoh. Prinsip-prinsip ini memandu tim kami dalam menyediakan solusi keamanan siber yang maju dan dapat diandalkan, memastikan keamanan digital klien kami dengan profesionalisme dan kecemerlangan tertinggi. Kami menjalankan nilai-nilai kami dan mewujudkannya setiap hari melalui hubungan kami dengan karyawan, klien, mitra, dan keluarga.



CORE VALUE, QALBU

Quick and High Quality Response:
Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything:
Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed:
Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver:
Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strenght
Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

PUNGGAWA cybersecurity

PUNGGAWA
cyber security services

Selamat datang di edisi ketiga majalah kami yang penuh dengan wawasan dan pengetahuan mendalam seputar dunia keamanan siber. Di edisi kali ini, kami akan membahas topik yang sedang hangat dan relevan: Generative AI in Cybersecurity. Dengan perkembangan pesat teknologi, kami percaya bahwa memahami dan memanfaatkan AI generatif akan menjadi kunci dalam menjaga keamanan digital di era transformasi ini.

Sebagai perusahaan yang relatif baru, Punggawa Cybersecurity berdedikasi untuk menjadi mitra pilihan dalam memberikan solusi keamanan siber yang inovatif dan handal. Kami selalu berusaha memberikan layanan dengan integritas tinggi, sesuai dengan slogan kami, "Cybersecurity Delivered with Integrity". Kepercayaan dan keamanan adalah pondasi dari setiap langkah yang kami ambil dalam menjaga aset digital Anda dan kami percaya bahwa kejujuran dan integritas adalah fondasi dari keberhasilan jangka panjang.

Visi Punggawa Cybersecurity, "To become a preferred Partner in cyber security capabilities as a key contribution to making the world safer for digital transformation," adalah komitmen kami untuk terus berkembang dan menjadi yang terbaik dalam bidang ini. Kami percaya bahwa dengan kolaborasi, edukasi, dan inovasi, kita semua dapat menciptakan lingkungan digital yang lebih aman dan terpercaya. Dengan visi ini, kami berkomitmen untuk terus berinovasi dan menyediakan solusi keamanan yang paling efektif dan terpercaya bagi klien kami. Kami ingin memastikan bahwa setiap langkah yang kami ambil sejalan dengan tujuan untuk menciptakan dunia digital yang lebih aman.

Dalam edisi Magazine Punggawa Volume 3 ini, pembaca akan menemukan berbagai artikel menarik dan informatif, seperti Integrasi Ollama dan AnythingLLM , UU PDP : Bukan Sekadar Regulasi, Unveiling CVE-2023-45866, hingga Patching The Human Vulnerability. Kami juga membahas tentang Serangan Ransomware Data Center : Enkripsi dan Penghapusan Backup, Strategi Efektif Analisis Forensik Menggunakan Hayabusa, serta berbagai artikel lainnya yang relevan dengan dunia keamanan siber.

Kami berharap majalah ini dapat menjadi sumber inspirasi dan pengetahuan bagi Anda semua. Terima kasih telah menjadi bagian dari perjalanan kami, dan selamat menikmati edisi kedua dari
Punggawa Cybersecurity Magazine.

Salam Hangat,

Iwan Setiawan
CEO PUNGGAWA CYBERSECURITY

TABLE OF CONTENTS

PUNGGAWA cybersecurity

MAGAZINE PUNGGAWA VOLUME 3

Our Contributors

AD Aji
Offensive Security Leader

M Jufri
Senior Penetration Tester

Ambar F
SOC Analyst

Kang Ali
Cyber Security - RND

Devanda CP
Cyber Security - RND

Rachmat AR
Senior Penetration Tester

MR El Ghiffari
Junior Penetration Tester

Danang AM
Junior Penetration Tester

Rezky DK
Cyber Solution Consultant

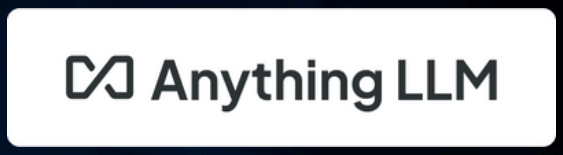
Editor-in-Chief

Fadhil N
Cyber Security Consultant

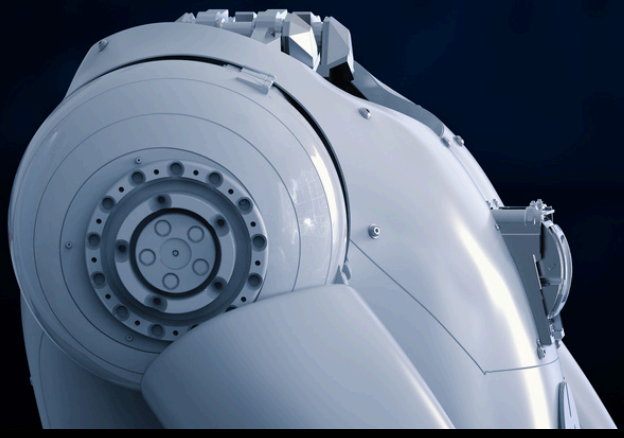
Managing Editor

Kang Ali
Cyber Security - RND

PUNGGAWA
cyber security services



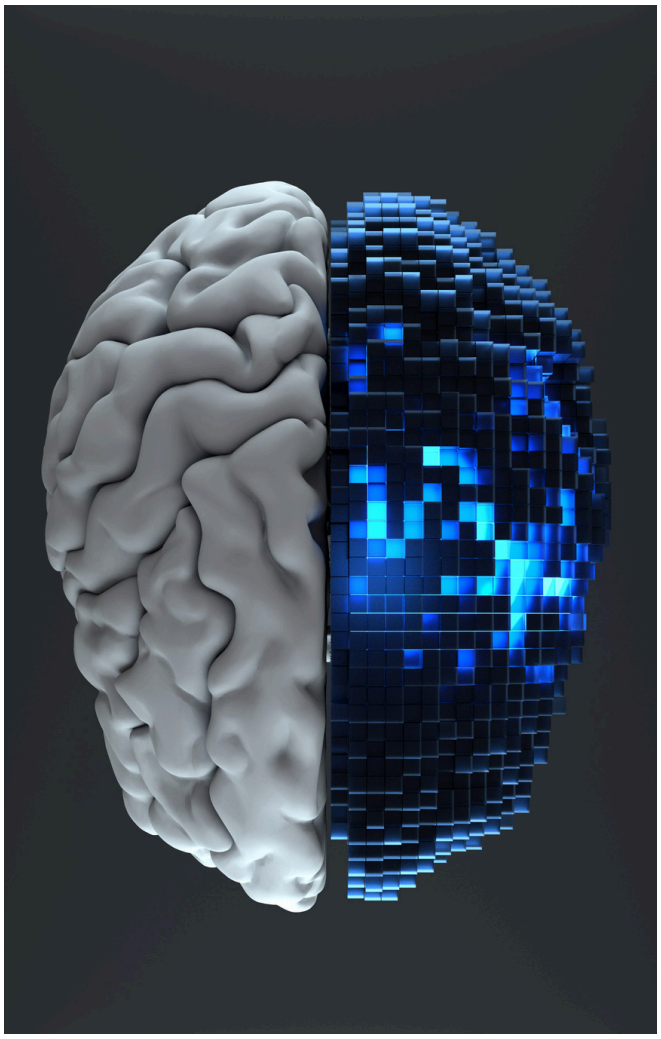
07



INTEGRASI OLLAMA DAN ANYTHINGLLM

By **Kang Ali**
Cyber Security - RND

Dalam era digital yang semakin mengandalkan teknologi kecerdasan buatan (AI), pengembangan aplikasi berbasis model bahasa besar (LLM) menjadi semakin lazim. Pengembang kini memiliki akses ke berbagai platform yang memudahkan integrasi LLM ke dalam aplikasi mereka, dan dua di antaranya yang menonjol adalah Ollama dan AnythingLLM. Artikel ini akan membahas bagaimana integrasi antara kedua platform ini dapat mempercepat pengembangan aplikasi AI dan mengatasi tantangan yang dihadapi oleh para pengembang.



Apa Itu Ollama dan AnythingLLM?

- Ollama adalah framework open-source yang berfokus pada penyederhanaan penggunaan model LLM dalam berbagai lingkungan pengembangan. Ollama memungkinkan model AI berjalan secara lokal atau cloud dengan manajemen yang lebih fleksibel.
- AnythingLLM, di sisi lain, adalah platform yang menyediakan antarmuka sederhana untuk mengintegrasikan berbagai model LLM ke dalam aplikasi. Platform ini dirancang untuk memberikan kemudahan bagi pengembang yang ingin memanfaatkan LLM tanpa harus berurusan dengan kompleksitas pengelolaan model.

Keunggulan Integrasi Ollama dan AnythingLLM

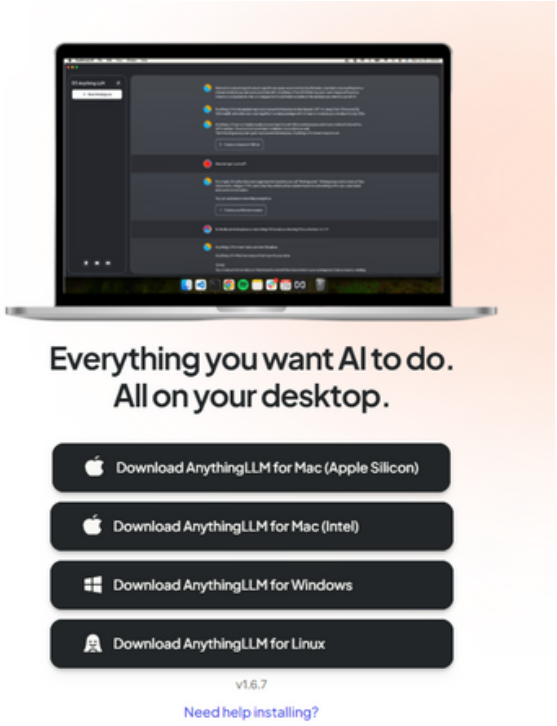
Menggabungkan Ollama dengan AnythingLLM memberikan keuntungan strategis bagi pengembang aplikasi berbasis AI. Berikut adalah beberapa keunggulan utama:

1. Fleksibilitas Implementasi Dengan Ollama, pengembang dapat menjalankan model AI di lingkungan lokal maupun cloud. Integrasi dengan AnythingLLM menambahkan lapisan fleksibilitas dengan memungkinkan pengembang memilih dan mengelola berbagai model LLM tanpa kendala teknis yang rumit. Hal ini mempercepat proses prototipe hingga tahap implementasi produksi.
2. Manajemen Model yang Lebih Mudah AnythingLLM memberikan pengembang antarmuka yang mudah digunakan untuk beralih antara berbagai model LLM, sedangkan Ollama menyediakan infrastruktur yang mendukung pelatihan dan deployment model secara efisien. Kombinasi ini memungkinkan pengembang untuk fokus pada pengembangan aplikasi tanpa harus khawatir tentang pengelolaan model.
3. Optimalisasi Kinerja Lokal Banyak pengembang yang menginginkan kinerja lokal optimal untuk aplikasi AI mereka. Ollama menyediakan dukungan untuk menjalankan model LLM secara lokal, yang bisa dimanfaatkan dengan integrasi AnythingLLM untuk mempercepat waktu respon, mengurangi latensi, serta mengurangi ketergantungan pada koneksi internet.
4. Dukungan Multi-Platform Ollama memungkinkan pengembangan lintas platform, baik itu untuk aplikasi web, desktop, maupun mobile. AnythingLLM melengkapi ini dengan dukungan untuk berbagai framework dan bahasa pemrograman, sehingga pengembang bisa dengan mudah mengimplementasikan solusi AI lintas perangkat.

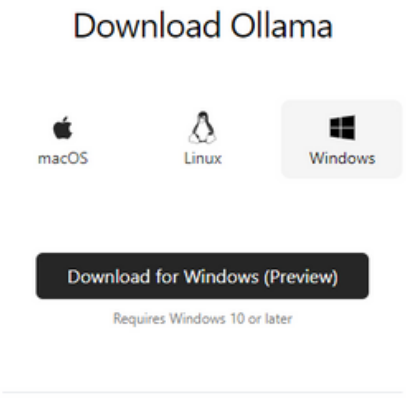
Bagaimana Integrasi Ini Bekerja?

Integrasi antara Ollama dan AnythingLLM biasanya melibatkan beberapa langkah teknis, namun AnythingLLM menyederhanakannya dengan antarmuka API yang sederhana. Berikut adalah gambaran umum bagaimana proses integrasi ini berlangsung:

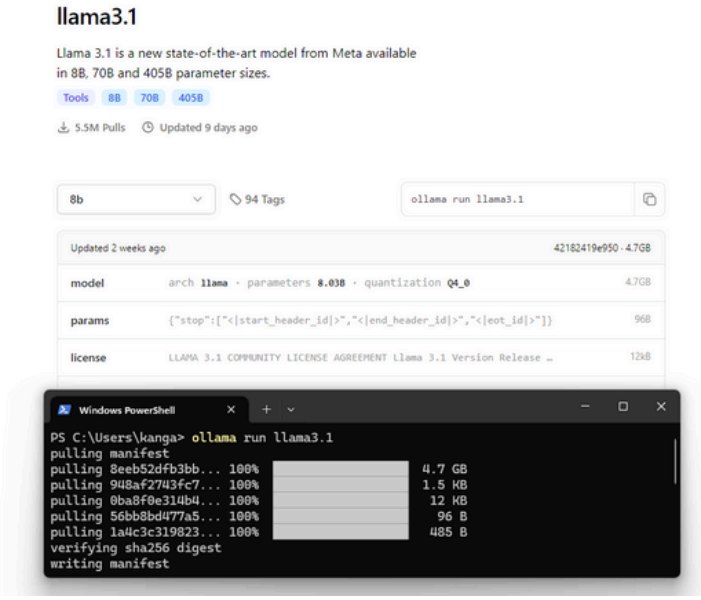
1. Pengaturan Model di Ollama: Pertama, pengembang mengonfigurasi model AI di lingkungan Ollama, baik lokal maupun berbasis cloud. Model ini dapat dilatih lebih lanjut atau dimodifikasi sesuai kebutuhan aplikasi.
2. Integrasi dengan AnythingLLM: Model yang sudah disiapkan di Ollama kemudian dihubungkan ke AnythingLLM melalui API. AnythingLLM mengelola interaksi antara aplikasi dan model, memungkinkan pengembang untuk mengakses kemampuan AI dengan mudah.
3. Pengelolaan dan Pembaruan: Setelah integrasi berhasil, pengembang dapat dengan mudah mengganti model, memperbarui versi, atau menambahkan fitur baru ke aplikasi menggunakan antarmuka yang disediakan oleh AnythingLLM.



Download Anythingllm di https://anythingllm.com/

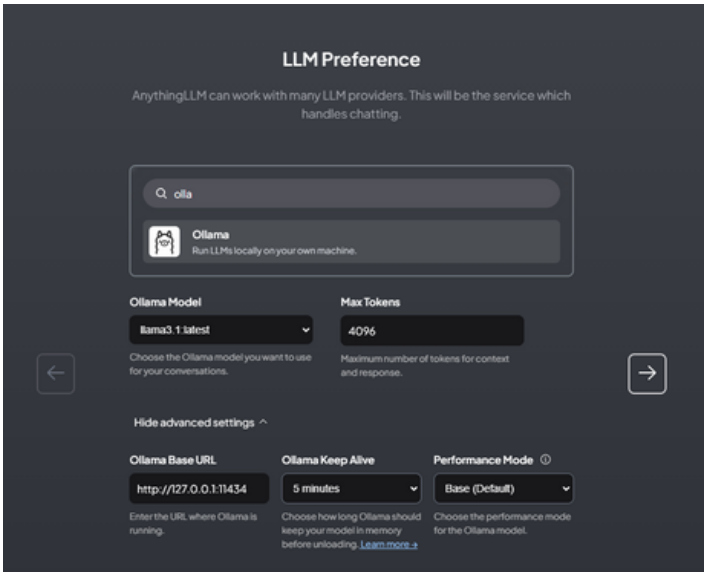


Download Ollama di https://ollama.com/

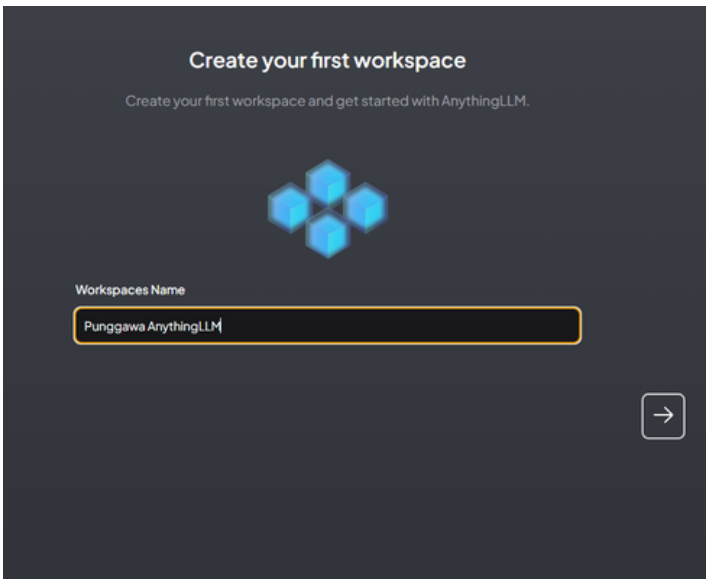


Download model ai llama3.1 https://ollama.com/library/llama3.1, perintah download model : ollama run llama3.1

