IBM Security

Relatório de Inteligência sobre Ameaças da X-Force 2020

IBM

Produzido por IBM X-Force IRIS (Serviços de Inteligência e Resposta a Incidentes)

Índice

Índice

Resumo e principais tendências

A IBM Security desenvolve soluções e serviços inteligentes de segurança corporativa para ajudar sua empresa a criar resiliência hoje para as ameaças à segurança virtual de amanhã.

Para atualizar os profissionais de segurança sobre as ameaças mais relevantes, a IBM® X-Force® lança regularmente blogs, documentos técnicos, seminários on-line e podcasts sobre novas ameaças e TTPs (táticas, técnicas e procedimentos) dos invasores.

A IBM Security lança o Relatório de Inteligência sobre Ameaças da IBM X-Force anualmente, resumindo o ano anterior em termos das ameaças mais importantes levantadas por nossas várias equipes de pesquisa para oferecer às equipes de segurança informações que possam ajudar a proteger melhor as organizações.

Os dados e as informações apresentados neste relatório são derivados dos serviços de segurança gerenciados da IBM Security, serviços de resposta a incidentes, testes de penetração e serviços de gerenciamento de vulnerabilidades.

As equipes de pesquisa da IBM X-Force analisam dados de centenas de milhões de endpoints e servidores protegidos, juntamente com dados derivados de ativos que não são de clientes, como sensores de spam e honeynets. A IBM Security Research também aplica armadilhas de spam em todo o mundo e monitora dezenas de milhões de ataques de spam e phishing diariamente, analisando bilhões de páginas da Web e imagens para detectar campanhas de ataque, atividade fraudulenta e abuso de marca, para proteger melhor nossos clientes e o mundo conectado em que vivemos.

O X-Force IRIS (Serviços de Inteligência e Resposta a Incidentes) compilou as análises de serviços de software e segurança da IBM Security no ano passado, que demonstram que 2019 foi o ano do ressurgimento de antigas ameaças, usadas de novas maneiras.

— De acordo com dados da X-Force, um aumento de 2.000% em incidentes visando a TO (Tecnologia Operacional) em 2019 pode ser um presságio do crescente interesse dos invasores em atacar sistemas industriais agora em 2020.

— Mais de 8,5 bilhões de registros foram comprometidos em 2019, um número 200% maior que o de registros perdidos em 2018. O insider inadvertido pode ser amplamente responsabilizado por esse aumento significativo. Os registros expostos devido a servidores mal configurados (como armazenamento em nuvem acessível ao público, bancos de dados em nuvem não protegidos e backups rsync protegidos incorretamente ou dispositivos de armazenamento de área de rede conectados à Internet abertos) representaram 86% dos registros comprometidos em 2019.

— O cenário de atuação do malware mudou em 2019, com os invasores retornando ao ransomware e criando botnets. Ao longo de 2019, o X-Force IRIS respondeu a ataques de ransomware em 12 países, 5 continentes e 13 setores diferentes. Além disso, atividades destrutivas de malware demonstram que essa tendência potencialmente catastrófica continua sendo uma ameaça crescente.

— Os três principais vetores de infecção inicial observados na atuação do X-Force IRIS em 2019 foram muito próximos: phishing (31%), varredura e exploração (30%) e credenciais roubadas (29%). Ataques de phishing, curiosamente, passaram de quase metade do total de incidentes em 2018 para menos de um terço em 2019. Por outro lado, ataques de varredura e exploração de vulnerabilidades aumentaram para quase um terço dos incidentes, representando apenas 8% em 2018.

— A análise da atividade global de spam feita pela X-Force indica que o e-mail de spam continua usando um subconjunto limitado de vulnerabilidades, com foco especial em apenas dois CVEs: 2017-0199 e 2017-11882. Ambas são vulnerabilidades corrigidas, responsáveis por quase 90% das ameaças que os invasores tentaram explorar por meio de campanhas de spam.

— Embora o setor de Serviços Financeiros tenha se mantido no topo como o mais visado em 2019, houve uma mudança clara de foco por parte dos invasores, com os setores de Varejo, Mídia, Educação e Governo subindo no gráfico global dos mais visados.

— O setor de Informações Geocêntricas é uma novidade no Relatório de Inteligência sobre Ameaças da X-Force deste ano, fornecendo dados sobre tendências observadas em todo o mundo. A IBM Security continua monitorando vários invasores que visam todas as regiões, e este relatório destaca os principais em cada uma delas, os ataques observados desde 2019 e as possíveis datas de interesse da segurança virtual em 2020.

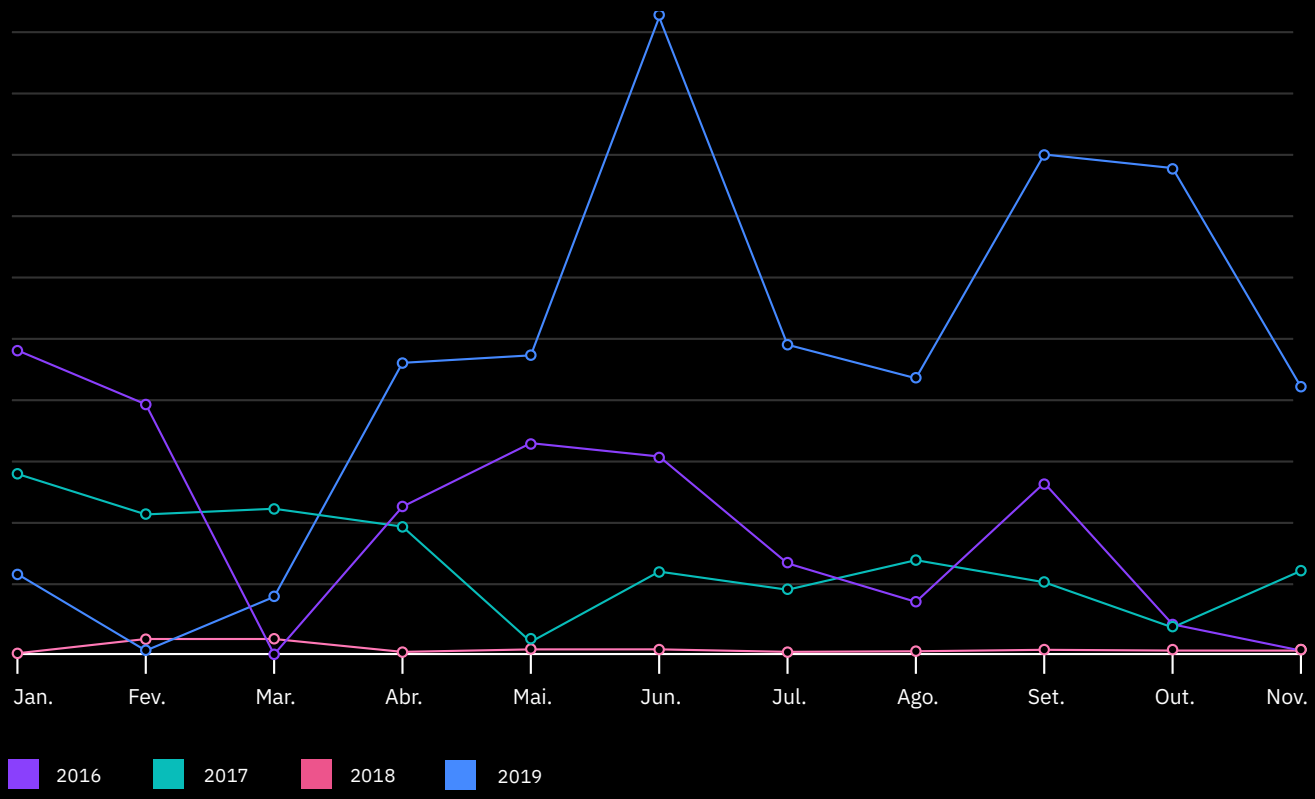
As seções a seguir deste relatório anual abordam as tendências de nível superior e detalham informações sobre o que as moldou em 2019.

Vetores de ataque e infecção inicial

Figura 1:

T’éwendências de ataques à TO (Tecnologia Operacional)

Volume de ataques à TO mensalmente, comparando os anos de 2016 a 2019 (Fonte: IBM X-Force)



Crescimento explosivo de ataques à infraestrutura de TO (Tecnologia Operacional)

Os dados da IBM X-Force indicam que os eventos nos quais os invasores visavam ICSs (Sistemas de Controle Industrial) e ativos similares de TO (Tecnologia Operacional) aumentaram mais de 2.000% desde 2018. De fato, o número de eventos direcionados aos ativos de TO em 2019 foi superior ao volume de atividades observado nos últimos três anos.

A maioria dos ataques observados se concentrou no uso de uma combinação de vulnerabilidades conhecidas nos componentes de hardware de SCADA e ICS, além de ataques de pulverização de senha usando táticas de login de força bruta contra alvos de ICS.

Algumas atividades relatadas focadas em ataques de ICS foram associadas a dois invasores conhecidos e coincidiram com o pico na linha do tempo do ataque que observamos na nossa telemetria. Duas campanhas específicas foram realizadas pelo grupo Xenotime e pelo IBM Hive0016 (APT33), que supostamente ampliou os ataques aos alvos de ICS.

A sobreposição entre as infraestruturas de TI e de TO, como PLCs (Controladores Lógicos Programáveis) e ICSs, continuou representando um risco para as organizações que dependiam dessas infraestruturas híbridas em 2019.

A convergência da infraestrutura de TI com a de TO permite que as violações à TI visem dispositivos de TO que controlam ativos físicos, o que pode aumentar bastante o custo da recuperação. Por exemplo, no início de 2019, o IBM X-Force IRIS ajudou a responder a uma violação em uma empresa de manufatura global, em que uma infecção por ransomware iniciada em um sistema de TI passou lateralmente para a infraestrutura de TO e interrompeu as operações da fábrica. O ataque não só impactou as operações da própria empresa, mas também causou um efeito cascata nos mercados globais.

As avaliações de segurança do X-Force IRIS entregues aos nossos clientes até 2019 destacaram a vulnerabilidade dos sistemas de TO, que geralmente usam software e hardware legados. Manter sistemas de produção que não podem mais receber patches e que estão repletos de vulnerabilidades mais antigas que se tornaram públicas significa que, mesmo que os sistemas de TO não estejam voltados para a Internet, esses sistemas sem patches podem ser presas fáceis. Em casos de movimentação lateral, depois que um invasor conquista a primeira posição, esses sistemas podem ser acessados de dentro da rede e prejudicados por técnicas de exploração relativamente simples.

Embora a tendência de ataques à rede de ICS mostrada na Figura 1 esteja em movimento descendente desde o início de outubro de 2019, a X-Force espera que os ataques contra alvos de TO/ICS continuem aumentando em 2020, conforme vários invasores planejam e lançam novas campanhas contra redes industriais em todo o mundo. Com mais de 200 novos CVEs relacionados a ICSs lançados em 2019, o banco de dados de vulnerabilidades da IBM X-Force mostra que as ameaças aos ICSs provavelmente continuarão crescendo em 2020.

A X-Force espera que os ataques contra alvos de ICS continuem aumentando em 2020, conforme vários invasores planejam e lançam novas campanhas contra redes industriais em todo o mundo.

Volume de registros vazados cresce drasticamente

O número de registros vazados aumentou significativamente em 2019, com mais de 8,5 bilhões de registros expostos. Isso é mais que o triplo em relação a 2018. O principal motivo desse aumento significativo é que os registros expostos devido a configurações incorretas aumentaram quase dez vezes em relação ao ano anterior. Esses registros representaram 86% dos registros comprometidos em 2019. É um aumento gritante em relação a 2018, quando observamos uma queda de 52% em relação a 2017 nos registros expostos devido a configurações incorretas, e esses registros compuseram menos da metade do total de registros.

Curiosamente, na verdade houve uma diminuição no número de incidentes de configuração incorreta em 2019 de 14% em relação ao ano anterior. Esse fato comprova que, quando realmente ocorreu um vazamento por configuração incorreta, o número de registros afetados foi significativamente maior em 2019. Quase três quartos dos casos em que houve mais de 100 milhões de registros vazados foram incidentes de configuração incorreta. Em dois desses incidentes de configuração incorreta que ocorreram no setor de Serviços de Consultoria, a contagem de registros expostos foi de bilhões para cada incidente.

Esse aumento significativo nos registros perdidos entre os setores destaca o risco crescente de vazamentos de dados, mesmo para organizações em setores que normalmente não eram considerados alvos principais.

