Ameaças cibernéticas ao setor de varejo

PwC Threat Intelligence
1º trimestre de 2022

pwc

Conteúdo

Introdução

O varejo tem sido um dos setores mais atingidos por incidentes cibernéticos nos últimos 12 meses. As ameaças envolvem principalmente tentativa de crime cibernético, ou seja, ações para obter ganho financeiro. As organizações que operam no setor do varejo devem estar atentas e centrar sua defesa cibernética contra essa categoria de ameaça, sem deixar de acompanhar os riscos e ajustar as defesas por ações de hacktivismo, espionagem e sabotagem. Os impactos dos incidentes cibernéticos têm ido muito além da paralisação das operações da empresa, muitas vezes acompanhadas de extorsões criminosas múltiplas e do comprometimento das operações de empresas parceiras.

Os agentes de ameaças são atraídos para o setor devido à ampliação crescente da superfície tecnológica de ataque. A inovação tecnológica das empresas de varejo e a expansão das operações digitais do setor (ou seja, via *apps*, *e-commerce*, *marketplaces* etc.) ampliam os caminhos que podem ser explorados pelos agentes de ataque. A realidade tem mostrado que ataques cibernéticos e seus impactos não ficam mais circunscritos à empresa atacada, mas se propagam e impactam empresas da cadeia de suprimentos e, muitas vezes, afetam também empresas de outros setores correlacionados, como manufatura, logística e financeiro.

A crescente ameaça trazida pela expansão digital da cadeia de suprimentos pode ser combinada com esses possíveis caminhos de geração de receita ilícita no setor do varejo. A grande quantidade de informações pessoais e financeiras de clientes processadas por varejistas, por exemplo, pode ser usada diretamente por um invasor para cometer fraudes ou mesmo para concretizar vendas ilícitas na *dark web* após a exfiltração dos dados.

O que torna a exfiltração e a publicação ilícita de dados pessoais atraente ao invasor, por exemplo, é o impacto financeiro para a empresa que pode advir de sanções da Autoridade Nacional de Proteção de Dados (ANPD), além do impacto reputacional pelo não cumprimento da Lei Geral de Proteção de Dados (LGPD), compondo argumentos fortes do invasor no processo de extorsão e de negociação de valores de resgate por um *ransomware*.

No caso de dados financeiros de clientes do setor, a atratividade está no número de opções de dados válidos disponíveis para serem utilizadas em operações de pagamento. De portais de compras on-line a sistemas de ponto de venda (PDV), existem vários caminhos para os agentes de ameaças obterem dados das vítimas, incluindo informações de identificação pessoal (PII, na sigla em inglês), dados de pagamento ou detalhes de login com credenciais válidas. Os operadores de *ransomware* também têm tido sucesso ao mirar em importantes redes de pagamento e operadores de serviços de dados negociados na *dark web*.

É vital, portanto, que as organizações não apenas desenvolvam um ambiente seguro, mas fiquem atentas ao cenário de ameaças atual e criem meios para detectar e responder a incidentes cibernéticos, a fim de minimizar impactos. A segurança cibernética é um risco a ser avaliado pela alta administração, e as organizações devem tomar medidas ativas para priorizá-la e monitora-las.

Este relatório fornece uma visão geral das ameaças cibernéticas enfrentadas atualmente pelo setor de varejo, a fim de conscientizar para sua importância, dar exemplos das motivações por trás desses ataques e apoiar iniciativas de defesa orientadas por inteligência.

Nossa análise se baseia em nossos dados de inteligência sobre ataques cibernéticos e abrangem diversos tipos de ameaças. É inteligência obtida a partir de nosso envolvimento com a respostas a incidentes em todo o mundo e relatórios públicos sobre ataques ao setor de varejo.

Cronologia dos ataques

As motivações por trás das ameaças no setor de varejo variam, mas identificamos que a maioria esmagadora dos ataques visa a atividade criminosa. Essa categoria de agentes de ameaças apresenta diversos graus de sofisticação. Há desde operações avançadas de *ransomware* e agentes de ameaças que criam um *malware* sob medida para atacar sistemas de ponto de venda até aquelas que empregam artefatos e ferramentas de uso corrente ou de código aberto. A motivação criminosa cibernética é, de longe, a que mais ameaça o setor. Por isso mesmo, as organizações que operam no universo do varejo devem intensificar a postura de segurança como um todo e aprimorar as defesas contra riscos cibernéticos associados a este tipo de ameaça.

No Apêndice 1 deste relatório, apresentamos um resumo de categorias de agentes de ameaças por motivação.

> “Setor de varejo no Reino Unido enfrenta um ataque cibernético a cada oito dias”
>
> Keeper Security, novembro de 2021.

2020

Um agente de ameaças desconhecido tentou validar mais de 620 mil logins do cartão do clube de clientes da Tesco com senhas usadas anteriormente.

2020

A maior varejista da Indonésia, a Tokopedia, teve seus servidores comprometidos por um agente de ameaças desconhecido, que conseguiu extrair mais de 91 milhões de contas de usuários. Essas contas foram encontradas à venda mais tarde em um fórum on-line por U$ 5 mil.

2020

A varejista norte-americana Kmart foi atingida por um ataque do *ransomware* Egregor, o que fechou várias lojas. O ransomware Egregor, operado por um agente de ameaças monitorado pela PwC como White Samyaza, não está mais ativo.

2020

A varejista de eletrônicos E-Land, com sede na Coreia do Sul, foi forçada a fechar 23 de suas lojas em todo o país depois de ter sido atingida por uma variante de ransomware CI0p operada – e provavelmente usada somente – por um agente de ameaças monitorado pela PwC como White Austaras.

2021

O agente de ameaças Red Kelpie (também conhecido como APT41), baseado na China, é classificado pela PwC como provável responsável por operações de coleta de dados de inteligência contra vários pontos de venda na Austrália e na Espanha. A atividade foi motivada por espionagem.

2021

A varejista britânica Fat Face foi atingida por um ataque do *ransomware* Conti. A empresa recebeu um pedido inicial de resgate de US$ 8 milhões.

2021

A varejista de moda Guess foi alvo de um agente de ameaças que usava o ransomware DarkSide em fevereiro de 2021, mas só no final do ano se descobriu que informações pessoais de clientes haviam sido roubadas no ataque.

2021

A Swedish Coop foi forçada a fechar 400 de suas lojas devido a um ataque de ransomware que afetou um fornecedor de TI terceirizado.