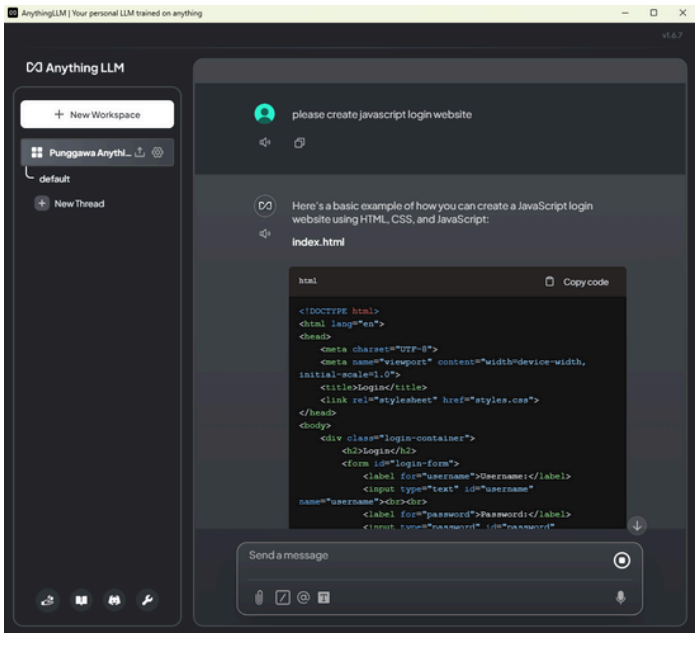
Setelah model berhasil di download, buka anythingllm untuk konfigurasi model ollama yang sudah di download dengan anythingllm



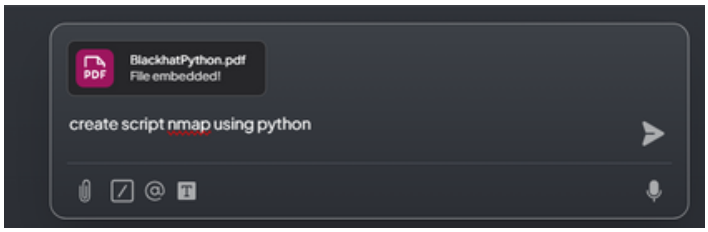
Konfigurasi anythingllm kita bisa memilih Ollama sebagai LLM Providers yang digunakan. Pastikan juga port dari Ollama base URL aktif di port http://127.0.0.1:11435/



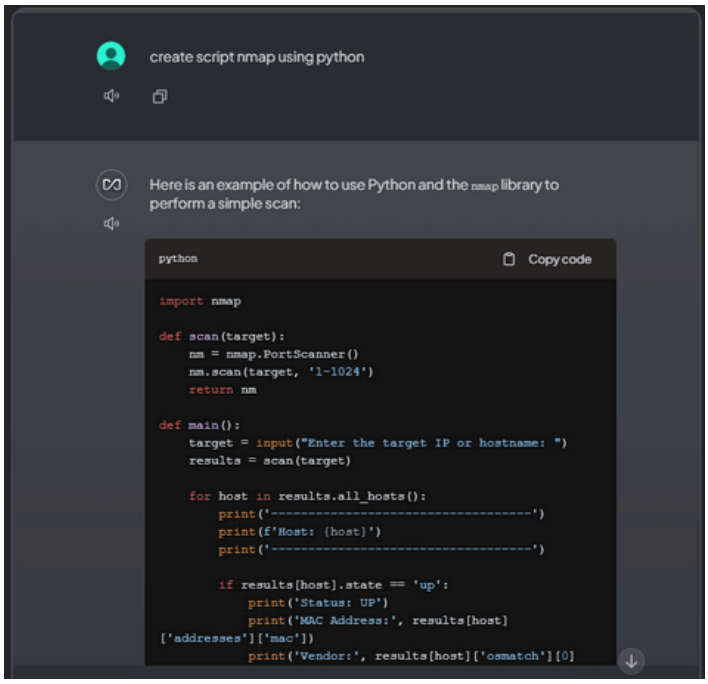
Setelah itu isi workspace name dengan nama yang diinginkan di sini saya memasukan nama PunggawaAnythingLLM



Setelah konfigurasi berhasil kita dapat melakukan pertanyaan atau chat pengujian langsung di kolom chat.



Di anythingllm juga sudah tersedia fitur RAG dimana kita bisa upload file pdf untuk menambah atau menghasilan output untuk tugas seperti menjawab pertanyaan yang sesuai dengan pdf yang di upload.



Contoh di sini saya membuat tugas atau pertanyaan untuk membuatkan script nmap menggunakan bahasa pemrograman python.

Kesimpulan

Integrasi Ollama dan AnythingLLM menciptakan ekosistem yang efisien dan fleksibel bagi pengembang yang ingin memanfaatkan kekuatan LLM dalam aplikasi mereka. Dengan menyediakan kemudahan pengelolaan model, fleksibilitas platform, dan kinerja optimal, integrasi ini menjadi solusi ideal untuk mempercepat adopsi teknologi AI di berbagai industri. Apakah Anda seorang pengembang yang baru mengenal LLM atau sudah berpengalaman, kombinasi Ollama dan AnythingLLM dapat membawa pengembangan aplikasi berbasis AI ke level berikutnya.

UU PDP : BUKAN SEKADAR REGULASI

INI ADALAH LANGKAH STRATEGIS UNTUK KEAMANAN DATA PERUSAHAAN

By **Devanda CPN**
Cyber Security - RND

Di era digital yang semakin terhubung, ancaman terhadap keamanan data pribadi kian meningkat. Teknologi yang berkembang pesat memang menawarkan kemudahan dalam berbagai aspek kehidupan, namun di sisi lain, membawa risiko baru terkait pelanggaran privasi. Kasus-kasus kebocoran data dan penyalahgunaan informasi pribadi semakin sering terjadi, yang mendorong perlunya regulasi yang efektif untuk melindungi hak-hak individu.

Sebagai respons atas situasi ini, pemerintah Indonesia mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) pada 17 Oktober 2022. UU PDP bertujuan melindungi hak privasi individu melalui pedoman yang jelas mengenai pengumpulan, penggunaan, dan pengelolaan data pribadi.

Hal ini disampaikan oleh Danny Kobrata, Partner di K&K Advocates, dalam diskusi "Corporate Insight: Strengthening PDP Law Governance Through Cybersecurity" yang diselenggarakan oleh Telkomsigma. Menurut Danny, meskipun pelindungan data pribadi dan keamanan siber merupakan dua hal yang berbeda, keduanya memiliki tujuan yang sama, yaitu menjaga integritas dan keamanan data pribadi dari risiko-risiko yang ada, termasuk melalui langkah-langkah mitigasi yang diatur dalam UU PDP.

Sejalan dengan penjelasan tersebut, perusahaan sebagai pengendali data memiliki tanggung jawab besar dalam memastikan bahwa seluruh proses pengelolaan data dilakukan dengan transparansi dan sesuai dengan ketentuan yang berlaku.

PRESIDEN
REPUBLIK INDONESIA

SALINAN

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 27 TAHUN 2022

TENTANG

PELINDUNGAN DATA PRIBADI

Kewajiban Pengendali Data dan Tindakan Preventif untuk Mencegah Kebocoran

Perusahaan atau entitas yang menyimpan dan memproses data pribadi, seperti pemerintah dan perusahaan swasta, diwajibkan untuk transparan dalam penggunaannya. Mereka harus mendapatkan izin dari pemilik data sebelum memprosesnya dan menjaga keamanan data agar tidak terjadi kebocoran.

Kewajiban tersebut diatur secara rinci dalam BAB VI UU Pelindungan Data Pribadi (UU PDP), yang mengatur tanggung jawab pengendali dan prosesor data pribadi. Salah satu kewajiban utama pengendali data adalah mencegah akses yang tidak sah terhadap data pribadi, sebagaimana diatur dalam Pasal 39 ayat (2) UU PDP. Pasal ini menegaskan bahwa pencegahan tersebut harus dilakukan melalui penerapan sistem keamanan yang andal, aman, dan bertanggung jawab dalam pemrosesan data.

Lebih lanjut, pengendali data pribadi juga bertanggung jawab atas seluruh proses pengelolaan data, termasuk menjaga kerahasiaan, integritas, dan ketersediaan data. Kegagalan melindungi data pribadi, baik dalam bentuk kerusakan, kehilangan, perubahan, maupun akses yang tidak sah, dianggap sebagai pelanggaran yang dapat berdampak serius bagi perusahaan.

Meskipun UU PDP tidak memberikan aturan teknis secara mendetail mengenai alat keamanan siber yang digunakan, regulasi dari Badan Siber dan Sandi Negara (BSSN) memberikan panduan lebih lanjut, seperti kewajiban sertifikasi untuk memastikan perusahaan mematuhi standar keamanan yang ada.

Setidaknya terdapat **beberapa hal yang harus diperhatikan** oleh perusahaan dengan mengacu pada rambu-rambu **UU No.27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)**, supaya perusahaan aman dari sanksi hukum baik sanksi administratif maupun sanksi pidana.

- **Penilaian Dampak Pelindungan Data Pribadi** – Setiap kegiatan baru yang melibatkan pemrosesan data pribadi harus didahului dengan penilaian dampak yang komprehensif untuk meminimalkan risiko pelanggaran.
- **Pelatihan Karyawan** – Karyawan harus dilatih secara berkala mengenai kewajiban perusahaan terkait penilaian dampak dan kebijakan perlindungan data pribadi.
- **Kebijakan Internal** – Kebijakan perusahaan harus secara eksplisit mengacu pada persyaratan perlindungan data pribadi yang diatur dalam UU PDP.
- **Audit dan Evaluasi Rutin** – Perusahaan diwajibkan melakukan audit dan evaluasi keamanan data secara berkala untuk memastikan sistem perlindungan tetap kuat.
- **Pelaporan Insiden** – Jika terjadi kebocoran data, perusahaan harus melaporkannya dalam waktu 72 jam kepada otoritas terkait dan subjek data pribadi yang terdampak.

Selain kewajiban tersebut, UU PDP juga menekankan pentingnya perusahaan memiliki strategi manajemen risiko yang berfokus pada ketahanan dan keamanan data sesuai dengan standar internasional, seperti ISO 27001.

Penerapan respons insiden yang terstruktur, pelatihan karyawan untuk menghadapi kebocoran data, dan strategi ketahanan siber adalah elemen penting untuk memastikan data pribadi tetap terlindungi.

Data Pengguna Bocor, Perusahaan Terancam Denda Besar

Regulasi ini memberikan waktu transisi dua tahun bagi perusahaan dan entitas terkait untuk menyesuaikan tata kelola data pribadi sesuai dengan ketentuan UU PDP. Pasal 74 UU PDP menetapkan bahwa jika dalam masa transisi tersebut perusahaan belum menyesuaikan prosedur pemrosesan data pribadi, mereka dapat dikenakan berbagai sanksi tegas.

Salah satu sanksi yang diatur adalah denda administratif maksimal 2% dari pendapatan atau penerimaan tahunan perusahaan berdasarkan jenis pelanggaran yang terjadi. Hal ini mencerminkan betapa seriusnya dampak hukum yang dapat dihadapi jika perusahaan tidak mematuhi aturan terkait pengelolaan dan perlindungan data pribadi.

Sanksi Administratif UU PDP:

1. Peringatan tertulis,
2. Penghentian sementara kegiatan pemrosesan data pribadi,
3. Penghapusan atau pemusnahan data pribadi, dan
4. Denda administratif hingga 2% dari pendapatan tahunan.

Berlakunya UU PDP pada Oktober 2024 mendorong perusahaan harus memberikan perhatian serius terhadap kewajiban ini. Risiko hukum dan denda besar dapat dikenakan jika mereka gagal menjaga keamanan dan kerahasiaan data pribadi. Penguatan kontrol serta implementasi sistem keamanan siber yang andal menjadi krusial untuk memastikan kepatuhan perusahaan dalam melindungi data pribadi dari potensi ancaman dan pelanggaran.

PRESIDEN
REPUBLIK INDONESIA

SALINAN

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 27 TAHUN 2022
TENTANG
PELINDUNGAN DATA PRIBADI

Jika Data Pribadi Bocor, Apa yang Harus Perusahaan Lakukan?

Dalam situasi di mana terjadi kebocoran data pribadi, UU PDP mewajibkan pengendali data untuk memberikan pemberitahuan tertulis kepada subjek data dan lembaga terkait dalam waktu maksimal 3 x 24 jam. Bahkan, dalam kondisi tertentu, perusahaan diwajibkan untuk memberitahu publik mengenai insiden tersebut.

Danny Kobrata, Partner di K&K Advocates, menjelaskan dalam diskusi "Corporate Insight: Strengthening PDP Law Governance Through Cybersecurity" yang diselenggarakan oleh Telkomsigma, bahwa sanksi dapat berupa administratif, perdata, atau bahkan pidana, tergantung pada tingkat pelanggaran. Jika sebuah perusahaan terbukti lalai dalam menjalankan kewajiban perlindungan data pribadi, seperti tidak memiliki prosedur standar operasional (SOP) atau tidak mematuhi aturan UU PDP, maka kebocoran data akan dianggap sebagai pelanggaran yang bisa berujung pada denda besar atau sanksi hukum lainnya.

Namun, apabila perusahaan telah melakukan segala upaya yang diwajibkan oleh UU PDP untuk melindungi data pribadi, maka situasi tersebut akan dipertimbangkan dalam investigasi. Dalam pemeriksaan, pihak berwenang akan menilai apakah perusahaan sudah berusaha memenuhi kewajiban hukumnya dan menerapkan langkah-langkah yang diperlukan untuk menjaga keamanan data pribadi.

Dengan demikian, penting bagi perusahaan untuk tidak hanya mematuhi regulasi UU PDP, tetapi juga memastikan bahwa mereka memiliki sistem keamanan siber yang kuat sebagai upaya pencegahan serta untuk menunjukkan kepatuhan hukum jika terjadi pemeriksaan.

Regulasi UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi bukan hanya sekedar pedoman yang harus dipatuhi atau kewajiban hukum yang harus dipenuhi untuk menghindari sanksi. Lebih dari itu, regulasi ini hadir sebagai bentuk perlindungan terhadap aset paling berharga di era digital—data pribadi. Bagi perusahaan, kepatuhan terhadap regulasi ini tidak hanya bertujuan untuk menghindari denda atau sanksi administratif, tetapi juga sebagai langkah proaktif dalam menjaga reputasi, kepercayaan pelanggan, serta keamanan sistem operasional.

Oleh karena itu, perusahaan perlu melihat regulasi ini sebagai peluang untuk memperkuat sistem keamanan mereka, membangun ketahanan siber yang kokoh, dan memastikan data pribadi yang dikelola tetap aman dari berbagai risiko ancaman. Upaya tersebut tidak hanya menciptakan kepatuhan terhadap hukum, tetapi juga meningkatkan keseluruhan keamanan perusahaan, sehingga mampu menghadapi tantangan di era digital dengan lebih baik. Keamanan data bukan hanya tentang memenuhi kewajiban, tetapi juga tentang melindungi bisnis itu sendiri.

UNVEILING CVE-2023-45866: A CRITICAL BLUETOOTH VULNERABILITY

By **Danang AM**
Junior Penetration Tester

Dalam dunia keamanan siber, kerentanan baru selalu muncul yang bisa membahayakan banyak sistem. Salah satu kerentanan kritis yang sedang ramai diperbincangkan adalah CVE-2023-45866. Kerentanan ini mempengaruhi berbagai platform dan dapat dieksploitasi oleh penyerang untuk mengambil alih kendali perangkat tanpa interaksi pengguna. Artikel ini akan membahas secara mendalam tentang kerentanan ini, bagaimana cara kerjanya, dampaknya, dan langkah-langkah mitigasi yang bisa diambil. Selain itu, kita akan melihat proyek BlueDucky yang digunakan untuk mengeksploitasi kerentanan ini.

Apa Itu CVE-2023-45866?

CVE-2023-45866 adalah kerentanan pada Bluetooth HID Hosts, terutama pada stack BlueZ yang digunakan dalam berbagai distribusi Linux. Kerentanan ini memungkinkan perangkat HID dalam peran Peripheral yang tidak terautentikasi untuk membentuk koneksi terenkripsi dan menginjeksi penekanan tombol tanpa interaksi pengguna.

Kerentanan ini ditemukan pada berbagai platform, termasuk Ubuntu, macOS, iOS, dan Android. CVE-2023-45866 telah diberi nilai CVSS sebesar 9.8, menunjukkan tingkat keparahan yang tinggi dan risiko signifikan terhadap kerahasiaan, integritas, dan ketersediaan data.

Bagaimana Kerentanan Ini Berfungsi?

CVE-2023-45866 memungkinkan perangkat HID dalam peran Peripheral untuk:

1. Memulai dan membentuk koneksi terenkripsi dengan Bluetooth HID Hosts tanpa memerlukan otorisasi dari peran Central.
2. Menginjeksi laporan keyboard HID, yang pada dasarnya memungkinkan penyerang untuk mengirimkan penekanan tombol ke perangkat yang rentan tanpa persetujuan pengguna.

Platform yang Terpengaruh :

Kerentanan ini mempengaruhi berbagai platform, termasuk tetapi tidak terbatas pada:

- BlueZ (misalnya, bluez 5.64-0ubuntu1 pada Ubuntu 22.04 LTS)
- macOS (Monterey 12.6.7, Ventura 13.3.3)
- iOS (iOS 16.6)
- Android (OS versi 4.2.2, 6.01, 10, 11, 13, 14)

PUNGGAWA
cyber security services

Dampak pada Kerahasiaan, Integritas, dan Ketersediaan

Kerentanan ini memiliki dampak signifikan pada ketiga aspek utama keamanan informasi:

- **Kerahasiaan**: Penyerang dapat mengakses informasi sensitif melalui injeksi penekanan tombol, seperti kata sandi atau informasi pribadi lainnya.
- **Integritas**: Penyerang dapat mengubah data atau pengaturan sistem melalui perintah yang dikirimkan.
- **Ketersediaan**: Penyerang dapat menyebabkan sistem crash atau menjadi tidak responsif dengan mengirimkan perintah yang merusak.

