[state of the internet] / segurança

Volume 5, Relatório especial de mídia

Preenchimento de credenciais: Ataque e Economias

Introdução

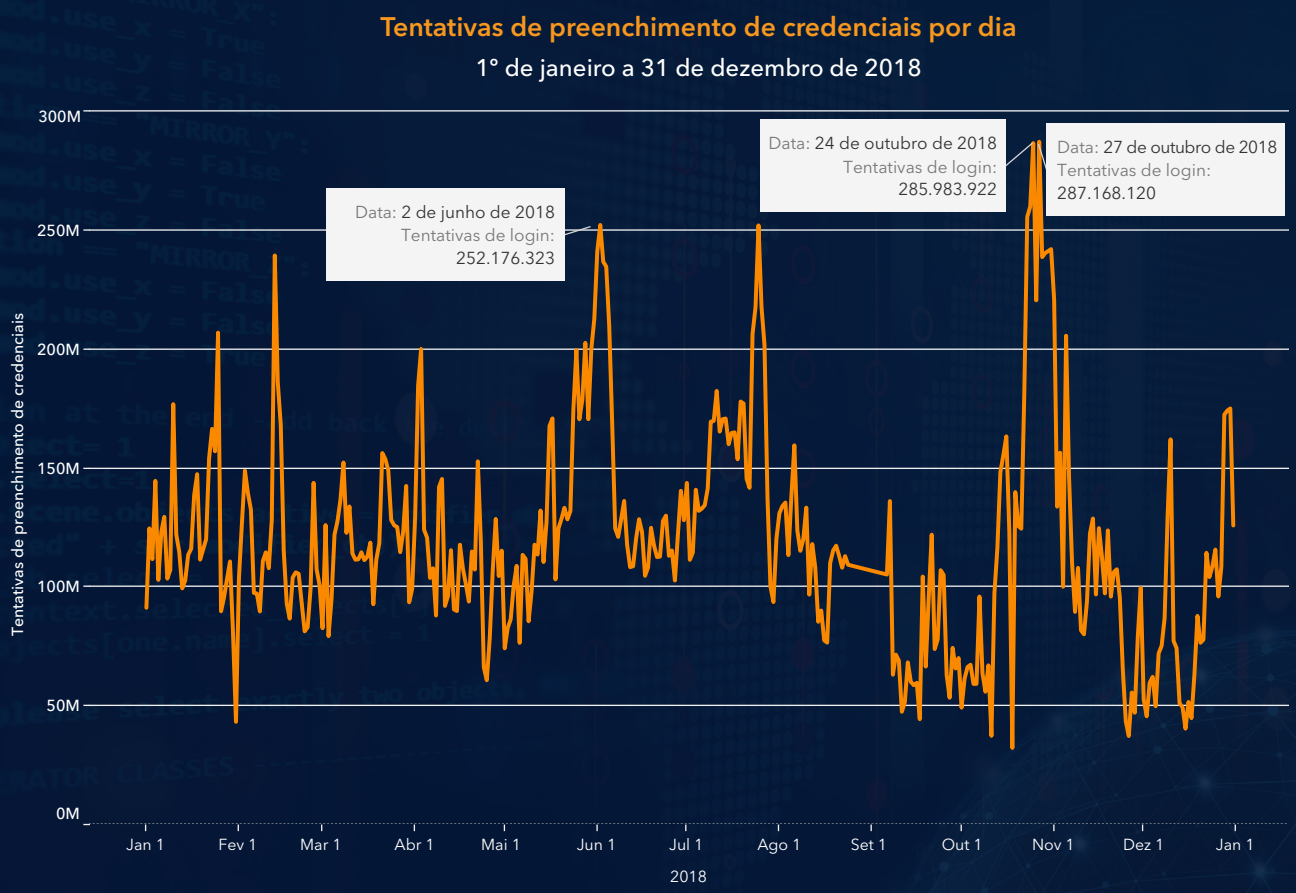
A Akamai registrou quase 30 bilhões de ataques de preenchimento de credenciais em 2018. Cada ataque representou uma tentativa de uma pessoa ou de um computador de fazer login em uma conta com um nome de usuário e senha roubados ou gerados. A grande maioria desses ataques foi realizada por botnets ou aplicações all-in-one.

Os botnets são grupos de computadores responsáveis por vários comandos. Eles podem ser instruídos a encontrar contas vulneráveis a serem acessadas por alguém que não seja o proprietário da conta. Elas são chamadas de ataques de controle de conta (ATO). As aplicações AIO permitem que um indivíduo automatize o processo de login ou o processo ATO e são as principais ferramentas para controles de conta e coleta de dados.

