O CRIME VIRTUAL ATINGE UMA GRANDE PARCELA DAS PEQUENAS EMPRESAS

Com a Kaspersky, agora é possível.
kaspersky.com/business

Be Ready for What's Next

KASPERSKY lab

1

O crime virtual voltado para pequenas empresas está aumentando e o custo das violações de dados para essas vítimas mais vulneráveis pode ser uma despesa grande demais. 31% das violações de dados ocorreram em empresas com 100 funcionários ou menos.[1] Os relatórios mostram uma variação do custo médio de um ataque virtual a uma empresa de pequeno porte de US$ 8.900[2] até mais de US$ 100.000.[3]

Para uma pequena empresa, a recuperação de um ataque tão significativo pode ser difícil e às vezes impossível. A falta de confiança dos clientes após uma violação de dados pode manchar a reputação da empresa de forma irrevogável. Além disso, o impacto econômico pode destruir toda a empresa de pequeno porte, juntamente com as finanças pessoais de seus proprietários e funcionários, que perdem seus meios de subsistência. Uma vez que apenas cerca de metade de todas as novas pequenas empresas sobrevive cinco anos ou mais, e aproximadamente um terço sobrevive 10 anos ou mais[4], uma violação de dados pode ter um impacto desastroso em um setor já vulnerável. De acordo com a National Cyber Security Alliance, " a cada ano, uma em cada cinco pequenas empresas é vítima do crime virtual. E, dentre essas, aproximadamente 60% abandona os negócios no prazo de seis meses após um ataque."[5]

Este *whitepaper* examina por que as pequenas empresas são tão vulneráveis, os diferentes tipos de ameaças virtuais e o que pode ser feito para evitar ataques e atenuar seus danos.

1 Unidade de análises de perícia da Verizon Communications Inc.
2 The National Small Business Association's 2013
3 CNBC, 9 de junho de 2014
4 Escritório de defesa da U.S. Small Business Administration, setembro de 2013
5 Hackers Put a Bulls-eye on Small Business (Hackers dirigem sua atenção às pequenas empresas), PC World, agosto de 2013

Vulnerabilidades comuns entre as pequenas empresas

2

Diferente das grandes organizações com departamentos de TI estabelecidos, frequentemente os pequenos empresários tratam da segurança cibernética por conta própria porque “alguém tem de fazê-lo” e não porque são especialistas em TI... às vezes, não têm nem mesmo o conhecimento básico. Esses verdadeiros gerentes de TI têm as competências essenciais e uma longa lista de tarefas que nada têm a ver com a defesa da empresa contra o crime virtual. Às vezes, eles herdam a responsabilidade pela segurança cibernética juntamente com algum *software* de segurança comprado anteriormente, sem levar em consideração se a solução continua atendendo às necessidades da empresa. A empresa pode ter aumentado o número de *endpoints* com apenas uma licença individual de um *software* de segurança para o consumidor protegendo o PC original. Para piorar a situação, as atualizações periódicas nunca são autorizadas, o que torna a empresa vulnerável devido à falta de correções dos *softwares* e aos dispositivos não protegidos. Alguns empresários que conhecem melhor a tecnologia cometem o erro de instalar um *software* de segurança criado para organizações maiores, em vez de implementar uma solução desenvolvida especificamente para empresas menores. Quando se trata da segurança cibernética, não há uma solução adequada para todos.

O orçamento é outro fator de risco que aumenta a probabilidade de uma pequena empresa se tornar alvo de criminosos virtuais. Com um orçamento limitado destinado à segurança virtual, os pequenos empresários muitas vezes fazem suas escolhas exclusivamente com base no preço e não no desempenho e na capacidade de proteção. Uma solução barata, ou, pior, gratuita projetada para um dispositivo individual não consegue proteger adequadamente uma pequena empresa e seus dados valiosos.

ORÇAMENTOS LIMITADOS DEIXAM PEQUENAS EMPRESAS VULNERÁVEIS AO CRIME VIRTUAL

Tipos de ameaças virtuais

3

Os criminosos virtuais estão armados com todo um arsenal de métodos para conseguir acessar informações financeiras confidenciais dos usuários. A maior parte dos ataques direcionados a dados financeiros tem a engenharia social como elemento básico. Ela pode ser usada para disseminar *malware* ou para roubar diretamente as credenciais do usuário.