Risiko Eksploitasi

Meskipun belum ada laporan eksploitasi kerentanan ini secara liar pada saat penulisan, kemungkinan eksploitasi tetap tinggi. Informasi lebih lanjut tentang kerentanan ini, termasuk skrip proof-of-concept, dapat dengan cepat meningkatkan risiko eksploitasi.

Langkah Mitigasi

Langkah mitigasi yang paling efektif adalah dengan menginstal patch yang disediakan oleh vendor perangkat lunak. Berikut ini adalah beberapa rekomendasi:

- **BlueZ**: Patch tersedia untuk stack BlueZ pada kernel Linux. Pengguna disarankan untuk memperbarui sistem mereka ke versi terbaru.
- **macOS dan iOS**: Apple telah merilis patch untuk mengatasi kerentanan ini pada iOS, iPadOS, dan macOS. Pengguna harus segera memperbarui perangkat mereka.
- **Android**: Patch telah dikirim ke produsen perangkat Android. Pengguna disarankan untuk memperbarui perangkat mereka segera setelah patch tersedia, dan mematikan Bluetooth ketika tidak digunakan sebagai tindakan pencegahan sementara.

Rekomendasi Tambahan

- Pengguna Android: Disarankan untuk mematikan Bluetooth ketika tidak digunakan sampai patch tersedia.
- Organisasi: Menggunakan perangkat manajemen keamanan untuk memastikan semua perangkat dalam jaringan diperbarui dan dipantau secara berkala.
- Pengguna Pribadi: Menjaga perangkat lunak keamanan selalu diperbarui dan menghindari penggunaan perangkat Bluetooth yang tidak dikenal atau tidak terpercaya.

"CVE-2023-45866 adalah kerentanan yang sangat serius yang memerlukan perhatian dan tindakan segera dari semua pengguna yang terkena dampak. Dengan memahami detail teknis kerentanan ini, dampaknya, dan langkah-langkah mitigasi yang diperlukan, kita dapat lebih siap untuk melindungi sistem kita dari potensi serangan. Proyek BlueDucky menunjukkan betapa mudahnya kerentanan ini dapat dieksploitasi, menyoroti pentingnya segera mengatasi masalah ini melalui pembaruan dan patch"

Referensi :

https://blog.tegalsec.org/unveiling-cve-2023-45866-a-critical-bluetooth-vulnerability/

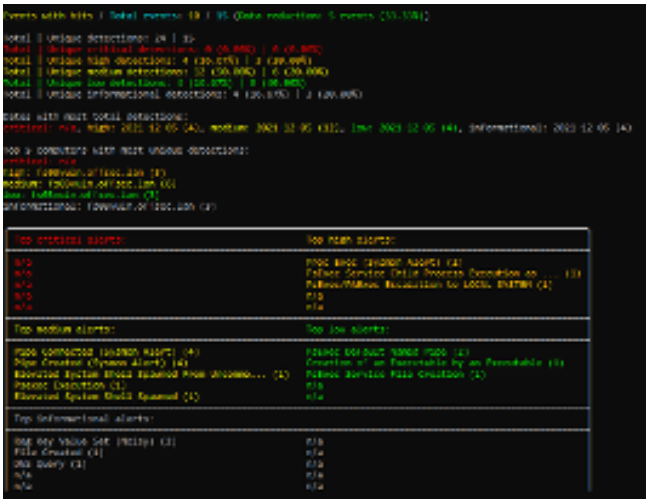
PUNGGAWA cybersecurity

STRATEGI EFEKTIF ANALISIS FORENSIK MENGGUNAKAN HAYABUSA

DALAM MENANGGULANGI SERANGAN KEAMANAN SIBER

By **Ambar F**
SOC Analyst

HAYABUSA



Dalam era digital yang semakin maju, serangan siber menjadi salah satu ancaman paling serius bagi organisasi di seluruh dunia khususnya pada bidang teknologi. Penjahat siber menggunakan berbagai teknik dan tools untuk meretas sistem serta mencuri data sensitif. Oleh karena itu, solusi keamanan siber yang kuat sangat diperlukan serta efektivitas dalam mendeteksi dan menganalisis ancaman memerlukan alat yang cepat dan akurat. Salah satu tools generator timeline forensic Windows event log yang dikembangkan oleh tim security Jepang yaitu Hayabusa merupakan tools yang digunakan untuk membuat timeline dan threat hunting dalam melakukan analisis forensik. Dengan memanfaatkan kemampuan multi-threading yang cepat, Hayabusa menjadi tools yang membantu dalam melakukan analisis forensik secara efisien.

Apa itu Hayabusa Tools?

Hayabusa adalah tools yang digunakan untuk membuat timeline dalam analisis forensik dan merupakan tools untuk threat hunting yang di kembangkan oleh tim Yamato Seurity di Jepang. Nama "Hayabusa" diambil dari burung peregrine falcon, yang merupakan hewan tercepat di dunia, handal berburu, dan mudah dilatih. Tools ini ditulis dalam bahasa pemrograman Rust dan mendukung multi-threading agar bisa berjalan secepat mungkin. Aturan deteksi Hayabusa, seperti Sigma, ditulis dalam format YML agar mudah diubah dan dikembangkan. Tools ini bisa digunakan di sistem yang sedang berjalan untuk analisis langsung atau dengan mengumpulkan log dari beberapa sistem untuk analisis offline. Hasil generate timeline dari Hayabusa dapat digabungkan dan disimpan dalam satu file format CSV untuk memudahkan analisis di Excel atau Timeline Explorer.

Proof of Concept (PoC) untuk Penggunaan Hayabusa dengan Log APT Attack

Serangan Advanced Persistent Threat (APT) merupakan salah satu bentuk serangan siber yang paling canggih dan berbahaya di dunia maya. Serangan APT biasanya dilakukan oleh kelompok yang terorganisir, baik oleh negara, perusahaan, atau aktor ancaman dengan sumber daya besar. Tujuan utama dari serangan APT adalah untuk mendapatkan akses yang tidak sah ke sistem korban dalam jangka panjang tanpa terdeteksi. Pelaku serangan APT biasanya menargetkan organisasi dengan data bernilai tinggi, seperti perusahaan keuangan, infrastruktur kritis, atau lembaga pemerintahan.

Salah satu tantangan terbesar dalam menangani serangan APT adalah kemampuan attacker untuk melakukan berbagai teknik serangan secara bertahap, dari tahap awal infiltrasi, eskalasi hak istimewa, pergerakan lateral di dalam jaringan, hingga akhirnya eksfiltrasi data. Serangan ini sangat sulit dideteksi karena sering kali melibatkan penggunaan alat-alat umum, teknik stealth, serta eksploitasi kerentanan zero-day yang belum diketahui publik.

Dalam investigasi serangan APT, analisis log event Windows memainkan peran penting. Setiap aktivitas yang terjadi dalam sistem Windows dicatat ke dalam Windows Event Log dengan ekstensi .evtx. Log ini berisi berbagai informasi penting tentang aktivitas sistem, seperti login yang berhasil dan gagal, proses yang dijalankan, koneksi jaringan, serta aktivitas berbagi file melalui protokol seperti SMB.

Mengingat volume dan kompleksitas log yang dapat dihasilkan oleh serangan APT, proses analisis manual sangat memakan waktu dan rentan terhadap kesalahan.

Pada studi kasus ini akan menggunakan tools Hayabusa sebagai alat bantu yang sangat efektif untuk melakukan analisis forensik dan threat hunting terhadap log event Windows. Hayabusa tidak hanya mendukung analisis secara lokal pada satu sistem, tetapi juga memungkinkan pengumpulan log dari berbagai sistem untuk analisis skala besar dalam lingkungan perusahaan. Dengan Hayabusa, analisis dapat dilakukan lebih cepat, efisien, dan fleksibel. Tool ini mendukung beberapa output format seperti CSV dan JSON, yang dapat diintegrasikan dengan berbagai tool lain seperti Elastic Stack, Timeline Explorer, LibreOffice, dan Timesketch untuk analisis lanjutan.

Dengan menggunakan tools Hayabusa untuk menganalisis file log EVTX yang mencakup beberapa teknik serangan yang sering digunakan dalam serangan APT. File log yang dianalisis mencakup log terkait eksekusi jarak jauh, eskalasi hak istimewa, dan serangan lateral movement melalui protokol SMB. Setiap file log mewakili tahapan spesifik dari serangan APT yang kompleks, yang mencerminkan langkah-langkah umum dalam kampanye APT yang sebenarnya. Dengan menggunakan Hayabusa, akan dilakukan identifikasi setiap tahapan serangan, termasuk identifikasi proses yang mencurigakan, percobaan privilege escalation, pembuatan task remote. Analisis ini akan memberikan wawasan bagaimana Hayabusa dapat digunakan secara efisien.

Sebelum melakukan analisis pastikan sudah melakukan instalasi dan memiliki file EVTX yang akan dianalisa. Untuk proses instalasi dapat mengakses link berikut https://github.com/Yamato-Security/hayabusa. Selanjutnya untuk memperoleh file EVTX dapat mengakses link berikut https://github.com/Yamato-Security/hayabusa-sample-evtx, Untuk memulai analisis awal, dapat menjalankan perintah computer-metrics untuk mengetahui dari mana log event tersebut dihasilkan. Dengan command sebagai berikut

D:\Hayabusa Test\hayabusa-2.17.0-win-x64>hayabusa-2.17.0-win-x64.exe computer-metrics -d "D:\Hayabusa Test\EVTX_full_APT_attack_steps"

```
Scanning finished. Please wait while the results are being saved.
```

Computer	Events
fs03vuln.offsec.lan	815
srvdefender01.offsec.lan	161
rootdc1.offsec.lan	57
fs01.offsec.lan	15
FS03.offsec.lan	6

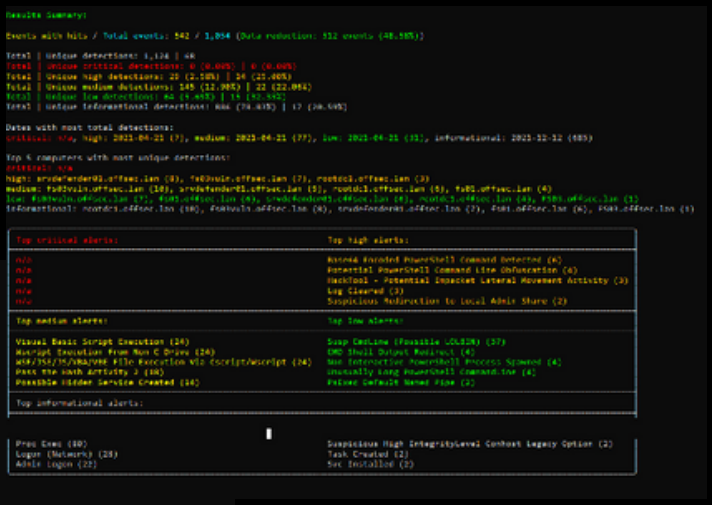
```
Total computers: 5
```

Dari hasil scanning terdapat lima computer yang digunakan, dengan event terbanyak berasal dari fs03vuln.offsec.lan sejumlah 815 events.
Selanjutnya untuk menganalisa event terbanyak dapat menggunakan perintah eid-metrics, dapat dilihat frekuensi dan jenis Event ID yang ada di file log.
D:\Hayabusa Test\hayabusa-2.17.0-win-x64>hayabusa-2.17.0-win-x64.exe eid-metrics -d "D:\Hayabusa Test\EVTX_full_APT_attack_steps"

```
First Timestamp: 2021-04-21 21:56:41.780 +07:00
Last Timestamp: 2021-12-14 21:42:50.049 +07:00
```

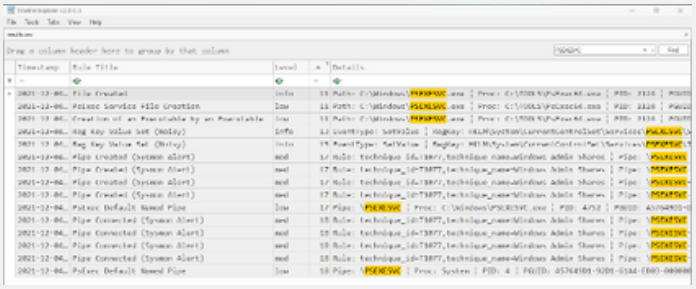
Total	%	Channel	ID	Event
413	39.2%	Sec	5145	Network share object checked for client access
371	35.2%	Sec	5140	Network share object accessed
80	7.6%	Sec	4688	Process created
30	2.8%	Sec	4624	Logon success
22	2.1%	Sec	4964	Special groups assigned to new logon
22	2.1%	Sec	4672	Admin logon
20	1.9%	Sec	4674	Privileged object operation attempt
11	1.0%	Sec	4662	Object operation performed
8	0.8%	Sec	5447	Firewall filter changed
6	0.6%	Sec	4742	Computer account changed
6	0.6%	Sec	4658	Object handle closed
5	0.5%	Sec	4776	DC attempted to validate account credentials
5	0.5%	Sec	4627	Unknown
4	0.4%	Sysmon	18	Named Pipe Connection
4	0.4%	Sysmon	17	Named Pipe Created
3	0.3%	Sec	4690	Object handle duplication attempt
3	0.3%	Sec	1102	Audit log cleared
3	0.3%	Sec	4673	Privileged service called
3	0.3%	Sec	4656	Object handle requested

Dari output tersebut diperoleh informasi mengenai Event ID 5140 dan 5145: Aktivitas terkait file sharing SMB dengan total sebanyak 413 kali. Selanjutnya adalah Event ID 4688 merupkana proses berjalan dengan jumlah 80 kali.
Untuk mempermudah analisa maka akan dibuat timeline yang dapat melihat urutan serangan secara keseluruhan, timeline tersebut akan disimpan dalam format CSV dan dapat ditampilkan menggunakan Timeline Explorer. Berikut adalah command yang digunakan untuk membuat timeline.
D:\Hayabusa Test\hayabusa-2.17.0-win-x64>hayabusa-2.17.0-win-x64.exe csv-timeline -d "D:\Hayabusa Test\EVTX_full_APT_attack_steps"



Dari proses tersebut dapat dilihat beberapa alerts yang terdeteksi berdasarkan sigma rule. Maka langkah selanjutnya akan dilakukan Analisis Privilege Escalation dan Lateral Movement. Analisis ini dapat dimulai dengan melihat Event ID yang berhubungan dengan eksekusi proses dan upaya pengambilan privilege access.
D:\Hayabusa Test\hayabusa-2.17.0-win-x64>hayabusa-2.17.0-win-x64.exe logon-summary -d "D:\Hayabusa Test\EVTX_full_APT_attack_steps"

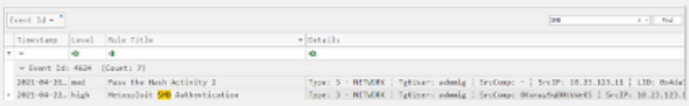
“PSExec adalah alat umum yang digunakan untuk lateral movement”



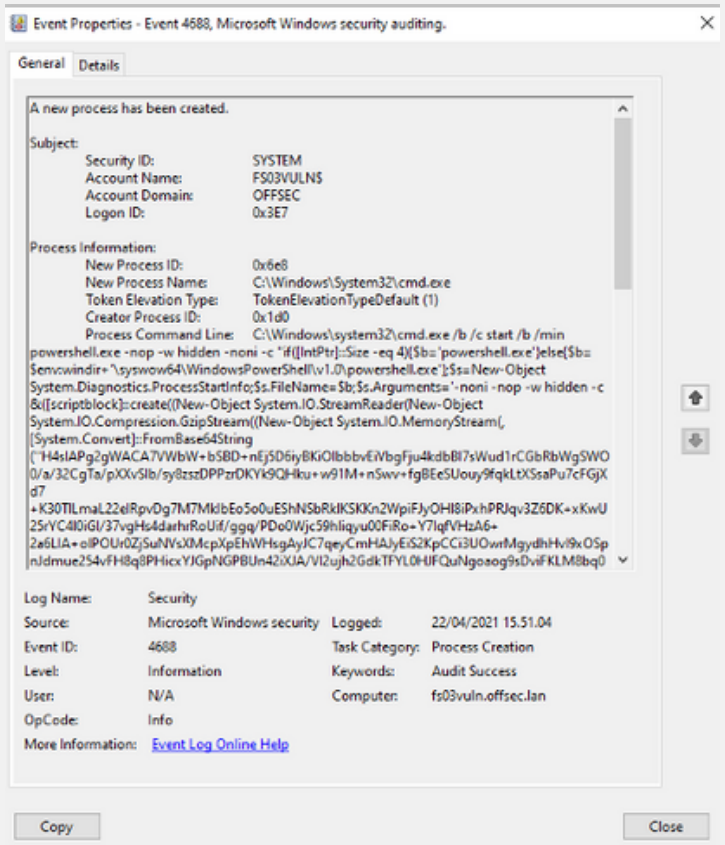
PSExec adalah alat umum yang digunakan untuk lateral movement. Saat dieksekusi sebagai SYSTEM, ini menunjukkan bahwa attacker memiliki kontrol penuh atas sistem dan dapat menjalankan perintah apapun.PSExec digunakan oleh attacker untuk mengeksekusi perintah di sistem jarak jauh dengan system privileges. Eksekusi PSExec yang dicatat dalam event log ini menunjukkan eksekusi sebagai SYSTEM, yang memberikan kontrol penuh kepada attacker atas mesin yang diserang.