O que isso tem a ver com as organizações de mídia, as empresas de jogos e o setor de entretenimento? Muito. Essas organizações estão entre os maiores alvos de ataques de preenchimento de credenciais. As pessoas por trás desses ataques percebem o valor de uma conta, seja em um site de streaming, em um jogo ou na conta de rede social de alguém. E estão dispostas a fazer o que for necessário para roubá-los.

Neste relatório, apresentaremos uma visão geral dos ataques de preenchimento de credenciais em 2018 contra os setores mencionados anteriormente e analisaremos os riscos desses ataques. Também analisaremos algumas maneiras como os adversários realizam esses ataques.

As organizações de mídia, as empresas de jogos e o setor de entretenimento estão entre os maiores alvos de ataques de preenchimento de credenciais.



Ataques por dia

Em 2018, a Akamai observou milhões de ataques de preenchimento de credenciais todos os dias. Esses ataques foram direcionados a uma variedade de setores, desde mídia e entretenimento até varejo e jogos. Como visto na Figura 1, em três dias houve um pico de mais de 250 milhões de tentativas. Os ataques de preenchimento de credenciais estão se tornando os favoritos de criminosos em todos os níveis de habilidade. Embora os relatórios "State of the Internet" (SOTI) anteriores tenham examinado seu impacto no varejo, esta edição examina os setores de mídia e de entretenimento.

Os criminosos visam grandes marcas de vídeo e de entretenimento, pois o acesso a contas verificadas pode ser vendido ou comercializado em mercados clandestinos. Caso já tenha transmitido uma música, um filme ou um programa de TV online, você possivelmente já estará familiarizado com algumas das contas que a maioria dos criminosos favorece. As informações associadas a essas contas também têm valor.

Figura 1

Três dos maiores ataques observados em 2018 são destacados, incluindo dois que ocorreram em datas próximas

Maiores ataques

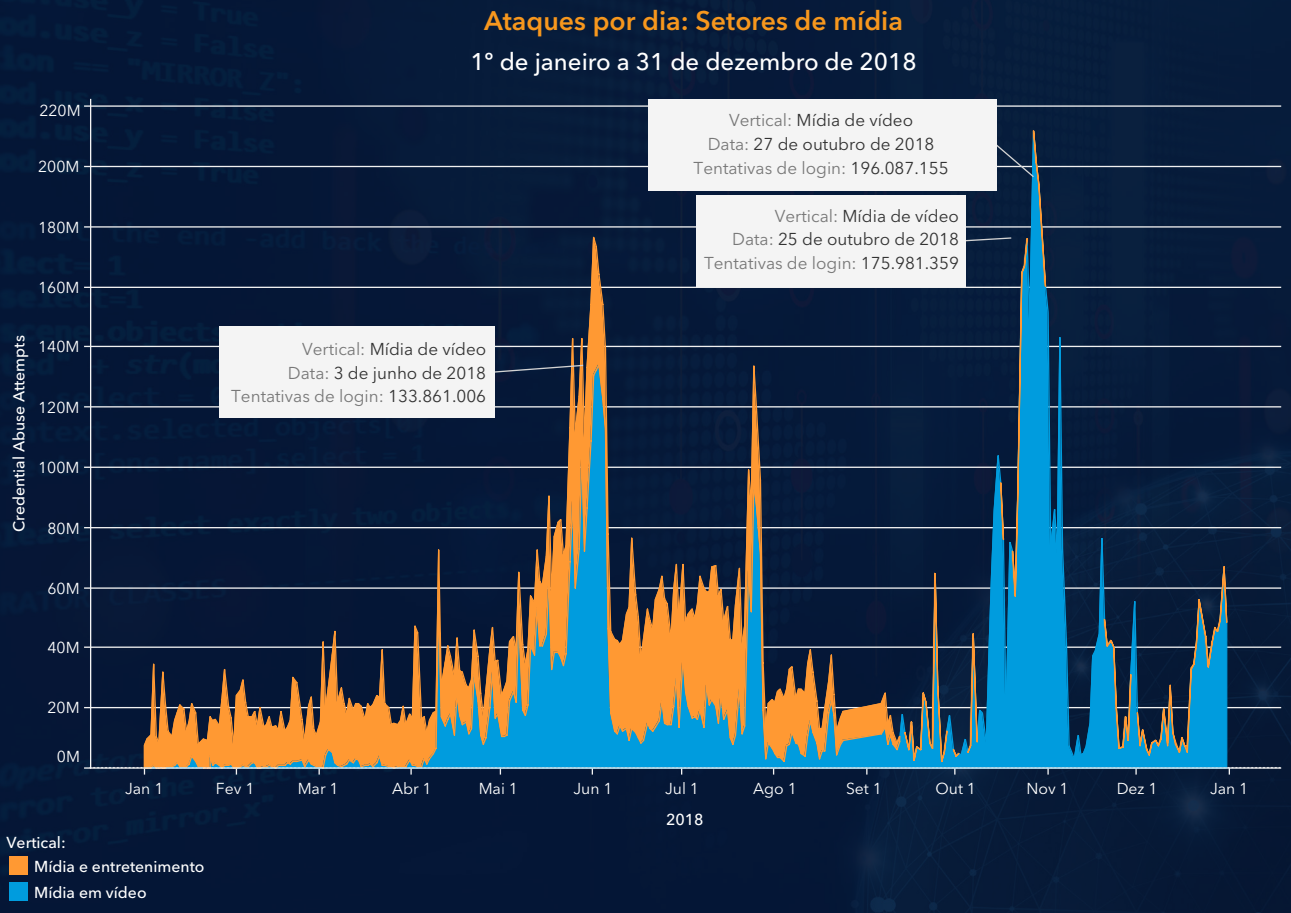
Somente no setor de mídia de vídeo, três dos maiores ataques de preenchimento de credenciais em 2018 saltaram de 133 milhões para quase 200 milhões de tentativas. Isso é significativo, pois as datas dos ataques estão sincronizadas com violações de dados conhecidas: os vendedores podem ter testado as credenciais antes de elas serem vendidas. No início de fevereiro de 2019, cerca de 620 milhões de nomes de usuário, senhas e outros registros, obtidos de 16 organizações com violações de dados divulgadas, foram colocados à venda na darknet.

