POR DENTRO DO MANUAL DO HACKER

DEZ TÉCNICAS DIRECIONADAS QUE PODERÃO ROMPER A SUA SEGURANÇA

Trustwave®

Leia para conhecer dicas de como pará-los!

Ataques diretos dão certo por serem furtivos, específicos e desconcertantemente pessoais. Se planejarem bem, os agressores avançados conseguem infiltrar-se em uma rede e roubar dados ou informações à vontade por meses ou mesmo anos.

Saiba como pará-los aprendendo diretamente com uma página do manual deles - literalmente. A Trustwave apresenta uma cópia inédita de um manual de técnicas de um agressor avançado. **Use-a bem para projetar uma segurança que combata seus ataques com perfeição.**

Um manual sobre como lucrar com ataques diretos

Antes de irmos direto para as técnicas mais avançadas de ganhar dinheiro com golpes cibernéticos, vamos falar um pouco sobre os princípios básicos deste negócio, que tal?

Primeiramente, o que não estamos tentando fazer: não estamos tentando cobrir toda a Internet com spam nocivo Viagrow ou injeção de SQL em massa em milhares de sites.

Estamos restringindo nosso trabalho a uma empresa ou setor específico da indústria com base nas oportunidades de vulnerabilidade que arranjarmos. Nossa maior abrangência será atingir uma gama de empresas com uma vulnerabilidade específica, seja algo nunca descoberto pelos pesquisadores de segurança ou algum patch aplicado recentemente por um colaborador.

Faça da maneira certa e você conseguirá por as mãos em grandes quantidades de dados importantes de clientes, podendo até mesmo tirar a sorte grande e chegar às propriedades intelectuais mais importantes. Com isso, você pode extorquir pessoas ou vender as informações para concorrentes – ou até para outros países.

Você não vai só comprar uma Ferrari nova.
Você comprará uma frota inteira delas.

Conheça seu inimigo

Com um pouco de pesquisa, uma redação astuta e a tecnologia certa, os golpistas podem ganhar a vida com ataques diretos para roubar dados corporativos e governamentais. Quanto mais soubermos sobre suas técnicas, melhor poderemos combatê-las.

Ao darmos uma espiada em cada um dos golpes deste manual de instrução dos bandidos, busquemos maneiras de virar estes conhecimentos internos contra os feiticeiros. Também oferecemos conselhos sobre como bloquear cada técnica de ataque.

Ato 1: Preparando o ataque

Vamos ganhar dinheiro fácil! Na maioria das vezes, existem cinco estágios para um ataque direto realmente eficiente:

PESQUISA: Comece fazendo o reconhecimento no alvo visado. Busque informações disponíveis publicamente e use a engenharia social para explorar informações sobre os sistemas de TI.

INTRUSÃO: Use as informações para encontrar o funcionário correto e a vulnerabilidade correta, visando a carga nociva; depois que morderem a isca, você terá o ponto de apoio inicial para a rede do alvo.

PROPAGAÇÃO: Após dominar uma máquina, use suas conexões de rede para espalhar malware para as outras, para que você tenha controle de outras máquinas mesmo que você seja detectado nesta.

CONTAMINAÇÃO: Após fazer o reconhecimento através das suas diferentes conexões, instale mais ferramentas para realmente começar a roubar e agregar dados.

EXTRAÇÃO: Finalmente, você precisa retirar todos os dados do local. Entre outras opções, tráfego de rede público tende a funcionar bem.

76%

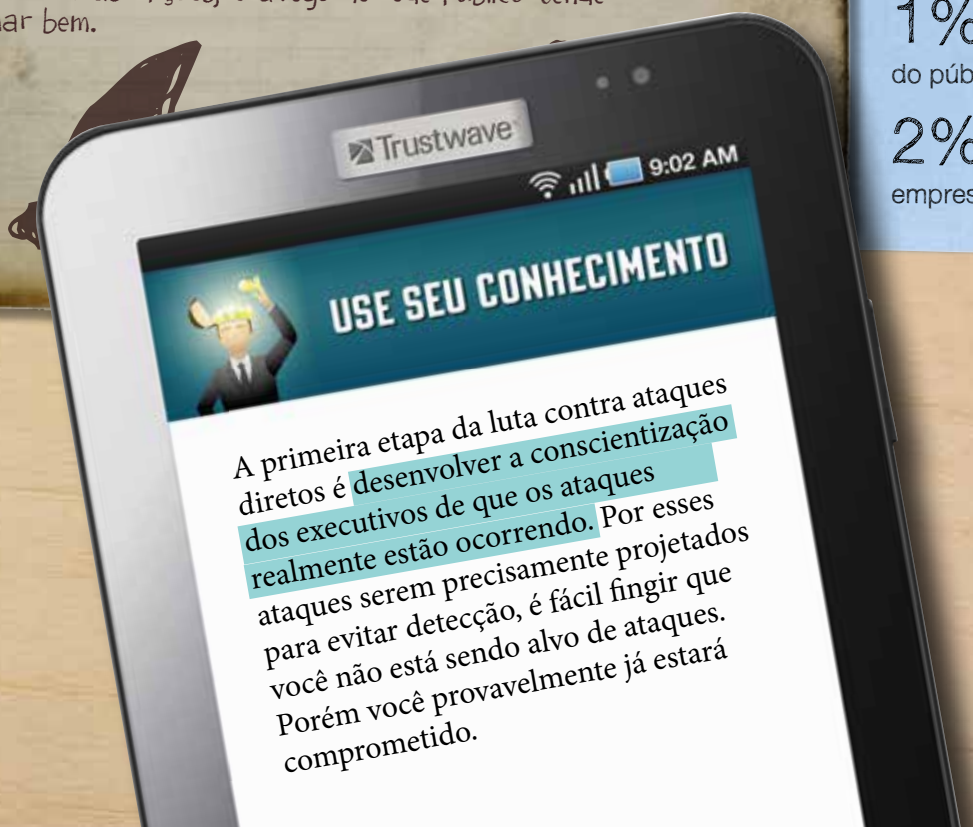
das organizações infiltradas precisam que alguém lhes avise que foram comprometidos

48% foram avisados por órgãos regulatórios

25% por agentes da lei

1% por descoberta do público

2% por outras empresas

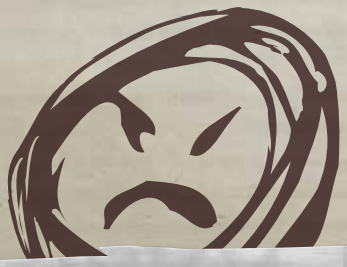


Ato 2: Especialize-se e terceirize

A questão não é o que você conhece, mas quem você conhece. Reúna sua própria quadrilha com especialistas que trabalham em conjunto para manter sua campanha de múltiplas etapas em curso. Assim como os homens das cavernas dividiam o trabalho em caça e colheita, você deve dividir o serviço em hack e scan.