2021

A varejista alemã de eletrônicos MediaMarkt foi atingida pelo *ransomware* Hive (operado por um agente de ameaças monitorado pela PwC como White Bennu). O pedido inicial de resgate foi de US$ 240 milhões.

2021

A cadeia britânica de supermercados SPAR, de propriedade da holandesa, foi atingida por um ataque de *ransomware* a um de seus provedores de TI terceirizados – James Hall and Company. O ransomware, operado por um agente de ameaças conhecido em código aberto como Vice Society, forçou a SPAR a fechar mais de 600 lojas em todo o Reino Unido, pois seus sistemas de PDV ficaram off-line.

Temas de incidentes

Com base em incidentes anteriores e tendências do setor, avaliamos que o varejo está sendo alvo principalmente de invasores com motivações criminosas. Desses agentes de ameaças cibernéticas, os mais relevantes e disruptivos são os operadores de *ransomware* e seus programas de afiliados, que infelizmente têm tido sucesso ao visar organizações do setor de varejo com suas técnicas de extorsão dupla.

Ameaça criminosa

As organizações do setor de varejo devem ser mais cautelosas com os agentes de ameaças cibernéticas e com as ferramentas, técnicas e procedimentos utilizados por eles. Nos últimos 12 meses, agentes de ameaças com motivação criminosa buscaram exfiltrar informações financeiras de clientes. A investida incluiu desde operadores de *ransomware* sofisticados e organizações criminosas usando um *malware* sob medida para atacar sistemas de ponto de venda a agentes de ameaças criminosas menos sofisticados.

Um dos fatores determinantes por trás da escalada da atividade criminosa cibernética no setor são as muitas vias potenciais de lucro ilícito. No setor de varejo, os fluxos de receita existem tanto on-line como em meio físico, nas lojas. Isso permite que os invasores atinjam operações digitais e do mundo real de várias maneiras. Além disso, o varejo tem um fluxo contínuo de transações financeiras entre a organização e o cliente, seja por meio de um sistema de ponto de venda em um caixa ou uma plataforma on-line. Todos esses métodos representam um desafio à segurança, na medida em que os agentes de ameaças cibernéticas encontram métodos novos, testados e comprovados capazes de usar os procedimentos operacionais padrão e que surgem constantemente no varejo para obter ganhos financeiros ilícitos.

Ransomware

Nos últimos 12 meses, as organizações de varejo foram fortemente atacadas por agentes de *ransomware*. A pesquisa da PwC sobre alguns dos operadores de *ransomware* mais ativos mostra que o varejo fica atrás apenas do setor de produção industrial entre os alvos visados.[1] [2] [3] O *ransomware*, pelo menos na forma organizada atualmente, passou por várias evoluções operacionais ao longo de seu ciclo de vida, aperfeiçoando-se e tornando-se a ameaça mais preocupante para as organizações em todos os setores e regiões.

As principais mudanças estão associadas a novos artefatos e procedimentos a novas ferramentas e técnicas, com o propósito de aumentar a proliferação de *ransomware* como serviço (RaaS, na sigla em inglês) e a aplicação, agora padrão, do método de extorsão dupla, em que os agentes exfiltram e usam os dados da vítima como forma de fazer pressão, além de criptografar seus sistemas. Essas mudanças fundamentais na forma como as operações de *ransomware* são conduzidas ocorrem desde o início de 2020 e aumentaram bastante sua eficácia, resultando em lucros ilícitos recordes em pagamentos de *ransomware* em 2021. Provavelmente isso aumentará em 2022. No setor de varejo especificamente, o pagamento médio de *ransomware* em 2021 foi de US$ 147.811 (acima da média de outros setores), sem incluir a remediação e a perda de negócios, que, em média, custam ao setor de varejo US$ 1,97 milhão a cada incidente.

Houve vários incidentes importantes de *ransomware* que afetaram a indústria de varejo, todos enfatizam a vulnerabilidade do setor a esse tipo de ataque. Esses incidentes causaram o fechamento de lojas, a paralisação operacional do *backoffice* e da logística, em alguns casos até em todo o país. Em muitos casos, o *ransomware* foi detonado em um servidor responsável por sistemas de pontos de venda de várias lojas, prejudicando a capacidade da organização atacada de permitir que clientes realizem pagamentos.

[1] Nothing else BlackMatters', PwC Threat Intelligence, CTO-TIB-20211209-01A

[2] 'Causing more Grief', PwC Threat Intelligence, CTO-TIB-20211028-01A

[3] 'White Dev 101 does not Rust on its laurels', PwC Threat Intelligence, CTO-TIB-20220121-03A

Com a crescente tendência à digitização do espaço físico de varejo, incluindo caixas de autoatendimento e pagamentos por aproximação, as organizações do setor precisam priorizar sua arquitetura e segmentação de rede. Variantes de *ransomware* como BlackCat (operado por um agente de ameaças monitorado pela PwC como White Dev 101) e Lockbit 2.0 (operado por um agente de ameaças monitorado pela PwC como White Janus) começaram a implementar propriedades semelhantes a *worms* em sua funcionalidade. Com isso, o *malware* consegue se propagar para outras máquinas. Essas evoluções na sofisticação do *malware* podem permitir que um agente de ameaças de *ransomware* danifique sistemas em toda a rede de uma organização, caso ela não tenha implantado as defesas e a segmentação adequadas.

Roubo de dados do cliente

Como o varejo é um setor que depende muito de alto volume de transações de clientes, as organizações tomaram medidas para facilitar ao máximo os pagamentos, incluindo a modalidade por aproximação, checkouts de autoatendimento e a capacidade de salvar informações para pagamento on-line. Além disso, com a proliferação das compras on-line, vários pontos de venda também precisam armazenar outras informações de identificação pessoal, como CPF, celular, endereço e detalhes de contato. Todos esses dados são valiosos para criminosos cibernéticos, como operadores de *ransomware*, organizações criminosas sofisticadas e agentes de ameaças com menos recursos. A PwC realizou pesquisas nos fóruns da *dark web* por onde esses dados coletados podem ser escoados. Eles funcionam como uma via que pode ser usada pelos agentes de ameaças para vender ou comprar dados roubados. Nossas análises revelam que o varejo é um dos setores mais visados. Em sua maior parte, as informações vendidas são credenciais de clientes ou acesso como serviço (AaaS, na sigla em inglês) para páginas de comércio eletrônico hackeadas que redirecionam para um site de coleta de credenciais controlado pelo comprador.[4] [5]