Preenchimento de credenciais

No início de 2019, você pode ter ouvido as notícias de que um indivíduo anônimo lançou um conjunto de endereços de e-mail e senhas, aqui referidos como "lançamentos de 1 a 5", para preenchimento de credenciais.

Figura 2

Três dos maiores ataques de preenchimento de credenciais contra o setor de mídia de vídeo durante o ano de 2018 aumentaram de 133 milhões para quase 200 milhões de tentativas



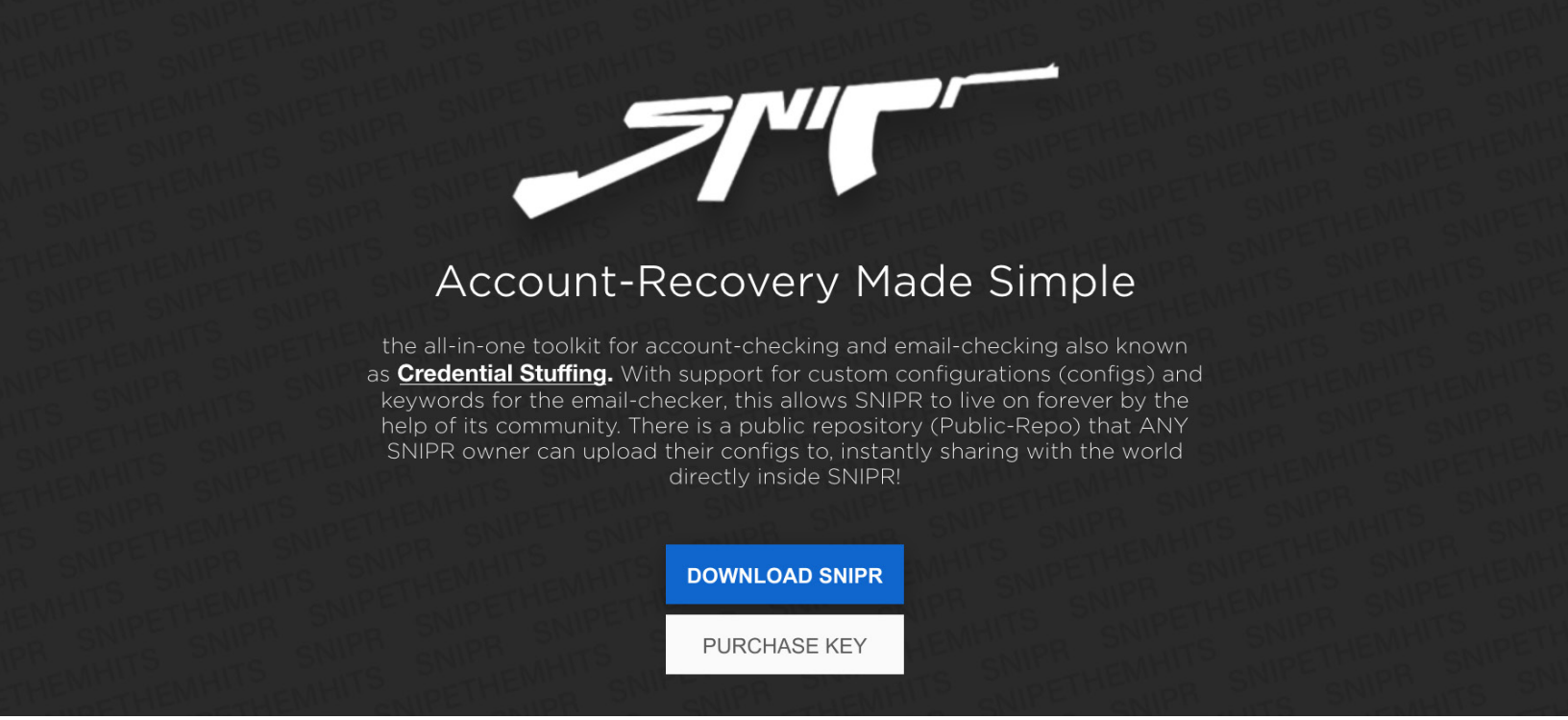


Figura 3

O SNIPR é um AIO de baixo custo usado para preenchimento de credenciais e é vendido por US$ 20

Desses cinco conjuntos, essa pessoa anônima publicou cerca de 1 TB de dados, totalizando mais de 25 bilhões de combinações de endereços de e-mail e senhas. Depois que as entradas duplicadas e inutilizáveis foram removidas, ainda havia bilhões de combinações disponíveis em vários locais online no momento em que este relatório foi escrito.

As versões de 1 a 5 são apenas conjuntos básicos de nomes de usuário e senhas, embora representem o maior conjunto já lançado em uma única instância. Um conjunto tão grande é uma exceção, e não a norma. Porém, conjuntos como esses são criados pela mesclagem de listas de combinação de outras violações de dados, incluindo aquelas altamente notáveis.

Os ataques de preenchimento de credenciais são um grande risco para as empresas online, portanto, ter um pool de mais de 1 bilhão de possíveis combinações reduz significativamente a barra de entrada de qualquer possível criminoso que queira lucrar com a tendência de preenchimento de credenciais. No entanto, listas como essas não são a única maneira de os criminosos coletarem os dados que precisam para realizar ataques de preenchimento de credenciais.