Crie a equipe da maneira que quiser. Contrate pessoas, terceirize fornecedores de kits de malware ou até mesmo trabalhe em parceria igualitária. Apenas lembre-se do que se diz sobre a honra entre ladrões...

Pense: Sem noobs. Se eles não conseguem digitar, achar o caps lock ou escrever código melhor do que um garoto de script qualquer, é hasta la vista, baby.



A lista do FBI de especialidades de crimes cibernéticos

Agressores diretos criam negócios baseados em roubar o seu negócio. Assim como você dedicaria muitos funcionários e colaboradores especializados para solucionar seus problemas de negócio, eles terceirizam as habilidades necessárias para infiltrar-se nas suas defesas. Estas são as cinco maiores das dez especialidades mais comuns listadas pelo FBI:

CODIFICADORES: escrevem malware e ferramentas de exploração e roubo de dados

FORNECEDORES: negociam e vendem os dados roubados, kits de malware e dispositivos para redes comprometidas

HACKERS: buscam e exploram vulnerabilidades de aplicações, sistemas e redes

PESSOAL DE TI CRIMINOSO: mantém infraestrutura de TI criminosa como servidores e ISPs blindados

FRAUDADORES: criam e executam golpes de engenharia social como phishing e invasão de domínio

Ato 3: Escale seus ataques

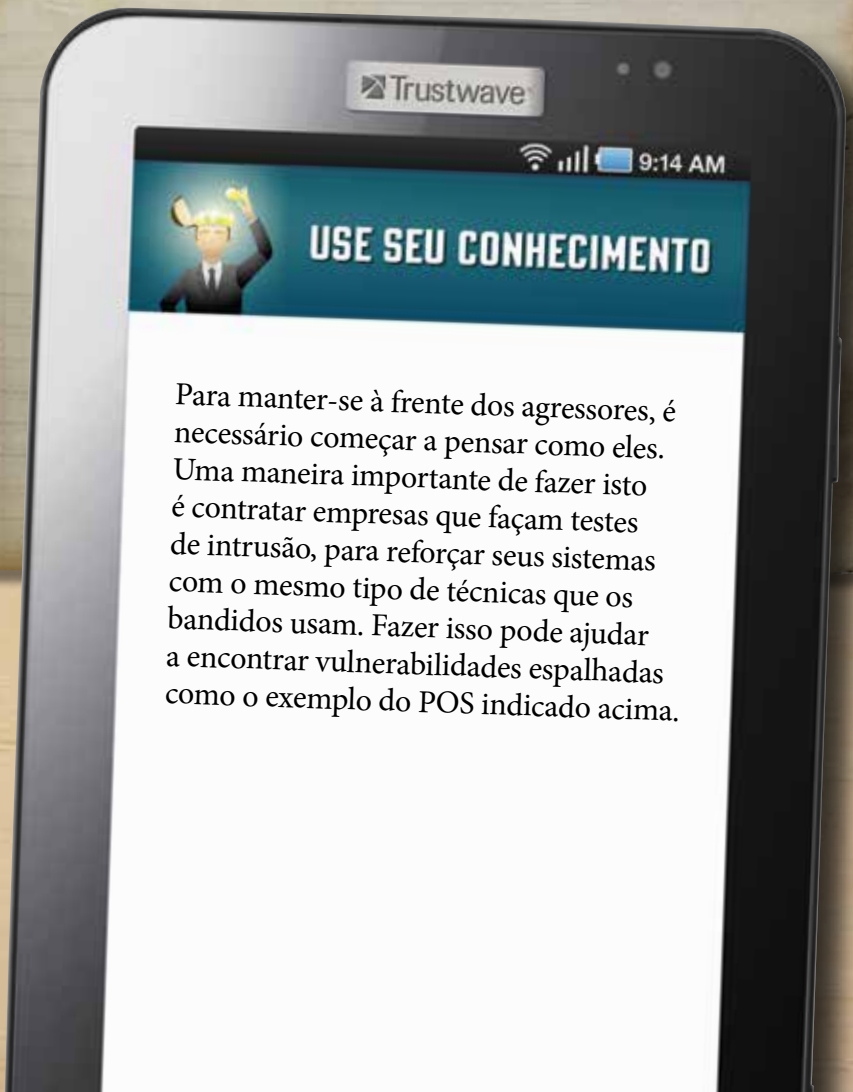
Após reunir o time perfeito, você vai explorar totalmente cada vulnerabilidade.

Desenvolveu ou comprou uma maneira de explorar uma nova vulnerabilidade em uma pobre empresa antiga de sistemas de ponto de venda (POS)? Talvez seja de uma pequena mercearia em São Francisco, mas talvez esta mesma vulnerabilidade e configuração de sistema funcionem em pontos de venda de outras lojas da mesma marca.

Nesse caso, a cama está feita. Você roubará dez vezes mais dados, mas somente precisará se dar ao trabalho de invadir um único local.

>1/3

Mais de um terço das investigações de violação de dados ocorrem em franquias



48%

das grandes empresas sofreram 25 ou mais ataques de engenharia social nos últimos dois anos[1]

70%

dos trabalhadores jovens ignoram regularmente as políticas de TI[2]

Ato 4: Jogue o jogador, não o jogo

Há uma boa chance de que os funcionários do seu alvo sejam muito prestativos mesmo sem saber. Eles lhe darão informações, ajudarão a carregar malware em suas máquinas e até mesmo segurarão a porta para você se for necessário entrar em um prédio. Esses camaradas devem ser seus melhores amigos durante os dois primeiros estágios do ataque: pesquisa e intrusão. Portanto, use isso em seu favor. Aqui vão algumas dicas:

- Se quiser informações sobre o organograma, localização de um centro de dados, a tecnologia usada ou qualquer outra coisa, ligue para alguém que teria essa informação, finja ser de outro departamento e simplesmente pergunte. Nove dentre dez vezes eles dirão livremente de boa vontade.

- Emergências que parecem oficiais funcionam sempre. Aja como se precisasse de ajuda para concluir um projeto "crítico para a missão" ou cabeças rolarão. Funciona melhor se você souber o nome do chefe de segunda linha.