- Event ID 11: Mencatat pembuatan file eksekusi di disk, khususnya terkait dengan PSExec.
- Event ID 13: Mencatat perubahan registry yang berhubungan dengan eksekusi PSExec, yang sering kali digunakan untuk menetapkan persistence.
- Event ID 17: Menunjukkan pembuatan pipe untuk komunikasi antar proses dalam sistem.
- Event ID 18: Menunjukkan penghapusan file PSExec setelah eksekusi.

Perubahan registry mengindikasikan kemungkinan persistence yang telah dilakukan, memastikan bahwa attacker dapat mengakses kembali sistem.



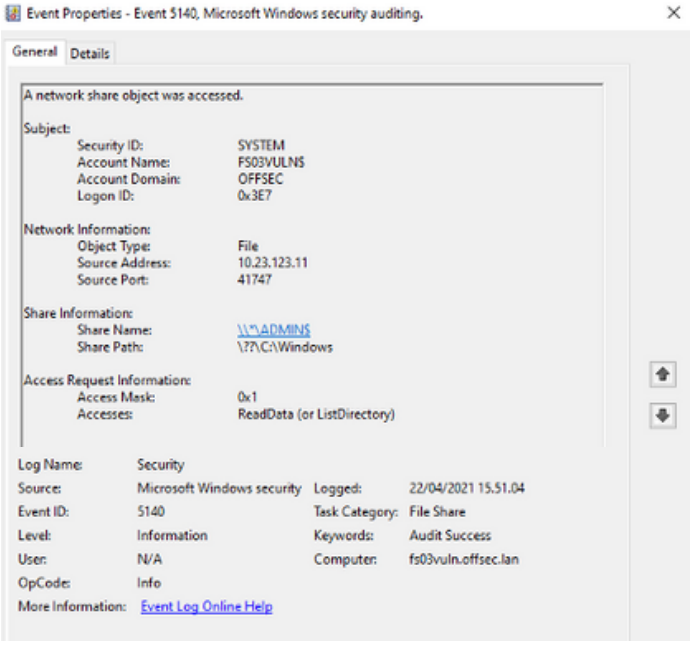
Event ID 4624: Mencatat keberhasilan autentikasi menggunakan SMB. Terdapat upaya akses yang mencurigakan terhadap akun **administratif** (admmig) dari sumber yang tidak dikenal, yang terdeteksi dengan workstation name **0Konuy9q8HtkWeKS** dengan IP **10.23.123.11.**



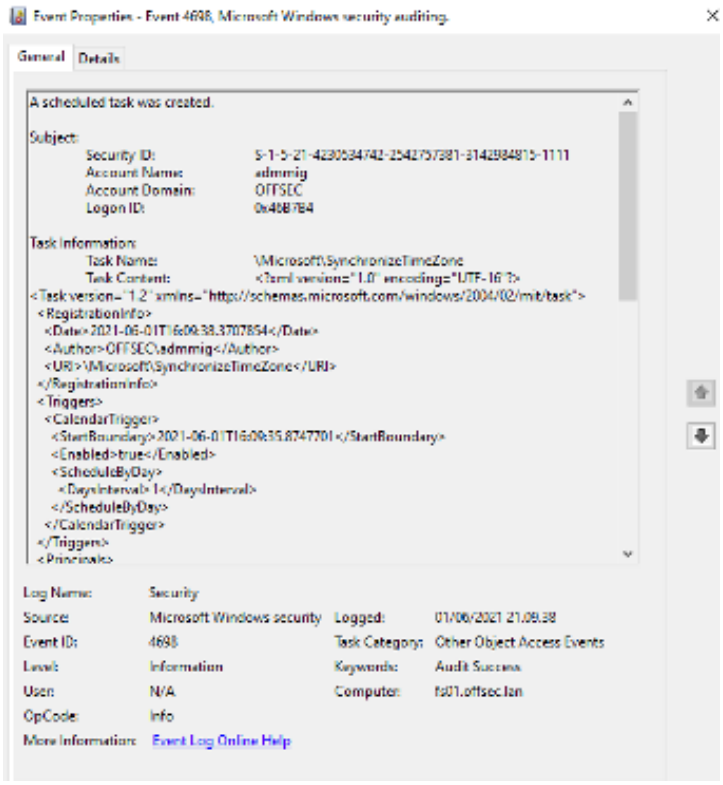
PUNGGAWA cybersecurity

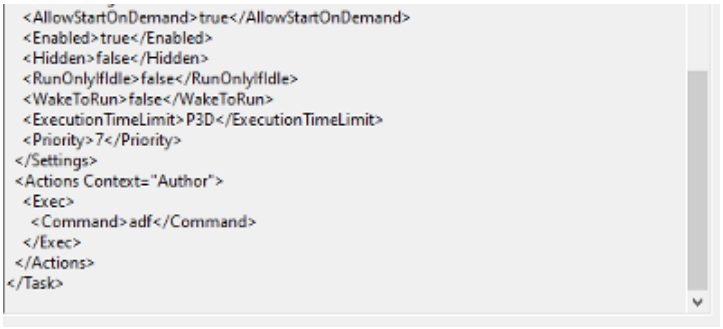
HAYABUSA

Event ID 4688: Mencatat proses eksekusi, yang biasanya menunjukkan remote code execution. Skrip tersebut menunjukan bagian dari teknik remote code execution, di mana skrip yang disembunyikan dan disamarkan diunduh kemudian dijalankan di latar belakang.



Event ID 5140 menunjukan informasi yang diberikan menunjukkan akses ke file melalui berbagi SMB pada direktori **administratif Windows (ADMIN$)**, dengan fokus pada powershell.exe di **System32\WindowsPowerShell\v1.0.** Pengguna yang terlibat **FS03VULN$** mengakses file ini dari IP 10.23.123.11, yang bisa menunjukkan aktivitas tidak biasa. PowerShell, sering digunakan untuk eksekusi skrip atau perintah, mungkin digunakan di sini untuk menjalankan kode berbahaya dari jarak jauh.





Task ini terlihat seperti konfigurasi task scheduler yang standar, namun perintah adf yang dijalankan tidak jelas dan mungkin merupakan indikasi adanya potensi tindakan berbahaya atau kode yang disembunyikan.

Dari hasil beberapa temuan tadi dapat disimpulkan bahwa terdapat beberapa indikasi penting terkait aktivitas yang mencurigakan dan potensi serangan APT:

1. Penggunaan PSExec: Ditemukannya penggunaan PSExec sebagai alat untuk lateral movement menunjukkan bahwa pelaku memiliki kontrol penuh terhadap sistem yang diserang. PSExec sering digunakan oleh attacker untuk menjalankan perintah dengan hak akses tinggi dan menciptakan persistence. Pengamatan pada Event ID 11, 13, 17, dan 18 menunjukkan bahwa attacker tidak hanya menjalankan perintah tetapi juga berusaha memastikan akses mereka tetap ada dengan melakukan modifikasi pada registry dan penghapusan file setelah eksekusi.
2. Keberhasilan Autentikasi dan Koneksi SMB: Event ID 4624 menunjukkan adanya autentikasi yang berhasil dengan akun administratif dari sumber yang tidak dikenal. Hal ini menunjukkan potensi penyalahgunaan kredensial administratif. Sementara itu, Event ID 5140 menunjukkan adanya koneksi ke share administratif ADMIN$ yang sering kali menjadi target eksploitasi. Akses ke share ini oleh akun FS03VULN$ dari IP yang sama berpotensi menunjukkan upaya eksploitasi kerentanan SMB, seperti EternalRomance, yang memungkinkan pelaku untuk mendapatkan akses ke sistem.
3. Remote Code Execution: Ditemukan juga indikasi remote code execution melalui Event ID 4688 yang menunjukkan proses eksekusi skrip dari jarak jauh.
4. Potensi Persistence: Penggunaan Task Scheduler untuk menjalankan kode berbahaya secara terjadwal.

Rekomendasi

Berdasarkan hasil analisis dan temuan yang diperoleh dari file log EVTX menggunakan Hayabusa, berikut adalah rekomendasi untuk menangani dan mengatasi potensi serangan APT yang telah terdeteksi:

1. Isolasi dan Pembersihan Sistem: Mengisolasi sistem terkompromi dan melakukan pembersihan menyeluruh.
2. Penguatan Kredensial: Menerapkan kebijakan password kuat dan autentikasi multi-faktor untuk akun administratif.
3. Implementasi Sistem Deteksi: Menggunakan IDS/IPS untuk memantau aktivitas mencurigakan dengan konfigurasi log yang tepat.
4. Audit Rutin dan Analisis Log: Melakukan analisis log secara berkelanjutan menggunakan alat SIEM.
5. Menggunakan EDR/Antivirus: Untuk mendeteksi dan mencegah eksekusi malware lebih jauh.
6. Segmentasi Jaringan: Memisahkan jaringan untuk membatasi pergerakan lateral pelaku.

Kesimpulan

Hayabusa memberikan solusi forensik yang efektif dan efisien dalam menangani serangan siber, terutama serangan yang melibatkan log Windows Event. Dengan kemampuan multi-threading dan integrasi dengan aturan Sigma, Hayabusa mampu menghasilkan timeline yang mudah diakses untuk analisis mendalam.

Dalam studi kasus APT, penggunaan Hayabusa terbukti efektif dalam mengidentifikasi serangan. Dalam dunia yang semakin kompleks dan berbahaya terkait ancaman siber, Hayabusa memberikan pendekatan yang efisien dan dapat diandalkan untuk analisis forensik, yang pada akhirnya dapat meningkatkan kapabilitas deteksi dan respons ancaman organisasi. Kombinasi antara Hayabusa dan alat lain seperti Velociraptor akan memperkuat kemampuan organisasi dalam menghadapi ancaman skala besar dan canggih.

Referensi :

https://github.com/Yamato-Security/hayabusa
https://github.com/mdecrevoisier/EVTX-to-MITRE-Attakcs
https://mahim-firoj.medium.com/incident-response-and-threat-hunting-using-hayabusa-tool-383da273183a
https://medium.com/@lucideus/the-eternal-exploitation-bible-lucideus-research-20e3ed541d4

RANSOMHUB : THE RISING STAR IN THE ELUSIVE BUSINESS

By **MR El Ghiffari**
Junior Penetration Tester

RansomWare, satu kata yang membuat banyak pimpinan perusahaan di Indonesia ketakutan. RansomWare, satu kata yang membuat banyak orang Indonesia mengenang kenangan pahit.
RansomWare, satu kata yang sepertinya tidak berdampak apa apa terhadap menteri komunikasi dan informatika republik Zimbabwe Selatan.

“RansomWare, satu kata yang aslinya adalah dua kata Ransom dan Ware.”

Sebagai rakyat Indonesia tentu kita tidak asing dengan istilah ransomware. Banyak pil pahit yang sudah rakyat Indonesia rasakan dikarenakan ransomware mulai dari tidak bisa melakukan transaksi online, pengurusan paspor online hingga matinya layanan publik secara masif. Secara singkat ransomware dapat diartikan sebagai software pemeras. Definisi lainnya dari ransomware kira kira sebagai berikut.

Yap, sesuai namanya Ransom yang jika diartikan dalam bahasa Inggris adalah tebusan. Satu hal yang menjadi ciri spesifik ransomware adalah adanya tebusan. Dengan menyandera data penting suatu organisasi mereka meminta tebusan agar korban bisa mengakses datanya kembali. Tebusan biasanya diminta dalam bentuk mata uang digital untuk menjaga anonimitas.

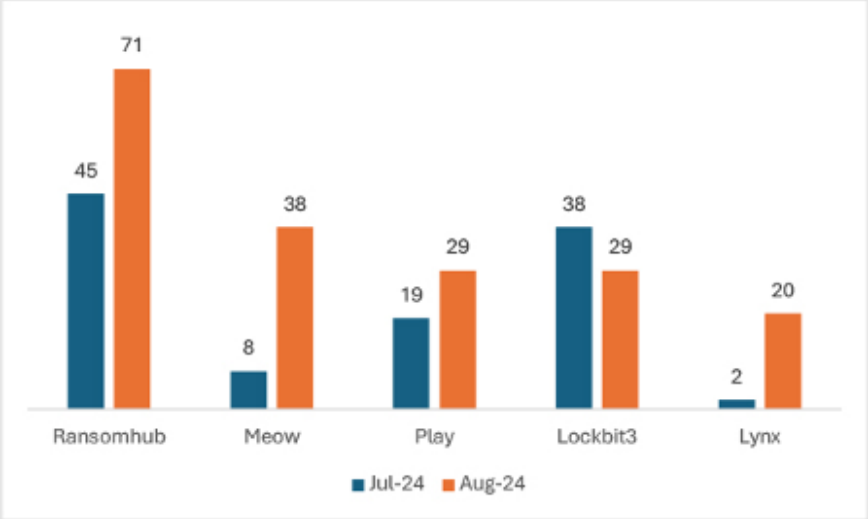
Modus operandi ransomware sekarang sudah menjadi fenomena global, banyak negara sudah menjadi korbannya. Perputaran uang dan portofolio korban tidak bisa dipandang sebelah mata. Di tengah perkembangan ransomware ada satu ransomware atau ransomware group yang akan kita bahas. Namanya RansomHub, dimohon untuk jangan tertukar dengan Hub Hub yang lain.

Pertama kali diidentifikasi oleh biro investigasi federal atau yang kerap dikenal sebagai FBI. Kelompok ini muncul setelah Biro Investigasi Federal (FBI) menghentikan operasi ransomware ALPHV pada 19 Desember 2023. Ada asumsi bahwa RansomHub adalah "penerus spiritual" kelompok ALPHV dan beroperasi dengan bantuan mantan afiliasi ALPHV.

#	THREAT ACTOR	ATTACKS	Q1 2024	Q2 2024	Q3 2024	Q4 2024
1	Lockbit	2877	213	239	83	0
2	Black Cat	708	51	0	0	0
3	Play	552	72	94	68	0
4	CLOP	466	8	9	2	0
5	Conti	422	0	0	0	0
6	8Base	387	69	53	0	0
7	BianLian	339	52	33	42	0
8	Akira	306	58	55	42	0
9	Medusa Blog	285	50	61	33	0
10	Ransomhub	270	22	76	172	0
11	Black Basta	252	74	57	8	0
12	HiveLeaks	217	0	0	0	0
13	Royal	204	0	0	0	0
14	Hunters	175	58	45	52	0
15	Vice Society	169	0	0	0	0

RansomHub mengumumkan korban pertamanya, perusahaan Brasil YKP. Hingga 22 Agustus 2024, kelompok tersebut telah menargetkan 190 korban di seluruh dunia. Menurut data dari CyberInt dan Darkfeed.io, RansomHub menduduki puncak daftar dengan jumlah korban tertinggi pada bulan Juli dan Agustus (sejauh ini). Khususnya, lebih dari 50% dari total serangan mereka dilakukan dalam kurun waktu dua bulan ini saja, yang menunjukkan adanya peningkatan operasi yang signifikan, yang kemungkinan didorong oleh peningkatan partisipasi afiliasi.

Berdasarkan informasi diatas RansomHub sekarang menduduki posisi 10 sebagai threat actor paling aktif. Namun yang perlu diperhatikan adalah bahwa RansomHub menjadi satu satunya threat actor yang menunjukan pertumbuhan jumlah serangan tiga kuartal berturut turut.



Pada bulan Agustus 2024, tren ransomware menunjukkan pergeseran yang signifikan, dengan kelompok yang baru muncul mendapatkan momentum. **RansomHub mengalami peningkatan korban sebesar 57,78% dibandingkan dengan bulan Juli,** sementara Meow melonjak sebesar 375%, dari 8 menjadi 38 korban. Ransomware Play juga mengalami peningkatan sebesar 52,63%. Sebaliknya, LockBit3 mengalami penurunan sebesar 23,68%, dari 38 menjadi 29 korban. Lynx mengalami lonjakan paling dramatis, dengan peningkatan sebesar 900%, dari 2 menjadi 20 korban.

RansomHub beroperasi pada model RaaS yaitu Ransomware-as-a-Service bukan Ruqyah-as-a-Service, yang menegaskan bahwa afiliasi harus mematuhi perjanjian dan persyaratan yang ditetapkan selama negosiasi, dengan ketidakpatuhan mengakibatkan larangan dan penghentian kolaborasi. Afiliasi menerima 90% dari tebusan, sedangkan kelompok utama mengambil 10% sisanya. Praktik ini agak lebih tinggi dari rata rata pasar yang biasanya pembagiannya ada di angka 70% - 80% untuk afiliasi. Strategi ini sepertinya memang didesain untuk menarik afiliasi berpengalaman untuk bermitra dengan RansomHub, dengan begini RansomHub bisa melancarkan serangan dengan lebih masif dan menarik profit lebih besar.

Apapun itu strategi RansomHub bisa dibilang sukses karena seperti yang sudah dipaparkan di atas, RansomHub satu satunya Threat Actor yang tumbuh secara jumlah serangan pada tiga kuartal berturut turut. Mengutip data dari CyberInt, dengan memeriksa pendapatan kelompok tersebut dengan menganalisis DLS mereka dan menghitung data yang dipublikasikan (yang menunjukkan korban yang menolak membayar tebusan), ditemukan bahwa 160 dari 190 korban memilih untuk tidak membayar. Dari 30 korban yang tersisa, sepuluh korban masih dalam negosiasi. Ini berarti bahwa, dari 180 korban yang telah memutuskan atau menolak pembayaran, hanya 11,2% yang benar-benar membayar tebusan (Not Stonks). Selain itu, negosiasi sering kali menghasilkan pengurangan jumlah tebusan awal yang diminta.

Menelisik dari website RansomHub sendiri, ada beberapa petunjuk tentang asal usul dari mastermind RansomHub.