Em um vídeo do YouTube assistido por pesquisadores da Akamai, uma pessoa orientou os espectadores com um tutorial passo a passo sobre como criar listas de combinação para usar contra o popular jogo de batalha real online.

O tutorial começou ensinando o conceito de "Google Hacking", que usa os operadores dos mecanismos de pesquisa do Google para localizar sites que possam estar vulneráveis à injeção de SQL. Depois que os sites foram localizados, o tutorial ensinou aos espectadores como explorar esses domínios vulneráveis usando uma ferramenta comum de injeção de SQL. Essa ferramenta baixa endereços de e-mail e senhas, desvenda senhas, se necessário, gera uma lista de combinação válida e, em seguida, acompanha um programa de "verificação" com proxies para testar a validade das listas recém-criadas.

Esses programas de verificação, ou aplicações All-in-One (AIOs), permitem que o invasor valide credenciais roubadas ou geradas. Dependendo da aplicação, os AIOs podem direcionar formulários de login diretamente ou APIs, ou ambos, dependendo da situação.

Depois que as contas são confirmadas como válidas, elas podem ser vendidas, negociadas ou coletadas para vários tipos de informações pessoais. Dependendo da situação, não é incomum que as três ações aconteçam.

Há pontuações de AIOs online. Alguns são vendidos abertamente, e outros são vendidos ou comercializados clandestinamente. Um deles, uma aplicação chamada SNIPR, é favorecido como uma ferramenta de nível básico por aqueles que procuram atingir jogos, rede social e mídia de transmissão.

Outro AIO, chamado STORM, usa configurações detalhadas que são vendidas ou negociadas por conta própria. No momento da elaboração deste relatório, um vendedor da darknet estava promovendo configurações STORM para uso contra uma das maiores plataformas de streaming online a um custo de US$ 52.