Registros vazados em 2019

8,5 bilhões

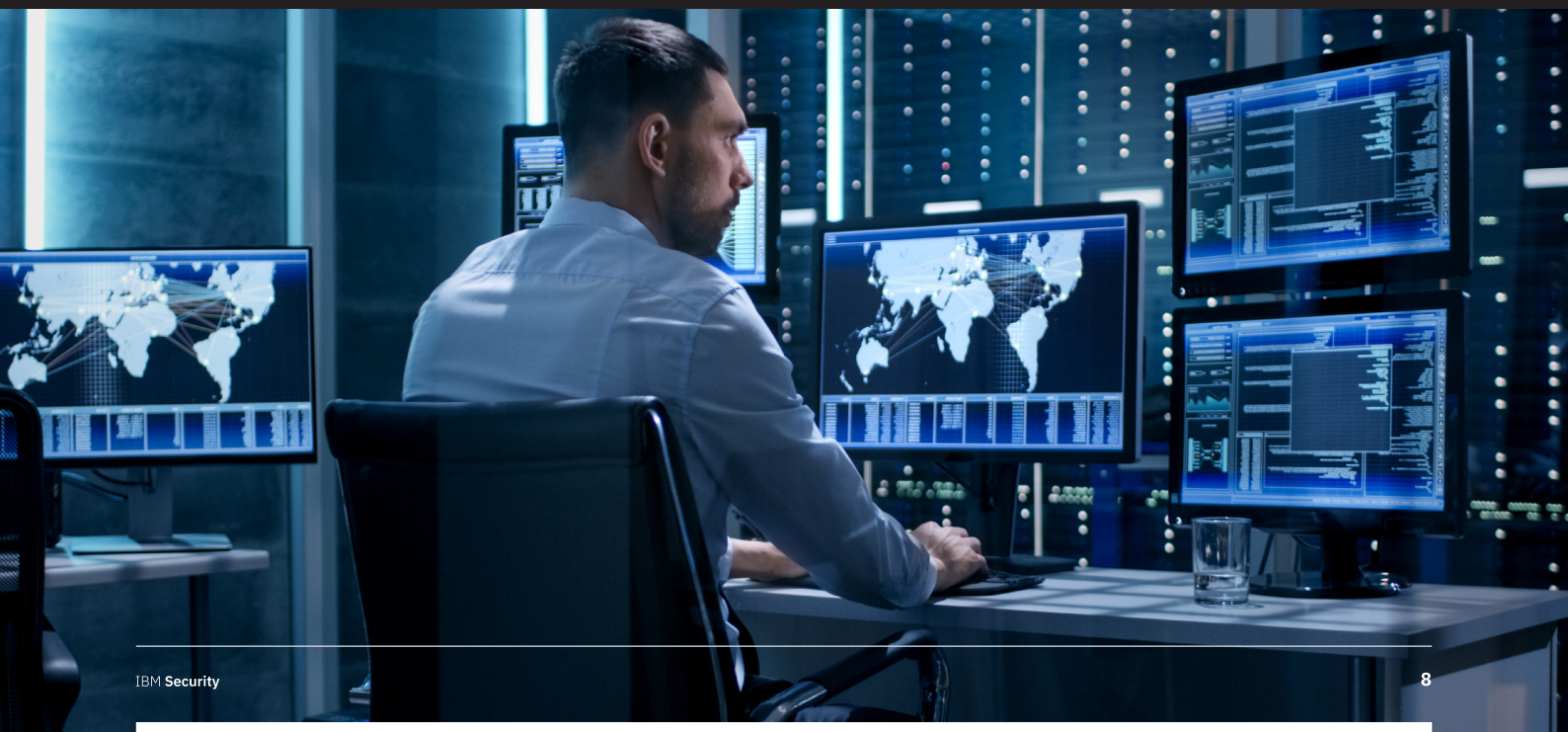
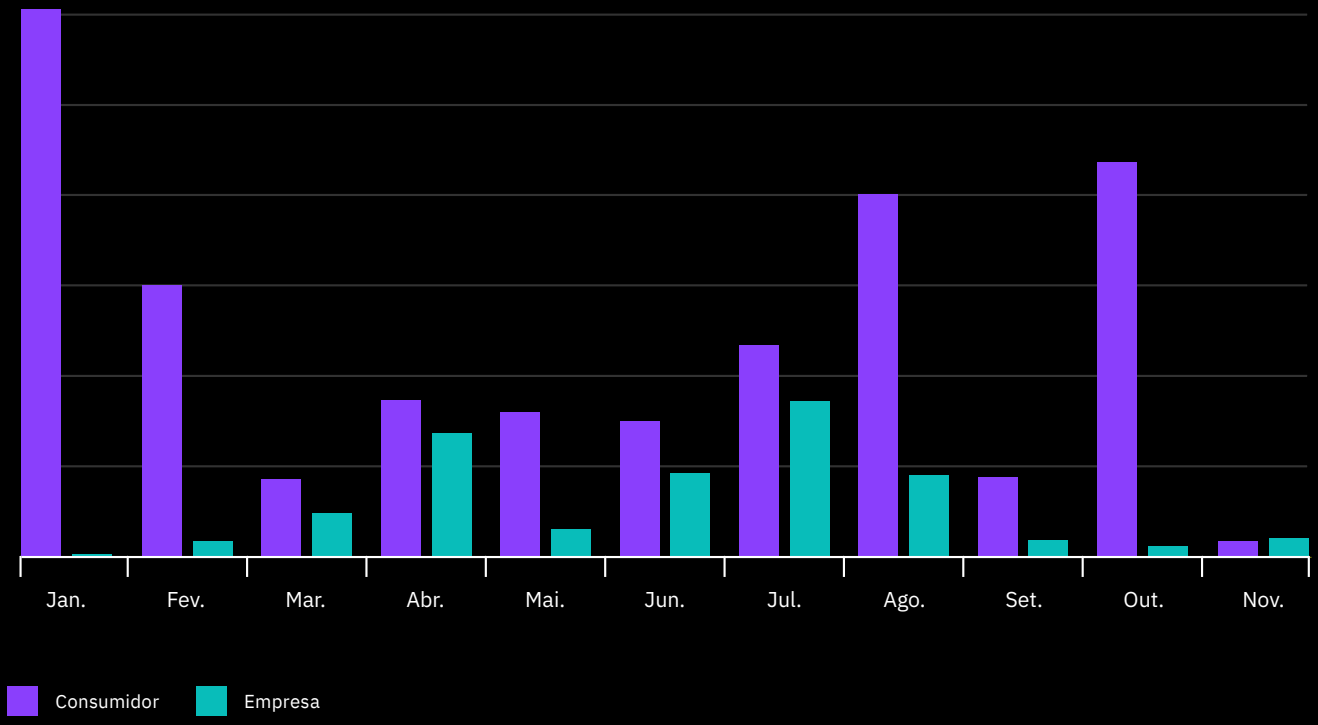


Figura 2:

Ataques à IoT de consumidores em relação a empresas

Volume mensal de ataques à IoT de consumidores em relação a empresas em 2019 (Fonte: IBM X-Force)



Ataques a dispositivos de IoT incluem o ambiente corporativo

Com a expectativa de mais de 38 bilhões de dispositivos conectados à Internet em 2020, o cenário de ameaças à IoT (Internet das Coisas) foi gradualmente se transformando em um dos vetores que podem afetar tanto os consumidores quanto as operações das empresas usando malware relativamente simplista e ataques automatizados, geralmente com script.

Na esfera do código mal-intencionado usado para infectar dispositivos de IoT, a pesquisa da IBM X-Force acompanhou várias campanhas de malware Mirai em 2019 que curiosamente deixaram de visar apenas os produtos eletrônicos comuns e passaram a incluir hardware de uso corporativo, atividade que não observamos em 2018. Dispositivos comprometidos com acesso à rede podem ser usados pelos invasores como um ponto de articulação em possíveis tentativas de estabelecer uma base de operações dentro da organização.

O Mirai é um malware prolífico de IoT que tem passado pelas mãos de vários invasores desde 2016 para causar interrupções em massa infectando um grande número de dispositivos de IoT e usando-os em ataques de DDoS (negação de serviço distribuída). Em nossa análise das campanhas de 2019, descobrimos que os TTPs daqueles que usam o malware Mirai mudaram fortemente desde 2018 e, em 2019, se concentraram em visar hardware corporativo, além dos produtos eletrônicos comuns.

Examinando os ataques que afetaram os dispositivos de IoT em 2019, observamos o uso generalizado de ataques de CMDi (injeção por comando), com instruções para fazer o download de cargas mal-intencionadas direcionadas a vários tipos de dispositivos de IoT. A maioria desses ataques de injeção é automatizada por scripts que buscam e tentam infectar dispositivos em massa. Se o dispositivo de IoT visado for suscetível a esses ataques de injeção, a carga será transferida e executada, transformando-o efetivamente em uma grande botnet de IoT. Um dos facilitadores mais comuns desses ataques são os dispositivos de IoT com senhas fracas ou padrão que podem ser facilmente adivinhadas por um simples ataque de dicionário.

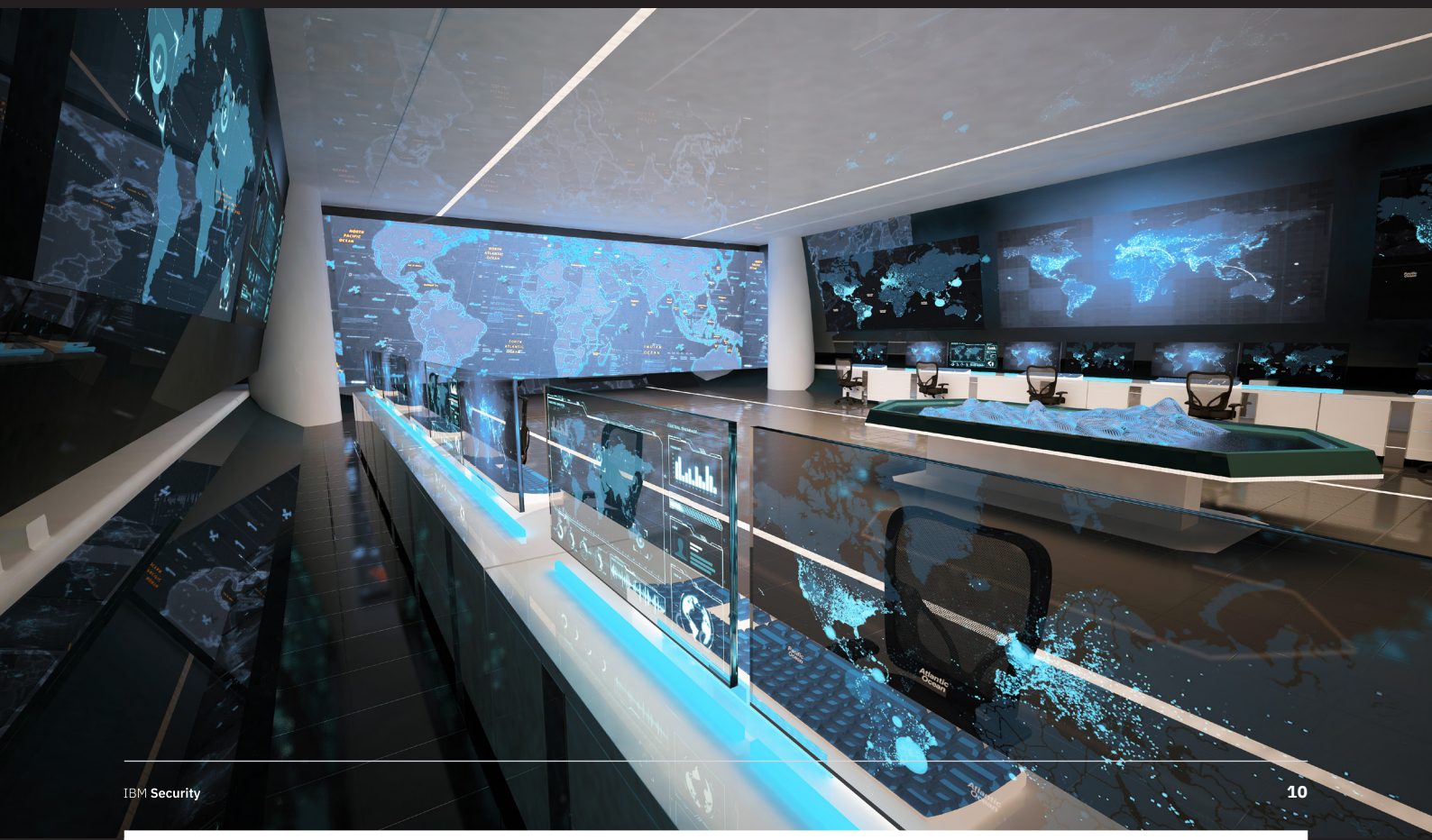
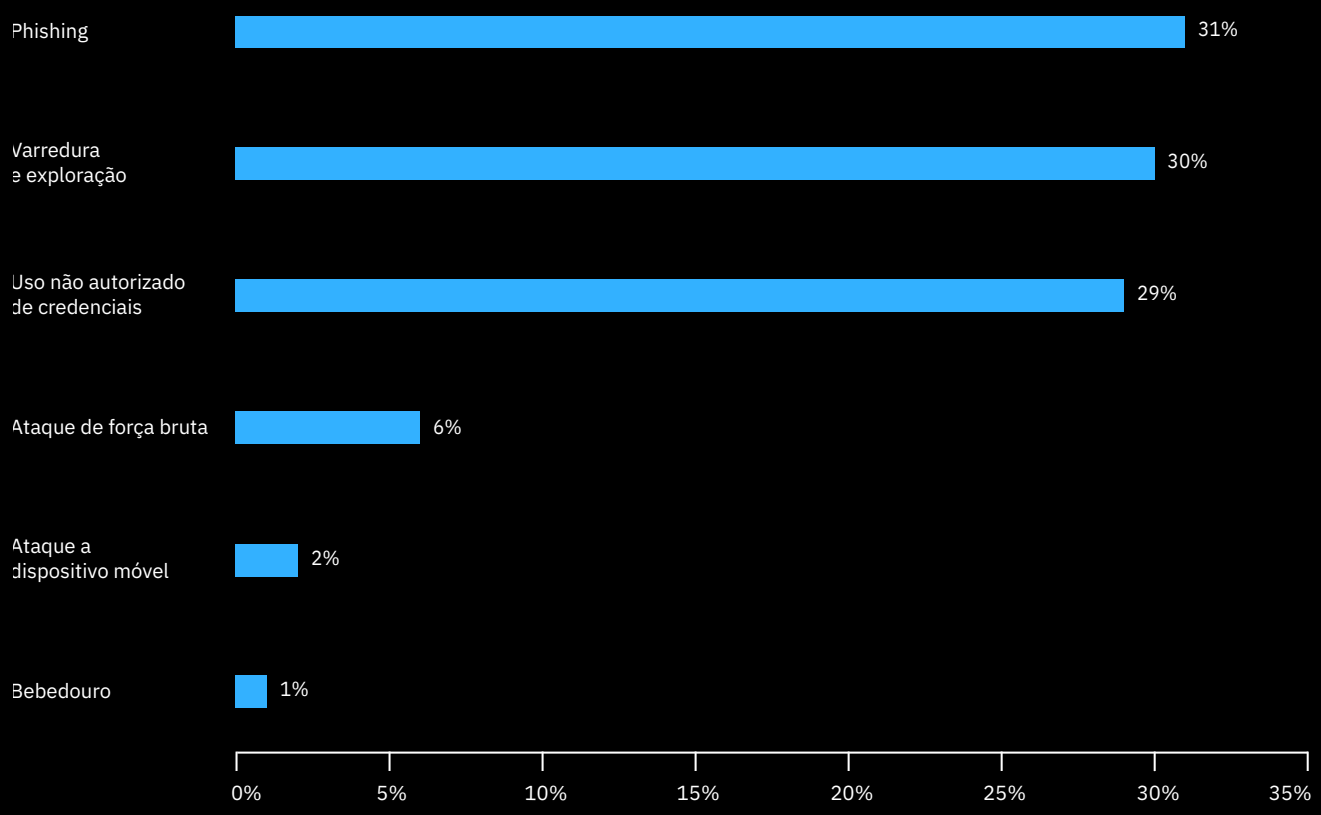


Figura 3:
principais vetores de ataque inicial

Distribuição dos seis principais vetores de ataque inicial em 2019, como uma porcentagem dos seis vetores de acesso mostrados (Fonte: IBM X-Force)

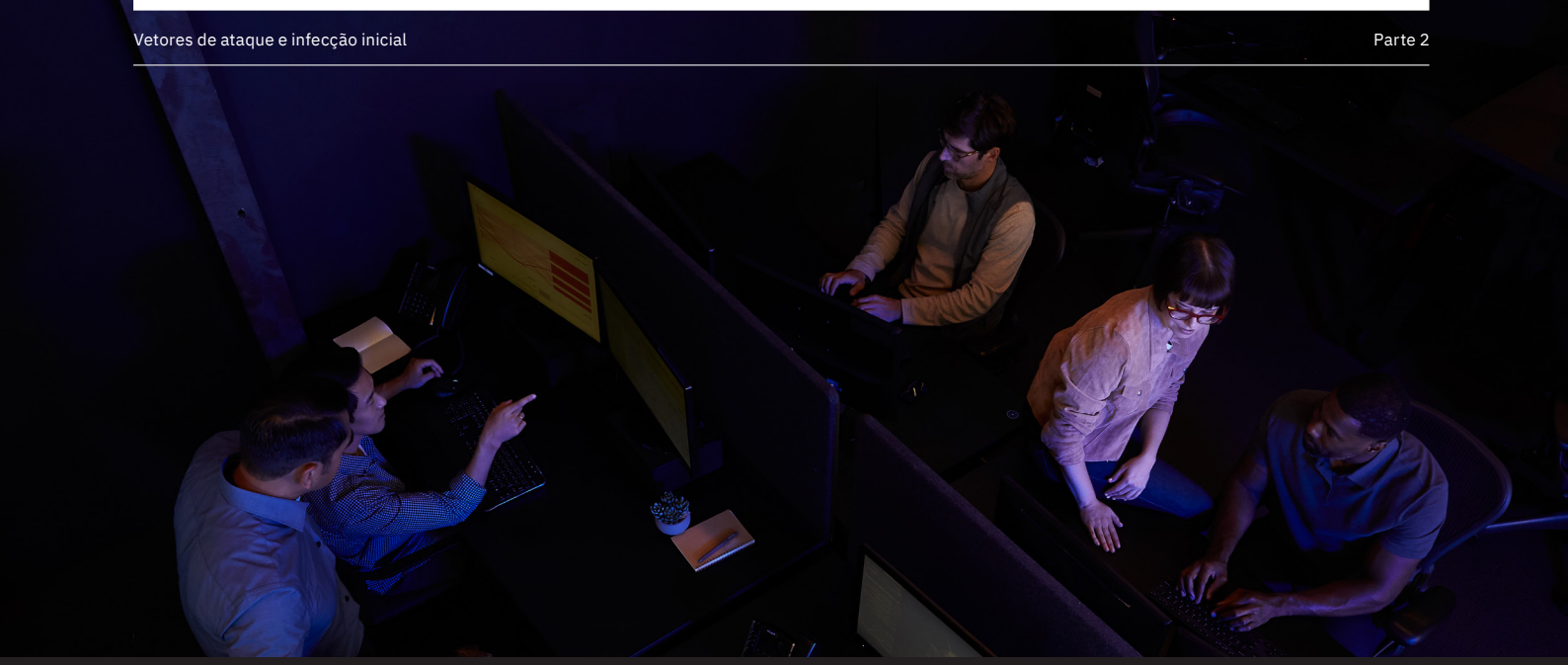


Phishing lidera vetores de acesso inicial em ataques de 2019

A ampla capacidade de resposta a incidentes do IBM X-Force IRIS oferece informações valiosas sobre os métodos e as motivações dos invasores.