[4] A unique peek at 13 weeks of leaks – Part 1, PwC Threat Intelligence, CTO-SIB-20211209-01A

[5] A unique peek at 13 weeks of leaks – Part 2, PwC Threat Intelligence, CTO-SIB-20211209-02A

Para um agente de ameaças, essas informações do cliente podem ser acessadas e coletadas por meio físico – como um *skimmer* (ou "chupa-cabras") de cartões[6] – ou por meio da rede de uma organização.[7] No extremo mais sofisticado desse espectro, agentes de ameaças como o White Gaki (também chamado FIN8) são conhecidos por desenvolver *malware* sob medida, com funcionalidades sofisticadas para burlar defesas e infectar vários dispositivos na rede de uma vítima – incluindo sistemas de ponto de venda – além de extrair informações deles.[7]

Também houve ataques em portais de pagamento on-line nos setores de varejo e a ele associados, em que os agentes de ameaças conseguiram penetrar no processo de pagamento, roubando dados à medida que os clientes os inseriam em portais – o chamado ataque "estilo MageCart".[9] [10] Essas técnicas são amplamente utilizadas por agentes de ameaças que buscam atingir portais de pagamento. Avaliamos que ataques dessa natureza devem continuar no setor de varejo, com o crescimento permanente das compras on-line.[11] [12]

[6] Beware card skimmers this Black Friday

[7] Fashion retailer Guess discloses data breach after ransomware attack

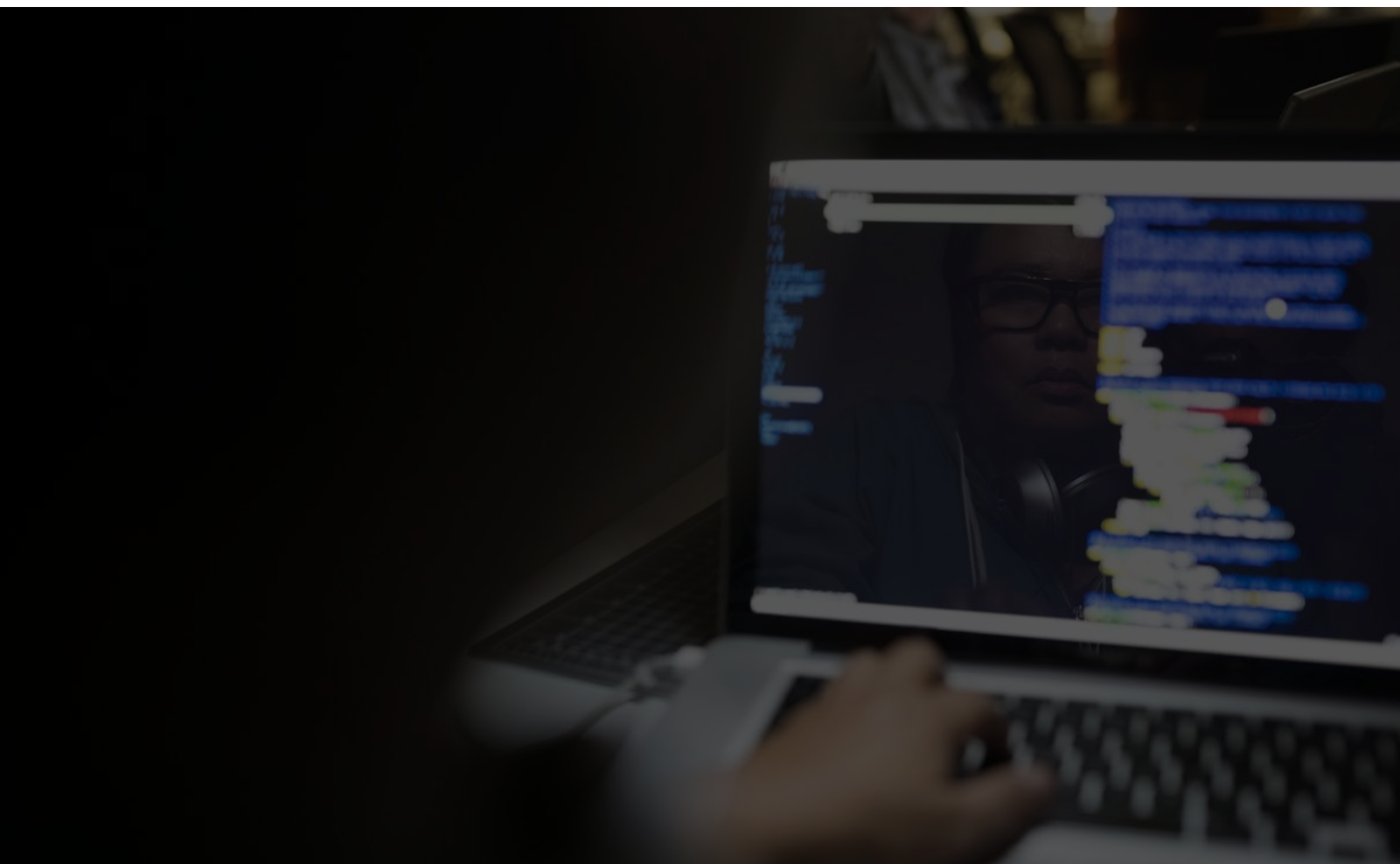
[8] FIN8 Returns with Improved BADHATCH Toolkit

[9] British Airways customer data stolen from its website

[10] Hackers Target Real Estate Websites with Skimmer in Latest Supply Chain Attack

[11] E-commerce in the United Kingdom (UK) - statistics & facts

[12] Over 4000 UK Retailers Compromised by Magecart Attacks



Espionagem

Embora os crimes cibernéticos representem a maior ameaça ao setor de varejo, existem agentes de ameaças envolvidos com espionagem que também miram esse setor para coletar informações. Como o varejo é uma atividade central na maioria das sociedades em todo o mundo, há uma grande quantidade de dados de inteligência a ser coletada de pontos de venda que podem beneficiar economias de países e empresas estatais. Além disso, a equipe de Inteligência de ameaças da PwC percebeu que vários agentes de ameaças visam o setor de varejo para aumentar a legitimidade de suas incursões. Eles veem a oportunidade de utilizar os domínios legítimos de organizações de varejo que podem ter segurança limitada – o que facilita sua violação – para lançar ataques com infraestruturas que, de imediato, dificilmente serão percebidas como fraudulentas pelos defensores.