O mesmo vendedor também está vendendo códigos de cartão-presente para a plataforma mencionada anteriormente com desconto, oferecendo cartões de US$ 30 por apenas US$ 7,80. Às vezes, esses códigos são gerados, mas, na maioria das vezes, eles são comprados com cartões de crédito roubados. Portanto, todo dinheiro arrecadado é puro lucro para o criminoso.

Esse mesmo varejista também tem um negócio estável na venda de listas de combinação de preenchimento de credenciais. Uma listagem corresponde a um lote de 5 bilhões de endereços de e-mail aleatórios e senhas por US$ 5,20. Uma outra é uma lista personalizada de 50.000 endereços de e-mail e senhas pelo mesmo preço. A opção personalizada permite que o comprador escolha o formato (email:pass ou user:pass), o provedor, o local etc.

Vídeos de treinamento do SNIPR no YouTube

Ao pesquisar fatos e dados para este relatório, os pesquisadores da Akamai se depararam com vários vídeos relacionados do YouTube que abordam o preenchimento de credenciais e ataques associados. Conseguimos confirmar que pelo menos 89.000 pessoas assistiram aos vídeos de demonstração e de tutorial sobre o AIO conhecido como SNIPR.

Existem dezenas de vídeos, que abrangem várias versões do SNIPR, detalhando como usar a aplicação, bem como obter o máximo retorno sobre o investimento em recursos. Como o SNIPR é uma ferramenta de nível básico, esses tutoriais são frequentemente solicitados pelos usuários da ferramenta, que são criados pelos desenvolvedores ou por outros usuários.

Uma economia crescente

O mercado de contas roubadas de mídia e de entretenimento está prosperando.

Os setores de mídia, jogos e entretenimento são alvos valiosos para criminosos que procuram trocar informações e acessos roubados. As contas são vendidas em massa, e o objetivo dos criminosos é mover seus bens por volume, em vez de fazer vendas de contas únicas.

Muitas contas comprometidas por meio do preenchimento de credenciais são vendidas por apenas US$ 3,25. Essas contas vêm com garantia: se as credenciais não funcionarem depois de vendidas, elas poderão ser substituídas sem custos, uma oferta dos vendedores de serviços para incentivar a repetição de compras. Esse serviço existe porque as marcas se tornaram cada vez mais rápidas ao detectar contas comprometidas e desativá-las.

Então, como os ataques de preenchimento de credenciais se transformarão em contas roubadas que serão vendidas em um mercado criminoso posteriormente? A resposta é simples: por meio do compartilhamento de senha.

As tentativas de preenchimento de credenciais podem avançar para aquisições e concessões de contas completas porque as pessoas tendem a usar a mesma senha em vários sites, ou as senhas usadas são facilmente adivinhadas e geram credenciais.

Principais origens de ataques

PAÍS DE ORIGEM	ATO HEUR.LOGINS
Estados Unidos	4.016.181.582
Rússia	2.509.810.095
Canadá	1.498.554.065
Vietnã	626.028.826
Índia	625.476.485
Brasil	585.805.408
Malásia	369.345.043
Indonésia	367.090.420
Alemanha	354.489.922
China	308.827.351

Figura 4

Principais origens de ataque classificadas por país. Os Estados Unidos continuam sendo a principal origem dos ataques de preenchimento de credenciais

Principais destinos de ataque

PAÍS DE DESTINO	ATO HEUR.LOGINS
Estados Unidos	12.522.943.520
Índia	1.208.749.669
Canadá	1.025.445.535
Alemanha	760.722.969
Austrália	104.655.154
Coreia	37.112.529
China	26.173.541
Gibraltar	6.559.360
Países Baixos	4.991.790
Japão	3.424.334
Itália	2.601.632
França	1.864.733
Hong Kong	1.305.262

Figura 5

Principais destinos de ataque classificados por país. Os Estados Unidos continuam sendo o principal destino dos ataques de preenchimento de credenciais

Portanto, uma violação de dados em um site ou um lançamento massivo de combinações conhecidas de nomes de usuário e senhas (como versões de 1 a 5) pode fazer com que uma pessoa tenha sua vida digital exposta. Depois que isso acontece, todas as informações associadas a esse indivíduo podem ser empacotadas e vendidas.

Como esperado, os Estados Unidos lideraram a lista de países de origem com ataques de preenchimento de credenciais. Isso porque é ali que a maioria das ferramentas comuns de preenchimento de credenciais é desenvolvida. A Rússia está em segundo lugar, e o Canadá, em terceiro. Além disso, os Estados Unidos são o principal local dos destinos de ataque, pois muitos dos alvos mais populares estão nesse país.

