COMO FUNCIONA A ESTRUTURA DE UM ATAQUE HACKER

Foto de cottonbro no Pexels

Os ataques hackers acontecem em fases, que vão progredindo em direção ao objetivo pretendido. Por isso é importante aprender sobre a abordagem utilizada pelos cibercriminosos, se tornando assim um hacker do bem, o hacker ético.

O Cyber Kill Chain é um modelo, que contém as fases de um ataque cibernético a uma rede de computadores, desde o reconhecimento inicial, ao objetivo de exfiltração de dados. Este modelo foi definido pela empresa Lockheed Martin em 2011 e é uma adaptação de um modelo anterior chamado Kill Chain.

Kill Chain é um termo originalmente usado pelos militares para demonstrar a estrutura de um ataque, que significa "cadeia de destruição". Esse modelo foi desenvolvido para ajudar os militares a decidir como empregar seus esforços, na luta contra seus adversários. Esses esforços vão desde o desenvolvimento de novas habilidades, alocação de tempo e dinheiro, e outros tantos recursos que fazem a diferença na hora de obter alguma vantagem sobre o adversário.

Segundo a abordagem Kill Chain usada pelos militares, para se ter um ataque bem-sucedido, você deve seguir quatro etapas:

1. Encontrar o alvo
2. Determinar a localização, curso e velocidade do alvo
3. Comunicar essa informação de forma coerente à plataforma de lançamento da arma
4. Lançar o ataque usando qualquer coisa, desde uma arma cinética a sistemas eletromagnéticos e cibernéticos

Ficou confuso, espera um pouco que nós vamos explicar melhor no decorrer desse relatório como funciona um ataque hacker.

Foto de Pexels

O modelo Kill Chain dos militares, ajuda você a determinar a maneira mais eficiente de completar a sua cadeia de destruição, no caso de um ataque contra as forças inimigas. Também ajuda a determinar a maneira mais eficiente de se proteger de um ataque adversário, quebrando a cadeia dele, no caso de uma defesa ou ação preventiva. Sendo assim, procura-se o elo onde o adversário tem alguma vulnerabilidade e nós uma vantagem, para que uma vez destruindo esse único elo ou todos os elos, a cadeia de destruição seja interrompida e o ataque do adversário destruído.

Um bom exemplo para quebrar o primeiro elo usado pelos militares, é buscar conseguir impedir que o radar adversário os veja, pois depois que esse elo é quebrado, o adversário tem problemas para completar o resto da cadeia e atacar de volta.

Um modelo militar construído em cima da estrutura do Kill Chain, é o "F2T2EA" onde cada letra representa uma ação a ser tomada, formando as seguintes etapas:

1. Find(Encontrar): Encontre o alvo.
2. Fix(Determinar/Estabelecer): Determine a localização do alvo e dificuldade nos movimentos.
3. Track(Monitorar): Monitore o movimento do alvo, até que seja tomada uma decisão.

4. Target(Alvo): Selecione o armamento ou recurso apropriado para usar no alvo, afim de criar o efeito desejado.
5. Engage(Engajar): Aplique o armamento selecionado na fase anterior no alvo.
6. Assess(Avaliar): Avalie os efeitos do ataque, incluindo qualquer informação coletada.

Foto de Tima Miroshnichenko no Pexels

Voltando ao Cyber Kill Chain, podemos dizer que ele é uma adaptação do Kill Chain criado pelos militares com foco na área de cibersegurança. Ele também pode ser usado como uma ferramenta de gerenciamento para ajudar a melhorar continuamente a defesa da rede. De acordo com a Lockheed Martin, as ameaças devem passar por várias fases do modelo, incluindo:

1. Reconnaissance (Reconhecimento do alvo): Compreende a pesquisa e coleta de informações sobre possíveis alvos durante um longo período de tempo. O atacante deve selecionar e avaliar informações sobre os alvos que podem conduzi-lo ao sucesso no seu ataque. Informações de várias fontes, como a darknet, podem ser usadas para encontrar alvos em potencial e explorar informações que vazaram. Pode-se coletar endereços de e-mail, analisar redes sociais, google, sites de empresas, blogs, reconhecimento de servidores expostos publicamente na internet e etc. A etapa de reconhecimento é classificada em dois tipos:
    a. Reconhecimento passivo: É a coleta de informações do alvo sem que ele perceba, ou seja, sem causar nenhum alarde. Uma das técnicas utilizadas nessa etapa é a pesquisa em fontes abertas OSINT.
    b. Reconhecimento ativo: É uma análise mais completa do alvo, onde os dados não são apenas coletados “silenciosamente”, mas ativamente

interceptados. A engenharia social é usada como ferramenta de exploração do elo mais fraco, o ser humano, a fim de obter dados críticos de segurança e informações privilegiadas. Alguns exemplos de ferramentas usadas nessa etapa para fins legítimos são: Nmap para varredura de rede e porta, OpenVAS para verificação de vulnerabilidades conhecidas (CVEs) e DNSMap, Sqlmap e SMBMap para verificação dos respectivos serviços.

Potenciais contramedidas: É quase impossível detectar o reconhecimento no momento da execução, mas você pode coletar logs dos visitantes do site para alertas e pesquisa histórica, além de trabalhar com os administradores da web para alavancar a análise do navegador. Usando esses dados, você pode identificar comportamentos de navegação e priorizar defesas para grupos de pessoas e tecnologias.(Ondeso, 2021)

2. Weaponization (Preparação do ataque): Fase de planejamento, aqui os atacantes irão preparar suas "armas" e especificamente procurar vulnerabilidades das quais eles possam atacar. São selecionados os exploits, criados os backdoors, payloads, trojans e demais "armas" ou ferramentas que serão utilizadas no ataque. Também existe um mercado negro para os chamados exploits de dia zero, que ainda não são conhecidos pelo público em geral e podem ser explorados pelo invasor.

   Potenciais contramedidas: Durante esta fase, você só pode se defender de forma limitada. No entanto, execute análises para entender os artefatos de malware atuais e criar procedimentos para detecção precoce. Os arquivos e metadados coletados podem ser usados para realizar análises futuras e detectar novos ataques.(Ondeso, 2021)

   Para fazer isso, ferramentas familiares podem ser construídas e usadas:
   BeEF, MSFPC, Metasploit, Armitage, ExploitDB, Rubber Ducky(USB), Bot-Net, Custom Scripties.(Ondeso, 2021)

3. Delivery (Entrega/Inicio da execução): É onde acontece a entrega, o atacante transmite sua arma para o alvo. Ele pode enviar malware, ransomware, spyware, adware e etc. Aqui, os canais de comunicação "usuais" são e-mail(phishing), arquivos para download ou mídia de armazenamento usb.
   Os ataques geralmente são camuflados como arquivos "típicos", como documentos de aplicativos ou faturas. Muitas vezes, erros humanos (por exemplo, pen drives com a inscrição: "Folha de pagamento", "Fotos privadas", ...) são explorados. Mas também sites preparados (waterholing, drive-by download, ...) podem distribuir vírus ocultos ou espalhar arquivos maliciosos.(Ondeso, 2021)

   Potenciais contramedidas: A partir deste nível, você pode se defender ativamente contra ataques pela primeira vez. Para fazer isso, primeiro é necessário analisar quais meios de transmissão são usados para tentativas de intrusão e quais servidores e pessoas são visados. Ao usar os artefatos para preparação do ataque, novas cargas úteis podem ser detectadas no ponto de

transmissão. Além disso, medidas técnicas de proteção para o uso de mídia de armazenamento usb podem aumentar a segurança.(Ondeso, 2021)