Coleta de dados de inteligência

O setor de varejo é alvo de coleta de dados de inteligência por agentes de ameaças localizados na China há vários anos. A PwC apontou o Red Kelpie (também conhecido como APT41), por exemplo, como responsável por vários ataques direcionados a organizações de varejo na Austrália e na Espanha.[13] Essas descobertas estão alinhadas com a pesquisa de código aberto sobre o Red Kelpie, segundo a qual o agente da ameaça foi observado coletando informações de uma vítima envolvida na negociação de uma parceria comercial com uma empresa na China não divulgada publicamente. O relatório informou ainda que durante esse período de observação havia “um interesse focado em decisões estratégicas de negócios, incluindo entrada no mercado chinês, parcerias/M&A e expansão em outros mercados regionais”.[14]

A atividade do Red Kelpie evidencia as ameaças às organizações do setor de varejo, sobretudo aquelas que realizam negócios com empresas estatais. O acesso a essa inteligência pode dar à empresa estatal uma vantagem não natural durante o processo de negociação, com potencial acesso a táticas da outra parte, sua situação financeira e posição de mercado.

---

[13] Learning to ChaCha with Red Kelpie, PwC Threat Intelligence, CTO-TIB-20210624-02A

[14] Double Dragon: APT41, a dual espionage and cyber crime operation

Varejo como canal para ataques

A PwC identificou agentes de ameaças – envolvidos com espionagem, crime ou com qualquer outra motivação – aproveitando-se de práticas de segurança inadequadas e usando infraestruturas legítimas comprometidas como vetores para realizar seus ataques, com objetivo de burlar defesas e otimizar investimentos, porque, muitas vezes, é mais fácil fazer isso do que criar as próprias infraestruturas.[15] Além disso, a prática aumenta potencialmente a legitimidade aparente de suas ações.

Para que uma ação de espionagem maliciosa seja bem-sucedida, ela deve passar despercebida por um longo período. Uma maneira pela qual os agentes de ameaças tentam impedir que suas campanhas sejam descobertas é usar domínios e sites legítimos para hospedar seus artefatos maliciosos. Isso pode levar a vítima a interagir com um link que, embora pareça totalmente legítimo, na verdade a infecta com um *malware*.

Empresas de varejo de alcance regional foram alvo desses ataques. Na prática, agentes de ameaças miravam em domínios nativos do país onde seu alvo estava baseado. Por exemplo, um suposto agente de ameaças do Paquistão que a PwC monitora como White Dev 55 (também conhecido como SideWinder) foi flagrado usando uma livraria de varejo on-line com sede na Índia para hospedar seu *malware* durante ações direcionadas a vítimas na Índia.[16] O Black Artemis (também conhecido como Lazarus Group), ameaça baseada na Coreia do Norte, também tem um histórico de usar domínios legítimos de organizações de varejo para suas ações, embora em vários casos não fique claro se a escolha do alvo se deve à localização da organização de varejo ou à oportunidade de aproveitar alguma falha de segurança.[17] [18]

[15] A Peek into Top-Level Domains and Cybercrime

[16] White Dev 55 enjoys antiques, PwC Threat Intelligence, CTO-QRT-20201027-01A

[17] Mixed intentions, PwC Threat Intelligence, CTO-TIB-20191106-01A

[18] Paint me like one of your BMP files, PwC Threat Intelligence, CTO-TIB-20210428-01A

Em uma tática semelhante, mas ligeiramente diferente, a PwC identificou agentes de ameaças criando suas próprias marcas e domínios de varejo com o objetivo de convencer as vítimas de que o site de comércio eletrônico comandado e controlado por eles era, na verdade, um site e legítimo. Em uma investigação sobre o agente de ameaças Orange Yali (também conhecido como BITTER) localizado na Índia, pesquisadores da PwC descobriram o que parecia ser um site de comércio eletrônico controlado por um agente de ameaça que se passava por uma empresa de vestuário esportivo do Paquistão. Criou-se, inclusive, o que muito provavelmente era uma página falsa do Facebook.[19]

Sabotagem

Como as organizações do setor de varejo são altamente dependentes de tecnologia – seja de servidores para hospedar seus domínios ou de infraestrutura de rede para manter a operação dos sistemas de ponto de venda – há sempre o risco de interrupção operacional devido a ataques maliciosos. Esses ataques diferem das infecções por *ransomware* devido à intenção por trás deles. O *ransomware* está centrado no ganho financeiro, a sabotagem tem como objetivo principal degradar e causar dano de imagem.

Até o momento, os ataques maliciosos afetaram principalmente ativos críticos de infraestrutura de países, como redes e usinas de energia. Seria, portanto, incomum que uma organização de varejo fosse alvo de um ataque de sabotagem. Mas ataques à cadeia de suprimentos, por exemplo, podem ter um importante impacto secundário em várias organizações. Além disso, o *malware* usado em ataques maliciosos, como o *wiperware*, consegue se propagar pelas conexões de redes compartilhadas. Dessa forma, os pontos de venda, quando impactados por ataques maliciosos, geralmente são vítimas não intencionais de um ataque muito mais amplo.

[19] Orange Yali continues to set up shop in Pakistan, PwC Threat Intelligence, CTO-TIB-20210527-02A

Ainda assim, os perigos de sabotagem direcionadas ao setor de varejo não devem ser desprezados. Avaliamos que a ameaça de sabotagem ao setor é grande, principalmente em áreas com altas tensões geopolíticas. Um ponto de venda da varejista de roupas H&M com sede em Israel, por exemplo, sofreu um ataque de sabotagem originário de um agente de ameaças com sede no Irã.[20] Ele usou um *ransomware* conhecido como N3tw0rm.[21] Apesar de ser um *ransomware*, a equipe Inteligência de ameaças da PwC avaliou que o ataque provavelmente foi motivado por sabotagem, com base no fato de que nenhuma chave de descriptografia foi fornecida para vítimas específicas do *ransomware*.[22]

A sabotagem também pode ter uma abordagem menos sofisticada, embora ainda impactante. Os ataques de negação de serviço distribuído (DDoS, na sigla em inglês) tornaram-se mais comuns e mais perturbadores com o passar dos anos. Em 2021, houve o maior volume de ataques e o maior tráfeg o médio usado por ataque.[23] [24] Essas incursões tiveram como alvo varejistas de todos os portes e alcançaram números recordes em 2021.[25] Multinacionais como a Amazon conseguiram frustrar tentativas de DDoS,[26] mas nem todos os varejistas têm essa capacidade.