A Índia e o Canadá ocupam o segundo e o terceiro lugares dos destinos de ataque, mas são muito ofuscados em volume em comparação aos Estados Unidos.

> *"Os Estados Unidos são o ponto principal de destino dos ataques."*

Pensando no futuro

O possível impacto nas empresas dos criminosos que fazem preenchimento de credenciais é amplo. As listas de combinação, como as que foram lançadas anonimamente no início deste ano, são apenas a ponta do iceberg. Quando um ataque de preenchimento de credenciais é bem-sucedido, a marca absorve isso na sua reputação (mesmo que não tenha culpa) e enfrenta um aumento dos custos operacionais, como resposta a incidentes, folha de pagamento e comunicações de crise, e outras despesas associadas começam a surgir.

> *Quando um ataque de preenchimento de credenciais é bem-sucedido, a marca tem sua reputação prejudicada (mesmo que não seja culpa dela)...”*

Em fevereiro de 2019, um conhecido serviço fiscal online emitiu notificações de violação para alguns clientes. A carta de notificação explicou claramente como o ataque em si foi o de preenchimento de credenciais, pois todas as contas em risco estavam usando senhas expostas por violações de dados em outros lugares. O serviço de impostos redefiniu as senhas para impedir acesso adicional e alertar os clientes. Embora o incidente claramente não tenha sido culpa do provedor do serviço fiscal, os clientes não entenderam dessa forma e a reação pública à notícia foi negativa.

A parceria com um provedor de soluções sólidas para ajudar a detectar e interromper ataques de preenchimento de credenciais é a opção óbvia de se defender contra isso. Mas, lidar com a ameaça do preenchimento de credenciais não é uma situação simples. Uma organização precisa garantir que uma solução defensiva seja adaptada aos negócios, já que os criminosos ajustarão seus ataques para evitar configurações prontas e mitigações básicas.

Para corrigir o problema, ainda é preciso mais do que um único fornecedor ou um conjunto de produtos. Os usuários precisam ser informados sobre ataques de preenchimento de credenciais, phishing e outros riscos que colocam as informações de suas contas em risco. As marcas devem enfatizar o uso de senhas e gerenciadores de senhas exclusivos para os clientes e destacar o valor da autenticação multifator. Ao discutir os scripts ATOs e AIO, os criminosos sempre reclamam do uso da autenticação multifator, que é um método particularmente eficaz de interromper a maioria dos ataques.

O reforço constante dessas soluções, gerenciadas da mesma maneira que qualquer programa de conscientização, funcionou para organizações nos setores financeiro e de jogos.

Metodologias

Para fins deste relatório, as tentativas de preenchimento de credenciais são definidas como tentativas de login sem êxito para contas usando um endereço de e-mail como nome de usuário. Para identificar tentativas de abuso, em oposição a usuários reais que não conseguem digitar, dois algoritmos diferentes são usados. A primeira é uma regra volumétrica simples que conta o número de erros de login para um endereço específico. Isso difere do que uma única organização pode ser capaz de detectar porque a Akamai está correlacionando dados em centenas de organizações.

O segundo algoritmo usa dados dos nossos serviços de detecção de bots para identificar o preenchimento de credenciais de botnets e ferramentas conhecidas. Um botnet bem configurado pode evitar a detecção volumétrica, espalhando seu tráfego entre muitos alvos, usando um grande número de sistemas em sua varredura ou espalhando o tráfego ao longo do tempo. Esses são exemplos de algumas contramedidas.

A pesquisa sobre as ferramentas e as táticas de botnets de preenchimento de credenciais foi feita à mão, usando uma ampla variedade de buscas na Web e inteligência humana.

Créditos

State of the Internet/Contribuidores de segurança

Shane Keats, diretor de marketing do setor global, mídia e entretenimento – pesquisa do YouTube

Steve Ragan, pesquisador, escritor técnico sênior global — pesquisa do mercado darknet

Martin McKeay, diretor editorial – dados e análise de ataques de preenchimento de credenciais

Equipe editorial

Martin McKeay – diretor editorial

Amanda Fakhreddine – redatora técnica sênior, editora-chefe

Steve Ragan – redator técnico sênior, editor

Gerenciamento de programas

Georgina Morales Hampe, gerente de projetos – criativo

Murali Venukumar, gerente de programas – marketing