O ***Phishing*** (ou ***spearphishing***, em ataques direcionados) é um exemplo clássico do uso de engenharia social para conseguir informações financeiras, enganando os usuários para que forneçam informações confidenciais para os criminosos virtuais. Por exemplo, uma vítima desinformada pode receber uma carta "oficial" em nome de um banco, sistema de pagamento ou loja *on-line* respeitável afirmando que houve uma falha no servidor da organização, de modo que todos os clientes precisam fornecer urgentemente seus dados pessoais para verificação. O pretexto pode variar mas, de qualquer forma, é solicitado que o cliente envie suas credenciais de *login* por *e-mail*, digite-as em um formulário *Web* anexado ou no *site* "oficial" do banco, seguindo um *link* contido na mensagem. Todas as informações fornecidas pelo usuário chegarão às mãos dos criminosos virtuais.

Os remetentes de *phishing* usam *sites* falsos elaborados com habilidade para imitar os originais. Para que o *site* fraudulento não chame muita atenção, os criminosos virtuais usam URLs semelhantes aos dos *sites* originais, com diferentes variações na linha da barra de endereços. Em muitos casos, é muito difícil diferenciar as falsificações dos *sites* originais. Por isso, os especialistas recomendam que os usuários acessem *sites* financeiros usando os marcadores de seus navegadores, em vez de seguir o *link* contido em um *e-mail*. O *phishing* continua sendo o principal método de infecção por meio da engenharia social, especialmente quando se trata de funcionários de empresas.

ATAQUE DE *PHISHING* TÍPICO

Os **cavalos de Troia** são programas maliciosos especializados em roubar informações financeiras. Normalmente, eles coletam automaticamente informações sobre pagamentos efetuados em computadores infectados. Às vezes, também realizam transações financeiras em nome dos usuários de forma automática. Nos ataques de clientes de bancos por cavalos de Troia, também podem ser enviados *e-mails* de *phishing* em nome do banco envolvido. Nesses *e-mails* falsos, não é solicitado que os usuários enviem informações mas, sob algum pretexto, eles devem abrir um documento em anexo. Na verdade, o anexo é um arquivo malicioso.

Os criminosos virtuais usam tanto cavalos de Troia polivalentes, capazes de atacar clientes de vários bancos ou sistemas de pagamento, quanto cavalos de Troia com um único propósito, destinados a atacar clientes de bancos específicos. Depois de entrar no computador do usuário, o cavalo de Troia para sistemas bancários se estabelece no sistema e dá início a sua missão de roubar todos os tipos de informações financeiras do usuário.

Na maioria dos casos, os criminosos preferem usar combinações de várias técnicas para melhorar suas chances de sucesso na infecção e aumentar a eficácia do programa malicioso. O cavalo de Troia para sistemas bancários ZeuS (Zbot) é um dos mais avançados e de alta tecnologia usados por criminosos virtuais. Em todo o mundo, existem muitas variedades desse programa malicioso, incluindo seu clone funcional, cavalo de Troia SpyEye.

Principais características do ZeuS:

- O cavalo de Troia rouba todas as informações que o usuário configurou para serem lembradas pelo computador (por exemplo, marcando a caixa “Salvar senha”).
- O cavalo de Troia controla as teclas pressionadas pelo usuário. Se for usado um teclado virtual, o ZeuS faz uma captura da tela ao redor do cursor no momento em que o botão esquerdo do mouse é clicado. Assim, o criminoso virtual obtém informações sobre as teclas que foram pressionadas no teclado virtual e conhece as credenciais de *login* do usuário.
- O ZeuS usa injeções da *Web*. Quando um usuário abre uma página da *Web* que se encontra no arquivo de configuração do ZeuS, o cavalo de Troia adiciona novos campos em que o usuário deve inserir informações financeiras confidenciais interessantes para os criminosos virtuais.
- O ZeuS é capaz de burlar os mais avançados sistemas de segurança bancária.
- Esse programa malicioso é propagado com a ajuda da engenharia social e por meio da exploração de vulnerabilidades em *softwares* populares da Microsoft, Oracle, Adobe, etc. quando os usuários visitam *site*s comprometidos. Os *links* para esses *sites* são distribuídos principalmente por *spam*.
- O ZeuS é usado para roubar informações confidenciais para obter acesso não autorizado a contas dos maiores bancos do mundo. Em 2012, os pesquisadores registraram 3.524.572 tentativas de instalar esse programa malicioso em 896.620 computadores com produtos da Kaspersky Lab instalados, localizados em diversos países.