À medida que a barreira de entrada para ataques DDoS for reduzida, é provável que aumente a ameaça que as tentativas de DDoS representam para o setor de varejo. Além disso, com a transição contínua para o varejo on-line, os ataques DDoS significam um risco crescente para o setor, com potencial de trazer prejuízos mais longos e frequentes, especialmente em organizações que não estão adequadamente preparadas para resistir a inundações de tráfego da web.

---

[20] A PwC monitora esse agente de ameaça como Yellow Dev 15, conhecido em código aberto como Pioneer Kitten.

[21] Pay2Key to N3tw0rm, PwC Threat Intelligence, CTO-TIB-20210513-01A

[22] The mysteries of Pay2Key, PwC Threat Intelligence, CTO-SIB-20210113-01A

[23] Netscout Threat Intelligence Report: Issue 7: Findings From 1H 2021

[24] DDoS Attack Trends for Q4 2021

[25] Retail industry security incidents soaring, worsened by the supply chain crisis

[26] Amazon ‘thwarts largest ever DDoS cyber-attack’

Hacktivismo

As ações hacktivistas geralmente incluem o desejo de obter publicidade para uma causa específica por meio da desfiguração de sites ou mídias sociais ou por meio da interrupção do serviço usando uma técnica de ataque, como DDoS.[27] Embora a maioria desses ataques seja superficial e de baixo impacto por natureza, existe a possibilidade de um hacktivista mais capacitado perpetrar ações que impactem bastante as operações corporativas.

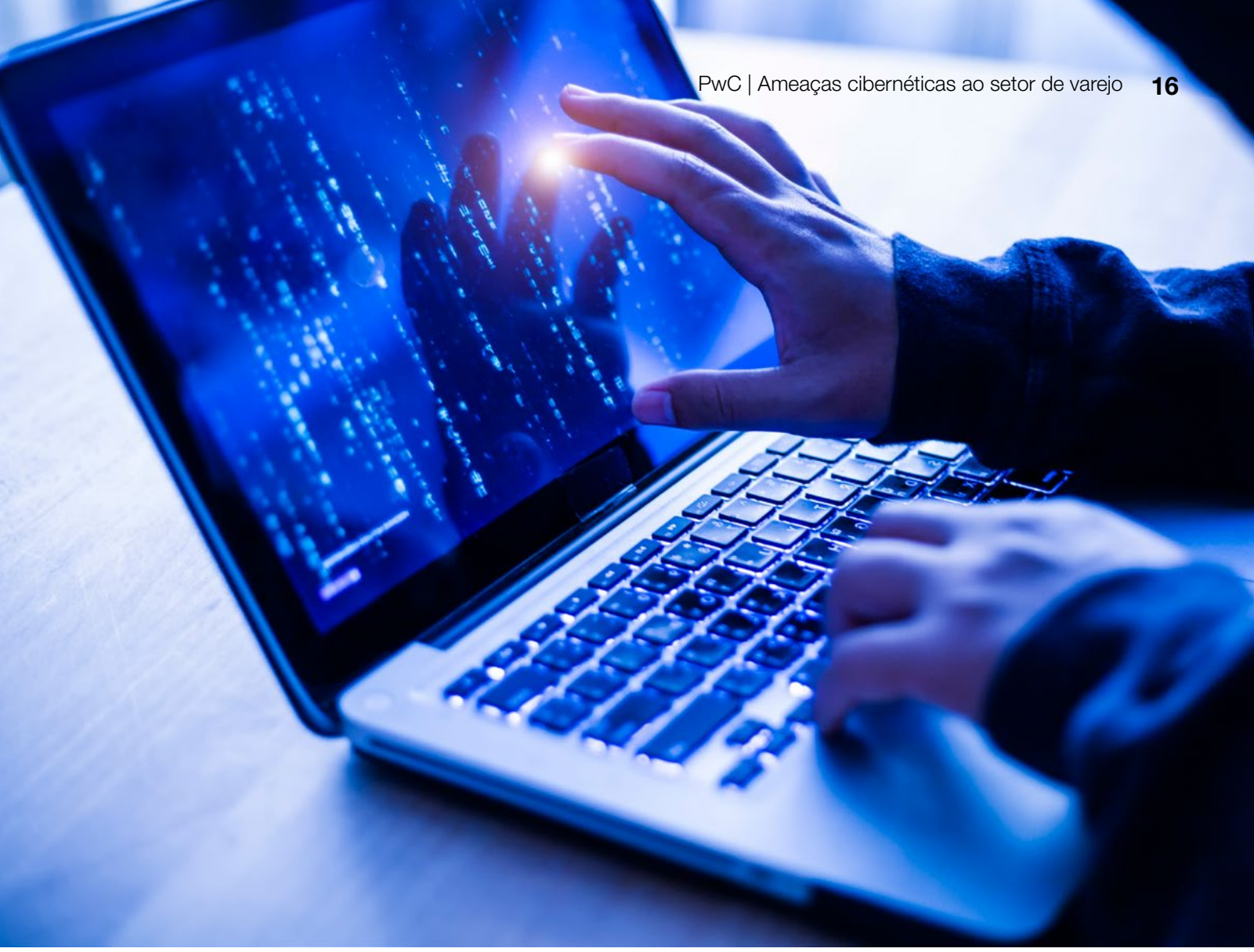
Hacktivistas mais sofisticados podem, por exemplo, tentar roubar informações confidenciais e/ou dados pessoais e expô-los ao público. No entanto, na maioria das vezes, a principal consequência dos ataques hacktivistas é de natureza reputacional. Ter sua imagem comprometida em decorrência de um ataque cibernético é uma grande ameaça para as organizações de varejo, e os hacktivistas têm a capacidade de atacar produtos e serviços de marcas específicas com suas campanhas, causando danos danos de longo prazo.

