Symantec

INTERNET SECURITY THREAT REPORT

Sumário Executivo

Relatório de Ameaças à Segurança na Internet 2019

ISTR

Volume 24

Sumário Executivo

Formjacking. Ataques direcionados. Uso de ferramentas do dia a dia. Sua empresa é alvo dessas ameaças.

Assim como as abelhas são atraídas pelo mel, bandidos são atraídos em bandos para os últimos exploits que prometem dinheiro rápido com um mínimo de esforço. *Ransomware* e *cryptojacking* já tiveram seu auge; agora é a vez do *formjacking*.

No Relatório de Ameaças à Segurança na Internet da Symantec, Volume 24, compartilhamos os conhecimentos mais recentes sobre atividades de ameaças globais, tendências cibercriminais e motivações dos grupos de ataque.

O relatório analisa dados da Global Intelligence Network da Symantec, a maior rede de inteligência de ameaças civis do mundo, que registra eventos de 123 milhões de sensores de ataque ao redor o mundo, bloqueia 142 milhões de ameaças diariamente e monitora atividades de ameaças em mais de 157 países.

{FORMJACKING}

Cibercriminosos enriquecem rapidamente com *formjacking*

Os ataques de *formjacking* são simples e lucrativos: cibercriminosos carregam códigos maliciosos nos sites dos varejistas para roubar informações dos cartões de crédito dos compradores, com 4.800 sites diferentes comprometidos, em média, todos os meses.

Tanto empresas bem conhecidas (Ticketmaster e British Airways) quanto médias e pequenas empresas foram atacadas, sendo que podemos estimar de forma conservadora que esses malfeitores roubaram dezenas de milhões de dólares no ano passado.

Apenas 10 cartões de crédito roubados por site comprometido resultam em um rendimento de até US$ 2,2 milhões por mês, já que cada cartão é vendido por até US$ 45 em fóruns clandestinos. Com mais de 380 mil cartões de crédito roubados, somente o ataque da British Airways pode ter gerado uma receita aos criminosos de mais de US$ 17 milhões.

RANSOMWARE

CRYPTOJACKING

Menor uso, mas ainda presente

Ransomware e *cryptojacking* eram métodos garantidos de receita para cibercriminosos. Mas o ano de 2018 trouxe rendimentos decrescentes, resultando em menor volume de atividades.

Pela primeira vez desde 2013, houve uma queda geral de 20% no uso de *ransomware*, mas um aumento de 12% focado em empresas.

Com uma queda de 90% no valor das criptomoedas, instâncias de *cryptojacking* caíram 52% em 2018. Ainda assim, *cryptojacking* continua popular devido ao baixo custo e as baixas barreiras à entrada. A Symantec bloqueou um número quatro vezes maior de ataques de *cryptojacking* em 2018 em comparação com o ano anterior.

ATAQUES DIRECIONADOS

Grupos de ataques direcionados têm um apetite por destruição

Ataques na cadeia de suprimentos e com o uso de Ferramentas do Dia a Dia (LotL - Living-off-the-Land) são agora um dos pilares do cibercrime: os ataques na cadeia de suprimentos aumentaram 78% em 2018.

Técnicas de uso de ferramentas do dia a dia permitem que os grupos de ataque fiquem escondidos dentro de processos legítimos. Por exemplo, o uso de *scripts* maliciosos de PowerShell aumentou em 1.000% no ano passado.

A Symantec bloqueia 115.000 *scripts* maliciosos de PowerShell mensalmente, mas esse número representa menos de 1% do uso geral do PowerShell. Uma abordagem agressiva para bloquear todas as atividades do PowerShell interromperia os negócios,

MAIS AMBICIOSO E FURTIVO

ilustrando ainda mais por que as técnicas de LotL se tornaram a tática preferida de muitos grupos de ataques direcionados, permitindo que se movimentem sem chamar atenção.

Os grupos de ataque também aumentaram o uso de métodos testados e comprovados como *spear phishing* para se infiltrar nas organizações. Embora a coleta de informações continue sendo o motivo principal, alguns grupos também possuem foco na destruição. Aproximadamente um em cada dez grupos de ataques direcionados agora usam *malware* para destruir e interromper as operações de negócios, um aumento de 25% em relação ao ano anterior.