4. Exploitation (Exploração de vulnerabilidade): Uma vez que a arma, o malware foi entregue, o código é disparado explorando vulnerabilidades para obter acesso total à sua rede em etapas posteriores. Isso pode ser feito "silenciosamente" apenas escaneando o alvo, mas também pode levar diretamente a uma influência ativa nos sistemas.(Ondeso, 2021)

   Tipos de ataques: DoS, Spoofing, XSS, SQL Injection, Man-in-the-middle, Brute-Force.(Ondeso, 2021)

   Potenciais contramedidas: Patches regulares e varreduras de vulnerabilidades executadas automaticamente em seu próprio hardware e software são essenciais aqui. O treinamento de usuários e os testes de phishing de e-mail para funcionários, bem como o treinamento em desenvolvimento de software seguro, também não devem ser negligenciados. (Ondeso, 2021)

5. Installation (Instalação/Acesso persistente): Depois que o invasor inspecionar e pesquisar seu sistema, ele começará a instalar seu malware, bem como o acesso ao sistema. Os métodos populares incluem a criação de backdoors em programas existentes ou o uso de um shell reverso para executar comandos no dispositivo afetado. A comunicação com o dispositivo pode ocorrer de várias maneiras.(Ondeso, 2021)
   Se o invasor tiver acesso de longo prazo ao seu sistema - isso é conhecido como uma "ameaça persistente avançada" (APT) - é fácil para ele expandir para redes de fornecedores e clientes ou se infiltrar em outras partes de sua própria rede.(Ondeso, 2021)

   Potenciais contramedidas: Aqui, com a ajuda das soluções de segurança implementadas, é necessário reconhecer e registrar os processos de instalação e criar novas medidas de segurança com a ajuda dessas análises. Entender os direitos do administrador ou apenas os direitos do usuário e restringi-los pode tornar alguns ataques mais difíceis.(Ondeso, 2021)

6. Command and control (Comando e controle de forma remota): A arma, o malware permite que o invasor tenha acesso persistente de fora da rede alvo. Os invasores precisam cobrir seus rastros e, neste estágio, muitas vezes deixam rastros falsos, comprometem dados e limpam logs para confundir e / ou desacelerar qualquer equipe forense.(Varonis, 2021)

   Potenciais contramedidas: Nesta fase, você pode tentar impedir a comunicação com servidores conhecidos, por exemplo, desabilitando conexões para botnets ou, conforme mencionado nas etapas anteriores, monitorar seu próprio tráfego ou volume de dados e habilitar alertas quando os limites forem excedidos.

7. Actions on objectives (Alcançando o objetivo/Terminar o ataque): Após o comprometimento do alvo, o atacante executa procedimentos de pós

exploração para atingir seus objetivos, tais como exfiltração de dados, destruição de dados ou criptografia para resgate.

Quanto mais tempo um invasor tem acesso aos sistemas, maior pode ser o impacto. Os exemplos incluem criptografia ou publicação de documentos e sua manipulação. Conforme comprovado no passado por Stuxnet e Co, não apenas os ambientes de escritório, mas também os processos de produção estão em risco, pois podem ser influenciados negativamente de maneira direcionada. Como resultado, não apenas os negócios diários estão ameaçados, mas também toda a existência da empresa pode estar em jogo.

Potenciais contramedidas: Entre outras coisas, o uso de TI forense pode ajudar na avaliação e reconstrução do ataque.

Foto de Mateusz Dach no Pexels

CRÍTICAS A CYBER KILL CHAIN

Entre as críticas ao modelo de cadeia de destruição cibernética da Lockheed Martin como ferramenta de avaliação e prevenção de ameaças está que as primeiras fases acontecem fora da rede defendida, tornando difícil identificar ou defender contra ações nessas fases. Da mesma forma, diz-se que esta metodologia reforça as estratégias tradicionais de defesa baseadas em perímetro e prevenção de malware.