Essa enorme disseminação de cavalos de Troia para sistemas bancários é auxiliada por ***exploits*** de vulnerabilidades do Windows e de outros *softwares* populares. Sem que o usuário saiba, esses *exploits* invadem o sistema através de vulnerabilidades de *software* e baixam outros programas maliciosos que roubam informações financeiras do computador da vítima. Para tornar o ataque efetivo, os criminosos virtuais usam os chamados pacotes de *exploits* para diversas vulnerabilidades e não *exploits* únicos. O pacote de ***exploits*** analisa os *softwares* instalados no computador do usuário e, quando encontra alguma brecha, escolhe um exploit adequado para infectar o computador. Os pacotes de *exploits* são hospedados em servidores dos criminosos virtuais ou em recursos invadidos. Os *links* para as *exploits* são distribuídos pelos criminosos em *e-mails phishing*, redes sociais, hospedagem em *site*s comprometidos ou mesmo legítimos, e *banners* de publicidade *on-line*. Os *exploits*, por sua vez, baixam cavalos de Troia para os computadores-vítima. A infecção de *site*s populares são especialmente perigosas porque eles recebem a visita de muitos usuários e, quando há um *link* malicioso presente, o computador de cada visitante é discretamente atacado por *exploits* que tentam colocar programas maliciosos neles.

As **injeções da *Web***, que modificam o conteúdo de páginas HTML, são um método popular entre os criminosos virtuais. O programa malicioso acrescenta campos adicionais quando a página da *Web* do banco é exibida no navegador, solicitando que o usuário insira informações confidenciais. Por exemplo, o cavalo de Troia Carberp usa uma injeção da *Web* para colocar campos adicionais na página inicial de um banco *on-line* e solicita que o usuário insira dados de seu cartão do banco, como número, nome do usuário, data de expiração e o código CVV/CVC. Se ele não faz isso, o cavalo de Troia exibe uma mensagem de erro e bloqueia a sessão.

As informações extras digitadas pelo usuário são enviadas para o criminoso, mas não chegam ao banco, pois são interceptadas durante o envio dos dados para o servidor do banco. Assim, nem a vítima e nem o banco ficam sabendo da fraude.

Esses programas maliciosos usam as seguintes técnicas:

- **Registro de teclas (*keyloggers*)** – os cavalos de Troia interceptam os pressionamentos de teclas quando o usuário digita informações de interesse dos criminosos virtuais, como credenciais de *login*.

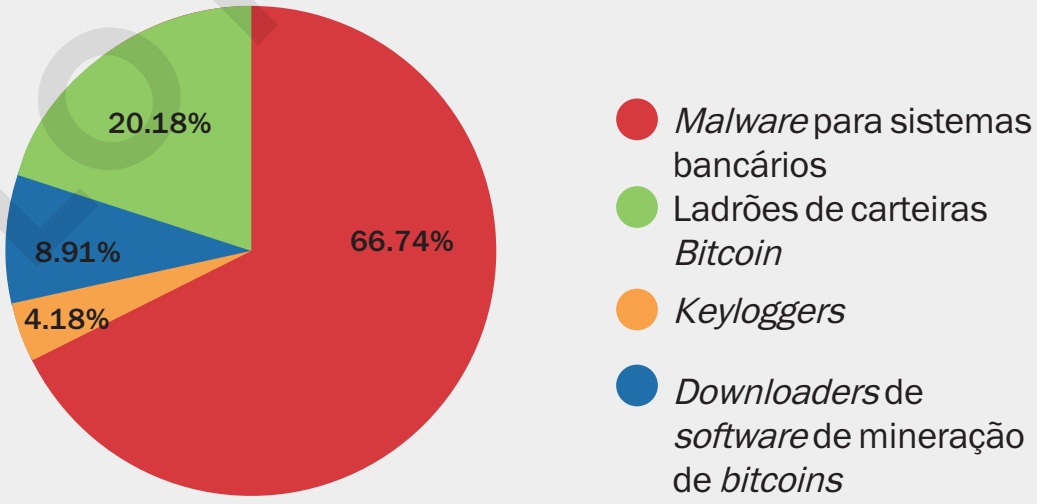
- **Capturas de tela** – os criminosos virtuais fazem capturas de tela do dispositivo da vítima para obter informações confidenciais financeiras digitadas usando o teclado físico. Nesse caso, os criminosos virtuais conhecem somente as informações mostradas durante a digitação, mas não podem acessar o *login* e a senha do usuário, pois os caracteres inseridos são substituídos na tela por asteriscos.