O hacktivismo ressurgiu nos últimos 12 meses. Os ataques não foram especialmente sofisticados e estavam relacionados a DDoS ou à descaracterização de mídia social – no último caso os alvos eram, principalmente, organizações governamentais.[28] Embora casos desse tipo de descaracterização de mídia social no setor varejista tenham ocorrido em anos anteriores, a motivação era financeira. Um exemplo foi o registrado com a conta da varejista britânica Tesco no Twitter. Ela foi adulterada para proliferar links falsos de criptomoeda.[29]

[27] Isso é diferente de um DDoS de sabotagem devido à intenção; se o hacktivista é capaz de atribuir tentativas de DDoS à sua causa, sua intenção é gerar e atrair atenção para sua causa.

[28] Office of Civil Defense's Twitter account hacked

[29] Tesco Twitter hacked by Bitcoin scammers



Avaliamos que a ameaça de agentes motivados por hacktivismo ao setor de varejo é menos grave do que as outras três categorias de ameaças relatadas antes (crime, espionagem e sabotagem). Isso se deve à falta de sofisticação observada durante esses ataques, o que significa um tempo de inatividade operacional real ou perda de receita provavelmente limitados.

Também avaliamos que o varejo como um todo não está atualmente no radar de hacktivistas. Essa falta de foco no setor – sobretudo sobre as grandes marcas – pode mudar com o tempo, pois é difícil prever o comportamento hacktivista. É possível que organizações de varejo se vejam no centro de uma questão política e atraiam a atenção de hacktivistas. Isso pode acontecer, por exemplo, se um hacktivista visar uma grande marca do setor de varejo para chamar a atenção para uma causa específica. Uma organização de varejo também pode ser alvo de cobertura negativa da mídia e, consequentemente, atrair atividades hacktivistas. Essa questão deve ser considerada em conjunto com as críticas cada vez maiores ao setor como um todo devido a seu envolvimento com temas como *fast fashion*,[30] práticas trabalhistas antiéticas e desperdício.[31] Tudo isso pode pôr organizações de varejo na mira dos hacktivistas.

[30] Fast fashion, explained

[31] Revealed: UK's largest supermarkets throw away enough food for 190 million meals each year

Cenário de ameaças

Os agentes de ameaças listados a seguir têm como alvo o setor de varejo, conforme constatado pela PwC. Os alvos variam de acordo com regiões, tipos de organização, motivações e intenções. O cenário de ameaças do setor de varejo pode ser usado para ajudar a definir e priorizar a cobertura contra agentes de ameaças que miram organizações específicas.

	Agente de ameaça	Nomes	País de origem
Espionagem	Red Kelpie	APT41, Wicked Panda	China
	Black Artemis	Lazarus Group, Silent Chollima	Coreia do Norte
	Orange Yali	BITTER	Índia
	White Dev 55	SideWinder	Em avaliação (suspeita sobre o Paquistão)
Ação criminosa	White Dev 101	Ransomware BlackCat	N/D
	White Janus	Ransomware LockBit 2.0	N/D
	White Onibi	Ransomware Ryuk e Conti	N/D
	Blue Lelantos	Ransomware Grief e DoppelPaymer	Rússia
	White Austaras	TA505, ransomware CL0P	Em avaliação
	White Magician	Trickbot	Em avaliação
	Blue Gulon	FIN7	Rússia
	White Gaki	FIN8	N/D
	White Giant	Magecart 6	N/D
	White Stribog	Magecart 5	N/D
	White Ursia	REvil, Sodinokibi	N/D

Estudos de caso

As informações descritas a seguir fornecem uma visão aprofundada das ameaças enfrentadas pelo setor de varejo.

1. Coop Suécia sofre ataque do *ransomware* Sodinokibi à cadeia de suprimentos

Motivação do agente de ameaça	Alvo	Ano
Crime	Setor de tecnologia	2021

Sumário executivo

O Coop Suécia fechou mais da metade de suas lojas em julho de 2021, depois que os sistemas de ponto de venda e autoatendimento das lojas pararam de funcionar devido a um ataque que afetou sua cadeia de suprimentos. A interrupção foi causada por uma ataque bem-sucedido de *ransomware* em um dos provedores de software de TI do Coop, o Visma Esscom, que foi comprometido via seu servidor Kaseya em um ataque à cadeia de suprimentos. O comprometimento do Kaseya evidenciou os perigos e importantes impactos de um ataque a terceiros relevantes. O agente da ameaça, nesse caso, era um afiliado do programa RaaS Sodinokibi, operado por um agente de ameaças que a PwC monitora como White Ursia (também conhecido como REvil). O Coop Suécia levou várias semanas para retomar suas operações à normalidade, embora algumas lojas tenham sido reabertas quatro dias após o fechamento.

Ferramentas, técnicas e procedimentos

O agente da ameaça conseguiu violar inicialmente o servidor VSA do Kaseya usando a técnica *main in the middle*, na interface web do servidor, o que forneceu a ele acesso autenticado. Isso, por sua vez, permitiu implantar seu *ransomware* no servidor a partir de uma “atualização”. Injetou-se um comando SQL para enviar a carga para a instância ativa e, assim, para todos os clientes que usavam servidor, bastando que instalassem a atualização maliciosa. Com isso, o *ransomware* ficaria apto a encriptar todas as pastas da rede da vítima e a infraestrutura de backup.

Impacto

Para o Coop Suécia, o impacto foi grande: mais de 400 lojas ficaram fechadas por um período de pelo menos três dias, em alguns casos, semanas. O impacto geral do comprometimento do Kaseya, deixou todo o setor em estado de alerta, pela possibilidade de operadores de *ransomware* começarem a visar prestadores de serviço para comprometer grandes marcas através da suspensão e degradação das operações comerciais diárias.

A PwC não recomenda que as organizações paguem um pedido de resgate, a menos que haja uma ameaça à vida, pois não há garantia de que os dados serão recuperados ou que os dados exfiltrados não serão vazados ou vendidos a terceiros. Esse pagamento também financia a atividade contínua de criminosos cibernéticos. Recomendamos trabalhar em estreita colaboração com um advogado externo especializado para investigar a legalidade de qualquer pagamento em potencial, principalmente no que diz respeito a sanções.