Outros notaram que a cadeia de destruição cibernética tradicional não é adequada para modelar a ameaça interna. Isso é particularmente problemático, dada a

probabilidade de ataques bem-sucedidos que violem o perímetro da rede interna, motivo pelo qual as organizações "precisam desenvolver uma estratégia para lidar com os invasores dentro do firewall. Eles precisam pensar em cada indivíduo da organização com acesso a recursos, como um potencial atacante".(Wikipedia, 2021)

OUTRO PONTO DE VISTA AS CRÍTICAS FEITAS A CYBER KILL CHAIN

O atacante reúne informações sobre o alvo antes do início do ataque. Muitos profissionais de segurança acham que não há nada que possa ser feito sobre esse estágio, mas isso está além do errado. Muitas vezes, os cibercriminosos coletam informações sobre seus alvos pretendidos pesquisando em sites da Internet como LinkedIn ou Instagram. Eles também podem tentar coletar informações por meio de técnicas como ligar para funcionários, interações por e-mail ou mergulhar no lixo.

É aqui que comportamentos seguros podem ter um grande impacto. Uma força de trabalho consciente saberá que eles são um alvo e limitará o que eles compartilham publicamente. Eles autenticam as pessoas por telefone antes de compartilharem informações confidenciais. Eles descartam e fragmentam documentos confidenciais com segurança. Isso neutraliza totalmente esse estágio? Absolutamente não, mas, novamente, nenhum controle é suficiente. No entanto, isso pode prejudicar os recursos do invasor para coletar informações. Uma força de trabalho devidamente treinada pode relatar atividades suspeitas, como telefonemas estranhos que procuram mais informações. (MEDIUM, 2021)

UNIFIED KILL CHAIN

O Unified Kill Chain combina os modelos existentes Cyber Kill Chain da empresa Lockheed Martin e ATT&CK do MITRE.

O MITRE é uma base de conhecimento globalmente acessível de táticas e técnicas hackers com base nas observações do mundo real. O MITRE mantém uma taxonomia de ações hackers conhecidas como MITRE ATT&CK. As táticas da ATT&CK não são ordenadas, pois ficam num um nível de abstração inferior e não descrevem uma cadeia de destruição. A estrutura ATT&CK modela táticas, técnicas e procedimentos usados por hackers com base no mundo real e é um recurso muito útil para red teams, blue teams, purple teams, green teams, yellow teams, orange teams e white teams.

Imagem de https://solvimm.com/blog/os-times-de-seguranca-da-informacao/

Todos esses teams são exemplos de equipes internas ou não, que muitas organizações tem adotado, a fim de estabelecer uma cultura de segurança, como forma de proteger seu ativo mais importante, a informação.

Red Team

O time vermelho é constituído por "hackers autorizados". O papel dele é encontrar vulnerabilidades na aplicação que podem ser exploradas para fins maliciosos. Para isso, esse time usa técnicas de ataque com autorização da organização e mapeia as vulnerabilidades encontradas para serem corrigidas.(Solvimm, 2019)

Blue Team

Enquanto o time vermelho deve atacar a aplicação para expor vulnerabilidades, o time azul tem o papel de defender e antecipar esses ataques. Ele é responsável pela segurança de toda a infraestrutura da organização e tem como funções o mapeamento de riscos, controle de danos, resposta a incidentes e segurança operacional.(Solvimm, 2019)

Yellow Team

Esse é o time dos desenvolvedores, onde suas tarefas envolvem o desenvolvimento seguro de aplicações da própria empresa e de aplicações desenvolvidas por terceiros para a própria empresa. Além de pensar no desempenho do backend e na experiência do usuário alvo.