- **Desvio do teclado virtual** – o criminoso virtual captura uma imagem da área da tela ao redor do cursor no momento em que o usuário clica no botão esquerdo do *mouse*. Assim, ele obtém os caracteres digitados pelo usuário no teclado virtual e fica sabendo o *login* e a senha do usuário.

- **Modificação do arquivo *host*** -- as informações armazenadas nesse arquivo têm prioridade sobre as informações que o navegador da *Web* recebe dos servidores DNS. Cavalos de Troia adicionam URLs de bancos a esse arquivo e atribuem os endereços IP de servidores dos criminosos a eles. Como resultado, os usuários que inserem essas URLs em seus navegadores são encaminhados para *site*s fraudulentos, embora ainda vejam o URL do banco no navegador. Quando o usuário digita suas credenciais de *login* em um *site* falso, essas informações são enviadas para os criminosos virtuais.

- **Invasão de um processo do navegador em execução** – com esse método, um cavalo de Troia pode controlar a conexão do navegador com o servidor. Assim, os criminosos podem obter as credenciais de *login* que os usuários inserem no *site* do banco e também modificar o conteúdo da página da *Web* (por meio de uma injeção da *Web*), conseguindo assim mais informações confidenciais. Para concluir a grande maioria das operações financeiras *on-line*, os usuários precisam usar navegadores da *Web*. As técnicas empregadas pelos cavalos de Troia modernos que visam sistemas bancários estão, de alguma forma, relacionadas a esses *softwares*.

DISTRIBUIÇÃO DE *MALWARES* MALICIOSOS PARA SISTEMAS BANCÁRIOS EM 2013



Burlando a autenticação de dois fatores

4

Os bancos investem bastante na proteção de seus clientes. Os cavalos de Troia voltados para sistemas bancários são tão eficientes que os bancos tiveram de introduzir uma camada de proteção extra — ferramentas de identificação dos usuários. Com credenciais de *login* padrão, os clientes criam um nome de usuário e uma senha. Com a autenticação de dois fatores em vigor, não é suficiente saber o *login* e a senha do usuário para poder controlar a conta bancária. Nesse caso, os bancos usam uma senha de uso único (o TAN, número de autenticação da transação). Na prática, pode ser um cartão com códigos impressos, mensagens SMS com senhas únicas que o banco envia para o celular do usuário (mTAN) ou um dispositivo exclusivo para isso (chipTAN).

Contudo, os criminosos virtuais encaram a proteção aprimorada como um novo desafio e buscam novas formas de passar por ela. Para burlar esses sistemas de segurança, os criminosos virtuais criaram novos métodos de roubo de dados e modificaram suas técnicas de engenharia social.

Senhas de uso único (OTP)

5

O cavalo de Troia para sistemas bancários ZeuS tem um conjunto de ferramentas em seu arsenal que pode burlar diferentes tipos de autenticação de dois fatores. O ZeuS usa uma ferramenta interessante para conseguir as senhas de uso único contidas em um cartão.

- Assim que o usuário entra em um sistema bancário *on-line* e digita uma senha de uso único, o ZeuS rouba os dados de autenticação, exibe uma notificação falsa dizendo que a lista atual de senhas de uso único é inválida e informa que o usuário deve obter uma nova lista de senhas.
- Para receber a "nova" lista, o usuário deve inserir seus códigos TAN atuais nos campos apropriados, supostamente para que eles sejam bloqueados.
- Todos os detalhes de *login* inseridos são enviados para os criminosos virtuais, que os utilizam imediatamente para transferir os recursos da vítima para suas contas.

mTAN

6

Em conjunto com o cavalo de Troia para dispositivos móveis *ZeuS-in-the-Mobile* (ZitMo), o ZeuS é capaz de roubar as senhas de uso único que chegam ao celular.

- Quando os usuários visitam a página de *login* de um banco *on-line*, o ZeuS usa injeções da *Web* para criar um campo adicional, onde os usuários devem inserir um número de telefone, supostamente para receber uma atualização de certificado.

- Quando o usuário digita as credenciais de *login* necessárias para a autorização e o número de telefone, o cavalo de Troia rouba essas informações e as envia para seus proprietários. Depois de algum tempo, é enviado para o *smartphone* do usuário um SMS com um *link* para o "novo" certificado de segurança. Quando os usuários tentam instalar esse certificado falso, o *smartphone* é infectado.

- Dessa forma, os criminosos podem acessar todos os dados necessários para operar remotamente a conta bancária do usuário e roubar seu dinheiro.

ChipTAN

5

O chipTAN é outro método de autenticação de dois fatores. Ele é usado por bancos da Europa Ocidental e exige que cada cliente tenha um dispositivo gerador de TANs. Ao estabelecer uma transação no *site* do banco, o usuário coloca seu cartão no chipTAN e digita o código PIN.

Em seguida, ele deve colocar o dispositivo ao lado do monitor do computador para verificar os detalhes da transação em andamento. Depois de verificar os detalhes da transação em relação aos dados exibidos na tela do dispositivo, o usuário insere um código adicional no dispositivo para confirmar a transação.

Atualmente, o chipTAN é a ferramenta mais avançada e eficaz de segurança bancária. Infelizmente, os criadores do cavalo de Troia bancário *SpyEye* também descobriram como burlar essa ferramenta de segurança de alta tecnologia.

- Usando injeções da *Web*, o cavalo de Troia modifica a lista de transações bancárias do usuário. Assim, quando o usuário entra no sistema do banco *on-line*, ele vê o crédito de uma transferência de grande valor, e o saldo da conta é alterado de forma correspondente.
- O *SpyEye* usa o nome do banco para notificar o usuário de que essa operação foi um erro e de que a conta será bloqueada até o estorno do valor supostamente recebido.
- Para evitar isso, o usuário realiza uma nova operação de pagamento para devolver o dinheiro. O *SpyEye* informa a conta bancária e o valor em dinheiro para a devolução. O cavalo de Troia não precisa roubar o código chipTAN gerado, pois o próprio usuário o insere e confirma a transação.
- Depois disso, o cavalo de Troia falsifica a página da *Web* para que ela mostre o saldo original da conta, enquanto o dinheiro é enviado para os criminosos virtuais.
- Esse método não requer nem mesmo artifícios técnicos extra por parte do criminoso, pois o ataque é baseado em injeções da *Web* e engenharia social.

USB Tokens

7

Um *token* é um dispositivo USB usado como ferramenta de segurança adicional que contém uma chave única solicitada pelo sistema cada vez que o usuário faz uma operação de pagamento. Os criadores do cavalo de Troia para sistemas bancários "Lurk" descobriram uma maneira bastante eficaz de burlar essa proteção:

- O usuário abre uma operação de pagamento no sistema do banco *on-line* e informa os dados.
- O cavalo de Troia Lurk intercepta esses dados e espera o sistema solicitar o *token*.
- O sistema do banco *on-line* solicita o *token*, e o usuário apresenta suas credenciais inserindo o token USB na conexão apropriada.
- O cavalo de Troia intercepta o evento e exibe uma "tela azul" falsa, que informa aos usuários que está sendo criado um despejo da memória física para análise posterior e solicita que o usuário não desligue o computador antes do término da operação.
- Enquanto o usuário aguarda a conclusão da "operação" (e seu *token* está conectado à porta USB), o criminoso virtual acessa a conta para realizar uma ordem de pagamento no nome do usuário e transferir o dinheiro para outra conta.

Ransomware

8

O *ransomware* é um tipo de *software* malicioso usado por criminosos virtuais desenvolvido para extorquir dinheiro de suas vítimas, seja por meio da criptografia de dados no disco ou bloqueando o acesso ao sistema. Geralmente, o *ransomware* é instalado acionando uma vulnerabilidade no computador da vítima, explorada quando os usuários involuntariamente abrem um *e-mail* de *phishing* ou acessam um *site* malicioso criado pelos invasores. Em março, os especialistas da Kaspersky Lab descobriram anexos de *ransomware* enviados em *e-mails* de phishing por invasores que alegavam ser de serviços populares de reservas *on-line*.

Uma vez que o programa é instalado, ele criptografa o disco do computador da vítima ou bloqueia o acesso ao sistema, deixando uma mensagem de "resgate" que exige um pagamento para descriptografar os arquivos ou restaurar o sistema. Essa mensagem aparece da próxima vez que o usuário reinicia o sistema. Basicamente, o invasor mantém o computador como refém e tenta extorquir dinheiro em troca do acesso à máquina. Porém, é importante saber que muitas vezes a vítima não recupera o acesso ao computador, mesmo após o pagamento do "resgate". Trata-se de um golpe.