FONTES:

[1]www.securingthehuman.org/blog/2011/09/22/justifying-your-awareness-program-with-social-engineering-survey

[2]www.eweek.com/c/a/Security/Younger-Employees-Ignore-IT-Policies-Dont-Think-About-Security-Says-Cisco-274940/

[3]www.securingthehuman.org/blog/2011/09/22/justifying-your-awareness-program-with-social-engineering-survey

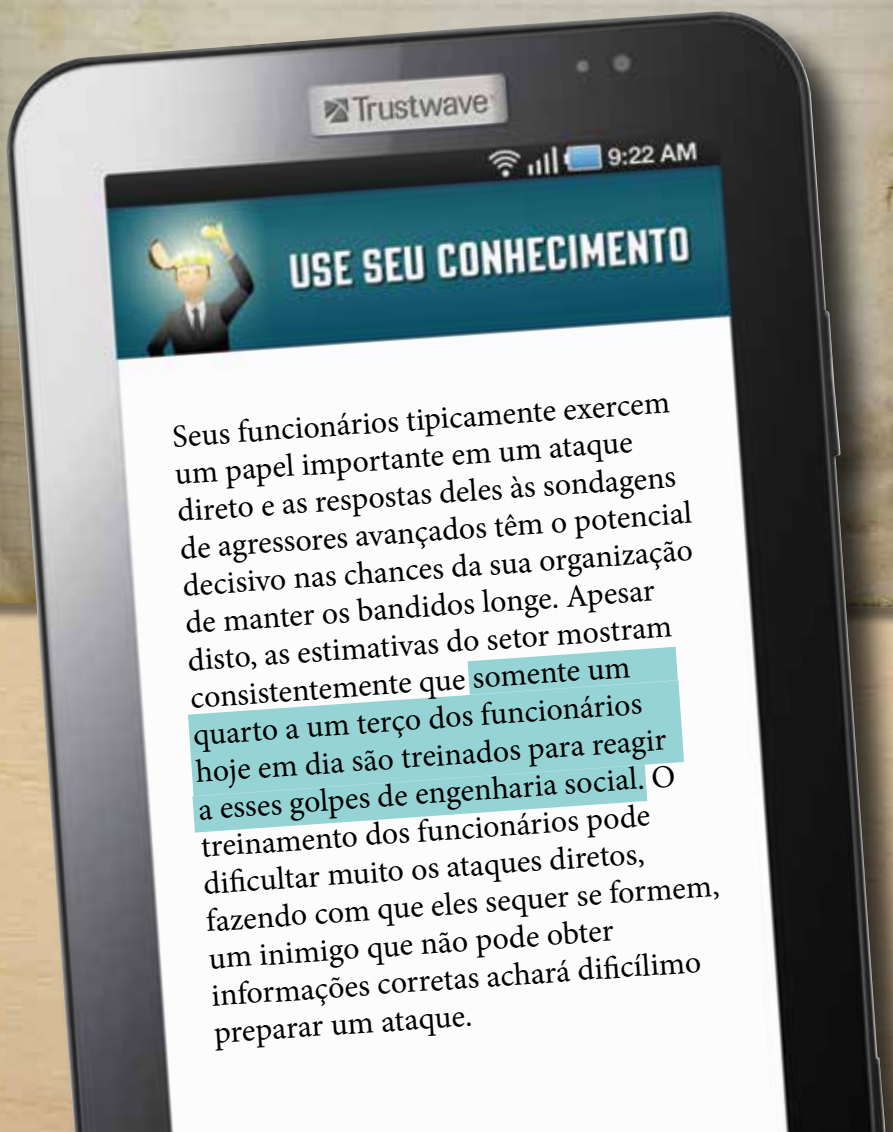
- Se o funcionário do seu alvo tiver um cargo alto e for paranoico demais para morder a isca, tente alguém que trabalhe com ele. Muitos administradores, ou mesmo funcionários temporários, trabalham em estações de trabalho que podem acessar os mesmos sistemas aos quais os computadores dos chefes estão ligados.

- Parabéns, você acaba de conseguir emprego no RH. Finja ser um recrutador. Neste mercado, o raciocínio das pessoas tende a ficar embaralhado se pensarem que há um novo emprego em vista.

- Dependendo do quanto você tem em jogo neste ataque, pode até mesmo investir em um pouco de engenharia social pessoalmente. Coloque um uniforme de entregas, traga algumas flores e veja se alguém lhe deixa entrar.

30%

das grandes empresas disseram que a engenharia social lhes custou uma média de $100.000 por incidente[3]



Ato 5: Socializar para um melhor reconhecimento

Às vezes você não precisa nem mesmo perguntar as informações para os funcionários, eles as oferecem livremente nas atualizações do Twitter. Use mídias sociais para descobrir todo tipo de informações importantes. Essas são algumas coisas que podem ser encontradas ao criar uma conta falsa do Facebook e convencer alguém a adicioná-la como amigo:

- Onde estudaram no ensino médio ou faculdade
- O nome de solteiro da sua mãe
- Data do aniversário
- Nome do cachorro
- Fatos sobre o emprego: Cargo, promoções, nome do chefe, grandes projetos em vista etc.