Mais informações

CTO-QRT-20210703-01A – Kaseya supply chain compromise

REvil ransomware attack on Kaseya VSA: What you need to know

Swedish Coop supermarkets shut due to US ransomware cyber-attack

2. O agente de ameaças Red Kelpie, baseado na China, foi flagrado conduzindo operações de espionagem contra o setor de varejo

Motivação do agente de ameaça	Alvo	Ano
Espionagem	Setor de varejo	2021

Sumário executivo

O agente de ameaças Red Kelpie (também conhecido como APT41, BARIUM), com base na China, tem um longo histórico de ataques a organizações no setor de varejo. Pesquisas realizadas pela PwC revelam que o agente provavelmente infectou empresas que operam na Austrália, Espanha e Itália em 2021. Em anos anteriores, informações de código aberto concluíram que o Red Kelpie provavelmente visou essas organizações devido a negociações em andamento – ou possíveis novas parcerias – com varejistas na China.

Ferramentas, técnicas e procedimentos

Embora o acesso inicial não tenha sido confirmado pela PwC, é provável que o agente da ameaça tenha conseguido se infiltrar em suas vítimas explorando em massa VPNs e outros serviços, pois esse é um comportamento relacionado a estea tipo de ameaça no passado.[32] A primeira fase do processo de ataque que a PwC pode confirmar é o uso de um *loader malware* conhecido como HEAVYHAND, que há muito tempo associamos a um agente de ameaças baseado na China, o Red Apollo (também conhecido como APT10). Nesse caso, porém, havia evidências de que ele estava sendo usado pelo Red Kelpie.[33] O *loader* HEAVYHAND conteria um loader adicional criptografado, exclusivo do Red Kelpie, identificado como Motnug. O *loader* Motnug contém uma carga útil criptografada, que – uma vez descriptografada durante a execução – revela-se um *beacon* Cobalt Strike, aparentemente usado como o *backdoor* principal do ataque.

[32] This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits

[33] Learning to ChaCha with Red Kelpie, PwC Threat Intelligence, CTO-TIB-20210624-02A

Impacto

O impacto resultante de uma intrusão dessa natureza é difícil de calcular, pois a coleta de dados de inteligência conduzida por esses agentes de ameaças é avançado e persistente (APT, na sigla em inglês) raramente é utilizado imediatamente. O agente da ameaça pode exfiltrar informações do ambiente da vítima por meses ou até anos. Além disso, os dados de inteligência coletados raramente são usados pelo próprio agente da ameaça, muitas vezes, são passados a um terceiro que solicitou as informações.

Em casos anteriores, os dados coletados e convertidos em inteligência foram usados por organizações em potenciais atividades de fusões e aquisições ou discussões de parceria com a vítima.[34] Isso permitiu uma vantagem na negociação, incluindo uma visão sobre a situação financeira da parte oposta, os potenciais planos de investimento futuro e objetivos durante as negociações. No caso específico do ataque do APT41 descrito acima, no entanto, não podemos fazer essa mesma avaliação com segurança, pois não estamos a par de discussões de fusão e aquisição em andamento ou anteriores entre a vítima e terceiros baseados na China. No entanto, existe a probabilidade de o Red Kelpie ter agido com a mesma motivação de seus ataques anteriores direcionados ao setor de varejo.

Como as intrusões muitas vezes não são detectadas imediatamente – ou nunca – as organizações podem ter dificuldade de priorizar a ameaça de espionagem tanto quanto uma ameaça de operadores de *ransomware* ou de outras organizações criminosas. A equipe de inteligência de ameaças da PwC, no entanto, enfatiza que a coleta de dados de inteligência de longo prazo pode levar a impactos que interferem nos negócios de organizações de qualquer setor. Operar ou negociar com um potencial parceiro de negócios que tenha conquistado uma posição de mercado por meio de informações confidenciais obtidas de forma ilícita pode criar situações em que uma empresa é adquirida ou torna-se parceira de uma entidade que detém uma vantagem competitiva inequívoca.

[34] Double Dragon: APT41, a dual espionage and cyber crime operation

Mais informações

CTO-TIB-20210624-02A - Aprendendo a ChaCha com Red Kelpie

Double Dragon: APT41, a dual espionage and cyber crime operation

The SideWalk may be as dangerous as the CROSSWALK

Considerações finais

Vários agentes de ameaças têm atacado organizações do setor de varejo nos últimos anos. Com base em tendências de incidentes, estudos de caso de ataques e nossas próprias análises, constatamos que os agentes de ameaças de crimes cibernéticos, em particular, têm se concentrado cada vez mais no setor. Embora seus objetivos possam diferir, os muitos meios para ganhos financeiros ilícitos – seja a venda de dados de clientes ou a extorsão de organizações por meio de *ransomware* – atraíram todos os tipos de agentes de ameaças com motivação financeira. Esse risco está aumentando, e avaliamos como altamente provável que tanto o *ransomware* como outros agentes de ameaças criminosas continuem a operar contra organizações de varejo.

Também identificamos atividades em que os agentes de ameaças motivados por espionagem buscaram coletar informações de organizações de varejo ou usar a infraestrutura delas para ações fraudulentas. Essas ações não são tão frequentes quanto as atividades conduzidas por agentes de ameaças com motivação financeira, mas isso se deve mais à natureza das operações de espionagem, que precisam se manter ocultas por longos períodos, às vezes até anos.

A dificuldade de perceber as ações de espionagem pode levar as organizações de varejo a dar à ameaça que elas representam uma prioridade muito menor do que a devida. A PwC avalia que o risco trazido por agentes de ameaças motivados por espionagem é grande. O nível de ameaça é grave para organizações de varejo que mantêm parcerias ou negociações com uma empresa estatal. Embora os impactos dessa intrusão possam não ser vistos imediatamente – como acontece em invasões motivadas por crime, como *ransomware* – as ramificações de longo prazo de uma operação bem-sucedida de coleta de dados de inteligência podem ser devastadoras tanto para a posição de mercado quanto para o valor de mercado futuro da empresa.

Saber quais agentes de ameaças são relevantes para um determinado setor é um passo importante para direcionar estrategicamente o investimento a defesas apropriadas. A visão apresentada neste relatório, no entanto, abrange o setor de varejo de maneira geral. Uma análise mais granular sobre as ameaças deve ser feita por organização. Examinar como as ameaças explorariam a infraestrutura da organização para atingir seu objetivo pode ajudar a identificar as lacunas existentes em seus controles de segurança e permitir que você adapte seu plano de preparação adequadamente.

Apêndice 1: Metodologia de análise

A maioria dos ataques cibernéticos tem uma motivação básica e principal. Embora os ataques de agentes de ameaças diferentes possam compartilhar objetivos, nem sempre eles compartilham a mesma motivação. Examinar o que motiva um ataque pode permitir a identificação da categoria do invasor.