O *ransomware* ganha cada vez mais popularidade em todo o mundo, embora as mensagens de resgate e os golpes para extorquir dinheiro sejam diferentes de acordo com o local. Em países onde a pirataria é comum, como a Rússia, muitas vezes os programas de *ransomware* que bloqueiam o acesso ao sistema afirmam ter identificado *software*s não licenciados no computador da vítima e solicitam o pagamento por eles.

Na Europa e na América do Norte, onde a pirataria de *software* é menos comum, essa abordagem não tem tanto sucesso. Em vez disso, são exibidas mensagens *pop-up* de falsas autoridades legais afirmando que foi encontrado conteúdo de pornografia infantil ou outros conteúdos ilegais no computador. Elas são acompanhadas por uma multa a ser paga.

RANSOMWARE FAZENDO-SE PASSAR PELO DEPARTAMENTO DE JUSTIÇA

Proteção contra exploits

9

Como os ataques direcionados usam *malwares* exclusivos, a detecção baseada em assinaturas não é suficiente para identificar o código malicioso utilizado. No entanto, os programas de segurança têm mais armas à disposição além da simples detecção baseada em assinaturas.

Mesmo que os fraudadores consigam atacar o sistema — por meio de uma exploração ou um programa malicioso iniciado pelo usuário — o controle de tráfego de rede e controle de aplicativos ajudam a evitar uma infiltração maior na rede corporativa.

Controle do tráfego de rede

10

Depois de entrar no sistema, geralmente o código malicioso (o código *shell* de um cavalo de Troia ou *exploit*) tenta executar uma ou mais das seguintes ações:

- Estabelecer conexão com um centro de comando (conexão de saída)
- Abrir portas para conexões de entrada
- Baixar módulos adicionais
- Implementar o código malicioso em outros processos para manter a conexão com o centro de comando
- Reunir informações sobre a rede, seus sistemas e usuários
- Enviar as informações coletadas (endereços IP, nomes de computadores e contas, *login*s, senhas, etc.) para o servidor do fraudador.

Em geral, depois de conectados ao sistema, os golpistas tentam coletar informações sobre a rede corporativa na qual o computador está localizado. Para a coleta de informações locais, os fraudadores não precisam de privilégios adicionais. A lista de processos em execução, *softwares* e correções instaladas, usuários conectados, etc. pode ser encontrada com bastante facilidade. As informações sobre a rede corporativa, incluindo a pesquisa de outros sistemas vulneráveis, sistemas de proteção, pastas compartilhadas, serviços de rede, servidores, etc., são coletadas usando *scripts* e utilitários especiais capazes de mascarar sua atividade e burlar os sistemas de segurança. Todas essas informações são enviadas pela Internet aos criminosos virtuais para análise antes da preparação da próxima fase do ataque.

Usando a tecnologia de controle do tráfego de rede (como um *Firewall*, IPS/IDS), sua empresa pode, além de bloquear a atividade perigosa, também detectar qualquer invasão da rede. Essas tecnologias de controle do tráfego de rede bloqueiam as conexões de entrada/saída por porta, nome de domínio, endereço IP, protocolo, e geram análises estatísticas do tráfego (fluxo da rede) de anomalias durante a detecção de tráfego de rede suspeito para análise posterior. Elas também detectam e bloqueiam a saída de comandos ou similares enviados pela Internet; *downloads* de arquivos suspeitos da Internet e transmissões de informações confidenciais (por exemplo, endereços IP, *login*s, nomes de computadores, documentos corporativos, números de cartões de crédito, etc.).

O *firewall* e o IPS/IDS podem detectar anomalias na interação dos nós da rede assim que o código malicioso tenta contatar o centro de comando ou examina ativamente a rede corporativa em busca de outros sistemas, portas abertas, pastas compartilhadas, etc. Essa detecção de anomalias permite que os especialistas em segurança respondam prontamente a eventuais ameaças, evitando novas invasões que podem comprometer a rede corporativa.

Controle de Aplicativos

11

Depois de acessar o sistema-alvo, os criminosos têm como meta consolidar seu sucesso: módulos e utilitários adicionais são baixados no sistema e, muitas vezes, um código malicioso que faz a conexão com o centro de comando é incorporado em processos confiáveis, como explorer.exe, csrss.exe, smss.exe, etc.