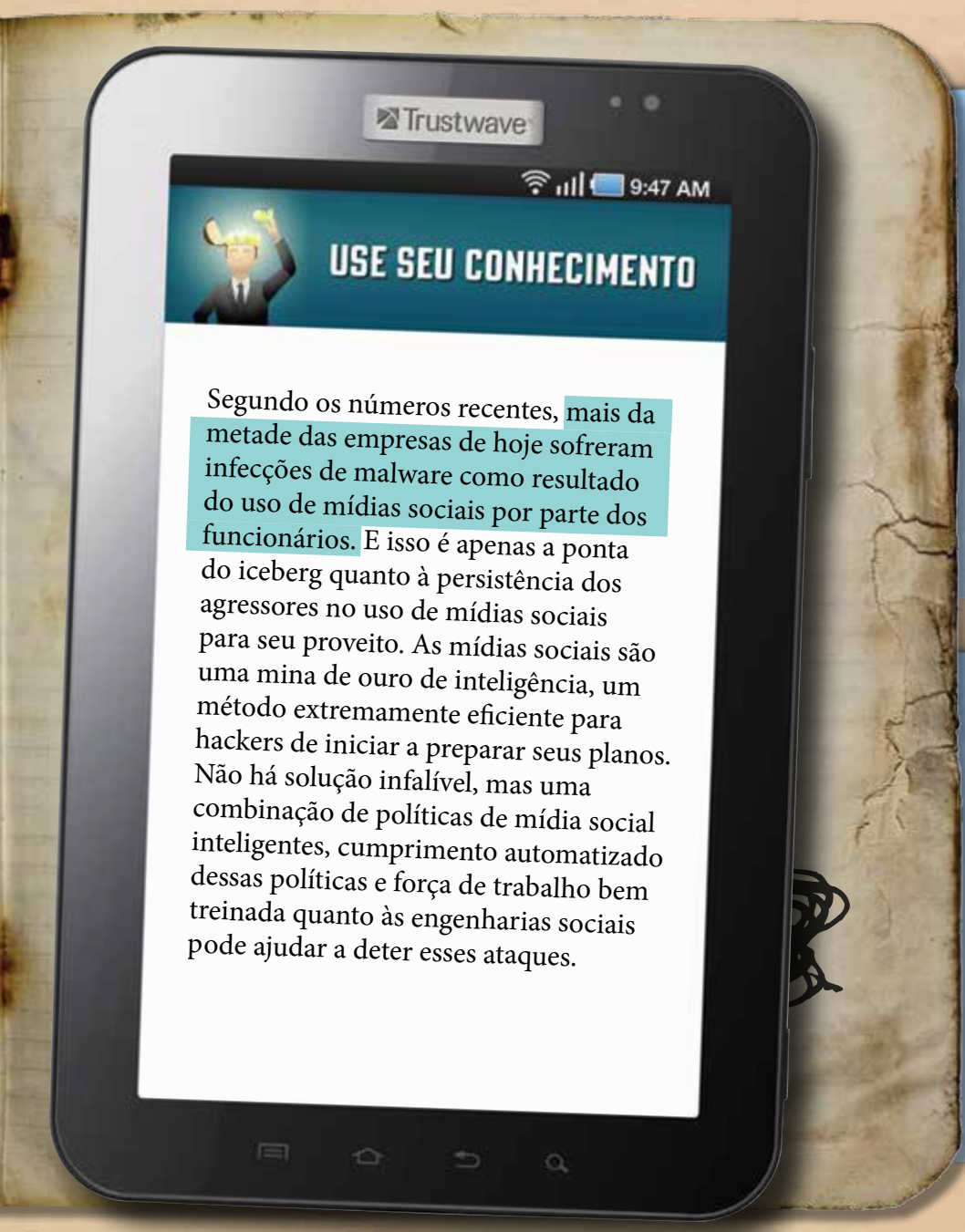
Todos esses dados são dicas valiosas para senhas, respostas de perguntas pessoais de sistemas e informações que vão ajudar a preparar sua campanha direta. Mesmo se você não for adicionado diretamente pela pessoa, poderá descobrir informações ao adicionar um dos amigos DA PESSOA. Maléfico, não é?

As mídias sociais também são imbatíveis para criar um perfil falso de um funcionário e pode ser o tipo de ferramenta para ajudá-lo na primeira intrusão na sua empresa-alvo. Se você souber quais são seus hobbies, para quais times torcem ou qualquer outra informação pessoal, você poderá bolar a isca perfeita para fazer com que eles visitem um site infectado por você ou convencê-los a abrir um documento nocivo.

"Criminosos cibernéticos estão usando os mecanismos de busca e redes sociais para ajudá-los a concentrar-se em funcionários específicos para golpes de engenharia sociais em uma ampla gama de empresas, firmas profissionais e agências do governo."

USA TODAY
A GANNETT COMPANY

— Byron Acohido
USA Today



32,8%

das senhas contêm um nome que figura em listas de 100 nomes mais usados para homens e mulheres

16,7%

das senhas contém um nome que figura na lista dos 100 nomes de cachorro mais usados

(este é o tipo de informação que as pessoas falam abertamente nas mídias sociais)

Ato 6: Sonde cada fraqueza

Por que quebrar uma janela se você tem a chave da porta da frente? Busque credenciais de usuário a cada etapa do caminho. A segunda meta é encontrar pistas sobre a arquitetura de TI da empresa-alvo para escolher o kit de malware certo ou para criar algo personalizado para ajudar a quebrar as barreiras se as chaves não estiverem disponíveis. Isto pode ser qualquer coisa, desde arquivos de senha não criptografados, listas de endereços IP da empresa ou informações de versão do sistema de ativos implementados.

Existem vulnerabilidades em todas as redes corporativas do mundo. Se sua empresa não as possuir, provavelmente um fornecedor ou empresa parceira com ligações com a sua empresa provavelmente as terá.

Será que você deve explorar vulnerabilidades do dia zero ainda não descobertas pela indústria de segurança ou aquelas que já possuem um patch? Ah, sim. Claro que sim. Se você for esperto, ambas farão parte do seu plano.

42%

de pessoal de TI das organizações compartilham senhas ou acessos a sistemas ou aplicativos[4]

48%

não mudam as senhas privilegiadas em 90 dias[5]

40%

ou mais empresas possuem processos de gerenciamento de patches informal ou inexistente[7]

FONTES:

[4]www.liebsoft.com/Password_Security_Survey/

[5]www.liebsoft.com/Password_Security_Survey/

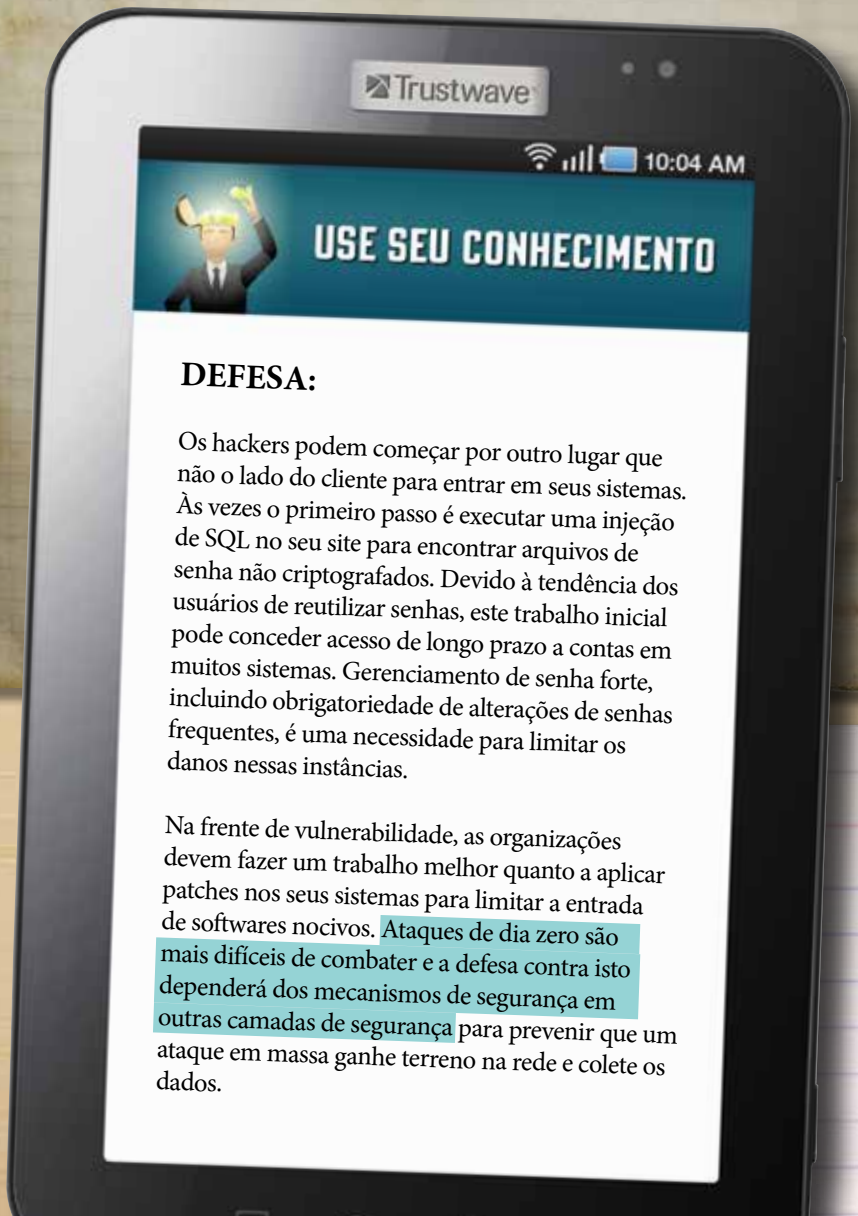
[6]www.trustwave.com/global-security-report