A PwC divide o cenário de ameaças de acordo com a motivação dos ataques cibernéticos. Para cada uma, são descritas algumas ferramentas, técnicas e procedimentos comuns observados pela equipe PwC Threat Intelligence. As divisões são:

Motivação	Descrição
Espionagem pela informação	Os agentes de ameaças de espionagem (geralmente chamados de “ameaças persistentes avançadas” – APTs na sigla em inglês) geralmente procuram roubar informações que fornecerão uma vantagem econômica ou política ao seu benfeitor. Os ataques motivados por espionagem geralmente se originam de concorrentes do setor ou de agentes de ameaças patrocinados por nações. Muitas vezes, o benfeitor é uma nação, e a atividade de espionagem alinhada aos objetivos dessa nação se refletirá na geopolítica e nos eventos do mundo real. Normalmente, as informações buscadas por invasores de espionagem são encontradas apenas em organizações específicas. Isso significa que eles visam repetidamente a mesma organização e seus fornecedores até que concluam a missão.
Crime pelo dinheiro	Os criminosos cibernéticos procuram um alvo de maneira indiscriminada, pois simplesmente buscam monetizar as atividades. A gama de sofisticação dos criminosos cibernéticos é vasta e apresenta um conjunto muito diferente de ferramentas, técnicas e procedimentos. O crime cibernético inclui tanto esquemas diretos de saque, em que um ganho financeiro imediato é obtido – por exemplo, a violação de e-mails comerciais, sequestro de caixa eletrônico ou roubo de carteiras de criptomoedas – como atividades que buscam monetizar dados roubados – coleta de detalhes de cartões de pagamento ou outras informações pessoais. Muitos criminosos cibernéticos são meros consumidores de dados roubados por agentes mais sofisticados. Esses dados são normalmente usados para cometer fraude ou roubo de identidade. O *ransomware* tornou-se motivo de preocupação especialmente prevalente, afetando grandes corporações do setor privado até instituições de caridade e governos locais.

Motivação	Descrição
Hacktivismo pela causa	Hacktivistas conduzem ataques para aumentar a visibilidade de seu perfil público e aumentar a conscientização sobre sua causa. Isso geralmente é feito por meio da interrupção de serviços, como ataques de negação de serviço (DoS) e descaracterização de sites. Em muitos casos, esses ataques são aleatórios. Os hacktivistas se importam pouco com a forma dos ataques ou quem é afetado, desde que sua mensagem seja promovida. Em alguns casos, no entanto, as ações atribuídas a uma organização ou um indivíduo, ou o apoio dado a um tema, tornam essa organização ou indivíduo alvo de ataque. Assim como a espionagem, os ataques de hacktivistas costumam ser influenciados por eventos do mundo real. Isso significa que o risco desses ataques está sujeito a mudanças.
Sabotagem pelo impacto	Sabotadores procuram danificar, destruir ou subverter a integridade de dados e sistemas. Os ataques maliciosos nem sempre são deliberados e têm sido usados para mascarar outras atividades maliciosas. As operações de sabotagem projetadas para desviar a atenção podem também resultar em danos colaterais significativos. Entre os exemplos de ataques estão o apagamento de discos rígidos, provocando o mau funcionamento dos sistemas de supervisão e aquisição de dados (SCADA, na sigla em inglês) ou alterando dados comerciais. Assim como os ataques de espionagem, os ataques de sabotadores tendem a ser influenciados por eventos do mundo real. Dependendo de determinados eventos ou questões políticas, o risco de ataques aumenta conforme a região onde a empresa atua e as ações que ela adota.

Apêndice 2: PwC Threat Intelligence

Quem somos

A PwC é reconhecida mundialmente como líder em segurança cibernética, uma firma capaz de atuar globalmente e apresentar soluções para os desafios de segurança e risco que seus clientes enfrentam. Apoiamos nossos serviços de assessoria e estratégia em segurança no nível do conselho na experiência e no conhecimento adquiridos nas linhas de frente de nossos serviços especializados em defesa cibernética, como Defesa Cibernética Gerenciada, *Red Teaming*, resposta a incidentes e inteligência de ameaças.

Nossa equipe de inteligência de ameaças é especializada em fornecer serviços que ajudam os clientes a resistir, detectar e responder a ataques cibernéticos avançados. Isso inclui eventos de crise, como violações de dados, espionagem econômica e invasões direcionadas, incluindo aquelas comumente chamadas de ameaças persistentes avançadas (APTs).

Temos como diferencial nossa capacidade de combinar profundo conhecimento técnico e pensamento estratégico com pesquisas, conduzidas por nossos especialistas, com experiência principalmente em órgãos governamentais, militares e serviços de segurança – o que nos dá uma perspectiva única e uma vasta gama de contatos. Nossas pesquisas exclusivas, inteligência de segurança, conhecimento técnico e compreensão do risco cibernético ajudam nossos clientes a obter a clareza necessária para se adaptar com confiança a um cenário de novos desafios e oportunidades.

Nossa pesquisa de inteligência de ameaças apoia todos os nossos serviços de segurança e é usada por organizações do setor público e privado em todo o mundo para proteger, conhecer o entorno de atuação e apoiar estratégias.

Assinatura de inteligência contra ameaças cibernéticas

Acesso aos *feeds* de indicadores sobre ataques direcionados da PwC, assinaturas de rede e *endpoint* e relatórios táticos e estratégicos.

Investigações e avaliações direcionadas

Acesso direto à equipe de pesquisa de ameaças da PwC para tarefas relacionadas a consultas pontuais ou de longo prazo – tanto pesquisas táticas como estratégicas sobre amostras maliciosas, agentes de ameaças ou suporte em análises.

Monitoramento de inteligência de ameaças cibernéticas

Pesquisa contínua, sob medida e focada, em complemento a nossos serviços de assinatura.

Consultoria e assessoria

Serviços de consultoria para ajudar as organizações a definir requisitos, consumir, aplicar e produzir inteligência de ameaças da maneira mais adequada à sua realidade.

Para mais informações sobre nossos serviços ou para discutir qualquer uma das ameaças contidas neste relatório, entre em contato conosco pelo e-mail larissa.escoar@pwc.com.

Contato

Eduardo Batista
Sócio e líder de *Cybersecurity* da PwC Brasil
eduardo.batista@pwc.com

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil