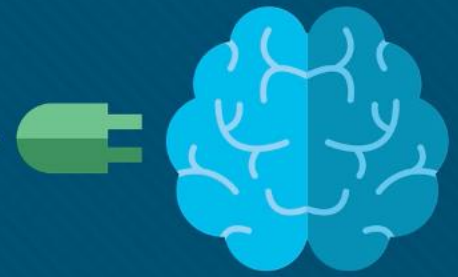

Módulo 2: Ataques, Conceitos e Técnicas

Introdução à Cibersegurança

Objetivos do Módulo

Título do Módulo: Ataques, Conceitos e Técnicas

Objetivo do Módulo: Explicar as ameaças, ataques e vulnerabilidades cibernéticas mais comuns.

Título do Tópico	Objetivo do Tópico
Analisando um ataque cibernético	Identificar os diferentes tipos de malware e seus sintomas.
Métodos de infiltração	Descrever os diferentes métodos de infiltração.
Exploits e vulnerabilidade de segurança	Explicar como encontrar as vulnerabilidades de segurança.
O cenário da Segurança Cibernética	Explicar como categorizar as vulnerabilidades de segurança.

2.1 Análise de um Ataque Cibernético

Tipos de Malware

- Os criminosos digitais usam muitos tipos diferentes de software mal-intencionado, ou malware, para realizar suas atividades. O uso de malware refere-se a qualquer código que possa roubar dados, burlar controles de acesso ou causar danos ou comprometer um sistema. Conhecer os diferentes tipos e como eles se espalham é fundamental para contê-los e removê-los.

Spyware:

- O spyware monitora sua atividade online e pode registrar cada tecla que você pressiona no teclado e capturar quase todos os seus dados, incluindo informações pessoais confidenciais, como dados bancários online. O objetivo dele é rastrear e espionar você. O spyware faz isso modificando as configurações de segurança dos dispositivos.

- Muitas vezes, o spyware se junta ao software legítimo ou a cavalos de Troia.

Tipos de Malware (continuação)

Adware:

- Freqüentemente o adware é instalado junto com algumas versões de software e seu objetivo é entregar anúncios automaticamente a um usuário, geralmente em um navegador da web. Você sabe quando vê! É difícil ignorar quando você enfrenta anúncios pop-up constantes na tela.
- É comum o adware vir com spyware.

Backdoor:

- Este malware obtém acesso não autorizado, ignorando os procedimentos normais de autenticação, para acessar um sistema. Como resultado, os hackers podem acessar recursos de dentro de um aplicativo e emitir comandos remotos de sistema.
- Um backdoor funciona em segundo plano e é difícil de detectar.

Tipos de Malware (continuação)

Ransomware:

- O projeto desse malware é manter como refém um sistema de computador ou os dados que ele contém até que seja feito um pagamento. O ransomware geralmente criptografa as informações para que você não possa acessá-las.
- Algumas versões de ransomware podem tirar proveito de vulnerabilidades específicas do sistema para bloqueá-lo. O ransomware é frequentemente disseminado por e-mails de phishing que o incentivam a baixar um anexo mal-intencionado ou uma vulnerabilidade de software.

Scareware:

- Este tipo de malware usa táticas de “sustos” para induzi-lo a realizar uma ação específica. O scareware consiste principalmente em janelas do tipo sistema operacional que avisam que seu sistema está em risco e precisa executar um programa específico para retornar à operação normal.
- Se você concordar em executar o programa específico, seu sistema será infectado por malware.

Tipos de Malware (continuação)

Rootkit:

- O objetivo desse malware é modificar o sistema operacional para criar um backdoor, que os invasores podem usar para acessar seu computador remotamente. A maioria dos rootkits usa vulnerabilidades de software para acessar recursos que não deveriam estar acessíveis (escalonamento de privilégios) e modificar arquivos do sistema.
- Os Rootkits também podem modificar as ferramentas forenses e de monitoramento do sistema, tornando-os muito difíceis de detectar. Se um rootkit infectar um computador, formate o computador e reinstale qualquer software necessário.

Tipos de Malware (continuação)

Vírus:

- Um vírus é um programa de computador que, quando executado, se replica e se anexa a outros arquivos executáveis, como um documento, inserindo seu código. A maioria dos vírus exige a interação do usuário final para iniciar a ativação e pode agir em uma data ou hora específica.
- Os vírus, como aqueles que exibem uma imagem engraçada, podem ser relativamente inofensivos. Ou podem ser destrutivos, como os que modificam ou excluem dados.
- Os vírus também podem ser programados para se modificar e evitar a detecção. Unidades USB, discos ópticos, compartilhamentos de rede ou e-mail espalham a maioria dos vírus.

Cavalo de Tróia

- Esse malware realiza operações mal-intencionadas mascarando sua verdadeira intenção. Parece legítimo, mas é muito perigoso. Os cavalos de Troia exploram os privilégios do usuário, e é comum encontrá-los em arquivos de imagem, arquivos de áudio ou jogos.
- Ao contrário dos vírus, os cavalos de Troia não se replicam automaticamente, mas agem como iscas para que o software malicioso passe despercebido pelos usuários desavisados.

Tipos de Malware (continuação)

Worms:

- Esse tipo de malware se replica para se espalhar de um computador para outro. Ao contrário de um vírus, que requer um programa hospedeiro, os worms podem ser executados sozinhos. Além da infecção inicial do host, eles não exigem a participação do usuário e podem se espalhar rapidamente pela rede.
- Os worms compartilham padrões semelhantes: eles exploram vulnerabilidades do sistema, têm uma maneira de se propagar e todos contêm código malicioso (carga útil) para causar danos a sistemas ou redes de computadores.
- Os worms são responsáveis por alguns dos ataques mais devastadores na Internet. Em 2001, o worm Code Red infectou mais de 300.000 servidores em apenas 19 horas.

Sintomas de Malware

Independentemente do tipo de malware que infecta um sistema, você pode observar alguns sintomas comuns. Isso inclui:

- um aumento no uso da unidade de processamento central (CPU), o que torna o dispositivo mais lento
- seu computador congelando ou travando frequentemente
- uma diminuição na velocidade de navegação na web
- problemas inexplicáveis com suas conexões de rede
- arquivos modificados ou excluídos
- a presença de arquivos, programas ou ícones desconhecidos na área de trabalho
- processos desconhecidos em execução
- programas desligando ou se reconfigurando
- envio e-mails sem o seu conhecimento ou consentimento.

2.2 Métodos de Infiltração

Engenharia Social

- A engenharia social está manipulando as pessoas para que realizem ações ou divulguem informações confidenciais. Os engenheiros sociais frequentemente contam com a disposição das pessoas em serem prestativas, mas também exploram suas fraquezas.
- Por exemplo, um invasor poderá ligar para um funcionário autorizado com um problema urgente que exija acesso imediato à rede e apelará à vaidade ou ganância do funcionário ou invocará autoridade usando técnicas de menção de nomes para obter esse acesso.

Pretexting

- É quando um invasor liga para um indivíduo e mente para obter acesso a dados confidenciais.
- Por exemplo, fingir que precisa dos dados pessoais ou financeiros de uma pessoa para confirmar a sua identidade.

Engenharia Social (Cont.)

- **Tailgating (seguir de perto)**
  - Isso ocorre quando um invasor segue rapidamente uma pessoa autorizada até um local físico seguro.

- **Algo por algo (Quid pro quo)**
  - É quando um invasor solicita informações pessoais de alguém em troca de algo, como um presente.

Negação de Serviço (DoS)

Os ataques de negação de serviço (DoS) são um tipo de ataque de rede que é relativamente simples de ser realizado, mesmo por um atacante sem habilidades avançadas. Um ataque DoS resulta em alguma interrupção do serviço de rede para usuários, dispositivos ou aplicativos.

Quantidade Esmagadora de Tráfego

- Isso ocorre quando uma rede, host ou aplicativo envia uma enorme quantidade de dados a uma taxa que não consegue suportar. Isso causa uma transmissão ou resposta lenta ou faz com que o dispositivo ou serviço trave.

Pacotes formatados maliciosamente

- Um pacote é uma coleta de dados que flui entre uma fonte e um computador receptor ou aplicativo através de uma rede, como a Internet. Ao enviar um pacote formatado maliciosamente, o destinatário não consegue lidar com ele.
- Por exemplo, suponha que um invasor encaminhe pacotes contendo erros ou pacotes formatados incorretamente que um aplicativo não consegue identificar. Nesse caso, isso fará com que o dispositivo receptor funcione muito lentamente ou trave.

DoS Distribuída

Um ataque de Negação de Serviço Distribuído (DDoS) é semelhante a um ataque de Negação de Serviço (DoS), mas tem origem em múltiplas fontes coordenadas. Por exemplo:

- Um invasor constrói uma rede (botnet) de hosts infectados chamados zumbis, controlados por sistemas manipuladores.
- Os computadores zumbis examinam e infectam constantemente mais hosts, criando mais zumbis.
- Quando está pronto, o hacker instrui os sistemas controlador para fazer com que o botnet de zumbis execute um ataque de negação de serviço distribuído (DDoS).

Botnet

- Um computador bot normalmente é infectado ao visitar um site inseguro ou abrir um anexo de e-mail ou arquivo de mídia infectado. Uma botnet é um grupo de bots conectados pela Internet que um indivíduo ou grupo mal-intencionado pode controlar. Pode ter dezenas de milhares ou mesmo centenas de milhares de bots que, normalmente, são controlados por um servidor de comando e controle.

- A ativação desses bots distribui malware, lança ataques DDoS, distribui e-mails de spam ou executa ataques de força bruta de senha. Os cibercriminosos freqüentemente alugam botnets para terceiros para fins nefastos.

- Muitas organizações, como a Cisco, direcionam as atividades de rede através de filtros de tráfego de botnets para identificar possíveis localizações de botnets.

Botnet (cont.)

1. Os bots infectados tentam se comunicar com um host de comando e controle na Internet.

2. O filtro de botnet do Cisco Firewall é um recurso que detecta o tráfego proveniente de dispositivos infectados com o código mal-intencionado do botnet.

3. O serviço Cisco Security Intelligence Operations (SIO) na nuvem envia os filtros atualizados para o firewall, que corresponde ao tráfego de novos botnets conhecidos.

4. Os alertas vão para a equipe de segurança interna da Cisco para notificá-los sobre os dispositivos infectados que geram tráfego malicioso, para que possam prevenir, mitigar e remediar.

Ataques On-Path

- Os invasores no caminho interceptam ou modificam as comunicações entre dois dispositivos, como um navegador da Web e um servidor da Web, para coletar informações ou se passar por um dos dispositivos.

- Esse tipo de ataque se refere a um ataque do tipo "man-in-the-middle" ou "man-in-the-mobile".

Man-in-the-middle

- Um ataque de MitM acontece quando um criminoso digital assume o controle de um dispositivo sem o conhecimento do usuário. Com esse nível de acesso, um invasor pode interceptar e capturar informações do usuário antes de enviá-las ao destino pretendido. O uso desses tipos de ataques geralmente rouba informações financeiras.
- Existem muitos tipos de malware que possuem recursos de ataque de MitM.

Ataques On-Path (Cont.)

Man-in-the-Mobile

- Uma variação do man-in-middle, MitMo é um tipo de ataque usado para assumir o controle do dispositivo móvel de um usuário. Quando infectado, as instruções do dispositivo móvel exfiltram informações sensíveis do usuário e as enviam para os atacantes. O ZeuS é um exemplo de pacote de malware com recursos MitMo. Ele permite que os invasores capturem mensagens SMS de verificação em duas etapas enviadas aos usuários silenciosamente.

Envenenamento de SEO

- Você provavelmente já ouviu falar de otimização de mecanismos de pesquisa ou SEO, que consiste em melhorar o site de uma organização para obter maior visibilidade nos resultados de pesquisas.

- Mecanismos de pesquisa como o Google funcionam apresentando uma lista de páginas da web aos usuários com base em suas consultas de pesquisa. Essas páginas da web são classificadas de acordo com a relevância de seu conteúdo.

- Embora muitas empresas legítimas se especializem na otimização de sites para melhor posicioná-los, os invasores aproveitam termos de pesquisa populares e usam SEO para empurrar sites maliciosos para uma posição mais elevada nos resultados de pesquisa. Esta técnica é chamada de SEO poisoning.

- O objetivo mais comum do SEO poisoning é aumentar o tráfego para sites maliciosos que podem hospedar malware ou tentar engenharia social.

Ataques de Senha

Inserir um nome de usuário e senha é uma das formas mais populares de autenticação em um site. Portanto, descobrir a senha é uma maneira fácil para os criminosos digitais obterem acesso às informações mais importantes.

Pulverização de senha:

- Esta técnica tenta obter acesso a um sistema 'dispersando' algumas senhas comumente usadas em muitas contas. Por exemplo, um criminoso digital usa 'Password123' com muitos nomes de usuário antes de tentar novamente com uma segunda senha comumente usada, como 'qwerty'.
- Essa técnica permite que o perpetrador permaneça sem ser detectado e evite bloqueios frequentes de contas.

Ataques de dicionário:

- Um hacker tenta sistematicamente cada palavra de um dicionário ou de uma lista de palavras comumente usadas como senha para invadir uma conta protegida por senha.

Ataques a Senhas (Continuação)

Ataques de força bruta

- A maneira mais simples e comumente usada de obter acesso a um site protegido por senha, os ataques de força bruta fazem com que um invasor use todas as combinações possíveis de letras, números e símbolos no espaço da senha até acertar.

Ataques Rainbow

- As senhas em um sistema de computador não são armazenadas como texto simples, mas como valores hash (valores numéricos que identificam os dados de maneira exclusiva). Uma tabela de Rainbow funciona como um extenso dicionário de hashes e senhas pré-computadas.
- Ao contrário de um ataque de força bruta que precisa calcular cada hash, um ataque do arco-íris compara o hash de uma senha com os armazenados na tabela do arco-íris. Quando um invasor encontra uma correspondência, ele identifica a senha usada para criar o hash.

Ataques a Senhas (Continuação)

Interceptação de tráfego

- Ao interceptar comunicações, outros humanos e máquinas podem ler facilmente texto simples ou senhas não criptografadas.
- Se você armazenar uma senha em texto claro e legível, qualquer pessoa que tenha acesso à sua conta ou dispositivo, autorizado ou não autorizado, poderá lê-la.

Ameaças Persistentes Avançadas

- Os invasores também conseguem infiltração por meio de ameaças persistentes avançadas (APTs) — uma operação multifásica, de longo prazo, furtiva e avançada contra um alvo específico. Por essas razões, um invasor individual muitas vezes não possui o conjunto de habilidades, recursos ou persistência para executar APTs.

- Devido à complexidade e ao nível de habilidade necessários para realizar tal ataque, uma APT é geralmente bem financiada e tem como alvo organizações ou nações por razões comerciais ou políticas.

- Seu objetivo principal é implantar malware personalizado em um ou mais sistemas do alvo e permanecer lá sem ser detectado.

2.3 Exploits e Vulnerabilidade de Segurança

Vulnerabilidades de Hardware/fusão e Espectro

As vulnerabilidades de hardware são geralmente o resultado de falhas de design de hardware.

- Por exemplo, o tipo de memória chamada RAM consiste em muitos capacitores (um componente que pode acumular carga elétrica) instalados muito próximos uns dos outros.
- Porém, devido à sua proximidade, alterações aplicadas a um desses capacitores podem influenciar os capacitores vizinhos.
- Essa falha de design cria uma exploração chamada Rowhammer. Ao acessar repetidamente (hammering - martelar) uma linha de memória, o exploit Rowhammer desencadeia interferências elétricas que, eventualmente, corrompem os dados armazenados na RAM.

Vulnerabilidades de Hardware Meltdown e Spectre (continuação)

Meltdown e Spectre

- Os pesquisadores de segurança do Google descobriram o Meltdown e o Spectre, duas vulnerabilidades de hardware que afetam quase todas as unidades centrais de processamento (CPUs) lançadas desde 1995 em desktops, laptops, servidores, smartphones, dispositivos inteligentes e serviços em nuvem.

- Os invasores que exploram essas vulnerabilidades podem ler toda a memória de um determinado sistema (Meltdown) e dados manipulados por outros aplicativos (Spectre). As explorações das vulnerabilidades Meltdown e Spectre referem-se a ataques de canal lateral (a implementação de um sistema de computador obtém informações). Essas vulnerabilidades podem comprometer grandes quantidades de dados na memória devido ao grande número de vezes que os ataques são executados em um sistema, com mínima possibilidade de falhas ou outros erros.

Vulnerabilidades de Software

- Erros no sistema operacional ou no código do aplicativo geralmente introduzem **vulnerabilidades de software**.

- A vulnerabilidade SYNful Knock permitiu que os invasores ganhassem o controle de roteadores de nível empresarial, como os roteadores Cisco ISR antigos, dos quais poderiam monitorar toda a comunicação de rede e infectar outros dispositivos de rede.

- Quando uma versão alterada do IOS é instalada nos roteadores, essa vulnerabilidade é introduzida no sistema. Para evitar isso, sempre verifique a integridade da imagem do IOS baixada e limite o acesso físico do equipamento somente ao pessoal autorizado.

Categorizando Vulnerabilidades de Software

A maioria das vulnerabilidades de segurança de software se enquadra em várias categorias principais.

Buffer Overflow:

- Os buffers são áreas de memórias alocadas a um aplicativo. Ao gravar dados além dos limites de um buffer, ocorre uma vulnerabilidade. Ao alterar os dados além dos limites de um buffer, o aplicativo pode acessar a memória alocada para outros processos. Isso pode levar à queda do sistema, comprometimento de dados ou fornecer o escalonamento de privilégios.

Categorizando Vulnerabilidades de Software (Cont.)

Entrada não validada

- Programas frequentemente necessitam de entrada, mas esses dados recebidos podem conter conteúdo malicioso que, inadvertidamente, faz o programa se comportar de maneira inesperada ou prejudicial.
- Por exemplo, considere um programa que recebe uma imagem para processamento. Um usuário mal-intencionado pode criar um arquivo de imagem com dimensões de imagem inválidas. As dimensões criadas de forma mal-intencionada podem forçar o programa a alocar buffers de tamanhos incorretos e inesperados.

Condições de corrida:

- Esta vulnerabilidade descreve uma situação em que a saída de um evento depende de saídas ordenadas ou cronometradas. Uma condição de corrida tornou-se uma fonte de exposição quando os eventos ordenados ou cronometrados exigidos não ocorreram na ordem correta ou no momento adequado.

Categorizando Vulnerabilidades de Software (Cont.)

Fraquezas nas práticas de segurança:

- Autenticação, autorização e criptografia protegem sistemas e dados confidenciais. Os desenvolvedores devem usar técnicas e bibliotecas de segurança que já foram criadas, testadas e verificadas e não devem tentar criar seus algoritmos de segurança. É provável que elas introduzam novas vulnerabilidades.

Problemas de controle de acesso:

- O controle de acesso é o processo de controlar quem faz o quê e abrange desde o gerenciamento do acesso físico ao equipamento até ditar quem tem acesso a um recurso, como um arquivo, e o que pode ser feito com ele, como ler ou alterar o arquivo. O uso indevido de controles de acesso cria muitas vulnerabilidades de segurança.
- Quase todos os controles de acesso e as práticas de segurança poderão ser superados se o invasor tiver acesso físico ao equipamento de destino. Por exemplo, não importa as configurações de permissão em um arquivo, um hacker pode ignorar o sistema operacional e ler os dados diretamente do disco.

Atualizações de Software

- O objetivo das atualizações de software é manter-se atualizado e evitar a exploração de vulnerabilidades. Microsoft, Apple e outros produtores de sistemas operacionais lançam patches e atualizações diariamente. As empresas ou organizações, responsáveis por eles, atualizam aplicativos, como navegadores da web, aplicativos móveis e servidores web.

- Embora as organizações se esforcem muito para encontrar e corrigir vulnerabilidades de software, elas descobrem novas vulnerabilidades regularmente. Por isso, algumas organizações utilizam pesquisadores de segurança terceirizados especializados em encontrar vulnerabilidades em software, ou investem em suas próprias equipes de teste de penetração dedicadas a buscar, identificar e corrigir vulnerabilidades de software antes que possam ser exploradas.

- O Projeto Zero do Google é um excelente exemplo dessa prática. Depois de descobrir diversas vulnerabilidades em diversos softwares usados pelos usuários finais, o Google formou uma equipe permanente dedicada a encontrar vulnerabilidades de software. Você pode descobrir mais sobre a pesquisa de segurança do Google aqui.

2.4 O Cenário de Segurança Cibernética

Criptomoeda

- Criptomoeda é dinheiro digital usado para comprar bens e serviços, usando fortes técnicas de criptografia para proteger transações online. Bancos, governos e até empresas como a Microsoft e a AT&T estão muito conscientes da sua importância e estão aderindo ao movimento das criptomoedas!

- Os proprietários de moedas criptografadas guardam seu dinheiro em “carteiras” virtuais e criptografadas. Quando ocorre uma transação entre os proprietários de duas carteiras digitais, os detalhes são registrados em um sistema descentralizado, um registro eletrônico ou blockchain. Isso significa que é realizado de forma anônima e é autogerenciado, sem interferência de terceiros, como bancos centrais ou entidades governamentais.

Criptomoeda (cont.)

- Computadores especiais coletam dados sobre as últimas transações de criptomoedas a cada dez minutos, transformando-os em desafios matemáticos para manter a confidencialidade.
- A verificação destas transações passa por um processo técnico e altamente complexo conhecido como “mineração”. Esta etapa normalmente envolve um exército de “mineradores” trabalhando em PCs de última geração para resolver desafios matemáticos e autenticar transações.
- Uma vez verificado, o registro é atualizado, copiado eletronicamente e disseminado globalmente para qualquer pessoa dentro da rede blockchain, efetivamente concluindo uma transação.

Cryptojacking

- **Cryptojacking** é uma ameaça emergente que se esconde no computador, celular, tablet, laptop ou servidor de um usuário, usando os recursos dessa máquina para “minerar” criptomoedas sem o consentimento ou conhecimento do usuário.

- Muitas vítimas de cryptojacking nem sabiam que tinham sido hackeadas até que fosse tarde demais!

2.5 Questionário do Módulo

O que Aprendi Neste Módulo?

- Os criminosos digitais usam muitos tipos diferentes de software mal-intencionado, ou malware, para realizar suas atividades. O uso de qualquer código para roubar dados, contornar controles de acesso ou causar dano ou comprometimento a um sistema é considerado malware.

- Independentemente do tipo de malware que infecta um sistema, você pode observar alguns sintomas comuns. Isso inclui:

  - Um aumento no uso da unidade central de processamento (CPU), o que torna seu dispositivo mais lento
  - seu computador congelando ou travando frequentemente
  - uma diminuição na velocidade de navegação na web
  - problemas inexplicáveis com suas conexões de rede
  - arquivos modificados ou excluídos
  - a presença de arquivos, programas ou ícones desconhecidos na área de trabalho
  - processos desconhecidos em execução
  - programas desligando ou se reconfigurando
  - envio e-mails sem o seu conhecimento ou consentimento.

O que Aprendi neste Módulo? (Cont.)

- A engenharia social está manipulando as pessoas para que realizem ações ou divulguem informações confidenciais. Os engenheiros sociais frequentemente contam com a disposição das pessoas em serem prestativas, mas também exploram suas fraquezas.

- **Os ataques de negação de serviço (DoS)** são um tipo de ataque de rede que é relativamente simples de ser realizado, mesmo por um atacante sem habilidades avançadas. Um ataque DoS resulta em alguma interrupção do serviço de rede para usuários, dispositivos ou aplicativos.

- Um ataque DoS distribuído (DDoS) é semelhante a um ataque DoS, mas se origina de fontes múltiplas e coordenadas.

- Um computador bot normalmente é infectado ao visitar um site inseguro ou abrir um anexo de e-mail ou arquivo de mídia infectado. Uma botnet é um grupo de bots conectados pela Internet que um indivíduo ou grupo mal-intencionado pode controlar.

O que Aprendi neste Módulo? (Cont.)

- Os invasores no caminho interceptam ou modificam as comunicações entre dois dispositivos, como um navegador da Web e um servidor da Web, para coletar informações ou se passar por um dos dispositivos.
- Inserir um nome de usuário e senha é uma das formas mais populares de autenticação em um site. Portanto, descobrir a senha é uma maneira fácil para os criminosos digitais obterem acesso às informações mais importantes.
- **As vulnerabilidades** de hardware são geralmente o resultado de falhas de design de hardware.
- Erros no sistema operacional ou no código do aplicativo geralmente introduzem **vulnerabilidades de software.**

O que Aprendi neste Módulo? (Cont.)

- O objetivo das atualizações de software é manter-se atualizado e evitar a exploração de vulnerabilidades.

- **Criptomoeda** é dinheiro digital usado para comprar bens e serviços, usando fortes técnicas de criptografia para proteger transações online. Bancos, governos e até empresas como a Microsoft e a AT&T estão muito conscientes da sua importância e estão aderindo ao movimento das criptomoedas.

- O Cryptojacking é uma ameaça emergente que se esconde no computador, telemóvel, tablet, portátil ou servidor de um utilizador, utilizando os recursos dessa máquina para “minerar” criptomoedas sem o consentimento ou conhecimento do utilizador.