[7]https://securosis.com/assets/library/main/quant-survey-report-072709.pdf

Vulnerabilidades do dia zero são ótimas. Elas são caras para encontrar e explorar e vulnerabilidades conhecidas podem ser muito amplas. A maioria das áreas de TI estão ocupadas demais para se proteger com patches.

Em situações nas quais você está buscando informações muito específicas, como esquemas de fabricação que serão roubados para uma empresa ou país concorrente, e você não pode ser detectado, preparar os ataques para descoberta e exploração para o dia zero pode ser uma opção.

Porém, se tudo que você precisa é propagar o malware em uma empresa que você já sabe que possui sistemas sem patch (ou tem um palpite), a melhor opção é aproveitar vulnerabilidades antigas.



30%

de instalações de Apache Tomcat com interface administrativa acessível possuem credenciais padrão

A senha corporativa mais comum é Password1, pois atende minimamente os requisitos de complexidade do Diretório Ativo quanto à extensão, maiúsculas e caracteres numéricos.[6]

50%

dos ataques diretos ocorrem inicialmente através do uso da web

48%

dos ataques diretos ocorrem inicialmente através do uso de e-mail

2%

entram por dispositivos locais

Ato 7: Reinvente ataques da web e de e-mail antigos

Após sua equipe fazer o dever de casa em um alvo, é hora de lançar a isca e aguardar. Alguns dos atos de intrusão iniciais mais eficientes são fundamentalmente antigos em sua natureza, eles apenas fazem phishing em pessoas com mensagens de e-mail, mensagem instantânea ou mídia social falsos, para convencê-los a visitar um site infectado ou baixar um arquivo executável nocivo. Agora, use as informações coletadas para personalizar esta interação! Elabore uma isca que seja verossímil e construa um anzol que pareça tão inofensivo que ninguém sequer perceberá que você os fisgou.

Faça assim:

Exemplo 1: Seus hackers acabaram de encontrar uma vulnerabilidade crítica em uma plataforma de software, normalmente utilizada por empresas de entretenimento. Porém você precisa controlar uma máquina com acesso a ela para explorá-la. Felizmente para você, existem muitas pessoas que adoram fofocas desse ramo. Visto que a maioria das empresas-alvo está sediada em Hollywood, você usa uma injeção de SQL para comprometer estrategicamente a página inicial de alguns sites locais de fofoca com códigos nocivos que são baixados para as máquinas dos visitantes. Para evitar que os incômodos filtros de reputação descubram sua infecção do site, você o prepara de maneira que interaja somente com máquinas que trabalham à distância de um bloco de endereços de IP originados em Los Angeles.

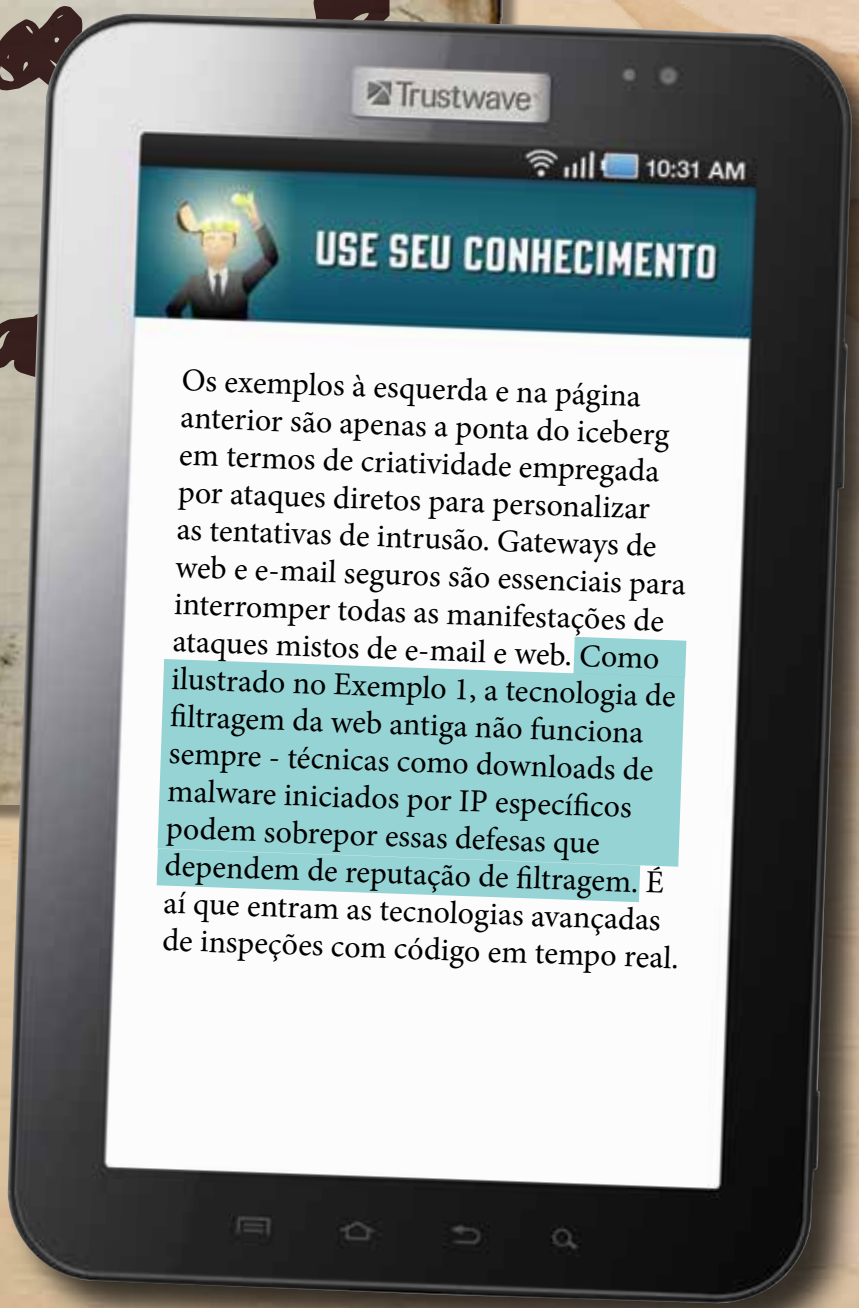
Informações sobre o inimigo

Atacantes avançados têm utilizado cada vez mais comprometimentos de redes estratégicas para infectar os alvos através de downloads rápidos: “A meta não é a distribuição de malware em grande escala através de comprometimento em massa. Em vez disso, os atacantes colocam seus códigos de exploração em sites específicos para um conjunto de visitantes que lhes interessam”

--Shadowserver

Exemplo 2: Você descobriu um gerente de primeira linha que possui acesso a sistemas que contêm toneladas de dados financeiros e de clientes comercializáveis. Você fica coleguinha dele pelo Facebook, convencendo-o de que você o conhece de uma conferência profissional de contabilidade. Através do seu status de amigo, você descobre que sua verdadeira paixão não são os livros-caixa, mas sim a fotografia. Assim, você ordena que seus hackers e codificadores criem um site falso de fotografia amadora com algumas cargas emitidas por download rápidos ocultos. Enquanto ele lê as dicas de SLRs digitais, sua carga nociva é carregada furtivamente em segundo plano.

Exemplo 3: Você pôs as mãos no organograma de uma empresa-alvo e lê no blog da empresa sobre a nova contratação estratégica de John Smith no departamento de marketing. Você cria uma conta do Gmail com o nome do gerente de RH e utiliza-a para escrever um e-mail dizendo como o RH fez um erro gravíssimo e repassou a todo mundo informações de salários e benefícios do Smith. Eles abrem um anexo, "JohnSmithcompensation.xls," e pronto, a curiosidade matou a rede.



Em **76%**

das investigações de resposta a incidentes, detectou-se que uma empresa terceirizada responsável por suporte ao sistema, desenvolvimento ou manutenção de ambientes de negócios introduziu deficiências de segurança.

88%

do malware direto não é detectado por antivírus tradicionais

Ato 8: Pense lateralmente

Uma backdoor da rede corporativa pode ser bom, mas quanto mais, melhor. Se você quiser se manter em uma rede por muito tempo, precisará usar aquele domínio inicial do lado do cliente para mover-se lateralmente pela rede. Desta maneira, se sua primeira intrusão for detectada e seu pacote de malware for eliminado da máquina, você ainda manterá as mãos na direção em outro ponto.

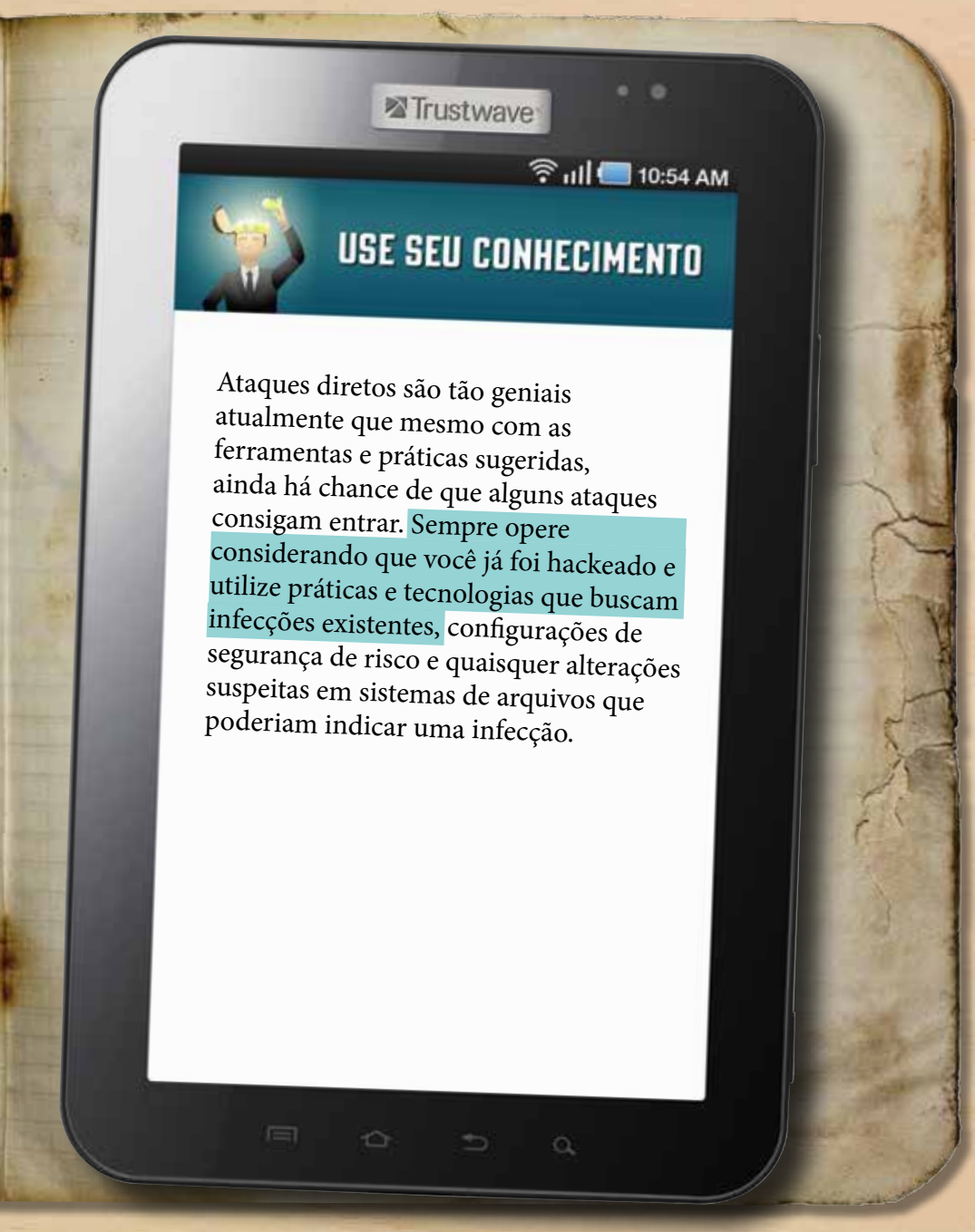
O segredo? Você precisa propagar-se com diversidade. É necessário usar tipos completamente diferentes de cargas em diferentes sistemas pois após um tipo ser descoberto, eles varrerão a rede buscando por qualquer coisa que pareça uma amostra semelhante. Porém, se você controlar alguns terminais com tipos diferentes de malware, eles provavelmente nunca sequer saberão que ainda estão comprometidos.

