ARTIKEL KAMSIB

Kamar Kamsib memiliki visi untuk meningkatan literasi keamanan informasi dan siber masyrakat Indonesia. Dengan pendekatan konten Instagram dan artikel mengenai *cyber security* yang mudah dipahami oleh seluruh kalangan masyarakat.

KAMSIB

Dokumen Terbatas Untuk Pembelajaran

Judul : Mengenal Cyber Kill Chain, Framework Serangan Siber
Penulis : Anton Lepari
Tanggal : Desember 11, 2022
Keterangan : Bisa diakses dalam bentuk artikel web dan PDF

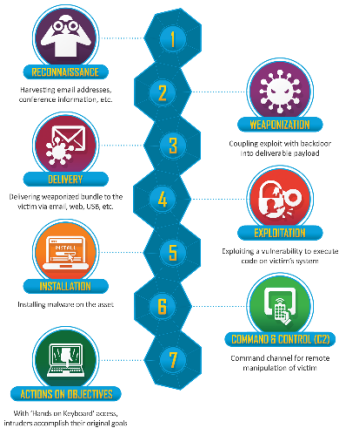
A. Framework

Menurut kamus Oxford, framework (kerangka kerja) dapat diartikan sebagai seperangkat keyakinan, ide atau aturan yang digunakan sebagai dasar untuk membuat penilaian, keputusan, dll [1]. Dalam praktik di kehidupan sehari-hari, banyak sekali macam-macam framework. Framework yang dipakai tentu berhubungan dengan bidang ilmu tempat framework tersebut diterapkan. Tidak terkecuali bidang keamanan informasi dan siber yang merupakan turunan dari bidang ilmu komputer. Salah satu framework dalam bidang ini adalah Cyber Kill Chain atau disingkat CKC.

B. Cyber Kill Chain (CKC)

Dikembangkan oleh Lockheed Martin, framework CKC adalah bagian dari model Intelligence Driven Defense® untuk identifikasi dan pencegahan aktivitas intrusi dunia maya. Model tersebut mengidentifikasi apa yang harus diselesaikan musuh untuk mencapai tujuan mereka. Tujuh langkah CKC meningkatkan kejelasan serangan dan memperkaya pemahaman analis tentang taktik, teknik, dan prosedur musuh [2].

Framework ini masih popular digunakan sekarang. Baik dari sisi implementasi dalam organisasi, maupun pembahasan akademik dalam tulisan ilmiah. Ada tujuh tahapan dalam CKC, yang dimulai dari Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), dan terakhir Actions on Objectives.



1. Reconnaissance

Reconnaissance atau dapat juga diartikan sebagai Pengintaian adalah kegiatan mengumpulkan informasi mengenai target. Target bisa sebagai perorangan (individu) maupun organisasi. Informasi yang diperoleh bermaca-macam, seperti profil personel di perusahaan, alamat email, alamat website, hingga isi dari hasil crawling website milik target.

2. Weaponization

Sesuai namanya, Weaponization adalah tahap penyerang mempersenjatai dirinya dengan peralatan yang sesuai dengan informasi target. Informasi target yang telah terkumpul sebelumnya pada tahap Recon, akan diidentifikasi untuk mengetahui metode dan alat apa yang cocok untuk menyerang ke dalamnya. Misalnya menyusun malware dan backdoor yang tepat untuk website target.

3. Delivery

Setelah senjata dibuat, kemudian dikirimkan ke target. Tahapan ini merupakan tahapan yang cukup krusial karena dalam tahapan ini penyerang harus tahu di mana letak kelemahan/kerentanan target. Penyerang harus memikirkan bagaimana cara menyampaikan peralatan atau persenjataan tadi ke target dengan efektif dan efisien.

4. Exploitation

Setelah berhasil mengirimkan senjata siber, Langkah selanjutnya adalah mengeksekusi senjata di sisi target. Pada eksekusi, langkah selanjutnya adalah memicu eksploit. Tujuan dari eksploitasi adalah untuk diam-diam menginstal/mengeksekusi payload.

5. Installation

Ketika kelemahan/kerentanan tersebut berhasil dieksploitasi, selanjutnya adalah memasang (instalasi) ke jaringan atau sistem milik target. Instalasi ini ditujukan untuk mendapatkan akses ke aset milik target.

6. Command and Control (C2)

Malware atau senjata siber tadi berhasil dipasang, kemudia melakukan komunikasi dengan target melalui malware tersebut. Dalam tahap C&C, penyerang bisa mengirimkan instruksi ke target sesuai dengan keinginan/tujuan penyerang. Tentu tahap pengiriman instruksi ini tidak diketahui oleh korban.

7. Actions on Objectives

Tahapan akhir, Actions on Objectives, ketika sistem milik target telah diambil sepenuhnya, maka selanjutnya adalah melaksanakan tujuan penyerang.

C. Contoh Tulisan Ilmiah Membahas Mengenai CKC:

Berikut ini adalah beberapa tulisan ilmiah yang membahas mengenai CKC yang bisa kamu unduh dan baca secara gratis:

1. Yadav, Tarun & Rao, Arvind. (2015). Technical Aspects of Cyber Kill Chain. 10.1007/978-3-319-22915-7_40. (https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain)
2. Zeng, Wen & Germanos, Vasileios. (2019). Modelling Hybrid Cyber Kill Chain. (https://www.researchgate.net/publication/335753886_Modelling_Hybrid_Cyber_Kill_Chain/citations)
3. Olzak, Tom. (2022). Use the Cyber Kill Chain to Secure End-user Devices. (https://www.researchgate.net/publication/360086038_Use_the_Cyber_Kill_Chain_to_Secure_End-user_Devices)

D. Referensi

1. https://www.oxfordlearnersdictionaries.com/definition/english/framework
2. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
3. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/
4. Yadav, Tarun & Rao, Arvind. (2015). Technical Aspects of Cyber Kill Chain. 10.1007/978-3-319-22915-7_40. (https://www.researchgate.net/publication/281148852_Technical_Aspects_of_Cyber_Kill_Chain)
5. Zeng, Wen & Germanos, Vasileios. (2019). Modelling Hybrid Cyber Kill Chain. (https://www.researchgate.net/publication/335753886_Modelling_Hybrid_Cyber_Kill_Chain/citations)
6. Olzak, Tom. (2022). Use the Cyber Kill Chain to Secure End-user Devices. (https://www.researchgate.net/publication/360086038_Use_the_Cyber_Kill_Chain_to_Secure_End-user_Devices)