Mereka mengklaim bahwa RansomHub memiliki anggota dari berbagai negara dan hanya tertarik dengan uang, sama seperti kebanyakan dari kita. Poin yang menarik ada di poin berikutnya yang menyatakan bahwa mereka tidak akan menarget negara CIS (Commonwealth of Independent State) yang merupakan negara-negara pecahan Soviet, Kuba, Korea Utara dan China plus mereka juga mengklaim tidak akan menarget organisasi non profit. Dari pernyataan ini kita tidak perlu menjadi Sherlock Holmes untuk tau asal usul dari RansomHub. Meskipun mereka mengklaim bahwa mereka adalah komunitas peretas global, operasi mereka sangat mirip dengan code of conduct ransomware tradisional Rusia.

Karena kemungkinan RansomHub memiliki asal usul Rusia, sudah pasti target utama tak lain tak bukan adalah Amerika Serikat. Ini selaras dengan fakta bahwa sejauh ini negeri burger dan senjata api ini telah menjadi target utama dengan 66 kasus. Di peringkat kedua secara mengejutkan ada negara Brazil dengan 17 kasus. Sepertinya RansomHub masih harus mempertimbangkan ulang code of conduct mereka dengan tidak menarget negara negara BRICS+ atau bersiap digerebek FSB.

Mengenai industri, layanan bisnis merupakan sektor yang paling terdampak oleh serangan RansomHub, dengan 45 organisasi dalam kategori ini.

Sekarang setelah melihat apa yang RansomHub telah lakukan dan mendapat perkiraan dampaknya, mari sekarang sedikit berbicara mengenai hal hal teknis yang akan membuat kebanyakan orang segera mengakhiri sesi membaca artikel ini.

RansomHub ditulis menggunakan bahasa Golang, sama seperti banyak grup ransomware lain seperti GhostSec, mengindikasikan sebuah trend diantara para kriminal siber dan mungkin diantara peminum vodka. RansomHub juga terlihat memiliki keterkaitan dengan grup ransomware ALPHV, maka dari itu tool dan TTP juga mungkin sama seperti yang digunakan oleh ALHPV.

Seperti yang sudah dijelaskan bahwa RansomHub dikembangkan dengan bahasa Golang dan juga C++, menargetkan mesin Windows, llnux dan juga instan ESXi. Fitur pembeda dari RansomHub adlah kecepatan enkripsi yang cepat dibanding kompetitor RaaS.

Menurut Sophos Research, RansomHub memiliki kesamaan dengan Knight Ransomware. Beberapa kesamaan itu diantaranya.

1. Payload ransomware yang ditulis menggunakan bahasa Golang.
2. Payload yang di obfuskasi menggunakan GoObfuscate.
3. Command Line menu saat ransomware dijalankan juga terlihat identik.

```
C:\malware\knight_VT>36e5be.exe --help
USAGE: 36e5be.exe [OPTIONS]
OPTIONS:
  -disable-net
        Disable network before running
  -host value
        Only process smb hosts inside defined host. -host //10.10.10.10/ -host //10.10.10.11/
  -only-local
        Only encrypt local disks
  -pass string
        Pass
  -path value
        Only process files inside defined path. -path C:// -path D:// -path//10.10.10.10/d/
  -safeboot
        Reboot in Safe Mode before running
  -safeboot-instance
        Run as Safe Mode instance
  -verbose
        Log to console

C:\malware\knight_VT>
```

```
C:\malware\Primary_sample>ransomhub.exe --help
USAGE: ransomhub.exe [OPTIONS]
OPTIONS:
  -disable-net
        disable network before running
  -host value
        only process smb hosts inside defined host. -host 10.10.10.10 -host 10.10.10.11
  -only-local
        only encrypt local disks
  -pass string
        Pass
  -path value
        only process files inside defined path. -path C:// -path D:// -path //10.10.10.10/d/
  -safeboot
        reboot in Safe Mode before running
  -safeboot-instance
        run as Safe Mode instance
  -sleep int
        sleep for a period of time to run (minute)
  -verbose
        log to console

C:\malware\Primary_sample>
```

RansomHub diketahui telah memulai untuk men-deploy tool baru yang memiliki kapabilitas untuk mematikan Endpoint Detection Response (EDR). Ini memungkinkan mereka untuk mem-bypass mekanisme keamanan dan mendapatkan kontrol penuh terhadap sistem yang diretas. Tool ini diketahui bernama EDRKillShifter, ditemukan oleh Sophos ketika percobaan peretasan yang gagal pada Mei 2024. EDRKillShifter berfungsi sebagai sebuah bootloader, memungkinkan serangan Bring Your Own Vulnerable Driver (BYOVD), dimana driver asli namun vulnerable di eksploitasi to mendapatkan hak akses, mematikan fitur keamanan dan mengambil alih kendali sistem.

Sophos mengidentifikasi 2 sampel EDRKillShiter. Satu sample dari EDRKillShifter menargetkan dan mengeksploitasi driver RentDrv2 dan lainnya menargetkan dan mengeksploitasi driver ThreatFireMonitor.

Proses eksekusi melibatkan tiga langkah: Pertama, penyerang menjalankan file biner dengan kata sandi untuk mendekripsi dan mengeksekusi sumber daya BIN bawaan di memori. Kode tersebut kemudian mendekompresi dan mengeksekusi payload akhir, memuat driver yang rentan untuk meningkatkan hak akses, menonaktifkan proses aktif, dan menetralkan sistem EDR. Malware kemudian membuat layanan baru untuk driver, memulainya, dan memuat driver tersebut, lalu masuk ke dalam loop tak terbatas di mana ia terus memantau proses yang berjalan dan menghentikannya jika nama proses tersebut sesuai dengan daftar target terenkripsi. Wooo... spooky...

Oke oke kita sudah membahas sana sini mengenai RansomHub tapi apa mereka seberbahaya itu dan bagaimana cara mencegahnya? Tenang we got you covered...

- Backup Data Secara Teratur: Buat strategi cadangan untuk pemulihan data kritis.
- Pelatihan Kesadaran Keamanan: Edukasi karyawan tentang ancaman dan praktik keamanan.
- Manajemen Patch: Perbarui sistem dan perangkat lunak secara rutin untuk menutup kerentanan.
- Segmentasi Jaringan: Isolasi sistem penting untuk mengurangi dampak serangan.
- Kontrol Akses: Terapkan prinsip akses minimal untuk mengurangi risiko penyebaran ransomware.
- Keamanan Email dan Web: Gunakan solusi pemfilteran untuk mencegah akses ke konten berbahaya.
- Perlindungan Endpoint: Gunakan antivirus dan alat deteksi untuk mengatasi ancaman di endpoint.
- Rencana Tanggapan Insiden: Siapkan dan uji rencana untuk menangani serangan ransomware.
- Audit Keamanan Rutin: Lakukan penilaian dan pengujian keamanan secara teratur.
- Berdoa : Tanpa kita sadari bahwa hacker juga manusia, punya rasa dan punya hati. Kita terlalu sibuk dengan permasalahan dunia hingga lupa meminta ke sang maha pembolak balik hati. Maka dari itu jika organisasi kita diserang ransomware tidak ada salahnya untuk berdoa agar para hacker mau memberikan key/decryptor secara gratis, cara ini terbukti sangat efektif ketika kasus peretasan PDNS dimana kominfo dengan segala kebijaksanaannya mampu membujuk threat actor untuk memberikan decryptor secara cuma cuma.

Referensi :

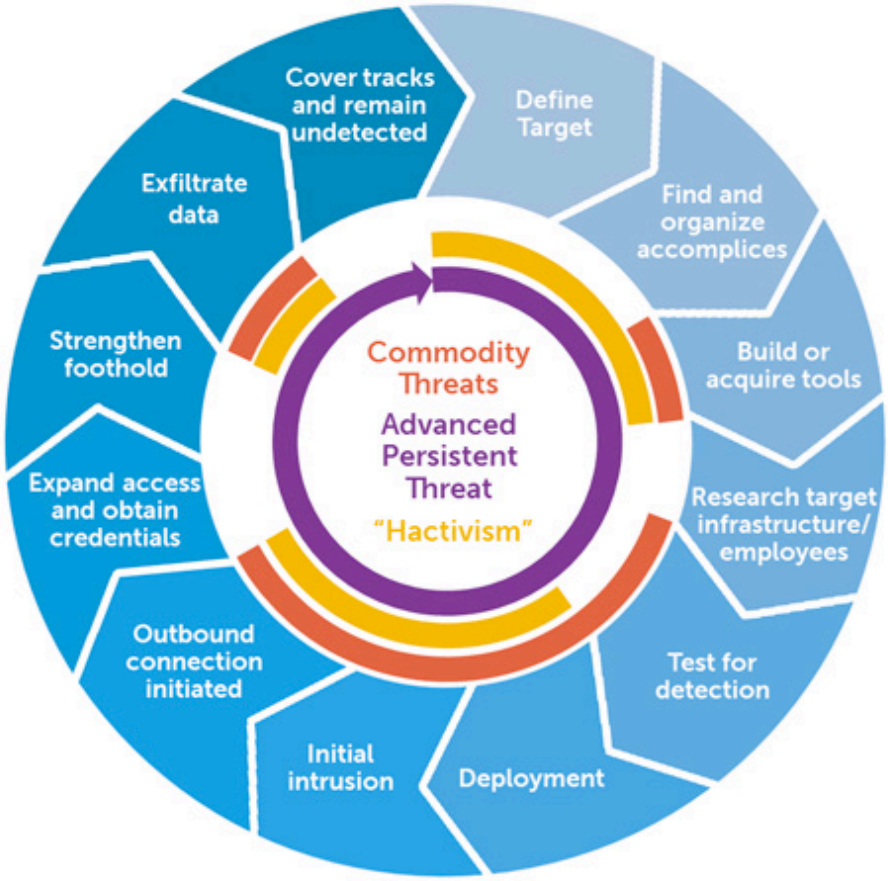
https://darkfeed.io/ransomgroups/
https://www.cyfirma.com/research/tracking-ransomware-august-2024/
https://cyberint.com/blog/research/ransomhub-the-new-kid-on-the-block-to-know/

MENGENAL APT (ADVANCED PERSISTENT THREAT)

By **Rachmat AR**
Senior Penetration Tester

Teknologi terus berkembang pesat dalam membantu manusia untuk menyelesaikan masalah dan membuat banyak pekerjaan menjadi lebih mudah. Dewasa ini, implementasi teknologi untuk meningkatkan kualitas hidup manusia menjadi lebih beragam. Mulai dari media sosial, finansial, kesehatan, administrasi, bahkan keamanan kini tak luput dari sentuhan teknologi. Namun penggunaan teknologi tanpa didasari pengetahuan yang utuh dan menyuluruh justru seringkali menimbulkan masalah baru. Salah satu ancaman itu muncul dari aktifitas kriminal di dunia siber, atau sering disebut sebagai **"Cyber Crime"**. Mungkin kita sudah biasa mendengar ancaman siber seperti account takeover, defacement, pencurian data bahkan aktifitas fraudulent. Namun pada Magazine Punggawa edisi ke-3 kali ini kita akan membahas ancaman siber yang berada pada level yang berbeda, yaitu **APT** atau **"Adavanced Persistence Threat"**.

APT atau Advanced Persistence Threat adalah ancaman siber yang datang dari Threat Actor yang terorganisir serta memiliki skill yang tinggi. APT biasanya memiliki dukungan dari entitas besar seperti negara atau kelompok tertentu. Lebih spesifik, APT ditujukan untuk menargetkan organisasi besar seperti negara, perusahaan, lembaga pemerintahan, dan infrastruktur penting dengan berbagai motivasi, diantaranya seperti pencurian data, spionase, dan sabotase. APT melakukan serangan dengan rahasia, sulit terdeteksi dan dilakukan secara terus menerus dalam waktu yang relatif panjang. Richard Bejtlich sebagai Chief Security Strategist di FireEye mendefinisikan APT sebagai berikut:



APT atau Advanced Persistence Threat adalah ancaman siber yang datang dari Threat Actor yang terorganisir serta memiliki skill yang tinggi.

Advanced

Threat actor memiliki kemampuan untuk melakukan berbagai jenis serangan komputer. Mereka bisa menggunakan exploit sederhana atau yang tersedia secara publik. Namun jika diperlukan mereka dapat meningkatkan kemampuan dengan meneliti kerentanan baru dan mengembangkan exploit yang relevan (Zero-day)

Persistent

Persistent berarti threat actor bekerja untuk menyelesaikan sebuah misi atau tujuan. Tidak seperti threat actor pada umumnya yang hanya memanfaatkan peluang. APT bisa digambarkan mirip dengan unit intelejen, dimana mereka bekerja sesuai dengan arahan dan tujuan yang telah direncanakan. Persistent tidak selalu berarti bahwa APT terus menerus melakukan exploitasi atau menjalankan program/kode berbahaya pada komputer target, tapi lebih mengarah ke upaya mereka untuk mempertahankan akses atau interaksi yang diperlukan untuk mencapai objektif dari misi mereka.

Threat

APT dianggap ancaman karena mereka memiliki kemampuan serta motivasi dalam operasi mereka. Serangan APT dilakukan dengan terkoordinasi, terorganisir, termotivasi serta didukung dengan support dan pendanaan yang kuat.

Tahapan Serangan APT

Sebagian besar APT mengikuti siklus yang sama, yaitu menyusup ke jaringan, memperluas akses, hingga mencapai tujuan serangan, yang paling umum adalah mencuri data dengan mengekstraknya dari jaringan target. Berikut tahapan serangan APT yang dirangkum dalam 3 fase utama dalam serangan APT

Stage 1: Infiltration

Pada tahapan pertama APT seringkali mendapatkan akses awal melalui serangan Social Engineering. Salah satu bentuk serangan Social Engineering yang dilakukan oleh APT adalah Phising. Serangan Social Engineering yang dilakukan oleh APT seringkali menargetkan individu yang memiliki posisi atau jabatan strategis, serangan ini umumnya disebut sebagai Spear Phishing. Spear Phishing yang dilancarkan oleh APT seringkali dilegitimasi menggunakan data atau informasi dari target itu sendiri yang telah bocor. Contohnya seperti mengirimkan email phishing dengan menyertakan referensi yang valid seperti proyek yang sedang berjalan atau informasi lain yang benar adanya.

Stage 2: Escalation and Lateral Movement

Setelah mendapatkan akses ke jaringan target, threat actor memulai menjalankan malware atau mungkin tools yang relevan untuk memperluas jangkauan mereka. Hal ini bertujuan untuk memetakan serta mengumpulkan informasi yang berguna untuk menunjang tujuan dari APT itu sendiri. Tak jarang, pada fase ini juga threat actor membuat backdoor atau titik masuk rahasia sebagai backup access ketika pintu masuk pertama yang digunakan telah ditutup atau diremediasi. Dan pada saat lateral movement APT biasanya mencari beberapa hal penting yang menunjang mereka untuk mencapai tujuan tau objective mereka, diantaranya:

1. Kredensial
Mengumpulkan nama pengguna dan kata sandi untuk mendapatkan akses ke sistem lain di jaringan.

2. Informasi Jaringan
Memetakan struktur jaringan untuk memahami bagaimana sistem dan perangkat terhubung satu sama lain.

3. Sistem Penting
Mengidentifikasi server dan perangkat yang menyimpan data sensitif atau memiliki akses ke informasi bisnis kritis.

4. Vulnerability
Mencari celah keamanan atau kelemahan di sistem lain yang bisa dimanfaatkan untuk penetrasi lebih lanjut.

5. Data sensif
Mengumpulkan informasi yang dapat digunakan untuk tujuan pencurian data, seperti rahasia dagang, informasi pelanggan, atau data keuangan.

Karakteristik Serangan APT

APT menggunakan serangkaian teknik yang tergolong lebih canggih dibandingkan dengan serangan oleh threat actor pada umumnya yang dapat dijadikan sebagai indikasi serangan. Berikut adalah beberapa karakteristik serangan yang dilakukan oleh APT:

1. Aktifitas yang tidak biasa pada akun pengguna
APT sering kai menggunakan kredensial yang mereka dapatkan untuk mengakses sistem dengan role atau hak akses yang tinggi. Penggunaan kredensial yang tidak biasa, seperti waktu login (larut malam atau mungkin diluar jam kerja) seringkali dikaitkan dengan aktifitas penyusupan oleh APT.

2. Backdoor/Trojan
Backdoor/Trojan digunakan oleh APT sebagai backup access untuk masuk kembali ke sistem atau jaringan yang telah disusupi. Dengan menggunakan backdoor/trojan APT dapat menjaga akses mereka untuk tetap berada dalam jaringan atau sistem dari target. Bahkan ketika titik awal masuk mereka telah ditutup atau diremediasi, APT tetap dapat mempertahankan akses yang mereka miliki.

3. Kumpulan data yang tidak biasa
Dalam aksinya APT seringkali mengumpulkan data atau informasi penting yang mereka peroleh dari aktifitas lateral movement kedalam satu tempat inti yang nantinya setelah objective mereka tercapai, mereka akan memindahkan data tersebut keluar dari jaringan target atau ke internet.

4. Traffic jaringan yang tidak biasa
Aktifitas APT mungkin menyebabkan anomali dalam aliran data keluar, seperti jumlah data yang tiba-tiba lebih besar dari biasanya atau transfer data yang terjadi secara terus-menerus ke server eksternal yang tidak dikenal. Selain itu, peningkatan mendadak dalam operasi basis data, seperti akses masif terhadap database yang menyimpan informasi sensitif, juga dapat mengindikasikan bahwa data sedang disalin atau diambil untuk disalahgunakan.

Indikasi ini jika tidak diperhatikan, bisa menjadi tanda bahwa jaringan telah disusupi oleh serangan APT yang canggih dan terencana.

APT28: Fancy Bear/Sofacy

Salah satu contoh APT yang terkenal adalahAPT28, juga dikenal sebagai Fancy Bear atau Sofacy, yang diyakini sebagai kelompok threat actor yang didukung oleh negara Rusia. APT28 terkenal karena melakukan serangan siber yang sangat terkoordinasi dan canggih terhadap berbagai target politik, militer, dan organisasi pemerintah di seluruh dunia.