Com 31%, o phishing foi o vetor mais frequente usado para o acesso inicial em 2019, mas está abaixo de 2018, quando comprometeu quase metade do total.[1]

1 O Relatório de Inteligência sobre Ameaças da X-Force de 2019 relatou que quase um terço (29%) dos ataques analisados pelo X-Force IRIS envolviam e-mails de phishing. Desde então, esse número foi corrigido em função de evidências adicionais que surgiram após a publicação de vários incidentes, aumentando essa porcentagem para 44% em 2018.



Mais notavelmente em 2019, os invasores passaram a examinar cada vez mais os ambientes-alvo em busca de vulnerabilidades. Segundo os profissionais de resposta, essa técnica foi usada em 30% dos incidentes, sendo que no ano anterior ela correspondeu a apenas 8%.

Os invasores têm muitas opções para examinar e explorar: a IBM X-Force detectou mais de 150 mil vulnerabilidades que foram divulgadas publicamente. Embora adversários sofisticados possam desenvolver explorações de dia zero, contar com explorações conhecidas ocorre com mais frequência porque elas permitem que os adversários conquistem uma posição inicial sem precisar gastar recursos para criar novos TTPs, reservando as melhores armas para redes mais protegidas. Além disso, os invasores apostam nas organizações que não estão atualizando os aplicativos de patch, mesmo para vulnerabilidades em que os patches estão disponíveis há algum tempo. Por exemplo, casos de infecção por WannaCry continuam sendo observados mais de dois anos após a infecção inicial e o patch (MS17-010) se tornar amplamente disponível.

O uso de credenciais roubadas, em que os invasores usam credenciais obtidas anteriormente para acessar as organizações-alvo, chegou a quase um terço, com 29%. Geralmente, essas credenciais são roubadas de sites de terceiros ou obtidas por meio de uma tentativa de phishing contra a organização-alvo. Os invasores podem usar credenciais roubadas para se misturar com o tráfego legítimo, tornando a detecção ainda mais desafiadora.

Os ataques de força bruta caíram ano após ano para uma distante quarta posição, com 6% de todos os casos, seguidos pelos dispositivos BYOD com 2% como ponto de acesso inicial às organizações-alvo.

Os pesquisadores da X-Force observaram um aumento notável na atividade dos invasores em junho e em julho de 2019, com o número de eventos ofuscando os totais de todo o ano de 2019 até esse ponto. Embora o motivo desse aumento repentino de atividade seja desconhecido, os meses de verão (no hemisfério norte) também parecem mais ativos em termos de spam, com o pico de volume registrado em agosto de 2019. É possível que os invasores só tenham ficado mais barulhentos e facilmente detectáveis ou que uma mudança nas táticas ou nas ferramentas deles tenha gerado essa atividade significativa. É menos provável que os picos de atividade de curta duração sejam o resultado da entrada de novos invasores no mercado, porque espera-se que essas novas entradas criem um aumento sustentado da atividade, em vez de algo temporário.

Tendências de malware

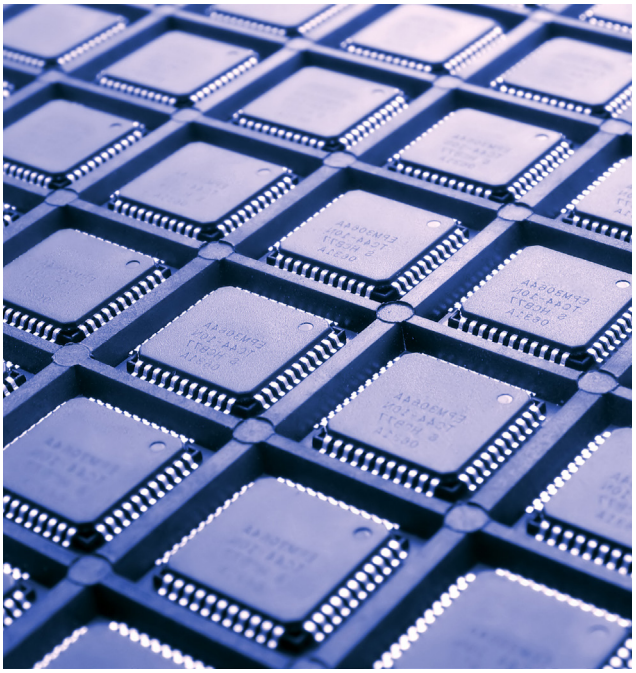
Ataques destrutivos de malware aumentam consideravelmente

As investigações do IBM X-Force IRIS indicam que ataques destrutivos de malware se tornaram mais frequentes e aumentaram em geografia e escopo em 2019.

Usado por criminosos virtuais e por agentes de estado-nação, o malware destrutivo é um software mal-intencionado com a capacidade de tornar inoperantes os sistemas afetados e de desafiar a reconstituição. A maioria das variantes de malware destrutivo causa destruição por meio da exclusão ou substituição de arquivos críticos para a capacidade de execução do sistema operacional. Em alguns casos, o malware destrutivo pode enviar mensagens personalizadas para equipamentos industriais para causar mau funcionamento. Incluído na nossa definição de malware destrutivo está o tipo de ransomware capaz de limpar ou de criptografar irreversivelmente os dados de uma máquina.

Entre o segundo semestre de 2018 e o segundo semestre de 2019, o X-Force IRIS respondeu ao mesmo número de ataques destrutivos em relação ao ano anterior, destacando que essa tendência de malware potencialmente catastrófica continua colocando as organizações em risco.

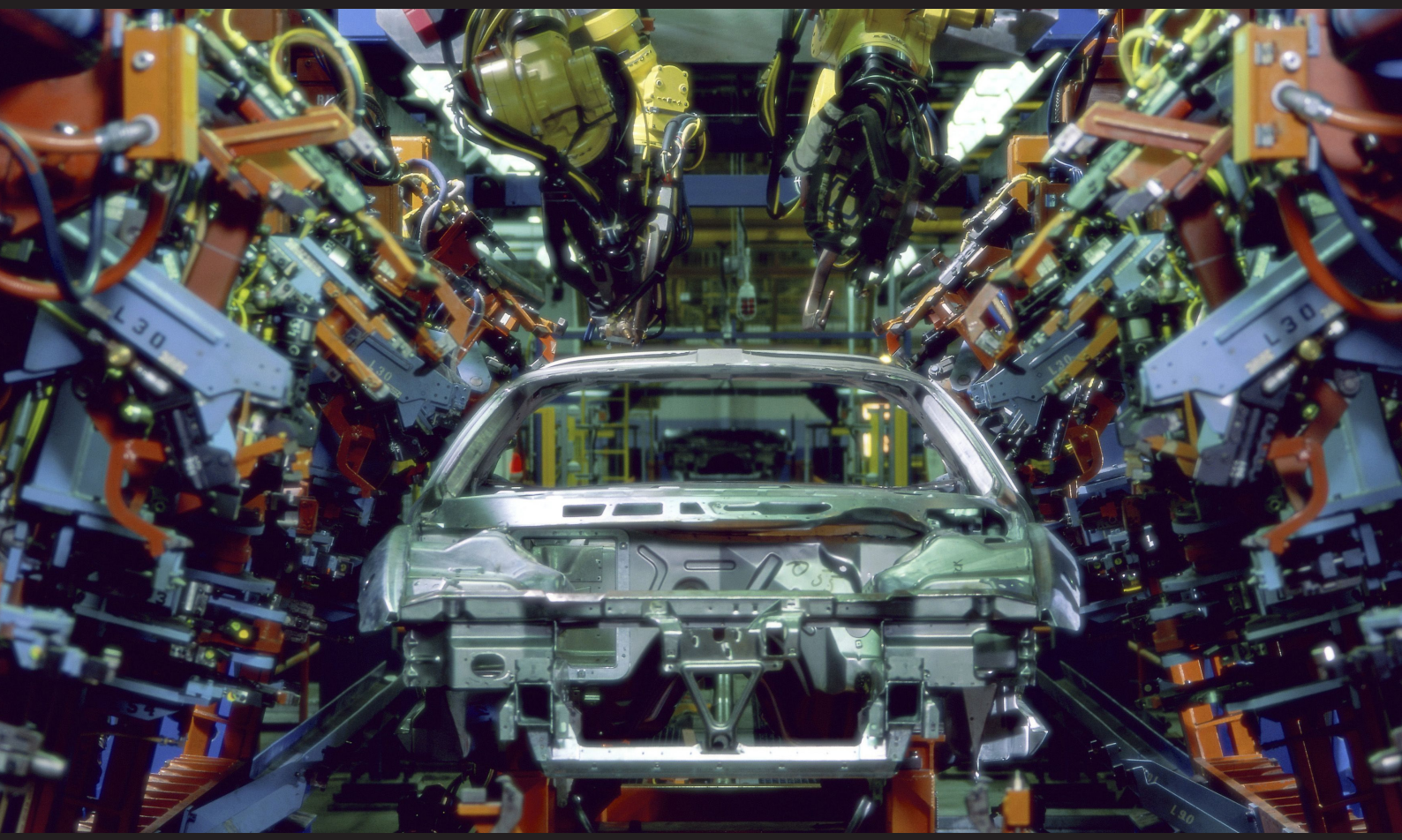
Historicamente, ataques destrutivos geralmente vinham de adversários de estados-nações. No entanto, temos observado uma tendência em que mais tensões de ransomware com motivação financeira incorporam elementos destrutivos ao ataque, com variantes como LockerGoga e MegaCortex estreando seu ataque destrutivo no final de 2018 e no início de 2019.



Estima-se que os ataques destrutivos custem em média US$ 239 milhões, mais de 60 vezes o custo médio de um vazamento de dados.

No final de 2019, o X-Force IRIS destacou a descoberta de um novo malware destrutivo a que demos o nome de ZeroCleare. Com o objetivo de limpar os dados, ele visava o setor de energia no Oriente Médio e foi atribuído pela IBM a um grupo APT afiliado ao Irã ITG13[2], conhecido também como APT34/OilRig.

O X-Force IRIS estima que o custo de um ataque destrutivo de malware a empresas possa ser particularmente alto, com grandes empresas multinacionais sofrendo um prejuízo de US$ 239 milhões por incidente, em média. Essa estimativa de custo é 60 vezes maior que o custo médio de um vazamento de dados em 2019, segundo os cálculos do Ponemon Institute. Diferentemente dos vazamentos que roubam ou expõem dados, esses ataques normalmente destroem até três quartos ou mais dos dispositivos nas redes da organização vitimada.



2 ITG significa IBM Threat Group, um termo que é discutido mais detalhadamente em “Setores mais visados”. A X-Force usa nomes do ITG, com nomes alternativos de grupos de ameaças indicados entre parênteses após o nome do ITG.

Ransomware e cryptominers agressivos em 2019

As contagens de variantes de malware e de ataques que usam malware aumentam e diminuem ao longo do ano, mas, mesmo assim, a percepção dos tipos de ameaças que devem ter prioridade pode ajudar as organizações a gerenciar melhor os riscos.

No primeiro semestre de 2019, aproximadamente 19% dos ataques observados foram relacionados a incidentes de ransomware, em comparação com apenas 10% dos ataques no segundo semestre de 2018. No quarto trimestre de 2019, houve um aumento de 67% nos ataques com ransomware em comparação com o quarto trimestre do ano anterior. Ao longo de 2019, o X-Force IRIS respondeu a ataques de ransomware em 12 países, 5 continentes e 13 setores diferentes.

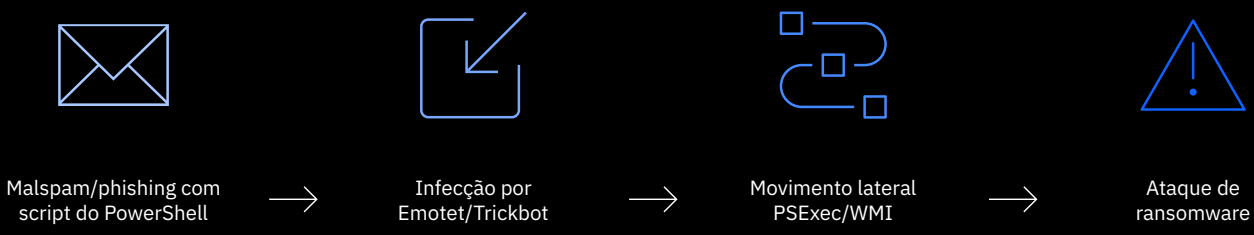
Esse aumento pode ser atribuído ao crescente número de invasores e de campanhas lançadas contra diversas organizações em 2019. Destacam-se instituições municipais e públicas que sofreram ataques de ransomware, bem como agências governamentais locais e prestadores de serviços de saúde. Os ataques a esses tipos de organização geralmente os pegam despreparados para responder, mais propensos a pagar um resgate e, em alguns casos, sob extremo estresse para se recuperar do ataque devido à ameaça à segurança pública e à vida humana.

Dados da X-Force comprovam que, nos casos de ataques de ransomware, o principal vetor de ataque em 2019 foi explorar as vulnerabilidades no protocolo SMB (Windows Server Message Block) para se propagar pela rede. Essa tática, usada anteriormente nos ataques do WannaCry, foi responsável por mais de 80% das tentativas observadas.

No quarto trimestre de 2019, houve um aumento de 67% nos ataques com ransomware em comparação com o quarto trimestre de 2018.

Figura 4:
infecção por ransomware em vários estágios

Ataque de ransomware por meio de uma rotina de infecção em vários estágios (Fonte: IBM X-Force)



Os ataques contra versões vulneráveis do protocolo SMB podem ser automatizados. Por isso, essa opção é mais barata para os invasores e mais fácil de escalar, visando afetar o maior número possível de sistemas no mesmo ataque.

Os invasores também costumavam usar downloaders de commodities, como Emotet e TrickBot, para executar ransomware em um sistema-alvo. Essa técnica geralmente usa o PowerShell para fazer o download do malware e disseminá-lo usando funções nativas, como PSExec ou WMI (Windows Management Instrumentation), que podem ser mais difíceis de detectar.

Os invasores usam vários estágios para infectar os usuários, em vez de um ataque direto com o ransomware, para dar a eles melhor controle sobre o ataque, evitar os controles e a detecção e plantar as sementes de uma operação de ransomware que abrangeria dispositivos suficientes para atrair as vítimas a pagar. O retorno do investimento em paciência e planejamento é grande: em cinco meses, os ataques de Ryuk arrecadaram mais de US$ 3,7 milhões para o bando de criminosos. Em outro exemplo, um ataque a casas de repouso nos EUA levou a uma demanda de resgate de US$ 14 milhões dos operadores do Ryuk.

O ransomware não foi o único tipo de malware a atacar em 2019. Outro tipo de malware extremamente popular em 2019 foi o código de mineração de criptomoedas.

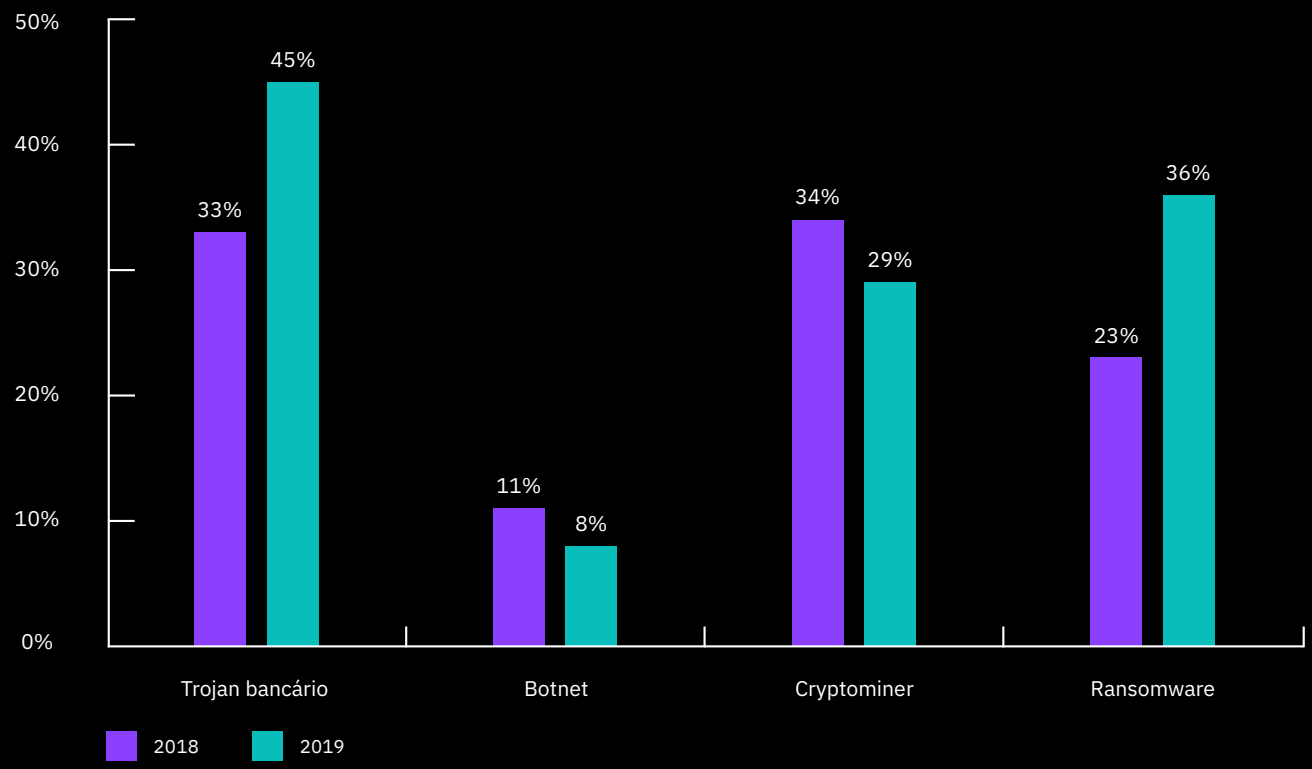
Segundo a telemetria da X-Force, a atividade de criptografia atingiu níveis sem precedentes em meados de 2019, com o volume de atividades em junho quase excedendo todas as outras atividades de criptografia durante todo o ano.

Embora as tendências de malware aumentem e diminuam de acordo com os motivos e os recursos dessas botnets operacionais, esse pico pode estar relacionado à triplicação no valor do Monero, uma criptomoeda frequentemente usada por mineradores de malware.

Figura 5:

Inovação no código genético de malware

Porcentagem de novo código (anteriormente não observado) por categoria em 2018 e 2019 (Fonte: Intezer)



Principais inovadores da evolução do código de malware de 2019

Com base na colaboração anterior da X-Force na detecção de novas variantes de malware, a Intezer usou sua tecnologia de análise genética de malware, revelando as origens genéticas de todo código de software para identificar semelhanças e reutilização de código para mensurar a "inovação" do malware. Essa medida de inovação representa o quanto os invasores investiram no desenvolvimento de um novo código, sugerindo que eles buscam expandir os recursos de ameaças e evitar serem detectados.

Dados da Intezer mostram que, em 2019, os invasores se concentraram principalmente no desenvolvimento e na evolução da base de código de trojans bancários e ransomware, mantendo um alto nível de esforço para modificar e criar cepas de malware com criptografia.

Esta seção do relatório foi escrita pelos pesquisadores da IBM X-Force e da Intezer de forma colaborativa. A Intezer realiza análise genética no código binário do malware.

Em 2019, os trojans bancários tiveram o nível mais alto de novo código (45%), seguido pelo ransomware (36%). Historicamente, a IBM tem observado um aumento no interesse e no investimento por parte dos invasores em tipos de malware eficazes contra usuários corporativos, sugerindo que essas famílias de malware podem atingir empresas em 2020. Se eles não evoluírem constantemente, os operadores de trojans bancários e ransomware enfrentarão a extinção, porque o malware terá uma detecção mais rápida e reduzirá o retorno do investimento dos ataques ao longo do tempo.

Os cryptominers mostraram uma queda de inovação em 2019, mas o volume de atividade de mineração ainda foi alto, sugerindo que os invasores continuam desenvolvendo novas versões de cryptominers, mas cada vez mais dependem do código anterior. Com base na experiência da IBM, esses códigos de malware simplistas geralmente dependem de outros antepassados não mal-intencionados, como o XMRig, por exemplo, modificados para coletar moedas de maneira ilegítima. Novos mineradores também são criados para diferentes propósitos, como coletar moedas em dispositivos de IoT ou, no outro extremo, em servidores infectados, onde a energia da CPU é maior do que em dispositivos menores e em PCs individuais.

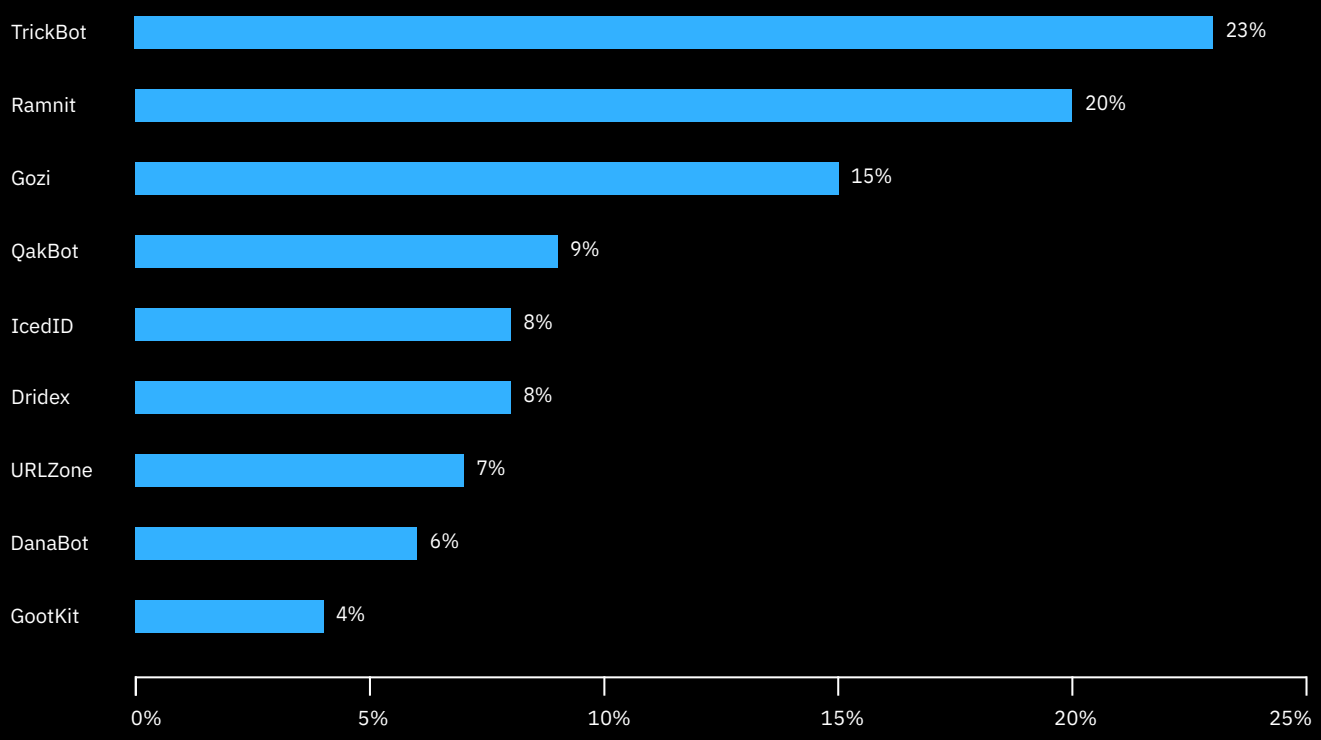
Por outro lado, o malware genérico de botnet (11%) teve menos inovação de código em relação ao ano anterior, indicando menor investimento na modificação dos recursos dele. A IBM observou que esses tipos de códigos são enviados aos usuários por spam ou publicidade mal-intencionada. O principal papel do malware genérico de botnet é conquistar uma posição em um dispositivo infectado, mas a funcionalidade dele permanece mínima, o que pode explicar por que não observamos um nível mais alto de evolução do código.

A partir de 2020, essas tendências de inovação de código podem ser indicativas dos tipos de malware que exigirão mais esforço para serem identificados e contidos devido ao investimento para evoluir constantemente o código deles.

Em 2019, os invasores se concentraram no desenvolvimento e na evolução da base de código de trojans bancários e ransomware.

Figura 6:
Principais famílias de trojans bancários

Distribuição das principais famílias de trojans bancários em 2019, como uma porcentagem das nove famílias mostradas (Fonte: IBM X-Force)



Trojans bancários e ransomware: um casamento traiçoeiro que só tende a piorar

O malware financeiro se transformou em um problema importante há pouco mais de uma década com o surgimento do Trojan Zeus, que na época foi o primeiro trojan bancário comercial disponível a todos no mundo do crime virtual. Uma análise do cenário de crimes financeiros de 2019 marca uma tendência clara das principais gangues de trojans bancários: essas botnets de malware estão sendo cada vez mais usadas para abrir as portas para ataques de ransomware direcionados e de alto risco.

Um gráfico das famílias de trojans mais ativos nessa categoria em 2019 é semelhante ao que produzimos no resumo anual de 2018. TrickBot, Gozi e Ramnit permanecem nas três primeiras posições. Esses trojans são operados por grupos organizados que oferecem modelos de negócios variados para outros criminosos virtuais, como esquemas de botnet como serviço e distribuição por meio de ativos comprometidos.

A gangue que opera o TrickBot tem sido, de longe, o grupo de crimeware mais ativo no cenário de crimes virtuais em 2019. Essa atividade foi expressa em vários aspectos:

— Frequência de atualizações e correções de código (evolução de código, versão e recurso)

— Frequência e escala de campanhas de infecção

— Frequência e volume da atividade de ataque

As gangues que estamparam as manchetes com ataques de ransomware de alto risco em 2019 também foram as que introduziram ataques de fraude eletrônica de alto risco ao cenário de crimes virtuais em 2015. Em certo sentido, a estratégia abrangente é a mesma, apenas as táticas são modificadas ao longo do tempo: visar empresas para conseguir uma recompensa maior.

Os principais exemplos de trojans bancários diversificando para ransomware são:

Dridex
Espalhava o LokiBot nos dispositivos dos usuários e agora implanta o BitPaymer/ DopplePaymer nas redes corporativas.

GootKit
Suspeita de implantação do LockerGoga em redes corporativas. O LockerGoga surgiu no início de 2019 e desde então faz parte de ataques incapacitantes às empresas.

QakBot
Implanta o MegaCortex em redes corporativas.

TrickBot
Implanta o Ryuk em redes corporativas.

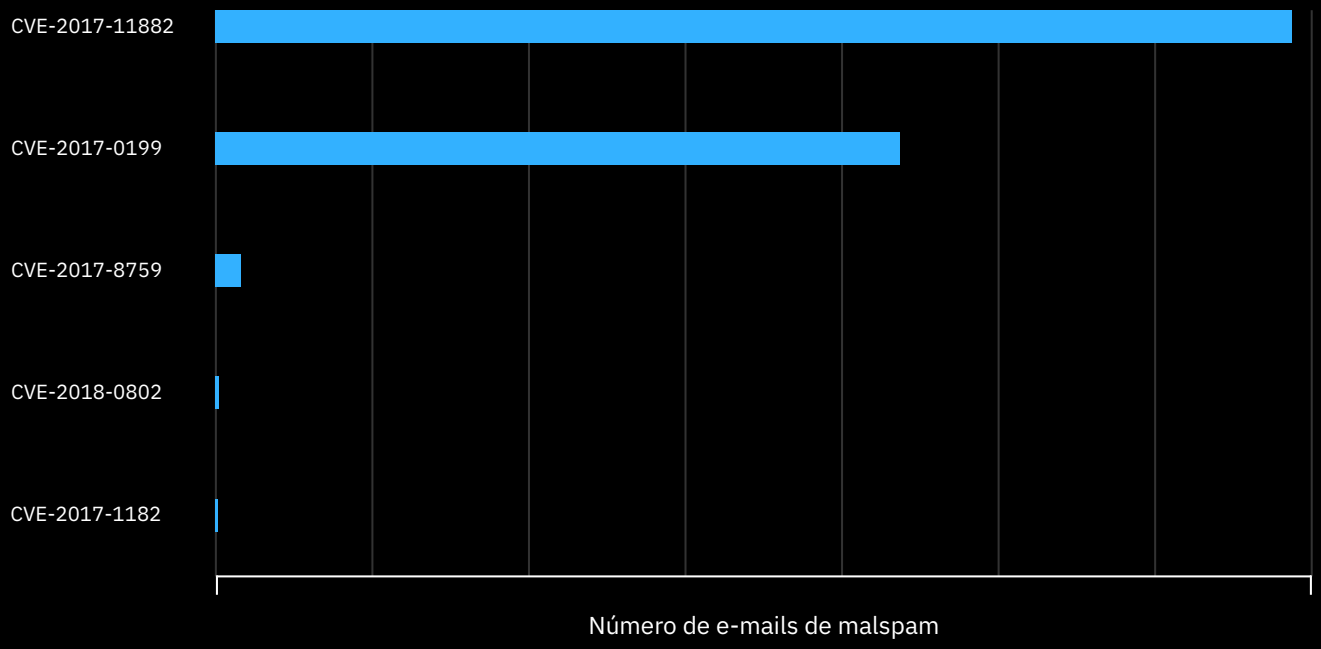
Além disso, os relatórios do final de 2019 indicam que o ITG08, (FIN6), que historicamente se concentra no roubo em massa de dados de cartões de pagamento, também está diversificando os TTPs. Agora, o objetivo é incluir a implantação de ransomware em redes corporativas. Acumular e depois vender ou usar dados de cartões roubados requer tempo e esforço para dar lucro, enquanto um ataque de ransomware tem o potencial de gerar milhões de uma só vez, fazendo com que mais gangues optem pelo ransomware e pela extorsão virtual.

Tendências de spam e phishing

Figura 7:

Principais vulnerabilidades exploradas em malspam

Distribuição das principais vulnerabilidades exploradas em anexos de spam em 2019, por volume (Fonte: IBM X-Force)



Spam: as vulnerabilidades de 2017 ainda brilham em 2019

A IBM X-Force executa armadilhas de spam em todo o mundo e monitora dezenas de milhões de mensagens de spam e e-mails de phishing diariamente. Nossas equipes e tecnologia analisam bilhões de páginas da Web e imagens para detectar atividades fraudulentas e abuso de marca.