O Controle de Aplicativos pode bloquear a execução e o *download* de programas e módulos não confiáveis do conjunto de invasão do fraudador e as políticas do HIPS devem ser usadas para bloquear comportamentos fora do padrão — e possivelmente perigosos — de *softwares* legítimos. Por exemplo, os navegadores não devem abrir portas para conexões de entrada, os processos do sistema (explorer.exe, csrss.exe, smss.exe, etc.) e outros aplicativos (calc.exe, notepad.exe, etc.) não devem se conectar a servidores externos, nem implementar código malicioso em outros processos confiáveis. Esses comportamentos devem ser proibidos.

Para impedir que os criminosos obtenham o controle do sistema, as pequenas empresas devem:

- Impedir a implementação de código em outros processos por programas confiáveis ou possivelmente vulneráveis
- Restringir o acesso dos aplicativos somente a recursos críticos do sistema e arquivos
- Bloquear funções potencialmente perigosas que não são recursos padrão dos aplicativos (acesso à rede, instalação de *drivers*, criação de capturas de tela, acesso à *webcam* ou ao microfone, etc.)

Os sistemas que exigem maior nível de proteção devem ser protegidos pelo modo Negação Padrão, que pode bloquear a inicialização de qualquer programa que não esteja na lista branca armazenada localmente ou na nuvem.

Mantendo a segurança de sua pequena empresa

12

- Todos os direitos e privilégios devem ser concedidos somente quando necessário.
- Todos os direitos e privilégios (de acesso) concedidos aos usuários devem ser devidamente gerenciados.
- Verifique regularmente vulnerabilidades e serviços de rede não utilizados nos sistemas.
- Detecte e analise serviços de rede e aplicativos vulneráveis.
- Atualize componentes e aplicativos vulneráveis. Se não houver uma atualização, o *software* vulnerável deve ser restrito ou bloqueado.
- Implemente uma solução de segurança eficaz.
- Use o bom senso.
- Instrua seus funcionários (e a si mesmo!).

Muitas dessas medidas podem ser automatizadas. Por exemplo, se as políticas de segurança forem violadas, um *software* específico mostra uma mensagem de aviso ao usuário. Para algumas pequenas empresas, a tecnologia de gerenciamento de sistemas é conveniente para procurar serviços de rede e dispositivos não autorizados, vulnerabilidades e atualizações automáticas de aplicativos vulneráveis.

QUAL É A SOLUÇÃO DE SEGURANÇA CERTA PARA PEQUENAS EMPRESAS?

- Inclui as principais tecnologias de segurança que você deseja usar e não tem complementos complicados desnecessários pelos quais você não precisa pagar
- Sua eficiência é confirmada por laboratórios independentes de pesquisa
- Tem as ferramentas certas para ser expandida conforme a empresa cresce
- Fornece proteção extra para transações financeiras
- Oferece criptografia e funcionalidades automatizadas de *backup*/ restauração para manter seguros seus dados empresariais essenciais

ALERTA DE SEGURANÇA PARA PEQUENAS EMPRESAS

WHAT TYPE OF BUSINESS ARE YOU?

KASPERSKY lab

WHETHER YOUR BUSINESS IS BIG OR SMALL, EXPANDING OR JUST STARTING-UP, KAPSERSKY LAB HAS THE IT SECURITY SOLUTION TO PROTECT YOU.

THE START-UP BUSINESS

- Setting up new business
- Buying new IT kit
- Safety measures mean one less thing to worry about—now and in the future

THE BUSINESS THAT'S HAD ITS FINGERS BURNED

- Established business that has recently fallen prey to malware or data loss
- The threat has meant that there's a real need to invest—and fast
- The business needs to be comprehensively covered so it will never happen again

THE BUSINESS THAT'S SWITCHING ITS SECURITY

- Established business – while IT not high on the agenda, existing security software has become an annoyance
- Slows up systems or fails to give adequate protection
- The license is up for renewal so it's an opportune time to look elsewhere

THE EXPANDING BUSINESS

- Employing more people
- Business is becoming more professional in its outlook
- Buying new IT kit to support new people
- The time is right to invest in IT security software

THE BUSINESS THAT KEEPS ITS FINGERS CROSSED

- An established business that's never really taken IT security threats seriously
- Have always had the attitude of "it won't happen to me" or "I hope it doesn't happen"
- A story in the press put IT security on their radar
- Interested in security if it's fast and affordable

TOP TEN POINTERS TO HELP PROTECT YOUR BUSINESS AGAINST CYBERCRIME, MALWARE AND OTHER SECURITY RISKS:

1. Assess the potential security risks and identify what needs to be protected.
2. Do you need to protect mobile or tablet devices?
3. Be aware of the legal and regulatory obligations.
4. Define some basic security policies to keep information/computers secure.
5. Set up an education program to improve awareness of security issues internally.
6. Evaluate all the security software products suitable to your needs.
7. Will your security software supplier offer the level of support you need?
8. Would you benefit from additional security features for the protection of online banking or financial transactions?
9. Check the suitability of cloud service providers' security and their contract terms.
10. Choose a security software product capable of protecting all of the computers and devices accessing the cloud.