Berikut adalah beberapa contoh operasi yang dilakukan oleh APT28:

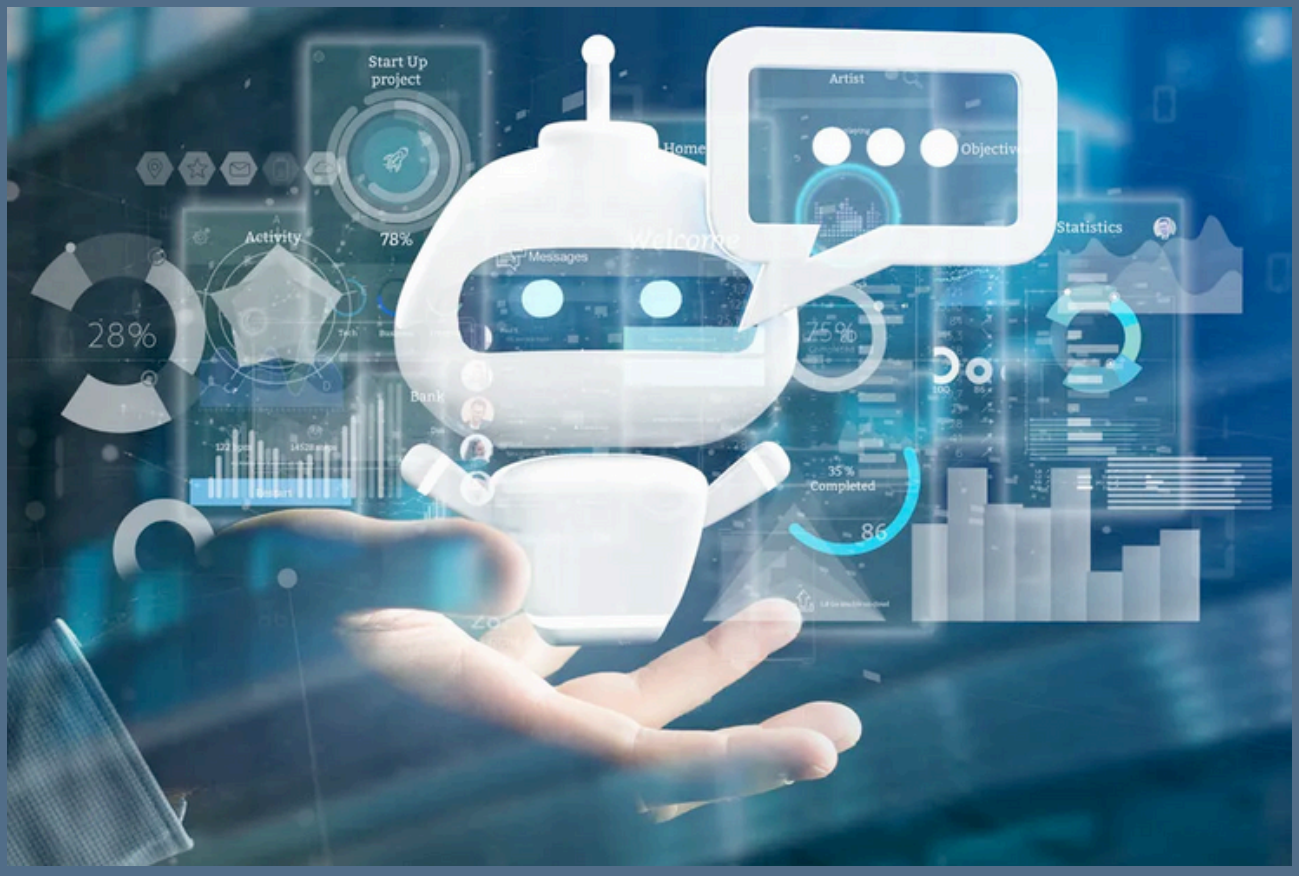
Serangan Terhadap Komite Nasional Partai Demokrat (DNC) pada 2016: APT28 terlibat dalam serangan terhadap DNC selama pemilihan presiden AS 2016. Mereka diduga mencuri ribuan email dari pejabat partai dan membocorkannya ke publik. Serangan ini menjadi bagian dari upaya yang lebih luas untuk mempengaruhi hasil pemilihan AS.

Operasi Pawn Storm: APT28 menjalankan kampanye spear-phishing yang disebut Pawn Storm, yang menargetkan lembaga-lembaga pemerintah, militer, media, dan politik di berbagai negara, termasuk AS, Jerman, Prancis, dan Ukraina. Serangan ini melibatkan penggunaan email phishing yang tampak berasal dari sumber tepercaya untuk mencuri kredensial dan mengakses sistem penting.

Serangan Terhadap Parlemen Jerman (Bundestag) pada 2015: APT28 juga diyakini berada di balik serangan besar terhadap parlemen Jerman. Dalam serangan ini, mereka berhasil mencuri data dari komputer anggota parlemen, termasuk informasi sensitif yang terkait dengan kebijakan luar negeri dan pertahanan Jerman.

KEAMANAN SIBER AI CHATBOT: APAKAH AMAN?

By **M Jufri**
Senior Penetration Tester



Namun, di balik keuntungan-keuntungan ini, terdapat potensi risiko yang perlu diwaspadai, terutama terkait keamanan siber.

Dalam beberapa tahun terakhir, banyak perusahaan telah mengadopsi AI chatbot untuk mempermudah interaksi dengan pelanggan. Teknologi ini mampu mengurangi waktu tunggu dalam menjawab pertanyaan dan memberikan layanan yang lebih efisien. AI chatbot dapat bekerja 24/7, menangani ribuan pertanyaan dalam hitungan detik, dan memberikan pengalaman yang lebih personal. Namun, seiring dengan adopsi luas teknologi ini, muncul pertanyaan yang krusial: Apakah AI chatbot aman?

PUNGGAWA
cyber security services

Keuntungan Penggunaan AI Chatbot

AI chatbot telah menjadi alat yang sangat populer di berbagai industri. Beberapa manfaat utama yang dirasakan oleh perusahaan antara lain:

1. Efisiensi Layanan: AI chatbot dapat menangani berbagai pertanyaan pelanggan secara otomatis, mengurangi waktu tunggu, dan mengurangi beban pada tim layanan pelanggan.

2. Peningkatan Kepuasan Pelanggan: Dengan respons yang cepat dan relevan, chatbot mampu meningkatkan pengalaman pelanggan. Mereka bisa memberi jawaban dalam hitungan detik, kapan pun dibutuhkan.

3. Skalabilitas: Chatbot bisa menangani volume pertanyaan yang sangat besar, memungkinkan perusahaan melayani banyak pelanggan tanpa harus meningkatkan jumlah staf.

Tantangan Keamanan pada AI Chatbot

Meskipun AI chatbot membawa efisiensi yang signifikan, implementasinya juga membawa beberapa tantangan keamanan, di antaranya:

1. No Rate Limit pada chatbot AI mengacu pada situasi di mana tidak ada pembatasan jumlah permintaan (request) yang dapat dikirimkan ke chatbot dalam periode waktu tertentu. Hal ini dapat terjadi jika tidak ada mekanisme pembatasan yang diterapkan atau jika mekanisme tersebut tidak efektif. Berikut adalah penjelasan lebih lanjut tentang konsekuensi dan dampak dari no rate limit pada chatbot AI:

- Peningkatan Biaya:

Detail:

Token Usage: Setiap permintaan ke chatbot AI menggunakan token, baik untuk input maupun output. Tanpa rate limit, jumlah token yang digunakan dapat meningkat secara signifikan.

Model	Pricing	Pricing with Batch API*
gpt-4o	$5.00 / 1M input tokens	$2.50 / 1M input tokens
	$15.00 / 1M output tokens	$7.50 / 1M output tokens
gpt-4o-2024-08-06	$2.50 / 1M input tokens	$1.25 / 1M input tokens
	$10.00 / 1M output tokens	$5.00 / 1M output tokens
gpt-4o-2024-05-13	$5.00 / 1M input tokens	$2.50 / 1M input tokens
	$15.00 / 1M output tokens	$7.50 / 1M output tokens

Pricing Model: Berdasarkan data harga Di atas ini, biaya per 1 juta token untuk model gpt-4o adalah

$ 5.00 untuk 1 juta input tokens

$ 15.00 untuk 1 juta output tokens

Contoh Perhitungan menggunakan model gpt-4o:

- Misalkan hacker mengirimkan 10 juta permintaan dalam satu jam, dengan setiap permintaan menggunakan 100 input tokens dan 200 output tokens.
- Total input tokens: 10 juta permintaan x 100 tokens = 1,000 juta tokens.
- Total output tokens: 10 juta permintaan x 200 tokens = 2,000 juta tokens.
- Biaya input tokens: 1,000 juta tokens x $5.00 / 1 Juta Tokens = $5000
- Biaya output tokens: 2,000 juta tokens x $ 15.00 / 1 juta tokens = $ 30.000
- Total biaya: 5,000(input)+30,000 (output) = $35,000 dalam satu jam.

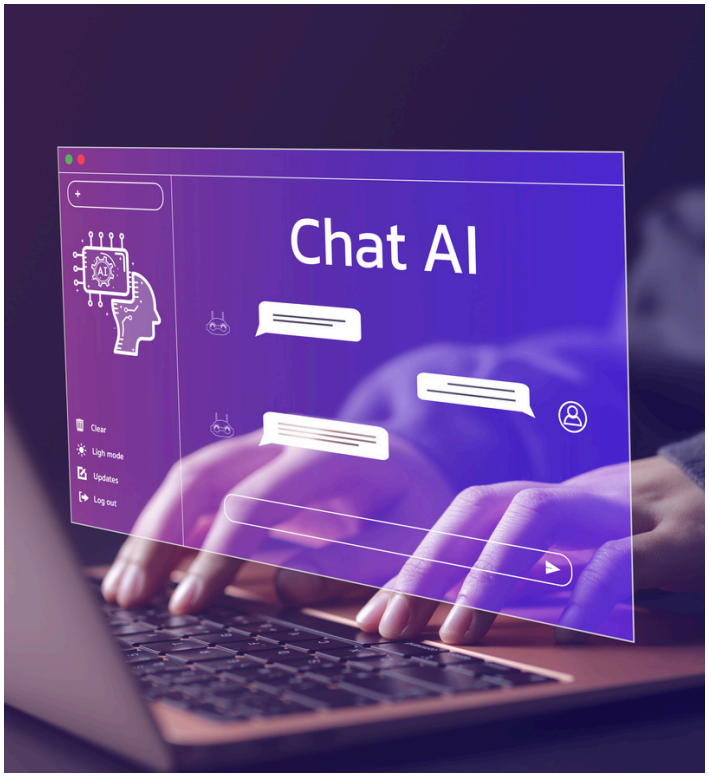
2. Serangan Prompt Hacking

Salah satu ancaman terbesar terhadap AI chatbot adalah prompt hacking, di mana peretas memberikan input atau perintah yang dimaksudkan untuk memanipulasi cara kerja chatbot. Serangan ini bisa memaksa chatbot mengungkapkan informasi sensitif atau bahkan menyebabkan kerusakan lebih lanjut pada sistem. Peretas dapat memanfaatkan celah ini jika chatbot tidak diprogram dengan pengamanan yang ketat.

Contoh Serangan Prompt Hacking :

- Prompt Injection
- SQL Injection
- Command Injection
- SSRF (Server-Side Request Forgery)

Contoh Prompt Hacking menggunakan Jailbreak Prompt dapat dilihat di : https://oxtia.com/chatgpt-jailbreak-prompts/



Beberapa Kerugian dari Serangan Hacker pada AI Chatbot pada Bisnis

Kerugian Finansial:

- Biaya Tambahan: Peningkatan penggunaan token akibat serangan dapat menambah biaya.
- Biaya Penanganan: Memerlukan biaya untuk penyelidikan dan perbaikan sistem.
- Kerugian Pendapatan: Layanan yang terhenti dapat menyebabkan kehilangan pendapatan.

Dampak pada Kinerja Layanan:

- Overload Server: Serangan dapat membuat chatbot tidak responsif.
- Peningkatan Latensi: Pengalaman pengguna memburuk karena latensi tinggi.
- Downtime: Layanan dapat mengalami gangguan yang berkepanjangan.

Pencurian Data:

- Kehilangan Data Sensitif: Data pengguna dan informasi penting dapat dicuri.
- Kerentanan Keamanan: Tanpa batasan, hacker dapat melakukan serangan lebih lanjut.
- Kerugian Reputasi: Kebocoran data merusak reputasi dan kepercayaan pengguna.

Kerugian Reputasi:

- Kehilangan Kepercayaan: Ketidakresponsifan dan kebocoran data merusak reputasi.
- Penggunaan Media Sosial: Berita negatif dapat menyebar cepat, memperburuk reputasi.
- Pelanggan Pindah: Pengguna mungkin beralih ke pesaing.

Dampak Pada Operasional Bisnis:

- Gangguan Operasional: Downtime mengganggu layanan pelanggan dan proses penting.
- Biaya Penanganan: Memerlukan biaya tambahan untuk perbaikan dan penguatan sistem.
- Peningkatan Risiko: Serangan berhasil dapat meningkatkan risiko serangan di masa depan.

Langkah-Langkah untuk Meningkatkan Keamanan AI Chatbot

Agar AI chatbot dapat beroperasi dengan aman dan menghindari risiko yang dapat merugikan perusahaan serta pelanggan, beberapa langkah pengamanan perlu diterapkan:

• **Enkripsi Data**

Salah satu cara terbaik untuk melindungi chatbot dari pencurian data adalah dengan menggunakan enkripsi yang kuat. Semua data yang dikirimkan antara pelanggan dan chatbot harus dilindungi dengan baik, sehingga data sensitif tidak mudah dicuri.

• **Validasi Input dan Deteksi Anomali**

Chatbot perlu dilengkapi dengan sistem yang dapat memvalidasi setiap input yang diterima. Deteksi anomali harus diimplementasikan untuk mengidentifikasi input yang mencurigakan atau yang berpotensi merusak sistem.

• **Pembaruan Berkala**

Seperti halnya aplikasi lainnya, AI chatbot harus secara rutin diperbarui untuk memperbaiki celah keamanan yang mungkin muncul. Peretas selalu mencari kelemahan baru, jadi penting untuk menjaga chatbot tetap up-to-date dengan pembaruan keamanan terbaru.

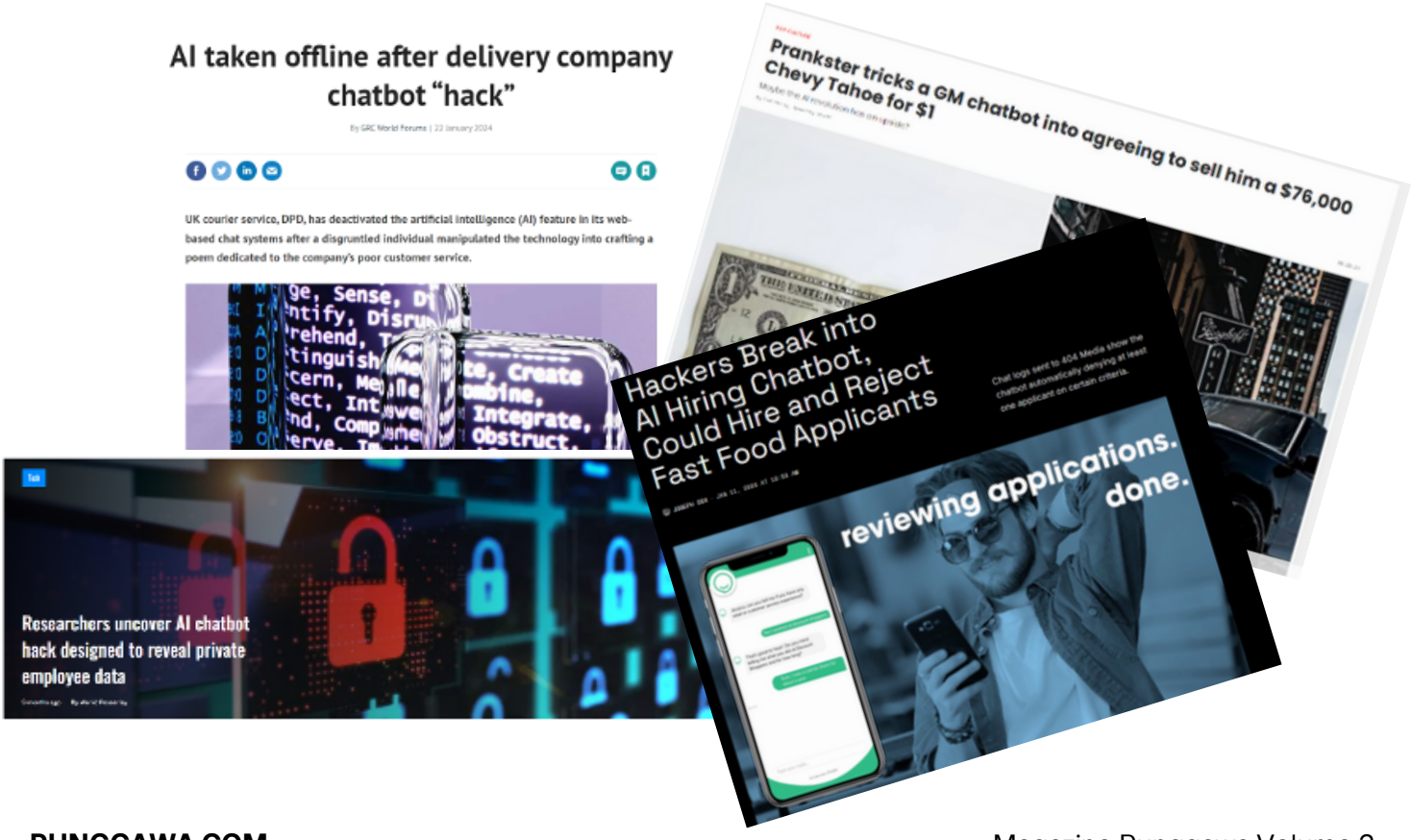
• **Audit Keamanan dan Pengawasan**

Pengawasan dan audit keamanan secara berkala sangat penting untuk mendeteksi potensi ancaman atau kelemahan dalam sistem AI chatbot. Dengan demikian, perusahaan dapat dengan cepat mengambil tindakan sebelum serangan terjadi.