A análise da atividade global de spam feita pela X-Force indica que o e-mail de spam continua usando um subconjunto limitado de vulnerabilidades, com foco especial em apenas dois CVEs: 2017-0199 e 2017-11882. Ambas são vulnerabilidades corrigidas, responsáveis por quase 90% das ameaças que os invasores tentaram explorar por meio de campanhas de spam. Esses dois CVEs afetam o Microsoft Word e não requerem interação do usuário além da abertura de um documento bloqueado.

Nossos dados de eventos mostram que a frequência com que essas duas vulnerabilidades foram usadas pelos invasores em 2019 excedeu o uso de qualquer outra vulnerabilidade de execução remota de código do Microsoft Word em uma proporção de quase 5 para 1.

Embora essas duas vulnerabilidades apareçam em quantidades consideráveis de e-mail de spam, não há indicação da eficácia delas na exploração dos usuários. Dito isto, o spam geralmente é uma questão de números: com volume suficiente, mesmo uma pequena taxa de sucesso é o bastante para dar lucro aos invasores. Como muitos usuários e até mesmo organizações podem demorar a corrigir certos problemas, ainda é possível ver dispositivos comprometidos por bugs mais antigos.

Pode haver muitas explicações para a popularidade das vulnerabilidades mais antigas, como a facilidade de incorporação e disponibilidade de geradores de documentos gratuitos, a eficácia contínua ou a versatilidade de descarregar uma variedade de cargas mal-intencionadas.

O uso continuado de vulnerabilidades antigas destaca a longa cauda de atividades mal-intencionadas e como vulnerabilidades significativas ainda podem ser aproveitadas contra os usuários anos após a divulgação e o lançamento do patch.

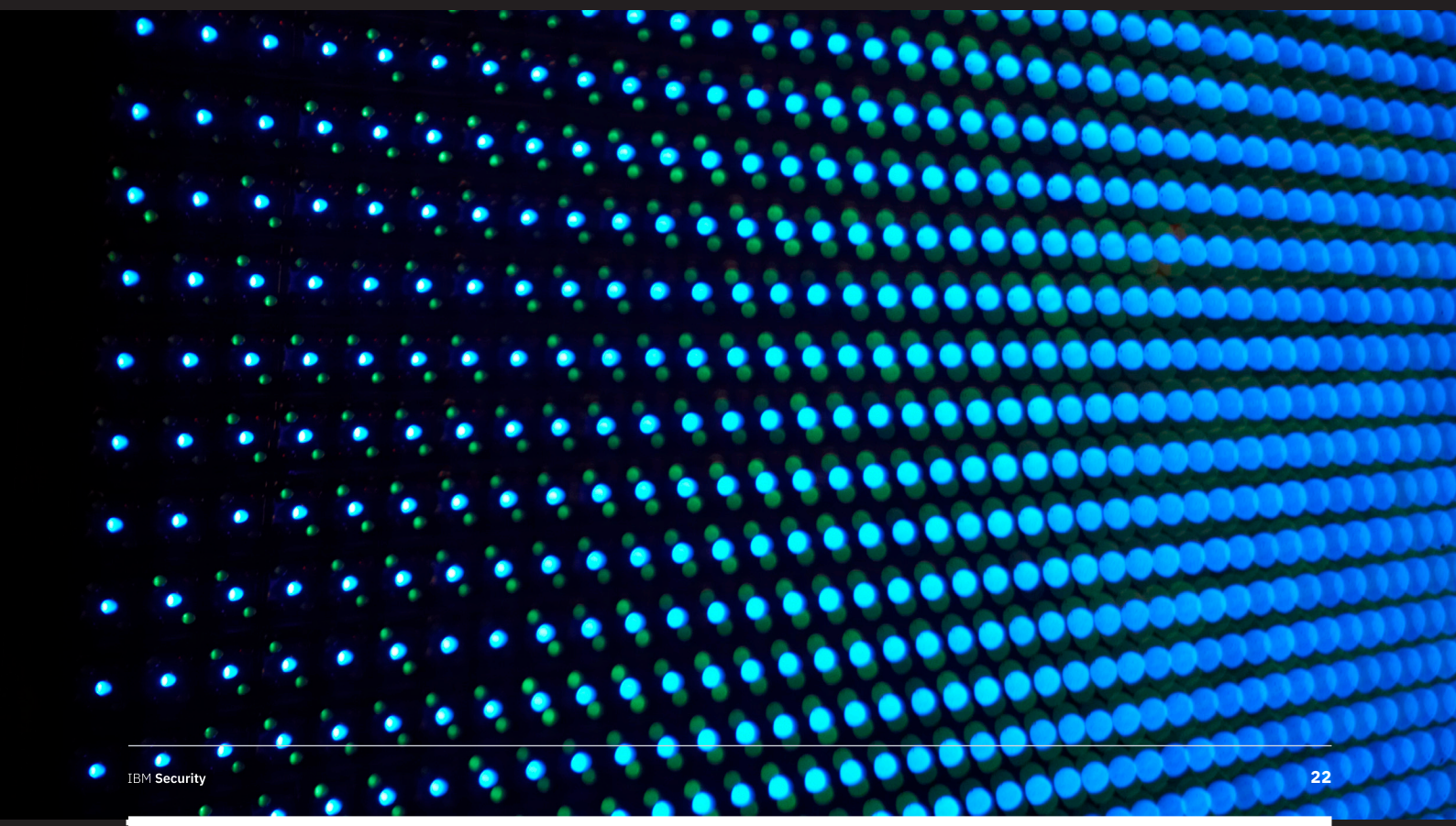
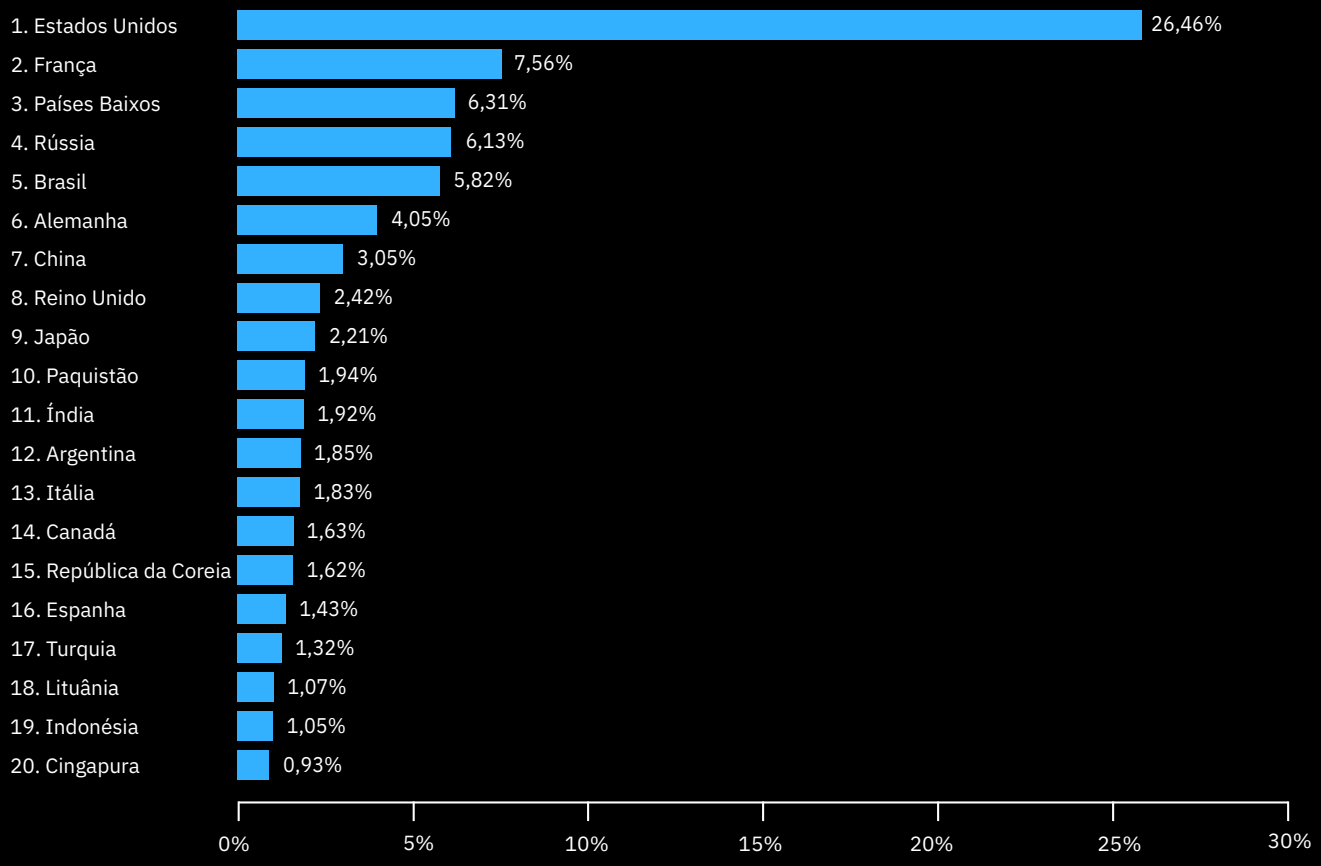


Figura 8:

Os 20 principais países que hospedam C2 de spam

Os 20 principais países de acordo com a participação deles nos servidores de comando e controle (C2) de spam em todo o mundo em 2019. (Fonte: IBM X-Force)



Botnets de spam hospedadas no Ocidente, impacto global

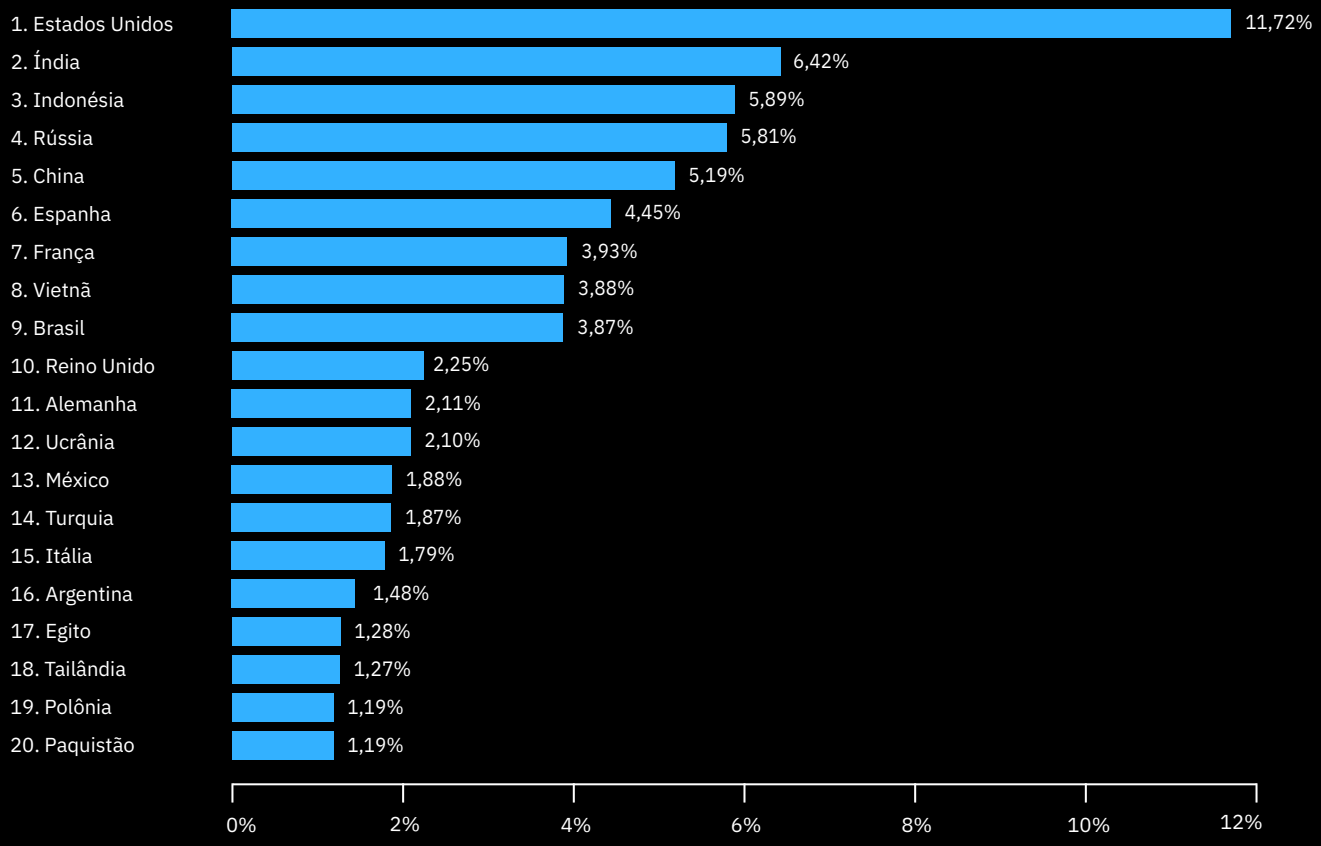
A pesquisa da IBM X-Force sobre botnets de spam analisa uma variedade de pontos de dados geográficos específicos vinculados à infraestrutura de C2 (comando e controle) para botnets de spam. Um dos parâmetros que analisamos é a localização geográfica em que os C2s da botnet estão hospedados. Em 2019, descobrimos que os C2s estavam hospedados principalmente nos países da América do Norte e da Europa Ocidental, respondendo por mais da metade de todos os casos de C2 observados em 2019. A hospedagem de C2 restante foi espalhada por uma variedade maior de regiões.

Em muitos casos, a infraestrutura de C2 de botnet de spam é hospedada em servidores comprometidos, e o uso de servidores norte-americanos e europeus está alinhado ao entendimento comum de que esses países geralmente têm um tempo de atividade do servidor mais consistente. Além disso, os criminosos virtuais preferem hospedar os ataques em recursos locais com menor probabilidade de apresentar sinais de alerta quando o tráfego desses servidores interage com dispositivos e redes na região-alvo.

Figura 9:

Os 20 principais países com vítimas de botnet de spam

Os 20 principais países de acordo com a participação deles nos clientes (vítimas) de botnet de spam em todo o mundo em 2019. (Fonte: IBM X-Force)



Vítimas de spam por região

As vítimas de botnets de spam em 2019 se espalharam pelo mundo, com os Estados Unidos apresentando o maior número de vítimas, seguidos pela Índia, Indonésia, Rússia e China. Essa distribuição de segmentação está alinhada à motivação dos remetentes de spam de alcançar o maior número possível de destinatários com campanhas de spam de alto volume. Naturalmente, os países onde a população é maior recebem um número maior de e-mails de spam.

Domínios mal-intencionados bloqueados destacam a prevalência dos serviços de anonimização

Quando se trata de manter as redes mais seguras contra ameaças on-line, uma prática comum é impedir que usuários e ativos se comuniquem com domínios potencial ou reconhecidamente mal-intencionados. Para minimizar o risco, a maioria das organizações coloca endereços IP suspeitos em listas de bloqueio. Com a mesma ideia em nível global, o Quad9, um serviço DNS (Servidor de Nome de Domínio) disponível gratuitamente[3], bloqueia uma média de 10 milhões de solicitações de DNS para sites mal-intencionados diariamente.

De acordo com uma amostra de dados do Quad9 correlacionados com a inteligência sobre ameaças da IBM Security, os URLs encontrados nos e-mails de spam compunham a maioria das solicitações de DNS suspeitas, com 69% de todas as solicitações em 2019. Embora abaixo de 77% em 2018, a categoria de URL de spam ainda é a mais significativa dos domínios mal-intencionados em geral. A queda de 8 pontos percentuais pode ser atribuída à categoria de serviços de anonimização, que representa 24% das solicitações de DNS.

O spam de e-mail ainda é uma das maneiras mais eficazes de alcançar o maior número de vítimas em potencial, graças às grandes botnets de spam, como a Necurs, que podem transmitir dezenas de milhões de e-mails de spam por dia. Os domínios mal-intencionados costumam espalhar malware para distribuir ransomware, scripts de roubo de credenciais ou links para outros golpes e são criados para enganar o usuário final, parecendo legítimo ou imitando uma marca conhecida.

Links para URLs mal-intencionados em e-mails de spam também são o método de escolha da grande maioria dos criminosos financeiros, porque permitem que eles ofereçam uma ampla rede com o mínimo esforço ou optem pela segmentação geográfica específica, o que pode limitar a exposição aos golpes.

O gráfico na Figura 10 mostra as distribuições de tipos de domínio mal-intencionados registrados pelo IBM Security em 2019.

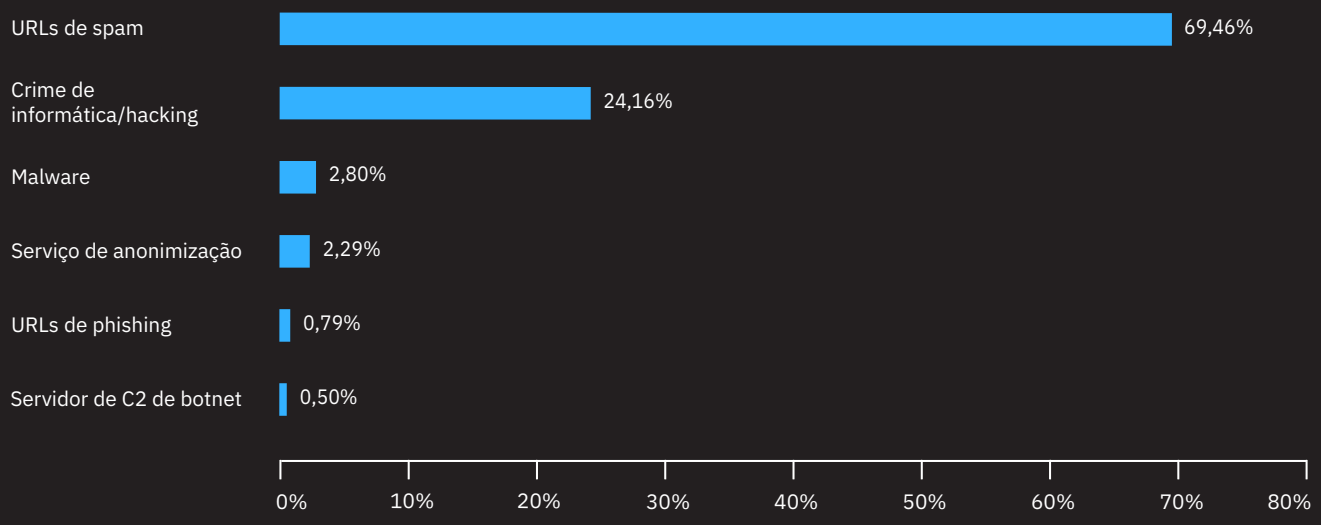
O spam de e-mail ainda é uma das maneiras mais eficazes de alcançar o maior número de vítimas em potencial.

3 O Quad9 foi criado e patrocinado por meio de uma colaboração entre a IBM, a Packet Clearing House (PCH) e a Global Cyber Alliance (GCA).

Figura 10:

Principais tipos de ameaças de domínio mal-intencionado

Distribuição dos principais tipos de ameaças de domínio mal-intencionado, como uma porcentagem dos seis tipos mostrados, em 2019 (Fonte: IBM X-Force e Quad9)



URLs de spam:
Domínios vinculados a sites afiliados a campanhas de spam, geralmente um transtorno, mas não afiliados a outras atividades criminosas

Serviços de anonimização:
Domínios vinculados a provedores de anonimização que ocultam o tráfego de outras visualizações

Crime de informática/hacking:
Domínios especificamente identificados como envolvidos em comportamento criminoso, como sites que hospedam scripts de exploração de navegador da Web

URLs de phishing:
Domínios disfarçados de outros domínios legítimos, geralmente na tentativa de obter dados credenciais ou outras informações confidenciais do usuário

Comando e controle de botnet:
Domínios vinculados à atividade de botnet e potencialmente infectando visitantes

Malware:
Domínios que hospedam malware conhecido

Os provedores de anonimização, como o Tor, por exemplo, permitem que os usuários anonimizem a origem do tráfego da Internet navegando nos nós operados por outros agentes. Embora os serviços de anonimização geralmente atendem a um propósito legítimo, que é oferecer aos usuários mais privacidade durante a navegação na Web, essa atividade também pode dificultar ou impossibilitar o rastreamento e o bloqueio de atividades mal-intencionadas.

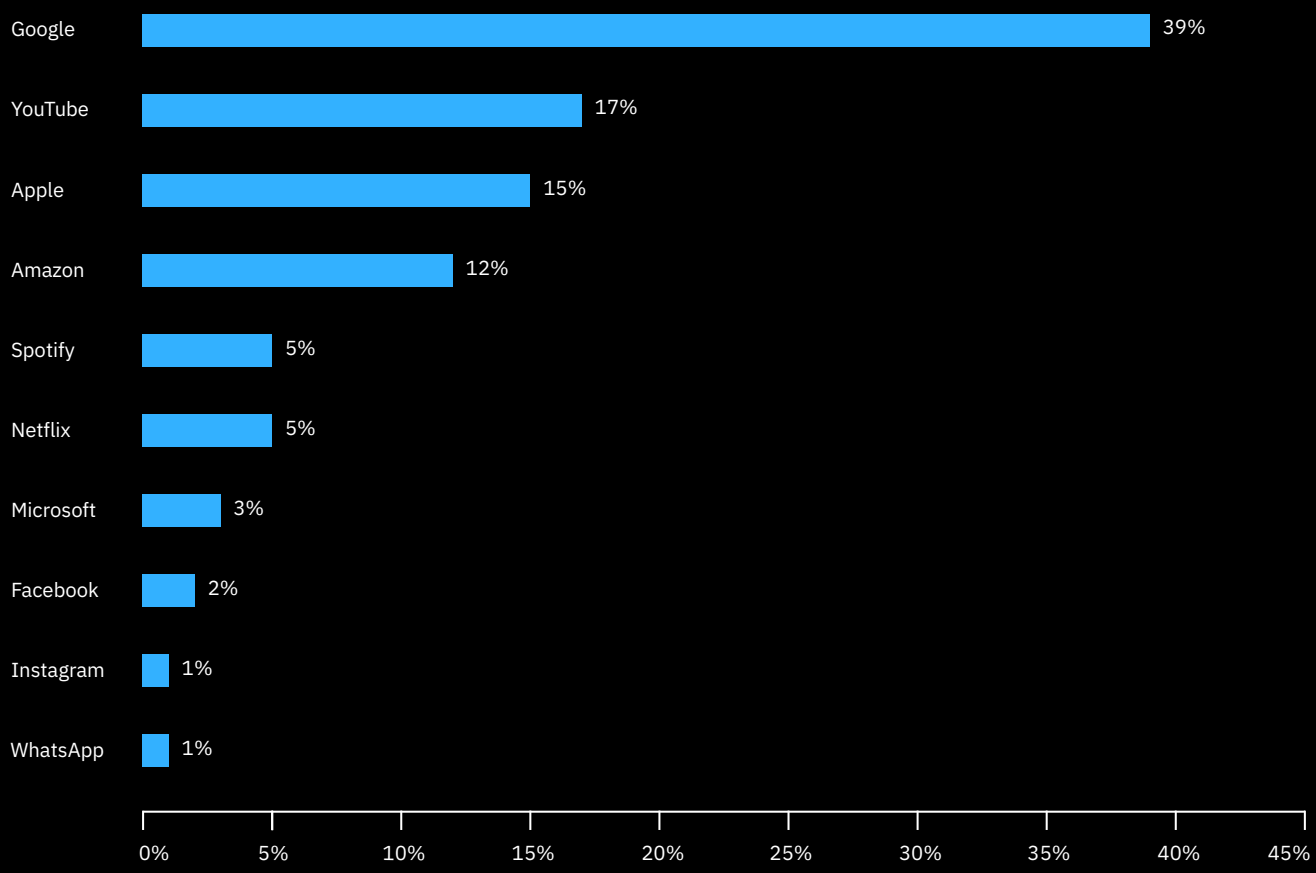
A anonimização é uma tática comum usada pelos criminosos virtuais que tentam encobrir os próprios rastros porque ela pode ser usada para ofuscar links mal-intencionados, exfiltrar dados sem acionar regras de DLP (prevenção de perda de dados) ou reduzir cargas úteis mal-intencionadas adicionais antes que o IP do servidor remoto possa ser bloqueado.

Quatro por cento das solicitações mal-intencionadas de DNS foram categorizadas como crime de informática ou páginas da Web de hackers blackhat, onde alguns criminosos tentam explorar o navegador, distribuir informações sobre fraudes ou se envolver em outros tipos de crime on-line. Esse número relativamente baixo provavelmente se deve ao fato de esses links serem roteados por meio de nós de anonimização ou detectados e bloqueados por proxies e firewalls da empresa e, consequentemente, encerrados.

Figura 11:

As dez principais marcas falsificadas

Distribuição das dez principais marcas falsificadas em spam em 2019, como uma porcentagem das dez marcas mostradas (Fonte: IBM X-Force)



Empresas de tecnologia clonadas por phishing, redes sociais

O phishing continuou a ser um vetor de ameaça importante em 2019, e os dados da X-Force mostram que as marcas mais falsificadas nas campanhas de phishing foram plataformas de tecnologia e rede social. Os domínios falsificados podem ser difíceis de discernir visualmente pelos usuários e geralmente refletem domínios legítimos usados pela empresa representada. Um site que parece verdadeiro pode ajudar a convencer um usuário a divulgar dados pessoais em um site mal-intencionado, por ser muito parecido com o original.

Esses dados foram obtidos analisando todos os domínios mal-intencionados bloqueados pelo Quad9 em 2019 e baseados na detecção de invasão de domínio da IBM X-Force.

Visar redes sociais ou sites de streaming de conteúdo, como o Instagram e o Spotify, pode não fornecer aos invasores dados facilmente monetizáveis, como roubar contas do Google ou da Amazon. No entanto, é possível que as pessoas usem as mesmas senhas entre contas e serviços, e os invasores podem usar essas credenciais coletadas para ter acesso a contas mais valiosas mantidas pelo mesmo usuário.

Setores mais visados

No cenário atual de ameaças, a especificidade de alguns tipos de ataques de acordo com as motivações dos invasores significa que o gerenciamento de riscos de segurança virtual pode parecer muito diferente de um setor para outro.

Para ter uma visão geral dos setores mais visados todos os anos, os pesquisadores da X-Force classificam o volume de ataques observado em cada um deles. Os setores mais visados foram determinados com base em dados de incidentes de ataque e segurança de redes gerenciadas pela X-Force, dados e insights derivados dos nossos serviços de resposta a incidentes e incidentes divulgados publicamente.

Figura 12:

Os dez setores mais visados

os dez setores mais visados classificados por volume de ataques, 2019 em comparação com 2018 (Fonte: IBM X-Force)

Setor	Ranking de 2019	Ranking de 2018	alterar
Serviços financeiros	1	1	–
Varejo	2	4	2
Transportes	3	2	-1
Mídia	4	6	2
Serviços de Consultoria	5	3	-2
Governo	6	7	1
Educação	7	9	2
Manufatura	8	5	-3
Energia	9	10	1
Assistência médica	10	8	-2

A Figura 12 é um gráfico comparativo dos principais setores mais atacados em 2019 e a posição deles em relação a 2018.

É fácil perceber que, embora não tenha havido surpresas no setor de serviços financeiros, o setor de varejo vem despertando um interesse crescente dos invasores. O mesmo aconteceu com as empresas de mídia e entretenimento, educação e órgãos governamentais.

As seções a seguir detalham a frequência relativa da segmentação com base em diversas fontes de dados e nossas descobertas para cada um desses setores em 2019. Algumas descrições de setor destacam os invasores que foram particularmente ativos na segmentação do setor nos últimos anos, mas essa lista não é exaustiva e inclui dados anteriores a 2019. O X-Force IRIS rastreia e perfila dezenas de grupos de criminosos virtuais e patrocinados por estados-nações. Atividade não atribuída e campanhas descobertas aleatoriamente são rastreadas na atividade “HIVEs”. Depois que a atividade atinge um limite analítico estrito, ela faz a transição para um ITG (IBM Threat Group), que se baseia em coleções de TTPs, infraestrutura, direcionamento e tradecraft.

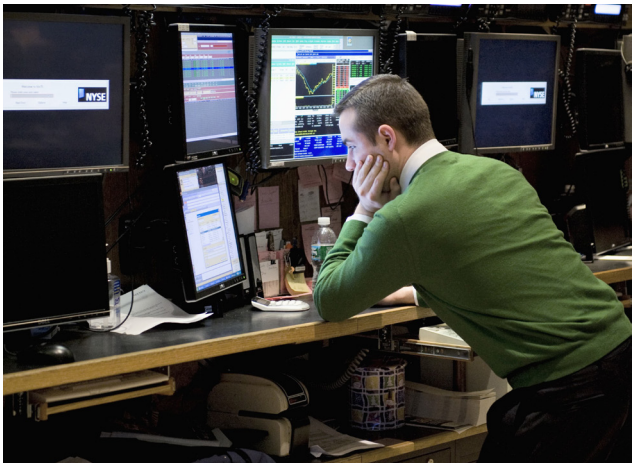
Finanças e Seguros

Por quatro anos consecutivos, o setor de Finanças e Seguros foi o mais atacado em 2019. Os ataques a esse setor corresponderam a 17% de todos os ataques nos dez setores mais atacados.

É provável que os criminosos virtuais motivados financeiramente constituíram a maior parte dos invasores virtuais ativos que visam entidades financeiras, e o fascínio que as empresas financeiras despertam nos criminosos virtuais é claro: a possibilidade de pagamentos significativos e rápidos, na casa dos milhões por um ataque bem-sucedido.

Os dados das ações de resposta a incidentes da X-Force mostraram que o setor de Finanças e Seguros foi o primeiro entre os principais setores-alvo, apesar de um número menor de vazamentos de dados divulgados publicamente.

Isso sugere que as financeiras e seguradoras tendem a sofrer um volume maior de ataques em relação a outros setores, mas provavelmente contam com ferramentas e processos mais eficazes para detectar e conter ameaças antes que se transformem em grandes incidentes. As financeiras também estão mais inclinadas a testar os planos de resposta sob ataque e compõem a maior parte das organizações que usam os IBM Security Command Centers para se preparar e praticar para um ataque virtual. Testar exaustivamente planos e equipes de resposta a incidentes em relação a cenários relevantes mostrou-se eficaz na mitigação de danos financeiros causados por um vazamento de dados, de acordo com o relatório "Prejuízo de um vazamento de dados"[4] de 2019 conduzido pelo Ponemon Institute e patrocinado pela IBM Security. As organizações invadidas que testaram exaustivamente um plano de resposta a incidentes, em um ambiente de alcance virtual, por exemplo, tiveram em média um prejuízo de US$ 320 mil a menos do que o prejuízo médio geral de um vazamento de dados de US$ 3,92 milhões.



Os grupos de ameaças dominantes visando as organizações do setor financeiro foram o ITG03 (Lazarus), o ITG14 (FIN7) e várias facções do Magecart em 2019. Trojans bancários como TrickBot, Ursnif e URLZone foram algumas das principais ameaças que assolaram os bancos em 2019, assumindo e fraudando as contas dos clientes.

4 O relatório "Prejuízo de um vazamento de dados" foi conduzido pelo Ponemon Institute e patrocinado pela IBM.

Varejo

O setor de varejo foi o segundo mais atacado de todos, de acordo com dados da X-Force de 2019. Esse setor foi afetado por 16% de todos os ataques nos dez principais setores, um aumento acentuado em relação ao quarto lugar e 11% em 2018. Esse setor sofreu o segundo maior número de ataques à rede em 2019.

O setor de varejo chegou à segunda posição em 2019 com base nos dados do X-Force IRIS e nas informações divulgadas publicamente sobre vazamentos de dados. Os tipos mais comuns de invasores que visam organizações de varejo são os criminosos virtuais motivados financeiramente, que buscam obter PII (informações de identificação pessoal) do consumidor, dados de cartões de pagamento, dados financeiros, histórico de compras e informações de programas de fidelidade. Os criminosos virtuais geralmente usam esses dados para controlar contas de clientes, defraudar clientes e reutilizar os dados em vários cenários de roubo de identidade.

Uma técnica popular de ataque usada pelos criminosos virtuais para atingir os varejistas em 2019 foi o desvio de malware de PDV (ponto de venda) e cartão de pagamento de comércio eletrônico, cada um com o objetivo de desviar informações do cartão de pagamento durante uma transação por meio de terminais de pagamento físico ou on-line, respectivamente.

Em particular, um grupo de facções criminosas virtuais, sob o termo geral Magecart, tem como alvo plataformas de pagamento de terceiros e conhecidos varejistas on-line diretamente para injetar código JavaScript mal-intencionado nas páginas de pagamento com cartão dos sites deles. O código é executado como parte do processo de pagamento para transmitir as informações do cartão de pagamento da vítima aos criminosos virtuais, além de obter o fornecedor desejado.

Os profissionais de resposta a incidentes do X-Force IRIS observaram esses tipos de ataques em primeira mão em várias violações em 2019 e apontam que, embora os trechos de código mal-intencionado possam ser bastante básicos, o comprometimento de back-end das plataformas subjacentes pode causar um impacto agregado onde os criminosos foram capazes de atingir milhares de estabelecimentos usando a mesma técnica de maneira geral.

Entre os principais grupos de ameaças que têm como alvo o setor de varejo estão:

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

Além dos skimmers de comércio eletrônico on-line, o malware no ponto de venda continua sendo uma técnica popular usada pelos criminosos virtuais contra varejistas nas lojas físicas para desviar dados de cartões de pagamento de máquinas de ponto de venda e servidores de back-end durante uma transação ou à medida que os dados são gravados na memória.

Transportes

O setor de transportes é considerado parte da infraestrutura crítica de qualquer país. As empresas desse setor mobilizam a economia por meio de três tipos principais de transporte: transporte terrestre, marítimo e aéreo, para serviços industriais e de consumo. Esse setor foi o terceiro mais atacado em 2019, com ataques caindo de frequência de 13% em 2018 para 10% em 2019.

O ranking do setor de transportes em terceiro lugar, depois de finanças e varejo, ressalta o crescente apelo de dados e infraestrutura operados por empresas de transporte. Esses ativos atraem criminosos virtuais e invasores de estados-nações. As informações mantidas pelas empresas de transporte representam um alvo atrativo para os criminosos virtuais, como informações pessoais, informações biográficas, números de passaporte, informações sobre programas de fidelidade, dados de cartões de pagamento e itinerários de viagens.

Nesse setor, as companhias aéreas e os aeroportos, em particular, estão sendo cada vez mais visados por criminosos virtuais e de estados-nações inimigos que procuram rastrear viajantes de interesse ou monetizar as informações pessoais dos viajantes vendendo-as na dark web.

As ameaças virtuais ao setor de transportes apresentam um risco adicional em comparação com outros setores, dado o potencial efeito cinético que um ataque poderia ter, colocando em risco a vida humana, bem como o potencial de causar um impacto em cascata em outros setores que dependem de serviços de transporte para realizar suas atividades.

Os grupos de invasores que visam o setor de transportes variaram até 2019, com grupos de criminosos virtuais e estados-nações inimigos lançando ataques a organizações em todo o mundo.

Entre os principais grupos de ameaças que têm como alvo o setor de transportes estão:

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

Mídia e Entretenimento

O quarto setor mais atacado no ranking de X-Force de 2019 foi o de mídia, sofrendo 10% de todos os ataques nos dez principais setores. O setor de mídia subiu de 8% em 2018 e passou da sexta para a quarta posição.

O setor de mídia inclui subsetores de alto padrão, como telecomunicações, bem como empresas que produzem, processam e distribuem mídia e entretenimento. O setor de mídia e entretenimento é um alvo de alto valor dos ataques virtuais que buscam influenciar a opinião pública, controlar o fluxo de informações ou proteger a reputação de uma organização ou um país. Em particular, grupos de estados-nações podem ver o conteúdo negativo da mídia como uma ameaça significativa à segurança nacional, enquanto os criminosos virtuais estão percebendo que os ataques à mídia e ao entretenimento são financeiramente lucrativos porque eles podem manter meios de comunicação roubados e pré-transmitidos em troca de resgate.

Criminosos virtuais oportunistas e estados-nações inimigos geralmente atingiram esse setor em 2019.

Entre os principais grupos de ameaças que têm como alvo o setor de mídia e entretenimento estão:

ITG03 (Lazarus)
Hive0003 (Newscaster)
Hive0047 (Patchwork)

Serviços de Consultoria

O setor de serviços de consultoria conta com várias empresas que prestam serviços de consultoria especializados para outros setores. Alguns exemplos são empresas que prestam consultoria jurídica, contábil, de RH e especializada ao cliente. Esse setor sofreu 10% de todos os ataques nos dez principais setores, de acordo com dados da X-Force, abaixo dos 12% de 2018.

As informações de vazamentos de dados divulgadas publicamente indicam que os serviços de consultoria também tiveram o maior número de registros vazados em todos os setores do nosso ranking. Muitas dessas empresas adquirem dados altamente confidenciais dos clientes, inclusive dados para processos jurídicos, contábeis e fiscais, que podem se tornar um alvo lucrativo para invasores que buscam ganhos monetários ou informações privilegiadas.

Além disso, esse setor inclui empresas de tecnologia, cada vez mais visadas por conta do acesso de terceiros que elas têm e que podem ser aproveitados por invasores que tentam invadir as organizações maiores e potencialmente mais seguras a que elas atendem.

Além disso, o fluxo de trabalho diário das empresas de serviços de consultoria tende a criar vetores de ataque naturais para criminosos por meio de e-mails de phishing e macros mal-intencionadas. Muitas empresas de serviços profissionais dependem muito de arquivos de produtividade, como anexos de documentos do Word e do Excel, para escrever contratos, se comunicar com os clientes e concluir as tarefas do dia a dia. O uso de macros é um dos mais notórios vetores de ataque que os criminosos virtuais exploram para plantar scripts mal-intencionados nos tipos de arquivos que nenhuma organização pode se dar ao luxo de bloquear completamente.

Grupos de invasores notórios que tiveram como alvo serviços de consultoria em 2019: ITG01 (APT10, Stone Panda), um grupo patrocinado por estado-nação que parece ser originário da China.

Governo

O setor governamental é o sexto mais atacado do nosso ranking, recebendo 8% dos ataques nos dez principais setores, inalterado em relação ao ano anterior, mas subindo no ranking geral da sétima posição em 2018.

O setor governamental é um alvo de alto valor dos criminosos virtuais de estados-nações que buscam obter vantagem sobre os adversários percebidos, os hacktivistas que procuram expor informações comprometedoras ou provar suas proezas técnicas, e os criminosos virtuais que buscam ganhos monetários por meio de extorsão ou dados roubados.

Os governos municipais foram os mais atacados nos últimos anos, porque os criminosos virtuais buscam coletar dinheiro de extorsão de organizações com menor probabilidade de serem tão seguras quanto as do setor privado. As entidades governamentais têm ativos de valor para os invasores, principalmente informações confidenciais e possíveis segredos de estado, que podem incluir informações de identificação pessoal sobre funcionários e agentes do governo, informações financeiras, comunicações internas e a funcionalidade de redes críticas.

Criminosos de estado-nação demonstraram interesse de longo prazo em atacar entidades do setor governamental, e o X-Force IRIS avalia que eles são os mais capazes de fazer isso. Cada vez mais em 2019, no entanto, os grupos de criminosos virtuais também visaram entidades governamentais, buscando criptografar e reter dados de resgate que os governos precisam para operar, particularmente no nível municipal.

Em 2019, mais de 70 entidades governamentais foram atingidas com ransomware apenas entre janeiro e julho. Os criminosos virtuais também roubaram dados, inclusive de sites de defesa, e depois os vazaram na dark web. Os hacktivistas notoriamente veem o governo como um alvo atraente, principalmente se houver uma questão controversa sobre a qual desejam fazer uma manifestação. As organizações governamentais geralmente carecem do mesmo nível de financiamento de segurança virtual que suas contrapartes do setor privado, embora ainda precisem manter um serviço consistente para os cidadãos, exacerbando ainda mais o desafio imposto a essas organizações pelos invasores.

Grupos de invasores notórios visando agências governamentais em 2019: diversos criminosos virtuais e grupos patrocinados por estados-nações.

Educação

O setor de educação sofreu 8% de todos os ataques nos dez principais setores, contra 6% em 2018, tornando-o o sétimo setor mais atacado do nosso ranking.

Ele apresenta uma variedade de ativos valiosos para criminosos motivados financeiramente e para estados-nações. De PI (propriedade intelectual) a PII, as organizações educacionais são um alvo amplo para diferentes tipos de invasores.

Cada um com uma motivação diferente, os inimigos usaram uma variedade de vetores de infecção inicial para invadir as redes de instituições acadêmicas, mas o método mais comumente observado continua sendo o e-mail de phishing, geralmente adaptado à instituição acadêmica ou à área de pesquisa específica.

As organizações do setor de educação geralmente têm uma infraestrutura de TI grande e variada e presença digital. Eles operam ativos diferentes que atendem a um número elevado de usuários, variando de funcionários a estudantes e prestadores de serviços. Essa vasta superfície de ataque que os invasores podem aproveitar para várias atividades mal-intencionadas é mais difícil de proteger. Relatórios publicados em outubro de 2019 indicaram que pelo menos 500 escolas foram atingidas por ataques virtuais, principalmente ransomware, em 2019, apenas nos EUA.

Alguns exemplos notáveis de ataques mais sofisticados nesse setor incluem invasores de estados-nações que comprometeram as redes das universidades e as usaram como palco para infectar organizações de mídia e prestadores de serviços militares. Da mesma forma, os invasores que buscam pesquisas financiadas pelos EUA procuram regularmente maneiras de invadir redes de universidades para roubar propriedade intelectual que às vezes pode ser inestimável. O IBM X-Force

Entre os principais grupos de ameaças que têm como alvo o setor de educação estão:

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IRIS avalia com grande confiança que esse setor continuará sendo alvo de criminosos motivados financeiramente e afiliados a estados que desejam obter acesso a informações valiosas.

Grupos de invasores notórios que visaram esse setor em 2019 incluíram facções criminosas virtuais oportunistas e estados-nações inimigos, oriundos de países como China, Rússia e Irã.

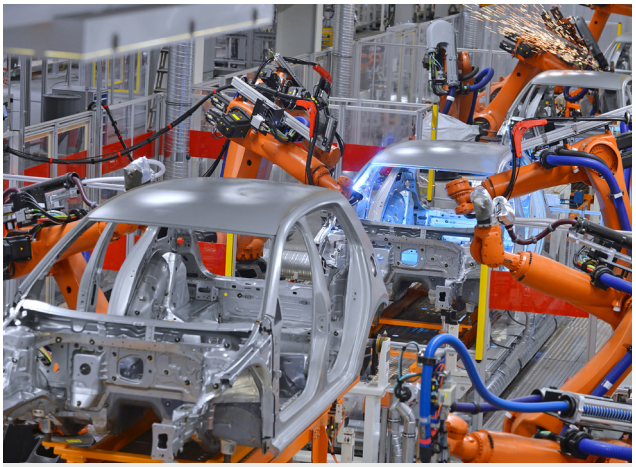
Manufatura

Movimentando a economia por meio de metais, produtos químicos, bens de capital e eletrônicos, os fabricantes não estão livres de ameaças à TI e ameaças que afetam o piso da TO conectada. Com 8% de todos os ataques nos dez principais setores atacados, a manufatura está classificada como o oitavo setor mais atacado do nosso ranking, caindo de 10% em 2018.

Embora seja possível que este setor tenha recebido menos ataques em relação ao ano anterior, a queda nos números pode refletir o fato de que, em muitos casos, vazamentos de dados no setor de manufatura não envolvem informações necessariamente sujeitas a divulgação e regulamentação legais. Como resultado, os ataques nem sempre são divulgados publicamente, o que pode fazer parecer que os fabricantes são atacados com menos frequência do que realmente acontece.

Os fabricantes também são organizações que operam ambientes de TI e TO e, portanto, estão sujeitos às mesmas ameaças que afetam os sistemas de ICS e SCADA. Mas enquanto a segurança da informação nesse setor ficou para trás no passado, a resposta pública bem-sucedida de um fabricante norueguês a um grande ataque de ransomware em 2019 pode ser um indicativo de mudanças nas abordagens de segurança virtual por esse setor.

Criminosos virtuais ou estados-nações inimigos que buscam ganhos financeiros e dados de PI provavelmente representam a maior ameaça virtual a empresas do setor de manufatura. Uma das técnicas de ataque mais comuns usadas contra os fabricantes em 2019 foi a fraude do Ataque de e-mail comercial (BEC), especialmente se eles frequentemente negociam com fornecedores estrangeiros. Nesses casos, os servidores de e-mail da empresa, ou mesmo apenas as contas de e-mail, são comprometidos pelos invasores que se inserem nos segmentos de comunicação existentes para, eventualmente, desviar milhões de dólares para as contas que controlam.



Entre os grupos de ameaças notórios que visaram o setor de manufatura estão:

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

Os fabricantes também são propensos a ataques à cadeia de suprimentos e podem ser explorados por estados-nações inimigos para plantar backdoors ou malware nos produtos que fabricam e enviam para outros países.

No front da motivação financeira, os invasores poderiam ter como alvo os fabricantes para buscar segredos comerciais e propriedade intelectual. Pesquisas que levaram anos para serem desenvolvidas por uma organização podem dar lucro rapidamente aos criminosos virtuais na dark web ou aumentar a vantagem econômica ou de defesa de um país, especialmente no caso de fabricantes de equipamentos de defesa e militares.

Os ataques de ransomware, phishing e injeção de SQLi também costumaram atingir o setor de manufatura, de acordo com dados da X-Force.

Energia

O setor de energia é o nono mais visado do nosso ranking, recebendo 6% de todos os ataques e incidentes nos dez principais setores em 2019. A posição desse setor permanece inalterada em relação a 2018, quando também sofreu 6% dos ataques.

As empresas do setor de energia provam ser alvos ricos para ataques virtuais, em parte devido à sua importância como espinha dorsal da infraestrutura crítica de todos os países. A energia, em suas diversas formas, é fundamental para a economia, a segurança nacional e o funcionamento diário de cidades e indústrias.

Os objetivos dos ataques ao setor de energia são variados. Alguns ativos lucrativos das empresas de energia, como dados de clientes, material financeiro, segredos comerciais e informações de tecnologia proprietária, têm valor semelhante aos encontrados em empresas de outros setores.

