ARTIGO

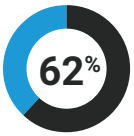
As pequenas e médias empresas enfrentam grandes ameaças

Introdução

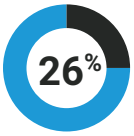
Os ataques cibernéticos em grandes empresas viram notícia, mas as pequenas e médias empresas (PMEs) enfrentam cada vez mais os mesmos riscos de cibersegurança que elas. Muitas das explorações atuais não as discriminam, porque os invasores estão preocupados apenas com o ganho financeiro. Eles não se importam com o tamanho de uma empresa se puderem ganhar dinheiro. Os criminosos usam diversos métodos para atingir os funcionários e os dispositivos dos quais dependem, até mesmo aqueles inteligentes e conectados que são amplamente usados. Os provedores de serviços de Internet estão bem posicionados para ajudar as PMEs a se defenderem.

Este breve documento descreverá algumas das ameaças mais comuns às quais as PMEs estão expostas e o impacto que causam.

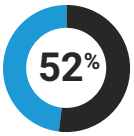
A pesquisa sobre tecnologia e pequenas empresas publicada pela National Small Business Association revelou uma série de estatísticas interessantes:



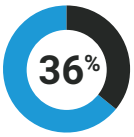
62% dos proprietários de pequenas empresas disseram que a cibersegurança é uma preocupação muito importante, outros 33% disseram que era relativamente importante e apenas 5% disseram que não era importante



Apenas 26% dos empresários disseram que sabiam lidar com problemas de cibersegurança



52% estão muito preocupados com o fato de que seus negócios podem ser afetados por um ataque cibernético e 44% estavam um pouco preocupados, enquanto 35% relataram que já foram vítimas desse tipo de ataque



36% disseram que informações foram falsamente enviadas de seus domínios ou endereços de e-mail, 5% disseram que informações confidenciais foram roubadas, 4% disseram que as contas bancárias foram acessadas e 52% relataram que um ataque causou interrupção no serviço

As atuais ameaças baseadas na Web podem ser amplamente categorizadas em duas áreas principais: malware e phishing. Botnets são um subconjunto importante de malware que requer atenção especial.

Malware é um software mal-intencionado instalado secretamente nos dispositivos. Websites comprometidos podem se beneficiar de falhas de software em um dispositivo para carregar malware. Os usuários também podem ser levados a navegar em um site mal-intencionado e clicar para carregar um arquivo malicioso. Alguns malwares podem ser ativados em um dispositivo e propagados em uma rede. Há muitos tipos diferentes de malware que têm as empresas como alvo:

Os **mineradores de criptomoeda** são programas que usam o poder de processamento de um dispositivo sem o consentimento da vítima. Os recursos das pequenas e médias empresas ficam comprometidos, e esses ataques podem ser difíceis de detectar porque, diferentemente do ransomware, os proprietários dos dispositivos não são solicitados a pagar nenhum dinheiro.

O **malware especializado** carregado em dispositivos de ponto de venda captura dados de cartão e os carrega em um adversário, gerando exposição para proprietários de empresas.

As **ameaças persistentes avançadas (APTs)** obtêm acesso às redes e coletam e extraem dados valiosos. As APTs foram projetadas para serem extremamente furtivas e assim poderem permanecer ativas por longos períodos. As PMEs podem perder dados valiosos ou, mais importante, a confiança do cliente. Elas também podem ficar sujeitas a ações regulamentares se dados pessoais forem expostos.

O **ransomware** bloqueia o acesso a arquivos criptografando tudo em um dispositivo ou servidor. Os invasores oferecem a chave de descriptografia a um custo significativo, embora em alguns casos eles coletem os fundos e não enviem a chave. Na melhor das hipóteses, as PMEs perdem os fundos de resgate. No pior dos casos, elas perdem os fundos e os dados críticos para os negócios.

O malware coleta dados valiosos de várias maneiras. O **spyware** procura dados, como credenciais de login e informações financeiras, e transfere relatórios para os criminosos. O malware de **exfiltração de dados** foi criado especificamente para localizar, identificar e extrair dados valiosos de computadores. Os **keyloggers** registram pressionamentos de teclas e podem ser treinados para permitir que criminosos acessem contas financeiras, logins em redes sociais ou outras informações valiosas. Os **trojans bancários** monitoram o comportamento do usuário para aprender credenciais de login e/ou personificar websites bancários para roubar dinheiro.

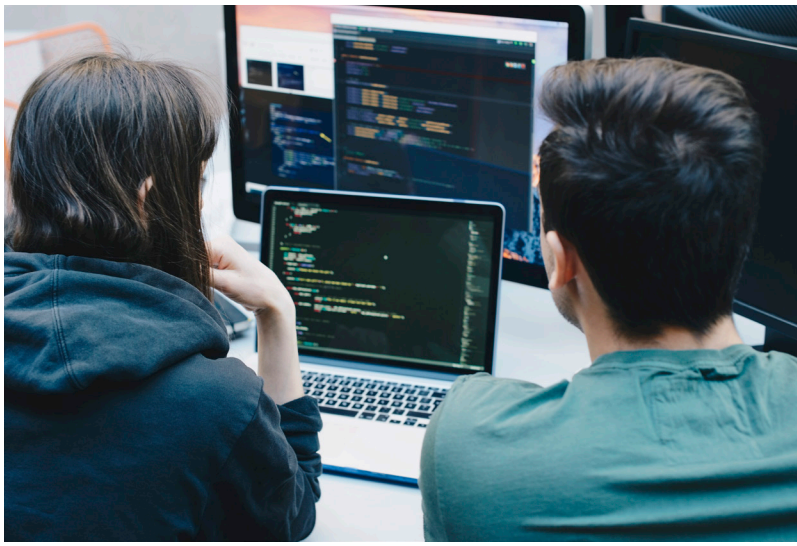
Os **botnets** são redes de dispositivos infectados com o mesmo malware e controlados em um canal central (chamado de comando e controle [C2]) por um criminoso ou grupo comum. Os botnets geralmente estão disponíveis para contratação, e a maioria pode executar muitas funções diferentes, como as descritas acima, para gerar dinheiro.

O **phishing** usa fraude, especialmente engenharia social, para levar as vítimas a revelar informações com as quais um invasor pode lucrar. No passado, os ataques de phishing induziam os usuários a clicar em links em e-mails de spam não solicitados e divulgar informações confidenciais. Os desenvolvedores de ataques de phishing diversificaram amplamente seus esforços; agora eles também incorporam URLs de phishing em postagens ou comentários de redes sociais, bem como em mensagens de texto, SMS, Skype, Messenger ou outros serviços.

Os dispositivos móveis são os principais alvos de phishing, pois têm telas pequenas e usuários realizando várias tarefas ao mesmo tempo que podem não perceber que um link é mal-intencionado. Para piorar, os phishers estão usando caracteres semelhantes de diferentes conjuntos de caracteres para imitar nomes de domínio legítimos.

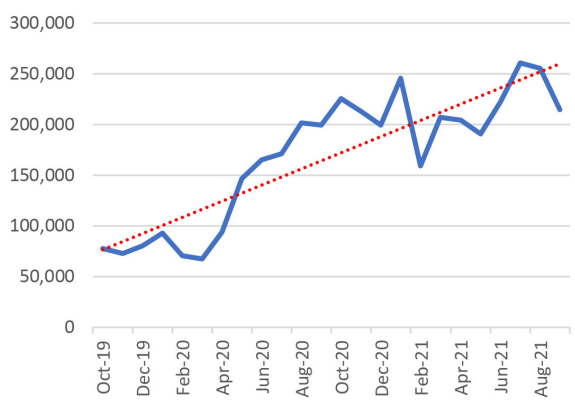
Estes são exemplos reais de strings de caracteres que foram usadas:

7eleven.com
Adîdas.com
adidąs.com
philippineairlines.com
rolex.com
singaporeair.com
thaiairways.com



Recentemente, o phishing vem apresentando tendência de crescimento. O relatório de tendências de atividades de phishing do terceiro trimestre de 2021 do Anti-Phishing Working Group informa: "Phishing atinge recorde mensal no terceiro trimestre. Os ataques dobraram desde o fim de 2019". O gráfico abaixo, retirado do relatório, ilustra a tendência. Isso ocorre porque pode ser mais fácil levar um usuário a realizar uma ação não intencional do que explorar falhas de software.

Ataques de phishing, quarto trimestre de 2019 ao terceiro trimestre de 2021



Os dados coletados pelas equipes de pesquisa de segurança corporativa e de operadoras da Akamai também mostram que a vida útil dos nomes de domínio usados para phishing está diminuindo, com média reduzida para aproximadamente 1,5 hora em março de 2019. Isso tem implicações diretas na proteção: as defesas precisam ser tão ágeis quanto os ataques.

Conclusão

Esta não é uma lista completa de ameaças da Web. Os invasores avaliam constantemente a viabilidade das suas explorações e inovam para maximizar seu retorno, mudando a face e a função do seu trabalho. Há também outros tipos de malware que são principalmente uma distração ou um incômodo, que mostram anúncios ou conteúdo indesejado.

As PMEs precisam estar protegidas contra ameaças baseadas na Web com soluções compatíveis com suas necessidades e restrições exclusivas. A Akamai oferece os serviços do Secure Internet Access projetados para PMEs. Eles protegem as PMEs contra os tipos de ataques descritos neste documento sem impor uma carga de gerenciamento. Cada dispositivo e cada pessoa em um local de trabalho, incluindo convidados, é automaticamente protegido. Os gerentes de negócios contam com um portal gráfico simples, onde podem ver instantaneamente o que está acontecendo em sua rede e quais ameaças foram detidas.

Os serviços do Secure Internet Access da Akamai foram criados especificamente para ajudar os ISPs a:

- Gerar receita com defesas de segurança de nível empresarial para PMEs
- Ir além da velocidade e da confiabilidade e diferenciar os serviços das pequenas e médias empresas com base na segurança
- Minimizar as barreiras de implantação, reduzir custos e simplificar a entrega de serviços com uma versão baseada em nuvem dos serviços do Secure Internet Access

O serviço pode ser totalmente personalizado com uma aparência alinhada à marca, e o conjunto de recursos e a inteligência contra ameaças também podem ser adaptados aos requisitos do mercado local.

Qualquer pessoa. Qualquer dispositivo. A qualquer momento. A Akamai pode ajudar.

Entre em contato com a Akamai agora mesmo para saber mais.