• **Pembatasan Akses Data**

Chatbot tidak harus memiliki akses ke semua data pelanggan. Pembatasan akses hanya pada data yang benar-benar diperlukan akan membantu mengurangi risiko kebocoran informasi sensitif.

BEBERAPA KASUS YANG TERJADI DALAM TAHUN 2024



PATCHING THE HUMAN VULNERABILITY

By **AD Aji**
Offensive Security Leader

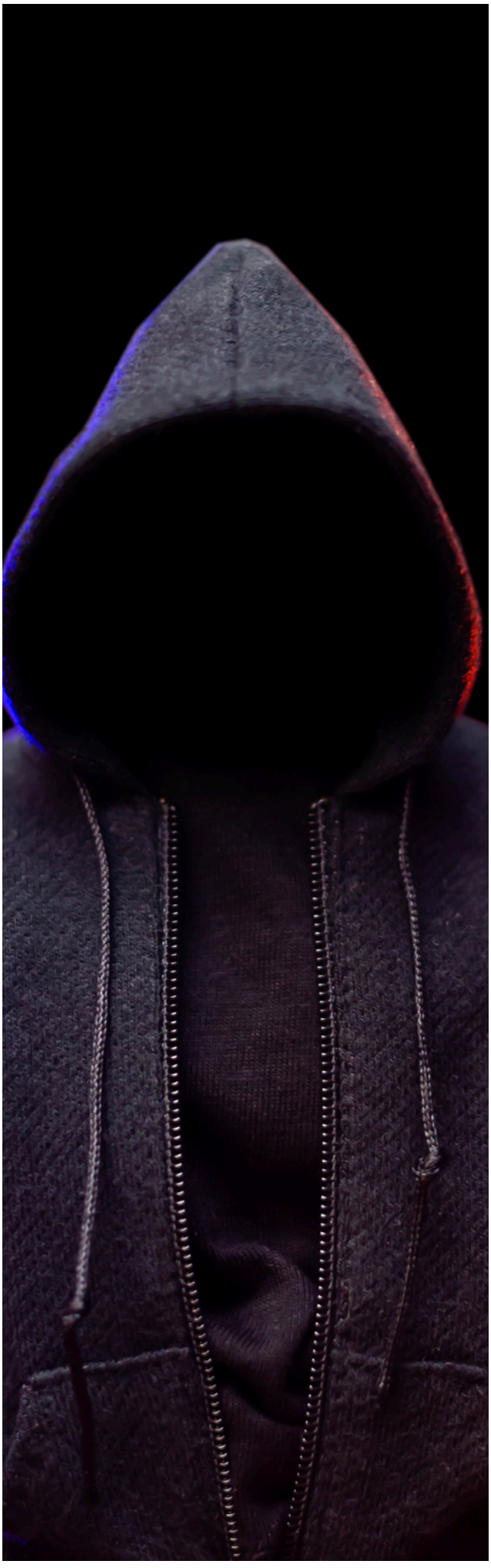
Dalam dunia keamanan siber, perhatian terbesar sering kali difokuskan pada teknologi, seperti firewall, antivirus, Intrusion detection system (IDS), dan Endpoint Detection and Response (EDR). Namun, dibalik semua perlindungan teknologi ini, ada satu kelemahan paling rentan yang sering kali terlupakan yaitu manusia.

Bahkan dengan pertahanan terbaik, serangan siber tetap dapat terjadi karena kesalahan manusia, entah dikarenakan ketidaktahuan, kelalaian, atau lainnya. Dalam banyak kasus, serangan ini memanfaatkan faktor psikologis, seperti rasa percaya atau rasa tergesa-gesa, yang membuat manusia menjadi target yang mudah. Seperti kata Bruce Schneier, seorang ahli keamanan siber, "Keamanan adalah sebuah proses, bukan produk" dan dalam proses tersebut, elemen manusia sering kali menjadi titik lemah.

Data dari Verizon Data Breach Investigations Report 2024 menunjukkan bahwa 68% pelanggaran yang disebabkan oleh kesalahan atau kelalaian manusia, 14% pelanggaran yang disebabkan oleh eksploitasi kerentanan sebagai langkah akses awal, 62% pelanggaran yang disebabkan oleh insiden yang bermotif finansial melibatkan ransomware atau pemerasan, dengan kerugian rata-rata $46.000 per pelanggaran, 15% pelanggaran yang disebabkan oleh pelanggaran melibatkan pihak ketiga, dari data tersebut dapat disimpulkan bahwa pelanggaran yang paling besar disebabkan oleh kesalahan atau kelalaian manusia.

Dalam beberapa tahun terakhir, Indonesia menjadi pusat perhatian dalam dunia keamanan siber akibat Serangkaian insiden kebocoran data yang menggemparkan berbagai sektor, kita telah melihat berbagai contoh nyata tentang bagaimana kesalahan manusia menyebabkan konsekuensi yang besar, termasuk serangan-serangan yang berhasil masuk ke infrastruktur penting dan mencuri data sensitif. Faktor kelemahan manusia mencakup berbagai hal, seperti penggunaan kata sandi yang lemah, ketidaktahuan tentang ancaman phishing, kesalahan konfigurasi sistem, serta kelalaian dalam menjaga perangkat fisik. Berikut beberapa contoh nyata insiden siber di Indonesia yang menggambarkan dan betapa seriusnya dampak dari human vulnerability:

Salah satu yang paling HOT adalah kebocoran data PDNS (Pusat Data Nasional). Insiden-insiden ini tidak hanya merusak reputasi lembaga, tetapi juga menimbulkan kekhawatiran besar terkait privasi masyarakat. Menariknya, di balik setiap serangan siber atau kebocoran data yang besar terdapat satu komponen krusial yang sering kali terabaikan yaitu manusia. Permasalahan yang ada pada pengelolaan PDNS yaitu pertama, belum adanya keseriusan pemerintah, khususnya Kemenkominfo RI dalam mempersiapkan pengamanan siber bagi PDNS.



Keinginan untuk mengimplementasikan Satu Data Nasional belum diimbangi dengan pondasi infrastruktur pengamanan yang memadai. Belum adanya infrastruktur pengamanan siber bagi PDNS tersebut berimbas pada permasalahan kedua, yaitu ketidaksiapan SDM yang berkompeten dalam menghadapi serangan siber. Adapun dua hal yang menjadi permasalahan inti penyebab lemahnya keamanan SDI yaitu masalah infrastruktur teknologi pengamanan siber dan SDM profesional pendukungnya belum ada secara jelas. Satu-satunya pasal yang menyinggung masalah SDM hanyalah Pasal 29 ayat (2) Perpres Nomor 39 Tahun 2019 yang menyatakan bahwa rencana aksi Satu Data Indonesia dapat mencakup: "pengembangan sumber daya manusia yang kompeten", dan itu pun induk kalimatnya menggunakan kata "dapat", sehingga tidak mencerminkan kewajiban. Ketidaktegasan kewajiban menyediakan SDM profesional dalam mengamankan data itulah yang tampaknya menyebabkan Kemenkominfo RI dan BSSN merasa penyediaan SDM tersebut adalah sesuatu hal yang bukan merupakan prioritas utama dan dapat ditunda.

Kebocoran data di Indonesia terus meningkat, dan manusia adalah salah satu faktor paling rentan dalam rantai keamanan. Dengan peningkatan pelatihan, kesadaran, dan penerapan teknologi keamanan yang kuat, organisasi dapat memitigasi risiko yang disebabkan oleh kelemahan manusia. **Melindungi data tidak hanya tentang memperbarui sistem teknologi, tetapi juga memastikan bahwa individu yang mengoperasikan sistem tersebut telah siap menghadapi ancaman yang terus berkembang.**

SERANGAN RANSOMWARE DATA CENTER ENKRIPSI DAN PENGHAPUSAN BACKUP

By **Rezky DK**
Solution Consultant

Sabtu yang Sibuk

Sabtu pagi biasanya adalah waktu untuk berkumpul bersama keluarga, menikmati sarapan, dan menikmati akhir pekan. Namun, tidak pada hari itu. Tepat pukul 07:00, HP saya berdering, dan muncul nomor salah satu customer kami di layar. "Ada apa pagi-pagi di hari Sabtu mereka menelepon?" batin saya.

"Halo, mas, maaf mengganggu weekend-nya. Kami terkena serangan semalam. Jaringan sudah terputus, akses ke cluster terblokir. Saat kami cek, semua LUN dan Volume di storage Data Center kami sudah tidak ada. Kami terpaksa memutuskan koneksi antara DC dan DRC. Kami butuh bantuan untuk segera recovery data dari DRC." Mendengar hal tersebut, saya langsung terduduk. Kekhawatiran segera melanda, memikirkan besarnya data yang mungkin hilang. Segera, saya koordinasi dengan tim internal dan membentuk grup percakapan khusus untuk menangani situasi ini.

Rencana recovery segera disusun dan dieksekusi. Proses ini memakan waktu hampir tiga pekan. Beberapa anggota tim dari pihak customer kami bahkan tidak pulang ke rumah selama tiga hari berturut-turut, semuanya demi satu tujuan: mengembalikan data berharga mereka yang terkena dampak serangan ini.

Pagi itu di Ibukota Baru

Pagi itu, di hari Sabtu yang lain. Saya sudah bersiap di depan televisi untuk menyaksikan momen bersejarah: upacara kemerdekaan Republik Indonesia yang untuk pertama kalinya diadakan di ibukota baru. Berbagai persiapan yang diberitakan oleh media menguatkan kecintaan serta kebanggaan saya sebagai rakyat Indonesia yang kini memiliki pusat pemerintahan baru. Namun, rencana santai saya berubah seketika. Di layar HP, puluhan notifikasi muncul secara tiba-tiba diwaktu yang hampir bersamaan di grup aplikasi percakapan online yang saya buat bersama customer.

Ketika membuka percakapan, ada satu pesan yang membuat saya tersentak. "Tolong segera lakukan video conference! Data center kami baru saja terkena serangan. Tolong isolasi jaringan, cek ini, cek itu, bantu eskalasi ke support perangkat, dan kirim teknisi baik ke DC maupun ke DRC."

Sontak, pagi yang seharusnya tenang berubah menjadi kesibukan luar biasa. Kami langsung bergerak cepat untuk merespons situasi kritis ini. Setelah video conference yang berlangsung hampir seharian penuh, kami mulai membantu pelanggan dalam proses recovery data mereka.

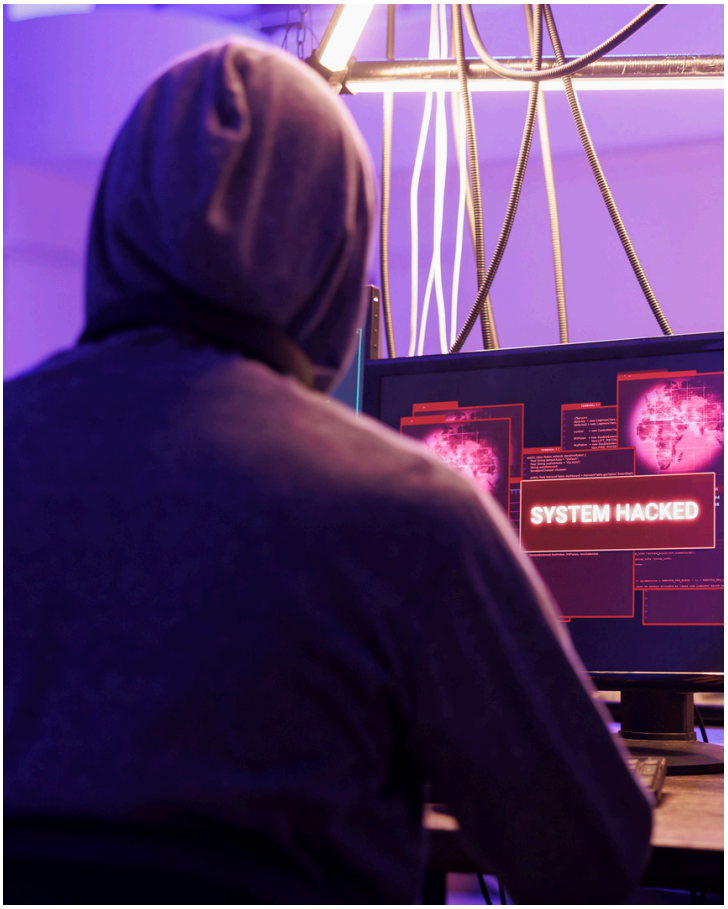
Pada sore hari yang sama, beberapa data dan aplikasi berhasil dipulihkan. Namun, proses recovery belum selesai. Pengecekan dan validasi data terus dilakukan untuk memastikan semuanya kembali seperti semula. Di saat yang sama, aktivitas forensik sudah dimulai oleh tim penanganan insiden cyber attack kami, yang bekerja keras untuk memahami asal usul serangan dan mencegah serangan serupa di masa depan.

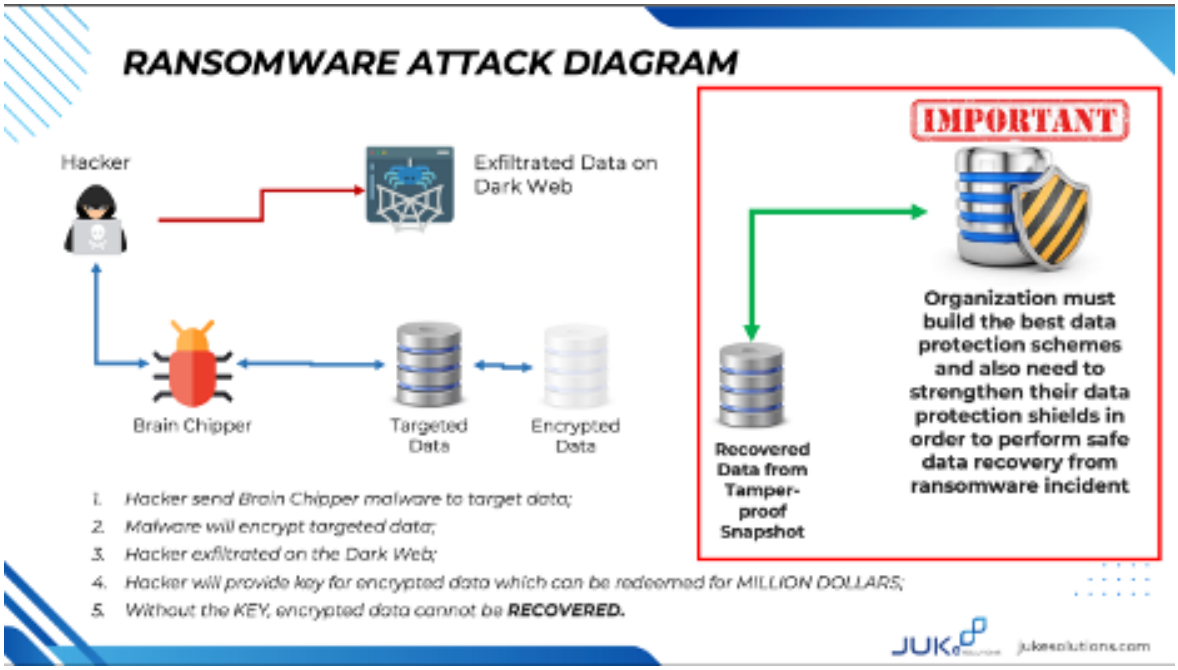
PUNGGAWA
cyber security services

Pola serangan yang mirip

Dari dua insiden serangan ransomware yang kami tangani, pola waktu serangan menjadi salah satu hal yang paling mencolok. Kedua serangan terjadi pada akhir pekan, ketika aktivitas pemantauan IT menurun karena banyak tim yang sedang libur atau tidak dalam mode siaga penuh. Para pelaku memanfaatkan celah ini untuk menyusup ke sistem, menyebabkan gangguan besar tanpa langsung terdeteksi. Kejadian ini mengingatkan kami bahwa ancaman siber tidak mengenal waktu, dan justru sering kali terjadi saat organisasi dalam posisi paling rentan.

Dari kedua peristiwa ini, kami mendapatkan pelajaran berharga terkait pentingnya kesiapan menghadapi serangan ransomware. Pada insiden pertama, proses pemulihan memakan waktu hingga beberapa minggu, sebuah periode yang panjang dan penuh tantangan baik dari sisi teknis maupun operasional. Di kasus kedua, kami berhasil mempercepat proses recovery secara signifikan. Banyak faktor yang mempengaruhi kecepatan pemulihan data sehabis serangan cyber, selain dari kewaspadaan operator yang melakukan monitoring perangkat secara berkala.





Faktor Komunikasi

Komunikasi adalah salah satu elemen terpenting dalam menghadapi serangan ransomware. Jangan takut atau ragu untuk segera melaporkan insiden. Transparansi sejak awal sangat diperlukan, karena proses recovery dan pencegahan tidak dapat dilakukan sendirian. Anda membutuhkan bantuan dari berbagai pihak, baik internal maupun eksternal, termasuk tim IT, vendor teknologi, dan pihak keamanan siber yang berpengalaman dalam menangani serangan semacam ini.

