CST0202-Ameaças, vulnerabilidades e ataques a Segurança Cibernética: Parte 2 - Ataques e Defesa aos e-mails e navegadores

Data do Post	@June 17, 2022 9:00 AM
Status	Done
Palavras-chave	Ameaças vulnerabilidades e ataques a Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Post- Linkedin

O e-mail corporativo é uma das principais formas de comunicação dentro das empresas, seja entre funcionários, com fornecedores e até clientes. Na mesma proporção que essa ferramenta facilita o dia a dia dentro de qualquer organização, ele também é um dos pontos mais vulneráveis quando falamos de segurança cibernética e risco de vazamento de dados.

Esse artigo apresenta as principais ameaças dos e-mails e dos navegadores.

Leia o artigo na integra

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/

#cybersecurity #technology #linux #programming #hacking #mailvuln #maliciouscode # #protection

---

Introdução

A 'internet' foi criada em 1969, nos Estados Unidos. Chamada Arpanet, tinha como função interligar laboratórios de pesquisa. Naquele ano, um professor da Universidade da Califórnia passou para um amigo em Stanford o primeiro e-mail da história.

A medida que tecnologia evolui, os meios de comunicação foram evoluindo, incluindo os e-mails e com isso, tornaram-se um sistema de comunicação padrão entre pessoas e empresas. Desse modo, pessoas mal intencionadas aproveitam-se das fragilidades de alguns desses sistemas de comunicação e da negligência e falta de conhecimento das pessoas para cometerem crimes virtuais.

Ataques e aos e-mails e navegadores

Spam

O e-mail é um serviço universal usado por bilhões de pessoas em todo o mundo. Como um dos serviços mais populares, o e-mail tornou-se uma grande vulnerabilidade para usuários e organizações. Spam, também conhecido como lixo eletrônico, é e-mail não solicitado, nem autorizado. Geralmente, o spam é um método de anúncio. Entretanto, o spam pode enviar links perigosos, malware ou conteúdo enganoso. O objetivo final é obter informações confidenciais,

como o número na previdência social ou informações da conta no banco. A maioria dos spam vem de vários computadores em redes infectadas por um vírus ou worm. Esses computadores infectados enviam o máximo de lixo eletrônico possível.

Mesmo com essas funcionalidades de segurança implementadas, alguns spams ainda podem passar. Observe alguns dos indicadores mais comuns de Spam:

- Um e-mail sem assunto.
- Um e-mail solicitando uma atualização de uma conta.
- O texto do e-mail tem erros de ortografia ou uma pontuação estranha.
- Links no e-mail são longos e/ou incompreensíveis.
- Um e-mail parece uma correspondência de uma empresa idónea.
- Um e-mail que solicita que o usuário abra um anexo.

Se receber um e-mail que contém um ou mais desses indicadores, o usuário não deverá abrir o e-mail ou os anexos. É muito comum que a política de e-mail de uma empresa exija que um usuário que recebeu esse tipo de e-mail denuncie para a equipa de segurança digital. Quase todos os provedores de e-mail filtram spam. Infelizmente, o spam ainda consome a largura de banda e o servidor do destinatário ainda precisa processar a mensagem.

Spyware

Spyware é o software que permite que um criminoso obtenha informações sobre as atividades do computador do usuário. O spyware frequentemente inclui rastreadores de atividade, coleta de toque de tela e captura de dados. Para tentar combater as medidas de segurança, o spyware quase sempre modifica as configurações de segurança. Muitas vezes, o spyware se junta ao software legítimo ou a cavalos de Troia. Muitos sites de shareware estão cheios de spyware.

Adware

Normalmente, o adware exibe pop-ups irritantes para gerar receita para seus autores. O malware pode analisar os interesses do usuário rastreando os sites visitados.

Em seguida, ele pode enviar anúncios pop-ups relacionados a esses sites. Algumas versões do software instalam Adware automaticamente. Alguns tipos de adware só oferecem anúncios, mas também é comum que o adware venha com spyware.

Scareware

O scareware persuade o usuário a executar uma ação específica por medo. O scareware simula janelas pop-up que se assemelham às janelas de diálogo do sistema operativo. Essas janelas transmitem mensagens falsificadas que afirmam que o sistema está em risco ou precisa da execução de um programa específico para retornar à operação normal. Na verdade, não há problemas e, se o usuário concordar e permitir a execução do programa mencionado, o malware infectará o sistema.

Phising

Phishing é uma forma de fraude. Os criminosos virtuais usam e-mail, mensagem instantânea ou outras medias sociais para coletar informações, como credenciais de ‘login’ ou informações da conta, ao colocar uma fachada de entidade ou pessoa confiável. O phishing ocorre quando uma parte mal-intencionada envia um e-mail fraudulento disfarçado de uma fonte legítima e confiável. A intenção da mensagem é enganar o destinatário para instalar o malware no dispositivo dele ou compartilhar informações pessoais, ou financeiras. Um exemplo de phishing é um e-mail falsificado para parecer que veio de uma loja de venda a retalho, solicitando que o usuário clique num link para receber um prémio. O link pode ir para um site falso que pede informações pessoais ou pode instalar um vírus.