Um exemplo de destaque é o Shamoon, que ressurgiu notavelmente após uma ausência de dois anos, implantando instâncias específicas de *malware* para excluir arquivos em computadores de organizações estabelecidas como alvos no Oriente Médio.

NUVEM

Desafios da nuvem: se estiver na nuvem, a segurança é sua responsabilidade

Uma única carga de trabalho ou instância de armazenamento configurada incorretamente na nuvem pode custar milhões à organização ou causar um pesadelo relacionado à conformidade. Em 2018, mais de 70 milhões de registros foram roubados ou vazaram de *buckets* do S3 mal configurados. Ferramentas de mercado na Web permitem que grupos de ataque identifiquem recursos na nuvem configurados incorretamente.

As vulnerabilidades em chips de *hardware*, incluindo o *Meltdown*, *Specter* e *Foreshadow*, permitem que intrusos acessem os espaços de memória protegidos das empresas nos serviços da nuvem hospedados no mesmo servidor físico. A exploração bem-sucedida fornece acesso a locais de memória normalmente proibidos.

Isso é especialmente problemático para serviços na nuvem, porque, embora as instâncias na nuvem tenham seus próprios processadores virtuais, elas compartilham conjuntos de memória. Isto significa que um ataque bem-sucedido a um único sistema físico pode resultar em vazamento de dados de várias instâncias na nuvem.

IoT

Seu dispositivo *IoT* favorito é o melhor amigo de um grupo de ataque

Embora os roteadores e as câmeras conectadas constituam 90% dos dispositivos infectados, quase todos os dispositivos *IoT* são vulneráveis, desde lâmpadas inteligentes até assistentes de voz.

Os grupos de ataques direcionados concentram-se cada vez mais na Internet das Coisas como um ponto de entrada inseguro, onde podem destruir ou apagar todas as informações de um dispositivo, roubar credenciais e dados e interceptar as comunicações de sistemas SCADA.

E a TI industrial foi estabelecida como um possível campo de batalha para uma ciberguerra, com grupos de ameaças como Thrip e Triton investidos no comprometimento de sistemas de controle operacional e industrial.

INTERFERÊNCIA NA ELEIÇÃO AMERICANA DE 2018

O feed de suas redes sociais influenciou uma eleição?

Com toda a atenção na eleição do Congresso e Senado dos EUA em 2018, felizmente, não houve grandes interferências. Mas as redes sociais permanecem um campo de batalha hiperativo.

Domínios maliciosos que imitam sites políticos legítimos foram descobertos e desativados, enquanto contas vinculadas à Rússia usaram terceiros para comprar anúncios em redes sociais.

As empresas proprietárias das plataformas de mídias sociais assumiram um papel mais ativo no combate à interferência eleitoral. O Facebook montou um *war room* para lidar com a interferência eleitoral; o Twitter removeu mais de 10.000 bots que postaram mensagens incentivando as pessoas a não votarem.

Conheça os detalhes. Faça o download do Relatório sobre Ameaças à Segurança na Internet de 2019 da Symantec (ISTR)
https://go.symantec.com/ISTR

Sobre a Symantec

A Symantec Corporation (NASDAQ: SYMC) é líder mundial em soluções de cibersegurança e ajuda organizações, governos e indivíduos a proteger seus dados mais importantes onde quer que estejam. Organizações em todo o mundo buscam a Symantec para soluções estratégicas e integradas para se defender contra ataques sofisticados em endpoints, nuvem e infraestrutura.

Da mesma forma, uma comunidade global de mais de 50 milhões de pessoas e famílias dependem da suíte de produtos Norton e LifeLock da Symantec para proteger suas vidas digitais em casa e todos seus dispositivos. A Symantec opera uma das maiores redes civis de ciberinteligência do mundo, possibilitando a proteção contra as ameaças mais avançadas. Para mais informações, visite www.symantec.com, registre-se em nossos blogs, ou siga-nos no Facebook, Twitter e LinkedIn.

Sede Mundial da Symantec
350 Ellis Street
Mountain View, CA 94043
EUA

+1 650 527–8000
+1 800 721–3934

Para escritórios regionais e números de contato específicos, por favor visite nosso website. Para informações sobre o produto nos EUA, ligue gratuitamente para 1 (800) 745 6054.

Symantec.com

ISTR