INFORMAÇÕES SOBRE O INIMIGO

41,2% DOS MALWARE USAM HTTPS PARA RETIRAR DADOS

29,4% USAM FTP

11,8% USAM SMTP


Trustwave
10:54 AM
USE SEU CONHECIMENTO
Ataques diretos são tão geniais atualmente que mesmo com as ferramentas e práticas sugeridas, ainda há chance de que alguns ataques consigam entrar. Sempre opere considerando que você já foi hackeado e utilize práticas e tecnologias que buscam infecções existentes, configurações de segurança de risco e quaisquer alterações suspeitas em sistemas de arquivos que poderiam indicar uma infecção.

Ato 9: Esconda-se em plena vista

A dissimulação é o segredo do jogo nesses ataques diretos. Ás vezes você só quer fazer o arroz com feijão de entrar e sair de uma rede com o máximo de informações possíveis ou com uma informação específica. Porém, geralmente a maneira mais lucrativa é drenar o banco de dados pouco a pouco por MUITO tempo.

Coloque alguns silenciadores técnicos nas suas intrusões. Você não vai querer derrubar um vaso caro ao roubar digitalmente a casa, quer? Cada movimento deve ser planejado para evitar disparar qualquer alarme. Ao emitir ferramentas nos sistemas para agregar dados e controlar backdoors, essas são algumas dicas:

- Evite malware autorreplicante
- Esconda malware nas pastas do sistema e faça com que pareçam processos comuns
- Use contas de webmail para rotear o tráfego de comando e controle SSL criptografado para suas backdoors
- Use programas de compactação para esconder códigos binários nocivos
- Se puder, armazene alguns componentes de malware na nuvem

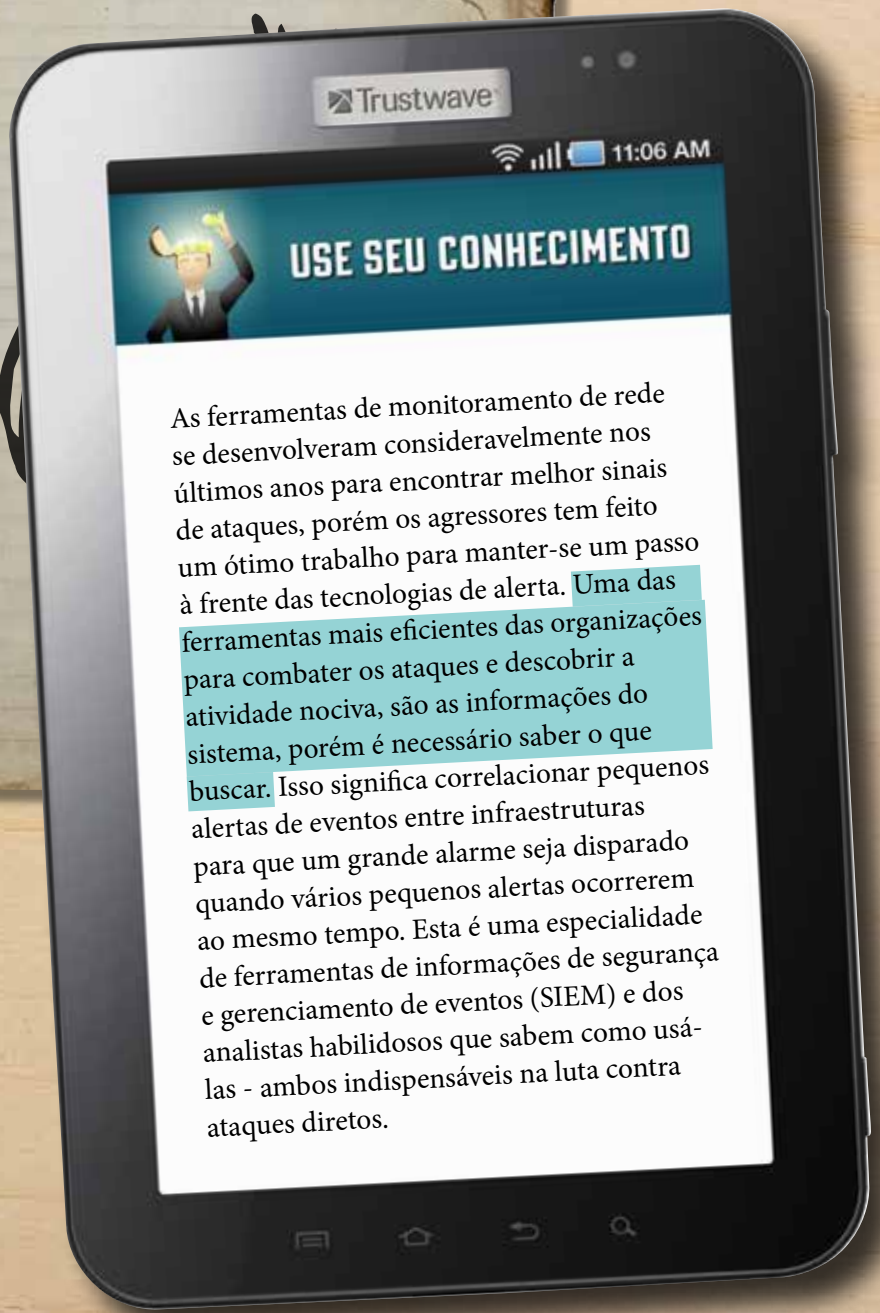
Informações sobre o inimigo

Como o objetivo final de qualquer ataque direto é roubar dados, somente fará sentido depender de ferramentas centralizadas em dados para frustrar os inimigos. Isto pode ser feito ao compreender o contexto dos dados e detectar o tráfego de aplicativos de rede maliciosos que está levando os dados através de firewalls de última geração alertas para aplicativos. O uso de criptografia para ocultar ataques e roubo de dados está em alta. Mais de 25% de todos os dados retirados pelos atacantes são criptografados por criminosos cibernéticos. Também é crucial utilizar técnicas de criptografia que inutilizem os dados se estes forem retirados.

Ato 10: Pegue os dados em silêncio

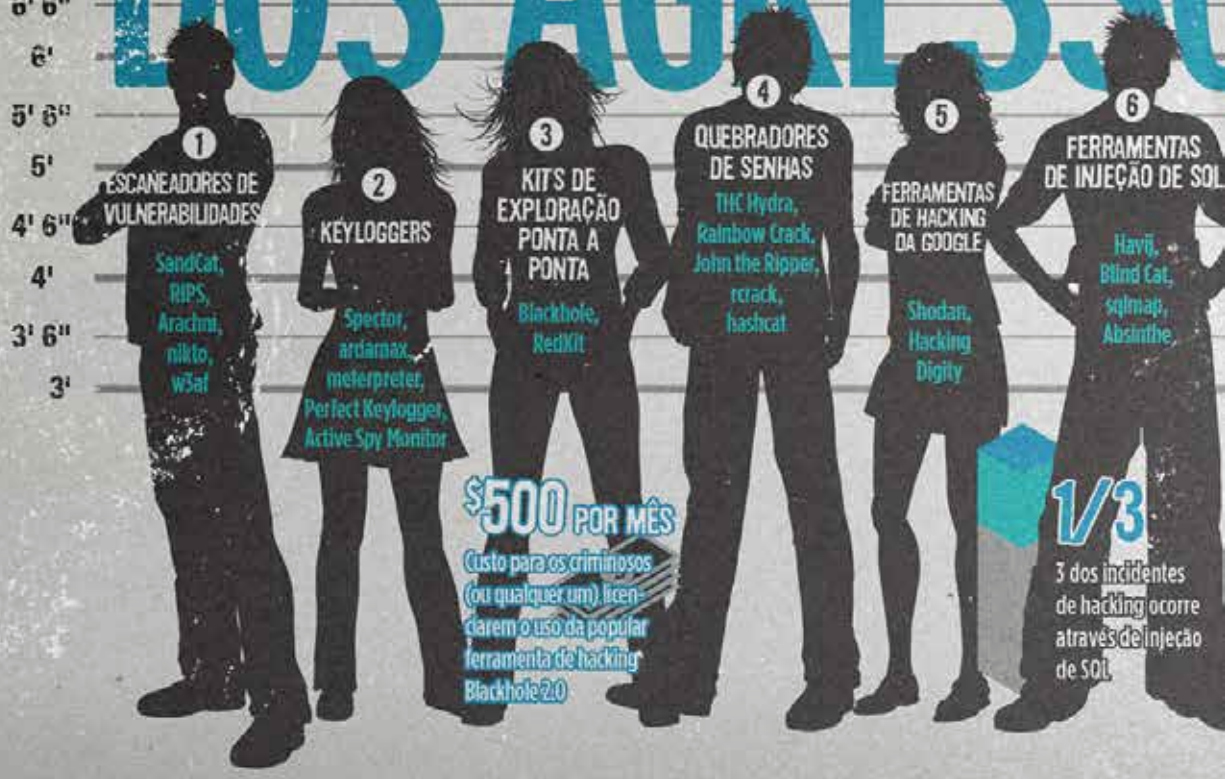
Talvez você seja um spearphisher da elite, daqueles muito bons em dominar uma rede e sabe descobrir dados preciosos como ninguém. Tudo isso não significará nada se você não conseguir retirar os dados da rede. Seja paciente! A extração silenciosa e lenta torna mais fácil o trabalho de roubar quantidades maiores de informação sem disparar alarmes que interromperão seu fluxo.

Por sorte, a maioria das empresas não configura os firewalls para bloquear tráfego de saída, então você tem muitas opções. O tráfego da web público pode vir a ser uma das maneiras mais eficientes de vazar dados lentamente de uma rede. O tráfego HTTPS proporciona o benefício adicional de manter-se longe de ferramentas de prevenção de violação de dados ao ocultar os dados em uma proteção de SSL.



OS INDOMÁVEIS:

DOS AGRESSO



1 Alguns desses escaneadores de vulnerabilidade percorrem redes já comprometidas em busca de vulnerabilidades, enquanto outros varrem a internet em busca de portas abertas e aplicativos vulneráveis da web para exploração

2 Geralmente integrado a cargas de malware infiltradas em máquinas através de engenharia social, os keyloggers registram a digitação dos usuários, aguardando silenciosamente para coletar as credenciais de senha

3 Kits ponta a ponta permitem que criminosas comuns executem uma campanha de hacking totalmente automatizada com pouquíssimo conhecimento técnico.

4 Após os agressores adentrarem um sistema ou rede, eles podem usar quebradores de senhas para atacar arquivos de senha criptografados e descobrir credenciais para comprometer ainda mais a rede.

5 Muitos dispositivos sensíveis conectados à Internet propagam informações sobre como hackeá-los para todo o mundo, essas ferramentas de busca automatizam a caça por essas dicas valiosas

6 Vulnerabilidades de injeção de SQL são alguns dos meios mais comuns usados para roubar bancos de dados em contato com a internet e descobrir de maneira fácil tais automatizadores de varredura e exploração

FONTES: www.trustwave.com/global-security-report
www.hackersmedia.com/2012/09/blackhole-exploit-kit-20-made-available.html

ORES DIRETOS

7 Hackers usam detectores de rede e ferramentas de mapeamento de rede para compreender melhor como uma rede foi desenvolvida e assim planejar ataques ainda mais profundos

8 Essas ferramentas ajudam os bandidos a mudar o comportamento do tráfego de rede, redirecionando o usuário a destinos nocivos, sequestrando sessões de web e captando o tráfego para obter informações úteis para o ataque

9 Os malware usam empacotadores e criptógrafos para ocultar os códigos binários a fim de dificultar a detecção pelos antivírus

10 Os agressores podem contornar técnicas fortes de criptografia usando essas ferramentas para capturar dados armazenados na memória do computador durante processos legítimos de retirada de criptografia iniciados pelo usuário

11 Criminosos usam o shell code para implantar backdoors de difícil detecção em servidores da web para conceder acesso a informações da rede

12 Essas ferramentas facilitam a RETIRADA dos dados da rede pelos bandidos ao enviar o tráfego por canais ocultos cuja saída é difícil de detectar

Trustwave
www.trustwave.com

A SEGURANÇA É UM PROCESSO, NÃO UM PRODUTO

É por isso que, através de uma abordagem integrada e automatizada, a Trustwave fornece uma segurança forte, conformidade contínua e menos problemas. Nosso amplo portfólio de tecnologias integradas, serviços de conformidade e risco, bem como pesquisa, testes e inteligência de risco de elite do SpiderLabs, ajudam a proteger seu negócio, centralizar a conformidade e obter inteligência significativa e factível que você precisa para tomar decisões mais rápidas e proativas. Além disso, nossa abordagem única ajuda a obter uma continuidade de negócio e conformidade, ao implementar, monitorar, auditar e reforçar rapidamente a proteção e o controle sobre os seus dados e ativos sensíveis. Interessado em como a Trustwave pode ajudar? **Visite www.trustwave.com.**

Trustwave®