



Módulo 1: O Perigo

Material do instrutor

CyberOps Associate v1.0





Módulo 1: o perigo

CyberOps Associate v1.0



Objetivos do módulo

Título do módulo: O perigo

Objetivo do módulo: explicar por que redes e dados são atacados.

| Título do Tópico | Objetivo do Tópico |
|---------------------|--|
| Histórias de guerra | Explicar por que as redes e os dados são atacados. |
| Agentes da ameaça | Explicar as motivações dos agentes de ameaças por trás de incidentes de segurança específicos. |
| Impacto de ameaça | Explicar o possível impacto dos ataques de segurança de rede. |

1.1 Histórias de guerra

Pessoas sequestradas

- Os *hackers* podem configurar *hotspots* sem fio “invasores” abertos, fingindo ser uma rede sem fio genuína.
- Os *hotspots* sem fio invasores também são conhecidos como *hotspots* “gêmeos malvados” (*Evil Twin*)



Empresas Chantageadas

- Funcionários de uma organização são muitas vezes atraídos para abrir anexos que instalam *ransomwares* nos computadores dos funcionários.
- Este *ransomware*, quando instalado, inicia o processo de coleta e criptografia de dados corporativos.
- O objetivo dos atacantes é o ganho financeiro, porque eles mantêm os dados da empresa para resgate até serem pagos.
- O WannaCry afetou 230 mil computadores em todo o mundo. O ataque atingiu um terço de todos os hospitais do Serviço Nacional de Saúde (NHS, *National Health Service*) do Reino Unido, causando danos estimados em 92 milhões de libras. Os usuários foram bloqueados e foi exigido um resgate em bitcoins.



O perigo das nações alvejadas

- Alguns dos *malwares* atuais são tão sofisticados e caros para criar que especialistas em segurança acreditam que apenas um estado-nação ou grupo de nações poderia possivelmente ter a influência e o financiamento para criá-lo.
- Esse *malware* pode ser direcionado para atacar a infraestrutura vulnerável de uma nação, como o sistema de água ou a rede elétrica.
- Um desses malwares foi o *worm* Stuxnet que infectou unidades USB e se infiltrou nos sistemas operacionais Windows. Ele então direcionou o software Step 7 que foi desenvolvido pela Siemens para seus Controladores Lógicos Programáveis (PLCs).



Vídeo de Perigo - Anatomia de um Ataque

Assista a este vídeo para ver detalhes de um ataque complexo.



1.2 Agentes de ameaças

Atores de Ameaça

- Os atores de ameaças são indivíduos ou grupos de indivíduos que realizam ataques cibernéticos. Eles incluem, mas não estão limitados a:
 - Amadores
 - Hacktivistas
 - Grupos de crime organizado
 - Grupos patrocinados pelo estado
 - Grupos terroristas
- Os ataques cibernéticos são atos maliciosos intencionais destinados a impactar negativamente outro indivíduo ou organização.

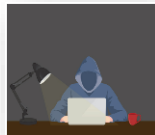


Atores Ameaças (Cont.)



Amadores

- Eles também são conhecidos como crianças de roteiro e têm pouca ou nenhuma habilidade.
- Eles costumam usar ferramentas existentes ou instruções encontradas na Internet para lançar ataques.
- Mesmo que usem ferramentas básicas, os resultados ainda podem ser devastadores.



Hacktivistas

- Estes são hackers que protestam publicamente contra uma variedade de ideias políticas e sociais.
- Eles publicam artigos e vídeos, vazando informações confidenciais e interrompendo serviços da Web com tráfego ilegítimo em ataques de DDoS (Distributed Denial of Service).



Ganho financeiro

- Grande parte da atividade de hacking que ameaça constantemente a nossa segurança é motivada por ganhos financeiros.
- Os cibercriminosos querem ter acesso a contas bancárias, dados pessoais e qualquer outra coisa que possam alavancar para gerar fluxo de caixa.



Segredos Comerciais e Política Global

- Às vezes, os Estados-nação invadem outros países, ou interferem com sua política interna.
- Muitas vezes, eles podem estar interessados em usar o ciberespaço para espionagem industrial.
- O roubo de propriedade intelectual pode dar a um país uma vantagem significativa no comércio internacional.

Quão segura é a Internet das Coisas?

- A Internet das Coisas (IoT) ajuda os indivíduos a conectarem coisas para melhorar sua qualidade de vida.
- Muitos dispositivos na internet não são atualizados com o firmware mais recente. Alguns dispositivos mais antigos nem foram desenvolvidos para serem atualizados com *patches*. Essas duas situações criam oportunidades para atores de ameaças e riscos de segurança para os proprietários desses dispositivos.



Lab - Aprenda os detalhes dos ataques

Neste laboratório, você pesquisará e analisará vulnerabilidades de aplicativos IoT.

Usando seu mecanismo de pesquisa favorito, realize uma pesquisa de vulnerabilidades da Internet das Coisas (IoT). Durante a pesquisa, encontre um exemplo de vulnerabilidade de IoT para cada uma das verticais de IoT: indústria, sistemas de energia, saúde e governo. Esteja preparado para discutir quem pode explorar a vulnerabilidade e o porquê, o que causou a vulnerabilidade e o que pode ser feito para limitar a vulnerabilidade.

1.3 Impacto das ameaças

PII de impacto de ameaças, PHI e PSI

- Informações Pessoais Identificáveis (PII) são todas as informações que podem ser usadas para identificar positivamente um indivíduo, por exemplo, nome, número de seguro social, data de nascimento, números de cartão de crédito, CPF etc.
- Os cibercriminosos têm como objetivo obter essas listas de PII que podem ser vendidas na *dark web*. As PII roubadas podem ser usadas para criar contas financeiras falsas, como cartões de crédito e empréstimos de curto prazo.
- A comunidade médica cria e mantém Registros Médicos Eletrônicos (EMRs) que contêm Informações de Saúde Protegidas (PHI), um subconjunto de PII.
- As Informações de Segurança Pessoal (PSI), outro tipo de PII, incluem nomes de usuário, senhas e outras informações relacionadas à segurança que os indivíduos usam para acessar informações ou serviços na rede.



Vantagem Competitiva Perdida

- A perda de propriedade intelectual para os concorrentes é uma séria preocupação.
- Uma grande preocupação adicional é a perda de confiança que ocorre quando uma empresa é incapaz de proteger os dados pessoais de seus clientes.
- A perda de vantagem competitiva pode resultar dessa perda de confiança em vez de outra empresa ou país roubar segredos comerciais.

Política de impacto de ameaças e segurança nacional

- Não são só as empresas que são hackeadas.
- *Hackers* apoiados pelo Estado podem causar interrupção e destruição de serviços e recursos vitais dentro de uma nação inimiga.
 - Energia Elétrica
 - Aeroportos
 - Abastecimento de água
 - Sistemas de comunicação
 - Segurança pública
- A Internet tornou-se essencial como meio de atividades comerciais e financeiras. A interrupção dessas atividades pode devastar a economia de uma nação.

Laboratório de impacto de ameaças - Visualizando os Black Hats

Neste laboratório, você pesquisará e analisará incidentes de segurança cibernética para criar cenários destacando como as organizações podem prevenir ou mitigar um ataque.

1.4 O resumo dos perigos

O que aprendi neste módulo?

- Os atores de ameaças podem sequestrar sessões bancárias e outras informações pessoais usando hotspots “gêmeos malvados”.
- Os atores de ameaças incluem, entre outros, amadores, hacktivistas, grupos do crime organizado, patrocinados pelo Estado e grupos terroristas.
- À medida que a Internet das Coisas (IoT) se expande, webcams, roteadores e outros dispositivos em nossas casas também estão sob ataque.
- Informações Pessoais Identificáveis (PII) são todas as informações que podem ser usadas para identificar positivamente um indivíduo.
- A comunidade médica cria e mantém Registros Médicos Eletrônicos (EMRs) que contêm Informações de Saúde Protegidas (PHI), um subconjunto de PII.
- As Informações de Segurança Pessoal (PSI) incluem nomes de usuário, senhas e outras informações relacionadas à segurança que os indivíduos usam para acessar informações ou serviços na rede.

Novos Termos

| | | |
|--|---|--|
| <ul style="list-style-type: none">• Evil twin hotspots• Programmable Logic Controllers (PLCs)• Threat Actors• Hacktivists• Cyberattacks• Distributed Denial of Service (DDoS) | <ul style="list-style-type: none">• Internet of Things (IoT)• Personally Identifiable Information (PII)• Protected Health Information (PHI)• Electronic Medical Records (EMRs) | <ul style="list-style-type: none">• Health Insurance Portability and Accountability Act (HIPAA)• General Data Protection Regulation (GDPR)• Personal security information (PSI)• Cyberwarfare |
|--|---|--|

1.5 Referências

Referências

- <https://www.kaspersky.com.br/resource-center/preemptive-safety/evil-twin-attacks>
- <https://secportfolio.com/custom-bluetooth-evil-twin-attack/>
- <https://spectrum.ieee.org/the-real-story-of-stuxnet>
- <https://pt.linkedin.com/pulse/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-davi-becker>