Purple Team

O time roxo consiste nas interações entre os times vermelho e azul e tem como objetivo maximizar os resultados do time vermelho e melhorar a capacidade de resposta do time azul. Assim, o time roxo integra os resultados dos testes de segurança à capacidade de defesa da organização.(Solvimm, 2019)

Orange Team

Fazem parte desse time as interações entre os times vermelho e amarelo. Essas interações são importantes para educar desenvolvedores a programar com segurança. Como as atividades do time vermelho envolvem atacar a aplicação construída pelo time amarelo e expor vulnerabilidades, as interações entre os dois times tendem a ser reativas: os problemas encontrados pelo time vermelho retornam para o amarelo, que busca resolvê-los.(Solvimm, 2019)

A implementação de um time laranja, no entanto, pressupõe uma atitude mais proativa por parte dos desenvolvedores. Ao aprender com o time vermelho sobre vulnerabilidades que podem ser evitadas a nível de código, menos problemas serão detectados pelos "hackers autorizados" e, consequentemente, menos tempo será gasto pelos dois times.(Solvimm, 2019)

Green Team

Esse time diz respeito à comunicação entre os times amarelo e azul. O seu objetivo é melhorar as defesas baseadas em código e design da aplicação. Isso acontece através do feedback do time azul em relação a aplicação e do compartilhamento de limitações do software por parte do time amarelo. Essas interações ajudam a

identificar vulnerabilidades e montar estratégias de defesa já no início do ciclo de desenvolvimento da aplicação.(Solvimm, 2019)

White Team

O time branco é responsável por manter os padrões de segurança exigidos por auditores internos e externos (PCI, ISO 27001, entre outros) e pelas políticas e requerimentos do negócio. Esse é um time neutro que organiza os demais, planeja e monitora o seu progresso, além de definir regras de engajamento.(Solvimm, 2019)

UNIFIED KILL CHAIN CONTINUAÇÃO...

Voltando ao Unified Kill Chain, ele foi desenvolvido em 2017 por Paul Pols em colaboração com a Fox-IT e Universidade de Leiden para superar críticas comuns contra a Cyber Kill Chain tradicional, a unindo com MITRE ATT&CK framework. A versão unificada da cadeia de destruição é um arranjo ordenado de 18 fases de ataque exclusivas que podem ocorrer num ataque cibernético de ponta a ponta, que abrange atividades que ocorrem fora e dentro da rede defendida. Como tal, a cadeia de destruição unificada melhora as limitações de escopo da cadeia de destruição tradicional(Cyber Kill Chain) e a natureza agnóstica do tempo das táticas no ATT&CK do MITRE. O modelo unificado pode ser usado para analisar, comparar e se defender contra-ataques cibernéticos de ponta a ponta, realizados por ameaças persistentes avançadas (APTs).(Wikipedia, 2021)

As 18 fases do Unified Kill Chain são as seguintes:

1. Reconnaissance (Reconhecimento do alvo): Pesquisar, identificar e selecionar alvos usando reconhecimento ativo ou passivo.
2. Weaponization (Preparação do ataque): Atividades preparatórias destinadas a configurar a infraestrutura necessária para o ataque, ou seja, preparação do armamento de ataque.
3. Delivery (Entrega/Inicio da execução): Técnicas que resultam na transmissão de um objeto armado para o ambiente do alvo.
4. Social Engineering (Engenharia Social): Técnicas que visam a manipulação de pessoas para realizar ações inseguras.
5. Exploitation (Exploração de vulnerabilidade): Técnicas para explorar vulnerabilidades em sistemas que podem, entre outras, resultar na execução de código.
6. Persistence (Persistência): Qualquer acesso, ação ou alteração em um sistema que dê a um invasor presença persistente no sistema.
7. Defense Evasion (Evasão de Defesa): Técnicas que um invasor pode usar especificamente para escapar da detecção ou evitar outras defesas.

8. Command & Control (Comando e controle de forma remota): Técnicas que permitem que os invasores se comuniquem com sistemas controlados em uma rede alvo.

9. Pivoting (Pivotar): Encaminhando o tráfego por meio de um sistema controlado para outros sistemas que não são diretamente acessíveis.

10. Discovery (Descobrir): Técnicas que permitem a um invasor obter conhecimento sobre um sistema e seu ambiente de rede.

11. Privilege Escalation (Escalar privilégio): O resultado de técnicas que fornecem a um invasor permissões mais altas em um sistema ou rede.

12. Execution (Execução): Técnicas que resultam na execução de código controlado pelo invasor em um sistema local ou remoto.

13. Credential Access (Credencial de acesso): Técnicas que resultam no acesso ou controle sobre credenciais de sistema, serviço ou domínio.

14. Lateral Movement (Movimento lateral): Técnicas que permitem a um adversário acessar e controlar horizontalmente outros sistemas remotos.

15. Collection (Coleção): Técnicas usadas para identificar e coletar dados de uma rede de destino antes da exfiltração.

16. Exfiltration (Exfiltração): Técnicas que resultam ou ajudam um invasor a remover dados de uma rede alvo.

17. Impact (Impacto): Técnicas destinadas a manipular, interromper ou destruir o sistema ou dados de destino.

18. Objectives (Objetivos): Objetivos sociotécnicos de um ataque que visam atingir um objetivo estratégico.

A Unified Kill Chain pode ser usada para analisar, comparar e se defender contra alvos e ataques cibernéticos não direcionados. Pesquisas mostram que o tradicional Cyber Kill Chain, conforme apresentado por pesquisadores da Lockheed Martin, é focado em perímetro e malware. Como tal, o modelo tradicional falha em cobrir outros vetores de ataque e ataques que ocorrem atrás do perímetro organizacional. A cadeia de destruição unificada oferece melhorias significativas sobre essas limitações de escopo do Cyber Kill Chain e a natureza agnóstica do tempo das táticas no modelo ATT&CK do MITRE.(Unifiedkillchain, 2021)

Outras melhorias sobre esses modelos incluem: explicar o papel dos usuários ao modelar a engenharia social, reconhecendo o papel crucial de pontos de estrangulamento em ataques modelando pivot, cobrindo o compromisso de integridade e disponibilidade, além de confidencialidade e elucidação de objetivos abrangentes dos invasores.(Unifiedkillchain, 2021)

Os tipos de invasores podem variar de grupos de ransomware empresariais com motivação financeira, até espionagem e sabotagem por estados-nação. O modelo Unified kill chain também foi aplicado com sucesso na defesa contra worms

ransomware, que implementam táticas que antes eram vistas principalmente em ataques direcionados.(Unifiedkillchain, 2021)

A cadeia de destruição unificada oferece uma base comprovada para realinhar estrategicamente as capacidades defensivas e investimentos em segurança cibernética dentro das organizações, nas áreas de prevenção, detecção, resposta e inteligência. A cadeia de destruição unificada permite uma análise estruturada e comparação de ameaças, inteligência sobre o modus operandi tático dos atacantes.(Unifiedkillchain, 2021)

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	√	✖	√
Weaponization	√	✖	√
Delivery	√	√	√
Social Engineering	✖	✖	√
Exploitation	√	✖	√
Persistence	√	√	√
Defense Evasion	✖	√	√
Command & Control	√	√	√
Pivoting	✖	✖	√
Discovery	✖	√	√
Privilege Escalation	✖	√	√
Execution	✖	√	√
Credential Access	✖	√	√
Lateral Movement	✖	√	√
Collection	✖	√	√
Exfiltration	✖	√	√
Impact	✖	√	√
Objectives	√	✖	√

Imagem de https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

Obrigado!

Muito obrigado por ter lido este artigo, espero que tenha sido de grande importância para você e de alguma forma tenha te ajudado na sua jornada. Para saber mais, me siga nas redes sociais e faça parte da nossa comunidade backendcore no discord, colabore com ideias, dúvidas, sugestões ou puxe um papo lá. Sucesso e até breve!

Próximo relatório sobre ataque hacker a ser lançado. Fique de olho na sua construção em nossa comunidade no discord, e saiba quando estará disponível para download no link a seguir: https://github.com/pinheiro-felipe/ataque-hacker/blob/main/2-Fase-de-reconhecimento.pdf

Autor: Felipe Pinheiro

Site: https://backendcore.io

E-mail: contato@backendcore.io

Redes Sociais:

Instagram: https://www.instagram.com/backendcore/

Youtube canal BackEndCore:
https://www.youtube.com/channel/UCNgwVnEvdOvA5hgpajiC_3g

Github: https://github.com/pinheiro-felipe

Facebook: https://www.facebook.com/backendcore

Linkedin: https://www.linkedin.com/in/pinheirofelipe/

Podcast: https://anchor.fm/backendcore

Entre em nossa comunidade backendcore, acompanhe a criação de todos os relatórios e troque ideias. Você é muito bem-vindo(a):
https://discord.gg/N95HY5YSAj

REFERÊNCIAS

[1] Fil, Jonatas. Cyber Kill Chain e MITRE ATT&CK. Linkedin, 11 de março 2020. Disponível em: <https://www.linkedin.com/pulse/cyber-kill-chain-e-mitre-attck-jonatas-fil/?originalSubdomain=pt>. Acesso em: 02 de setembro de 2021

[2] W. Greenert, Jonathan. Kill Chain Approach. Web.archive, 23 de abril de 2013. Disponível em:<https://web.archive.org/web/20130613233413/http://cno.navylive.dodlive.mil/2013/04/23/kill-chain-approach-4/>. Acesso em: 02 de setembro de 2021

[3] wikipedia, 11 de agosto de 2021 Disponível em: <https://en.wikipedia.org/wiki/Kill_chain>. Acesso em: 02 de setembro de 2021

[4] Chociai, Aroldo. O que é e como funciona a metodologia Cyber Kill Chain?, 16 de fevereiro de 2018. Disponível em: <http://labs.siteblindado.com/2018/02/o-que-e-e-como-funciona-metodologia.html>. Acesso em: 03 de setembro de 2021

[5] The Cyber Kill Chain: 7 steps to increase your security maturity level. Ondeso, 12 de abril de 2021. Disponível em: <https://www.ondeso.com/en/article/cyber-kill-chain/>. Acesso em: 03 de setembro de 2021

[6] Hospelhorn, Sarah. What is The Cyber Kill Chain and How to Use it Effectively. Varonis, 29 de março de 2020. Disponível em: <https://www.varonis.com/blog/cyber-kill-chain/>. Acesso em: 03 de setembro de 2021

[7] Renovaci, Rafael. Analise de Malwares — Cyber Kill Chain Model. Medium, 19 de abril de 2020. Disponível em: <https://medium.com/@rafaelrenovaci/analise-de-malwares-cyber-kill-chain-model-ef7bc245ba78>. Acesso em: 06 de setembro de 2021

[8] Martin, Lockheed. Gaining the advantage - Applying Cyber Kill Chain Methodology to Network Defense. Lockheed Martin, 2015. Disponível em: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>. Acesso em: 06 de setembro de 2021

[9] Pols, Paul. The Unified Kill Chain - Raising Resilience against advanced cyber attacks through attack modeling. Unifiedkillchain, 2021. Disponível em: <https://www.unifiedkillchain.com/>. Acesso em: 11 de setembro de 2021

[10] Solvimm. Os times de Segurança da Informação. Solvimm, 2019. Disponível em: <https://solvimm.com/blog/os-times-de-seguranca-da-informacao>. Acesso em: 12 de setembro de 2021

[11] Pols, Paul. The Unified Kill Chain - Raising Resilience against advanced cyber attacks. Unifiedkillchain, 2021. Disponível em: <https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf>. Acesso em: 12 de setembro de 2021