Eskalasi yang tepat waktu juga krusial, terutama jika insiden melibatkan teknologi yang kompleks. Segera eskalasikan dampak serangan kepada pihak yang relevan, baik itu vendor perangkat keras atau perangkat lunak, agar mereka dapat membantu mengendalikan situasi. Dengan melibatkan para ahli sejak dini, penanganan serangan dapat lebih efektif dan terkoordinasi dengan baik.

Selalu fokus pada pemulihan data sebagai prioritas utama. Komunikasi yang jelas dan terarah akan memastikan semua pihak bekerja sesuai tujuan yang sama, yaitu meminimalisir kerugian dan mempercepat pemulihan sistem. Dengan demikian, dampak finansial dan operasional akibat serangan dapat ditekan, dan bisnis dapat kembali beroperasi dengan cepat.

Faktor Tim Teknis

Ketersediaan dan kesiapan tim teknis merupakan salah satu faktor kunci yang menentukan kecepatan dan efektivitas pemulihan setelah serangan ransomware. Dalam situasi darurat seperti ini, seberapa cepat tim dapat dikumpulkan dan diaktifkan, baik dari sisi internal maupun eksternal, sangat mempengaruhi jalannya proses recovery. Tim internal yang terdiri dari para profesional IT harus siap dalam merespons serangan secara cepat, mulai dari mengisolasi sistem yang terinfeksi hingga mengidentifikasi titik masuk serangan. Namun, tak jarang, keahlian internal saja tidak cukup, terutama jika serangan melibatkan teknologi yang lebih kompleks atau sistem yang lebih luas. Di sinilah pentingnya dukungan dari tim eksternal.

Pihak eksternal, seperti vendor teknologi atau penyedia jasa keamanan siber, dapat memberikan perspektif dan alat tambahan yang tidak selalu dimiliki oleh tim internal. Mereka sering kali memiliki keahlian khusus dan pengalaman luas dalam menangani serangan ransomware, yang memungkinkan mereka memberikan solusi yang lebih terarah dan cepat. Oleh karena itu, keberhasilan pemulihan data sangat bergantung pada kecepatan eskalasi dan kolaborasi antara tim internal dan eksternal. Dengan adanya kolaborasi yang solid, setiap langkah dalam proses pemulihan dapat dieksekusi dengan baik, mulai dari mitigasi dampak serangan hingga pemulihan data yang tersandera, memastikan bahwa downtime dapat diminimalkan dan operasional bisnis dapat segera pulih.

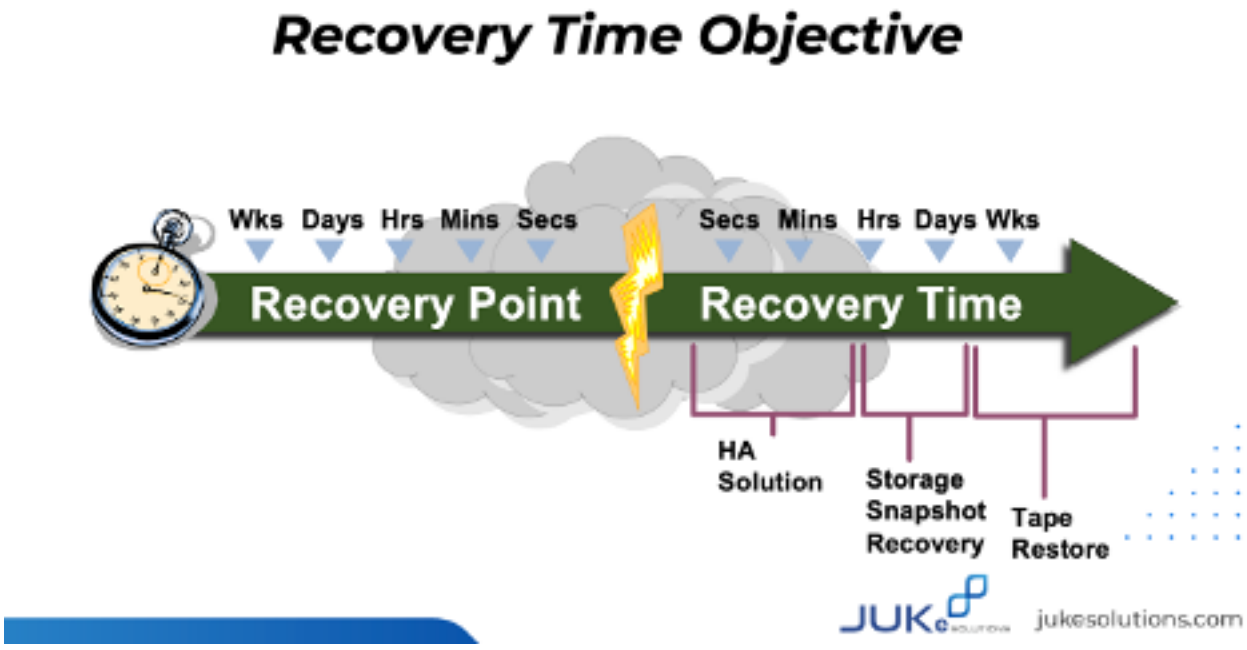
Faktor Teknologi

Pemilihan teknologi yang tepat dalam menyimpan data menjadi fondasi utama dalam melindungi informasi penting dari berbagai ancaman, termasuk serangan ransomware. Di era digital saat ini, data menjadi aset yang sangat berharga, sehingga metode penyimpanannya harus dirancang dengan memperhatikan keamanan dan keandalannya. Memilih solusi penyimpanan yang tangguh dan canggih bukan hanya soal kapasitas, tetapi juga fitur keamanan yang bisa memberikan proteksi berlapis terhadap risiko kehilangan data. Dengan teknologi penyimpanan yang tepat, perusahaan dapat lebih siap menghadapi ancaman ransomware, sekaligus mempercepat proses pemulihan jika terjadi insiden.

Sistem penyimpanan data yang ideal harus dilengkapi dengan berbagai fitur keamanan yang dirancang untuk menangkal serangan dan mendukung pemulihan. Salah satu teknologi penting dalam hal ini adalah immutable storage system, yang membuat data tidak bisa dihapus atau diubah setelah tersimpan. Teknologi ini sangat bermanfaat dalam melawan serangan ransomware, karena meskipun sistem utama berhasil disusupi, penyerang tidak akan dapat menghapus atau mengenkripsi data yang tersimpan secara immutable. Selain itu, fitur seperti Multi Admin Verification memungkinkan adanya perlindungan tambahan, di mana penghapusan data harus disetujui oleh setidaknya dua admin. Hal ini mencegah penyerang yang berusaha menghapus data secara ilegal, karena adanya kontrol yang ketat pada level akses administrasi.

Selain keamanan, kecepatan pemulihan data menjadi hal yang sangat penting setelah serangan terjadi. Teknologi snapshot adalah salah satu solusi yang memungkinkan pemulihan data secara cepat dan efisien dibandingkan metode tape konvensional. Snapshot mengambil gambaran data secara berkala, sehingga jika terjadi serangan, data dapat dengan mudah dipulihkan dari titik tertentu tanpa perlu melalui proses restore yang lama. Namun, teknologi ini harus dilengkapi dengan fitur yang memastikan snapshot tidak dapat dihapus oleh pihak yang tidak berwenang. Misalnya, teknologi SNAPLOCKTM dari NetApp yang membuat snapshot menjadi tamper-proof, sehingga data tetap aman dan tidak dapat dihapus bahkan oleh ransomware. Dengan kombinasi teknologi ini, perusahaan dapat mempercepat pemulihan sekaligus memastikan integritas data terjaga dengan baik selama dan setelah serangan.

Hubungan Kecepatan Pemulihan dengan Teknologi yang Dipilih



Kecepatan pemulihan data sangat dipengaruhi oleh teknologi penyimpanan yang dipilih, dan ini tercermin dalam konsep Recovery Time Objective (RTO), yang mengukur seberapa cepat sistem dapat kembali normal setelah terjadi gangguan. Dalam beberapa skenario, teknologi High Availability (HA) menawarkan RTO mendekati nol atau zero downtime, di mana sistem dapat terus berjalan meskipun terjadi gangguan. Namun, dengan meningkatnya kecanggihan serangan ransomware, pola serangan yang ditargetkan tidak hanya menyerang sistem utama, tetapi juga mencakup perangkat HA dan DRC (Disaster Recovery Center). Akibatnya, pemulihan dari serangan ransomware sering kali tidak bisa dilakukan melalui perangkat HA atau DRC, karena keduanya sudah menjadi target serangan.

Untuk menjaga integritas data dan memastikan adanya cadangan yang tidak terpengaruh oleh serangan, beberapa organisasi mengandalkan perangkat tape dengan teknologi Write Once, Read Many (WORM). Teknologi ini menjamin bahwa data yang sudah tersimpan di tape tidak dapat diubah atau dihapus, sehingga menjadi lapisan perlindungan yang kuat dari serangan ransomware. Namun, meskipun tape menawarkan keamanan yang solid, pemulihan data dari tape memerlukan waktu yang lebih lama dibandingkan teknologi lain. Proses restore yang memakan waktu ini dapat menyebabkan penundaan signifikan dalam pemulihan, yang berdampak langsung pada kerugian bisnis selama masa downtime.

Pemanfaatan storage snapshot telah menjadi metode umum dan andal dalam proses pemulihan data setelah serangan ransomware. Teknologi snapshot memungkinkan pengambilan salinan data secara berkala dan cepat, sehingga data dapat dipulihkan ke kondisi sebelum serangan terjadi. Namun, dengan berkembangnya ancaman siber, para penyerang kini juga menargetkan penghapusan snapshot untuk menghilangkan peluang pemulihan yang cepat. Hal ini membuat perlindungan terhadap snapshot menjadi sangat penting.

NetApp, dengan teknologi SnapLock, menawarkan solusi yang dapat mencegah penghapusan volume serta snapshot secara ilegal. SnapLock menciptakan mekanisme keamanan yang membuat snapshot dan data terkait tidak dapat dihapus oleh penyerang, bahkan jika mereka memiliki akses ke sistem penyimpanan. Dengan fitur ini, organisasi dapat lebih percaya diri dalam menggunakan storage snapshot sebagai bagian dari strategi pemulihan, karena data tetap terlindungi dan aman dari modifikasi atau penghapusan yang tidak sah, memastikan proses recovery berjalan lebih cepat dan efektif.

NetApp ONTAP SnapshotTM

NetApp ONTAP Snapshot™ menawarkan solusi logical air gapping yang efektif untuk melindungi data dari serangan ransomware. Snapshot merupakan salinan data yang hanya-baca dan diambil pada momen tertentu, sehingga tidak bisa diubah atau terinfeksi. Jika terjadi serangan, pemulihan data dapat dilakukan dengan mudah dari salinan Snapshot yang diambil sebelum serangan, memungkinkan proses recovery hampir seketika. Pemulihan dari Snapshot jauh lebih cepat dibandingkan metode backup tradisional seperti tape atau disk, yang biasanya membutuhkan waktu lama dan memperbesar biaya akibat serangan ransomware.

NetApp juga menyediakan perlindungan tambahan terhadap penghapusan Snapshot melalui fitur SnapLock® yang membuat data benar-benar immutable. SnapLock mencegah penghapusan salinan Snapshot bahkan oleh administrator atau penjahat siber yang menggunakan kredensial curian. Solusi ini memenuhi standar kepatuhan data, seperti HIPAA dan Sarbanes-Oxley, serta memberikan opsi penguncian data dalam periode tertentu agar tidak dapat dihapus. Dengan SnapLock, data dalam Snapshot terlindungi dari modifikasi atau penghapusan, menjadikannya solusi andal untuk melawan ransomware.

Kesimpulan

Tidak ada yang dapat menjamin keamanan data Anda secara 100%, namun langkah yang dapat diambil adalah meningkatkan keamanan untuk melindungi data dari serangan yang mungkin terjadi. Meskipun pemilihan teknologi terkadang terlihat mahal, anda dapat membayangkan kerugian yang dapat ditimbulkan oleh serangan siber: mulai dari staf IT yang terpaksa menginap di kantor demi pemulihan data hingga kehilangan bisnis yang dapat menguras sumber daya perusahaan hingga milyaran rupiah. Dan juga, jangan lupakan pula denda dari pelanggan yang merasa datanya telah dibocorkan!.

Oleh karena itu, keamanan siber merupakan sebuah investasi. Karena kerugian tidak hanya akan berdampak pada keuangan perusahaan, tetapi juga pada semua aspek berharga dari bisnis perusahaan. Dalam dunia yang penuh risiko ini, menjaga data dengan baik adalah langkah bijak yang tidak dapat kita diabaikan.

Referensi:
https://www.netapp.com/blog/ransomware-protection-snaplock/
https://www.netapp.com/blog/what-really-happens-during-ransomware-attack/

TOP 5 CVE KUARTAL 3 2024

47

Dalam kuartal ketiga tahun 2024, sejumlah kerentanan keamanan tingkat tinggi ditemukan dan ditangani di berbagai perangkat lunak yang banyak digunakan dalam lingkungan enterprise. Beberapa di antaranya mempengaruhi VMware, Microsoft, OpenSSH, dan Cisco. Berikut ini adalah lima kerentanan paling kritis yang membutuhkan perhatian segera dari para administrator dan profesional keamanan.

By **Kang Ali**
Cyber Security - RND

CVE-2024-6387: OpenSSH RegreSSHion Vulnerability (Severity: High)

Kerentanan RegreSSHion (CVE-2024-6387) ditemukan pada Agustus 2024 dan memengaruhi OpenSSH, sebuah alat yang sangat penting untuk akses jarak jauh yang aman. Kerentanan ini memungkinkan penyerang untuk melewati autentikasi, membuka peluang akses tidak sah ke sistem.

Dampak: Karena OpenSSH digunakan di banyak server untuk manajemen jarak jauh, bypass autentikasi ini memberikan potensi kontrol penuh kepada penyerang atas infrastruktur yang sangat kritis, terutama di lingkungan enterprise.
Mitigasi: Pengembang OpenSSH segera merespon dengan memperbaiki celah ini, dan para administrator harus segera memperbarui sistem ke versi terbaru untuk mencegah eksploitasi.

CVE-2024-38812: VMware vCenter Server (Severity: High)

VMware vCenter Server, yang merupakan inti pengelolaan lingkungan virtualisasi, mengalami kerentanan remote code execution (RCE) (CVE-2024-38812). Eksploitasi kerentanan ini memungkinkan penyerang mengeksekusi kode dengan hak istimewa tinggi pada sistem, membuatnya sangat berbahaya bagi perusahaan yang menggunakan VMware untuk mengelola infrastruktur cloud.

Dampak: Jika berhasil dieksploitasi, penyerang dapat mengontrol server vCenter, mendapatkan akses ke data sensitif, atau memodifikasi konfigurasi. Kerentanan ini berpotensi menyebabkan gangguan besar di lingkungan virtualisasi.
Mitigasi: VMware telah merilis patch untuk menangani masalah ini, dan para administrator harus segera memperbarui sistem.

CVE-2024-65412: Microsoft Exchange Server (Severity: High)

Microsoft Exchange Server, platform yang banyak digunakan dalam sistem email perusahaan, terdeteksi memiliki kerentanan remote code execution (RCE) (CVE-2024-65412). Penyerang dapat mengeksploitasi celah ini dengan menggunakan kredensial Exchange untuk menyisipkan perintah berbahaya, berpotensi mendapatkan kontrol penuh atas sistem email.

Dampak: Kerentanan ini bisa mengakibatkan gangguan komunikasi email, akses tak sah ke data sensitif, atau penyebaran malware dalam skala besar. Mengingat pentingnya email dalam operasional bisnis, ini adalah ancaman serius bagi keberlangsungan bisnis.
Mitigasi: Microsoft telah merilis patch pada September 2024 sebagai bagian dari pembaruan Patch Tuesday, dan penting bagi organisasi untuk segera menerapkan patch tersebut.

CVE-2024-38021: Microsoft Outlook Zero-Click RCE Vulnerability (Severity: High)

CVE-2024-38021, ditemukan pada Juli 2024, adalah kerentanan remote code execution tanpa memerlukan interaksi dari pengguna di Microsoft Outlook. Penyerang dapat menjalankan kode berbahaya hanya dengan mengirim email, tanpa memerlukan klik dari pengguna.

Dampak: Ini adalah ancaman serius bagi organisasi yang menggunakan Outlook sebagai klien email utama. Penyerang dapat mendistribusikan malware atau mengakses data sensitif hanya melalui email pratinjau.
Mitigasi: Microsoft merilis patch pada Agustus 2024. Selain itu, mematikan panel pratinjau hingga patch diterapkan bisa menjadi langkah mitigasi tambahan.

CVE-2024-32098: Cisco ASA VPN Buffer Overflow (Severity: High)

Cisco ASA VPN, yang merupakan perangkat penting untuk akses jarak jauh yang aman, terdeteksi memiliki kerentanan buffer overflow (CVE-2024-32098) pada Agustus 2024. Eksploitasi celah ini dapat menyebabkan penyerang merusak layanan VPN atau bahkan mengeksekusi kode berbahaya dari jarak jauh.

Dampak: Sistem VPN yang digunakan untuk komunikasi jarak jauh dapat terganggu, memungkinkan penyerang mencuri informasi sensitif atau menyusup ke jaringan tanpa terdeteksi.
Mitigasi: Cisco merilis patch untuk menangani kerentanan ini, dan administrator di organisasi yang menggunakan ASA VPN harus segera menerapkannya.

QALBU

Quick and High Quality Response: Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything: Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed: Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver: Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strenght : Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

MAGAZINE PUNGGAWA

VOLUME 3.0

PUNGGAWA cybersecurity

JUKe SOLUTIONS

ask.sales@punggawa.com

info@jukesolutions.com

punggawacyber

jukesolutions

PunggawaCyber

JUKe Solutions

Punggawa Cybersecurity

Juke Solutions