Spear phishing é um ataque de phishing altamente direcionado. Embora o phishing e o spear phishing usem e-mails para alcançar as vítimas, o spear phishing envia e-mails personalizados a uma pessoa específica. O criminoso pesquisas os interesses da vítima antes de enviar o e-mail. Por exemplo, um criminoso descobre que a vítima está interessada em carros, procurando um modelo específico de carro para comprar. O criminoso entra no mesmo fórum de

discussão de carros utilizado pela vítima, forja uma oferta de venda de carro e envia um e-mail para o alvo. O e-mail contém um link para as fotos do carro. Ao clicar no link, a vítima instala inconscientemente o malware no computador.

Tipos de Phising

Vishing: é o phishing que usa a tecnologia de comunicação de voz. Os criminosos podem falsificar as chamadas de origens legítimas usando a tecnologia VoIP (voice over IP). As vítimas também podem receber uma mensagem gravada que pareça legítima. Os criminosos querem obter números de cartão de crédito ou outras informações para roubar a identidade da vítima. O vishing se vale do fato de que as pessoas confiam na rede telefónica.

Smishing: (Short Message Service phishing) é o phishing que usa mensagens de texto em celulares. Os criminosos se passam por uma fonte legítima na tentativa de ganhar a confiança da vítima. Por exemplo, um ataque de smishing pode enviar à vítima o link de um site. Quando a vítima visita o site, o malware é instalado no telemóvel.

Pharming: é a representação de um site legítimo na tentativa de enganar os usuários para inserir as credenciais. O pharming leva os usuários para um site falso que parece ser oficial. Então, as vítimas digitam as informações pessoais, supondo que estão conectadas a um site legítimo.

Whaling: é um ataque de phishing que buscam vítimas de alto perfil numa empresa, como executivos seniores. Outras vítimas incluem políticos ou celebridades.

Plugins de navegador e envenenamento de navegador

As violações de segurança podem afetar os navegadores da Web, exibindo anúncios de pop-up, coletando informações pessoais identificáveis ou instalando adware, vírus ou spyware. Um criminoso pode invadir um arquivo executável, os componentes ou plugins do navegador.

Plugins

Os plugins Flash e Shockwave da Adobe permitem a criação de animações gráficas e desenhos interessantes que melhoram muito o visual de uma página da Web. Os plugins exibem o conteúdo desenvolvido usando o software apropriado.

Até pouco tempo, os plugins tinham um registro de segurança considerável. À medida que o conteúdo baseado em Flash cresceu e tornou-se mais popular, os criminosos examinaram os plugins e softwares Flash, determinaram vulnerabilidades e exploraram o Flash Player. A exploração com sucesso pode causar uma falha no sistema ou permitir que um criminoso assuma o controle do sistema afetado. Espera-se um aumento nas perdas de dados à medida que os criminosos continuem a analisar as vulnerabilidades dos plugins e protocolos mais populares.

Envenenamento de SEO

Os mecanismos de busca, como o Google, classificam as páginas e apresentam resultados relevantes com base nas consultas da pesquisa dos usuários. Dependendo da relevância do conteúdo do site, ele pode aparecer mais alto ou mais baixo na lista de resultado da pesquisa. SEO, abreviação de Search Engine Optimization (Otimização de mecanismos de busca), é um conjunto de técnicas usadas para melhorar a classificação do site por um mecanismo de pesquisa. Embora muitas empresas legítimas se especializem na otimização de sites para melhor posicioná-las, o envenenamento de SEO usa a SEO para que um site mal-intencionado fique mais alto nos resultados da pesquisa.

O objetivo mais comum do envenenamento de SEO é para aumentar o tráfego em sites maliciosos que podem hospedar malware ou executar engenharia social. Para forçar um site malicioso a obter uma classificação mais elevada nos resultados de pesquisa, os invasores utilizam termos de busca populares.

Sequestrador de navegador

Um sequestrador de navegador é o malware que altera as configurações do navegador de um computador para redirecionar o usuário para sites pagos pelos clientes de criminosos virtuais. Normalmente, os sequestradores de navegador são instalados sem a permissão do usuário e fazem parte de um download drive-by. Um download drive-by é um programa transferido para o computador automaticamente, quando um usuário visita um site da Web ou visualiza uma mensagem de e-mail HTML. Sempre leia atentamente os contratos do usuário ao baixar programas, para evitar esse tipo de malware.

Defesa contra os e-mails e navegadores

Os métodos de controle de spam incluem filtrar e-mails, ensinar o usuário a tomar cuidado com e-mails desconhecidos e usar filtros de host/servidor.

É difícil impedir um spam, mas existem maneiras de diminuir os seus efeitos. Por exemplo, a maioria dos ISPs filtram os spams, antes que eles atinjam a caixa de entrada do usuário. Muitos antivírus e programas de software de e-mail executam a filtragem de e-mail automaticamente. Isso significa que detectam e removem spam de uma caixa de entrada.

O Anti-Phishing Working Group (APWG) é uma associação do setor voltada para eliminar o roubo de identidade e a fraude resultantes de phishing e spoofing de e-mail.

Manter todo o software atualizado assegura que o sistema tenha todos os mais recentes patches de segurança aplicados para eliminar as vulnerabilidades conhecidas.

Conclusão

Quer pessoas singulares ou as empresas devem consciencializar os funcionários sobre os perigos de se abrir anexos de e-mail que possam conter um vírus ou um worm. Não se deve presumir que os anexos de e-mail são seguros, mesmo quando são enviados por um contacto confiável. Um vírus pode estar a tentar se espalhar a usar o computador do remetente. Sempre varra anexos de e-mail, antes de abri-los.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/

#cybersecurity #technology #linux #programming #hacking #mailvuln #maliciouscode # #protection