PROTECT YOUR CUSTOMERS. PROTECT YOUR BUSINESS.

Spend less time on security and more time running your business.
For essential tips on defending your business against malware and cybercrime, download this easy to read, free guide now!

FREE 64 PAGE GUIDE

Download now

KASPERSKY lab

Kaspersky Small Office Security

13

O Kaspersky Small Office Security oferece proteção superior criada para ser avançada, rápida e fácil para muitas pequenas empresas.

PRINCIPAIS RECURSOS:

- Protege seus PCs Windows, servidores e dispositivos móveis Android em tempo real contra ameaças conhecidas e emergentes.
- Protege suas transações *on-line* contra fraudes financeiras.
- Protege você e sua empresa contra ameaças *on-line*.
- Permite regular ou bloquear o acesso de funcionários à Internet.
- Protege seus dados e os dados de seus clientes contra roubo, perda e corrupção.

Para saber mais sobre o Kaspersky Small Office Security ou solicitar uma demonstração, visite o Small Business Cybersecurity Learning Center.

Kaspersky Endpoint Security for Business

13

O Kaspersky Endpoint Security for Business, nossa plataforma de segurança avançada para empresas, está disponível em níveis progressivos que permitem ampliar a segurança de acordo com o crescimento da empresa.

PRINCIPAIS RECURSOS:

- Proteção *antimalware* gerenciada centralmente para *endpoints* Windows, Macintosh e Linux.
- Os Controles de Endpoints gerenciam o uso dos dispositivos conectados, como os USB, limitam os *softwares* que podem ser executados e controlam o acesso dos funcionários à Internet.
- O Gerenciamento de Dispositivos Móveis (MDM) ajuda a implementar e gerenciar *smartphones* e *tablets*.
- A criptografia total do disco, de pastas ou arquivos protege os dados perdidos ou roubados (para usuários do nível *Advanced*).
- O Gerenciamento de Sistemas oferece diversas ferramentas e medidas de segurança para reduzir os riscos e simplificar sua rede (para usuários do nível *Advanced*).

Para saber mais sobre o Kaspersky Endpoint Security for Business e usar nosso conveniente seletor de produtos para determinar a solução de segurança cibernética certa para sua empresa, visite o Kaspersky Business Knowledge Center.

Sobre a Kaspersky Lab

A Kaspersky Lab é a maior fornecedora privada de soluções de proteção de *endpoints* do mundo. A empresa está classificada entre as quatro principais fornecedoras de soluções de segurança para usuários de *endpoints* do mundo.* Durante todos os seus 16 anos de história, a Kaspersky Lab continua sendo inovadora em segurança de TI e fornece soluções de segurança digital eficientes para educadores, consumidores, pequenas e médias empresas e grandes corporações. Atualmente, a empresa opera em quase 200 países e territórios ao redor do globo, fornecendo proteção para mais de 300 milhões de usuários em todo o mundo.

Ligue para a Kaspersky agora mesmo no número (11) 2359-4641 ou entre em contato com a nossa equipe de vendas em brazil.kaspersky.com/produtos/contato-com-vendas, para saber mais sobre o Kaspersky Endpoint Security for Business.

brazil.kaspersky.com/produtos-para-empresas

VEJA A TI. CONTROLE A TI. PROTEJA A TI.
Com a Kaspersky, agora é possível.

* A empresa ficou na quarta posição na classificação da IDC de Worldwide Endpoint Security Revenue by Vendor (Receita em segurança de endpoints no mundo por fornecedor), 2012. Essa classificação foi publicada no relatório da IDC "Worldwide Endpoint Security 2013-2017 Forecast and 2012 Vendor Shares (Previsão de 2013-2017 de segurança de endpoints em todo o mundo e participações de fornecedores em 2012) (IDC #242618, agosto de 2013). O relatório classificou os fornecedores de software de acordo com as receitas de vendas de soluções de segurança de endpoints em 2012.