O que diferencia o setor de energia dos outros é a possibilidade de interrupção e destruição física dos sistemas de ICS e dos sistemas de SCADA que os gerenciam. Esses sistemas podem ser alvos de grande valor para inimigos que desejam monitorar ou mesmo controlar operações dentro de uma instalação específica, especialmente quando se trata de situações de guerra virtual e que toca em instalações nucleares em países rivais, por exemplo. Esse setor também foi alvo de malware destrutivo, como o ZeroCleare.

Um ataque bem-sucedido a um sistema de ICS projetado para interromper as operações pode ter efeitos devastadores sobre os clientes que dependem de energia, gás, petróleo ou qualquer outro recurso proveniente do setor de energia. Exemplos desses ataques e seus efeitos prejudiciais foram observados no passado em uma série de incidentes direcionados a usinas de energia na Ucrânia, supostamente realizados pela Rússia e visando à destruição física.

Entre os grupos de ameaças notórios que têm como alvo esse setor estão:

- ITG01 (APT10)
- ITG09 (APT40)
- ITG07 (Chafer)
- ITG11 (APT29)
- ITG12 (Turla Group)
- ITG13 (APT34)
- ITG15 (Energetic Bear)
- ITG17 (Muddywater)
- Hive003 (APT35)
- HIVE0006 (APT27)
- Hive0016 (APT33)
- Hive0044 (APT15)
- Hive0045 (Goblin Panda)
- Hive0047 (Patchwork)
- Hive0076 (Tick)
- Hive0078 (Sea Turtle)
- Hive0081 (APT34)

Assistência médica

O décimo setor mais visado, o de assistência médica, recebeu 3% de todos os ataques nos dez principais setores, abaixo da oitava posição e 6% dos ataques em 2018.

preponderância de evidências sugere que os criminosos virtuais motivados financeiramente são os principais invasores de redes e dispositivos médicos do setor de assistência médica, com o objetivo de roubar e depois vender prontuários médicos na dark web ou criptografar dispositivos conectados à rede para interromper a atividade e dominar as empresas em troca de resgate.

A interrupção das redes de hospitais e casas de repouso conseguiu pressionar as organizações de saúde a pagar por ataques de ransomware, a fim de restaurar as operações mais rapidamente e proteger vidas humanas. Em alguns casos, o resgate é absurdo demais, como uma demanda de US$ 14 milhões que se seguiu ao ataque de Ryuk em 2019.

À medida que avançamos para 2020, o setor de assistência médica precisará continuar evoluindo sua postura de segurança para proteger os dados. Em vista dos frequentes ataques de ransomware, os hospitais devem fortalecer os recursos de resposta a incidentes e procurar novos ataques a dispositivos médicos inseguros que possam ser explorados para levar a um comprometimento fácil e à articulação por invasores motivados.

Grupos notórios de invasores que visaram esse setor incluíram grupos de crimes virtuais com motivação financeira, como os que operam o ransomware Ryuk. Embora os ataques de ransomware realcem a crise que poderia se desenvolver quando os hospitais fossem afetados, não estamos vendo um interesse persistente do estado-nação nesse setor.

Informações Geocêntricas

Os invasores tiveram como alvo todas as regiões em 2019, com os maiores níveis de atividade observados na América do Norte, na Ásia e na Europa.

Os pesquisadores da X-Force também encontraram atividade invasores visando o Oriente Médio e a América do Sul em 2019, sendo o primeiro constituído por mais ataques hacktivistas e de estado-nação, enquanto a América do Sul foi impactada principalmente por criminosos com motivação financeira.

Nesta seção, aprofundaremos os ataques nessas regiões geográficas para entender melhor a natureza dos alvos observados pela X-Force, os principais invasores focados em cada área e as principais datas a serem observadas em 2020 para possíveis aumentos na atividade de invasão. Algumas regiões destacam os invasores que foram particularmente ativos na segmentação da área nos últimos anos, mas essa lista não é exaustiva e inclui dados anteriores a 2019. Esta seção usa a nomenclatura do IBM Threat Group, conforme descrito acima, e dados da resposta global a incidentes da IBM, bem como dados de vazamentos divulgados publicamente.

América do Norte

A América do Norte ficou em primeiro lugar em todas as categorias de alvo dos invasores, constituindo 44% dos incidentes em 2019.

A América do Norte contém uma série de alvos em potencial e mantém uma quantidade significativa de infraestrutura da Internet, o que a torna um alvo maduro para os criminosos. Em 2019, a América do Norte teve mais de 5 bilhões de registros comprometidos.

A IBM respondeu a vários incidentes norte-americanos em 2019 que usavam malware comoditizado, códigos que podem ser comprados em mercados clandestinos ou obtidos gratuitamente. O malware de commodities pode ser difícil de atribuir, mas muito eficaz para alcançar objetivos ilícitos.

A atividade dos criminosos de estado-nação que visa a América do Norte permaneceu constante, mas nenhum incidente importante foi observado em 2019. As recentes negociações comerciais entre os Estados Unidos e a China podem levar ao aumento do direcionamento a organizações que fazem negócios nas duas regiões, e essas organizações deverão se manter vigilantes enquanto essas negociações permanecerem inconclusivas.

Próximos eventos com importância histórica em segurança virtual:

13 de julho
(Convenção Nacional do Partido Democrata, Estados Unidos)

24 de agosto
(Convenção Nacional do Partido Republicano, Estados Unidos)

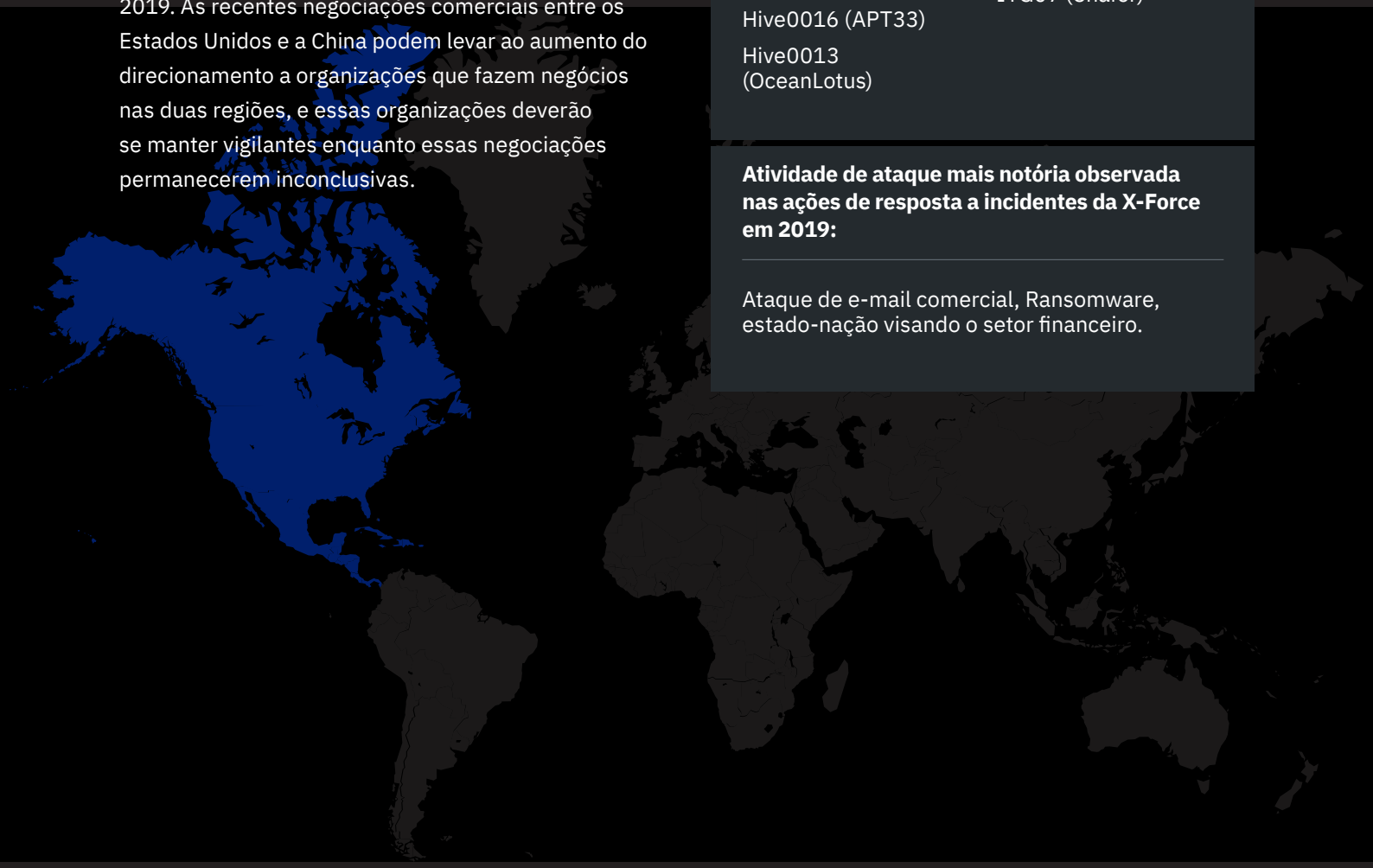
3 de novembro
(Eleição Presidencial dos EUA)

Entre os grupos de ameaças que tiveram como alvo essa região estão:

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

Atividade de ataque mais notória observada nas ações de resposta a incidentes da X-Force em 2019:

Ataque de e-mail comercial, Ransomware, estado-nação visando o setor financeiro.



Ásia

A Ásia recebeu a segunda maior classificação de risco na análise da X-Force, tendo a segunda maior contagem de incidentes em violações públicas e constituindo 22% dos incidentes em 2019. A Ásia teve mais de 2 bilhões de registros vazados em 2019, perdendo apenas para a América do Norte nesse ano.

Um número significativo de invasores concentrou-se em organizações afiliadas à Ásia, especialmente na península coreana, no Japão e na China. Muitos ataques observados nessa região seguiram os TTPs dos estados-nações. Um exemplo foi o ITG10, prováveis criminosos norte-coreanos que têm como alvo entidades sul-coreanas. Outro exemplo é o ITG01, prováveis atores chineses visando o Japão.

Eventos geopolíticos recentes na Ásia aumentaram a probabilidade de atividade afiliada ao estado-nação nessa região. Os protestos pela democracia em Hong Kong e a repressão subsequente colocaram a China no limite. O aumento das tensões entre a Coreia do Norte e seus vizinhos encorajou o regime. A anexação da região da Caxemira pela Índia também levou ao aumento das tensões na região.

Em 2020, o monitoramento dessas participações geopolíticas potencialmente voláteis é crucial para entender o risco representado pelas organizações que operam nessa região.

Próximos eventos com importância histórica em segurança virtual:

24 de julho
(Jogos Olímpicos de Tóquio 2020)

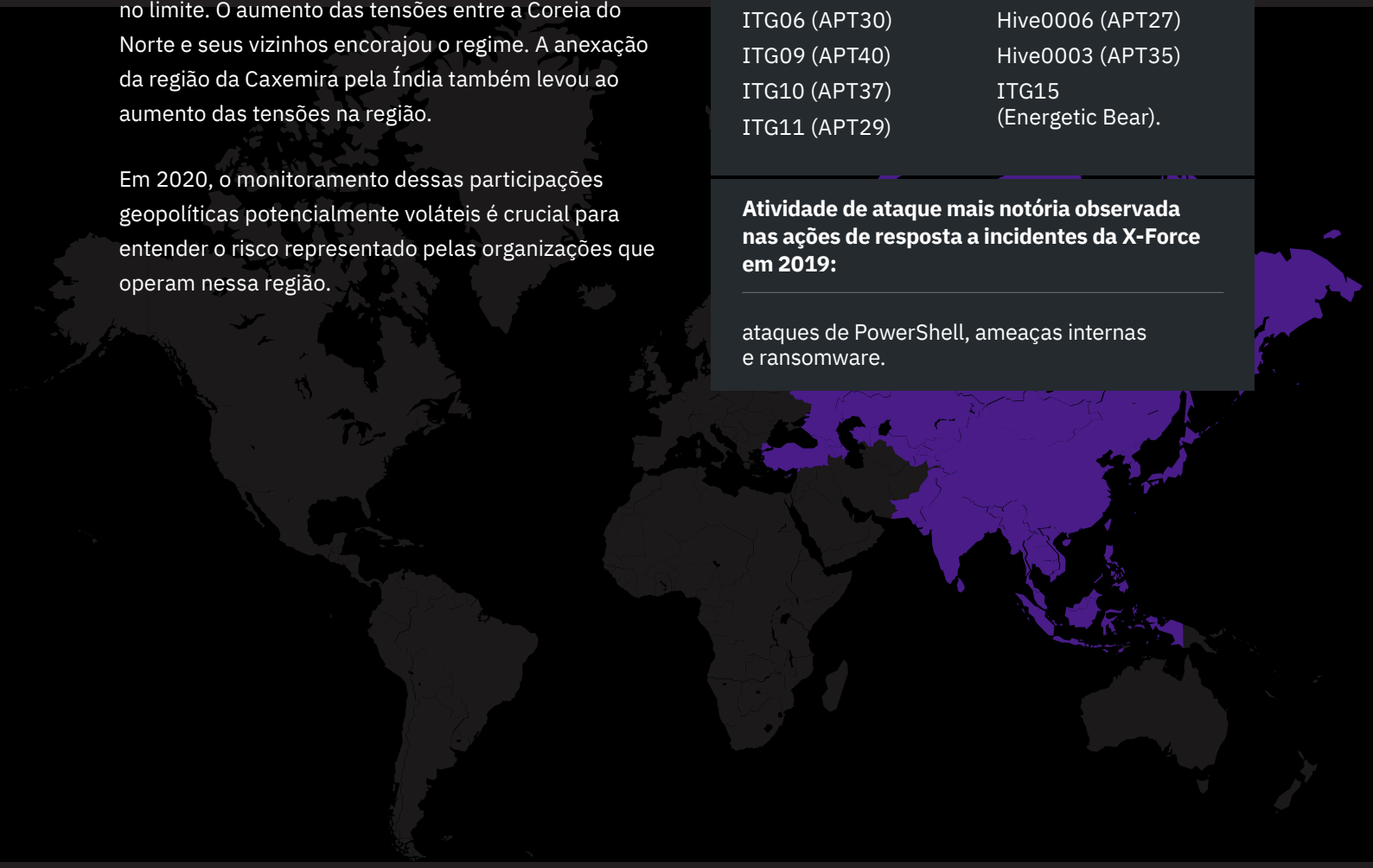
10 de outubro
(Independência de Taiwan).

Entre os grupos de ameaças que tiveram como alvo essa região estão:

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

Atividade de ataque mais notória observada nas ações de resposta a incidentes da X-Force em 2019:

ataques de PowerShell, ameaças internas e ransomware.



Europa

A Europa foi vítima de níveis semelhantes de atividades mal-intencionadas como a Ásia, chegando a 21% dos incidentes.

Ao contrário da Ásia, que é principalmente afetada pelos estados-nações rivais, a Europa parece ser alvo principalmente de invasores motivados financeiramente. Essa diferença pode ser explicada pelo maior potencial de roubo de empresas europeias com base nas taxas de câmbio. Como alternativa, motivações criminais poderiam estar em busca de propriedade intelectual, que pode ser vendida aos concorrentes por ganhos significativos.

A saída britânica da União Europeia (Brexit) pode ter reverberações nos círculos hacktivistas em 2020, mas nenhuma atividade foi observada em 2019. Além disso, as próximas eleições nos principais países da UE (Alemanha e França) podem ser potencialmente alvos de estados-nações que desejam influenciar a política nesses países.

Próximos eventos com importância histórica em segurança virtual:

31 de janeiro
(Reino Unido sai da União Europeia nos termos do Artigo 50)

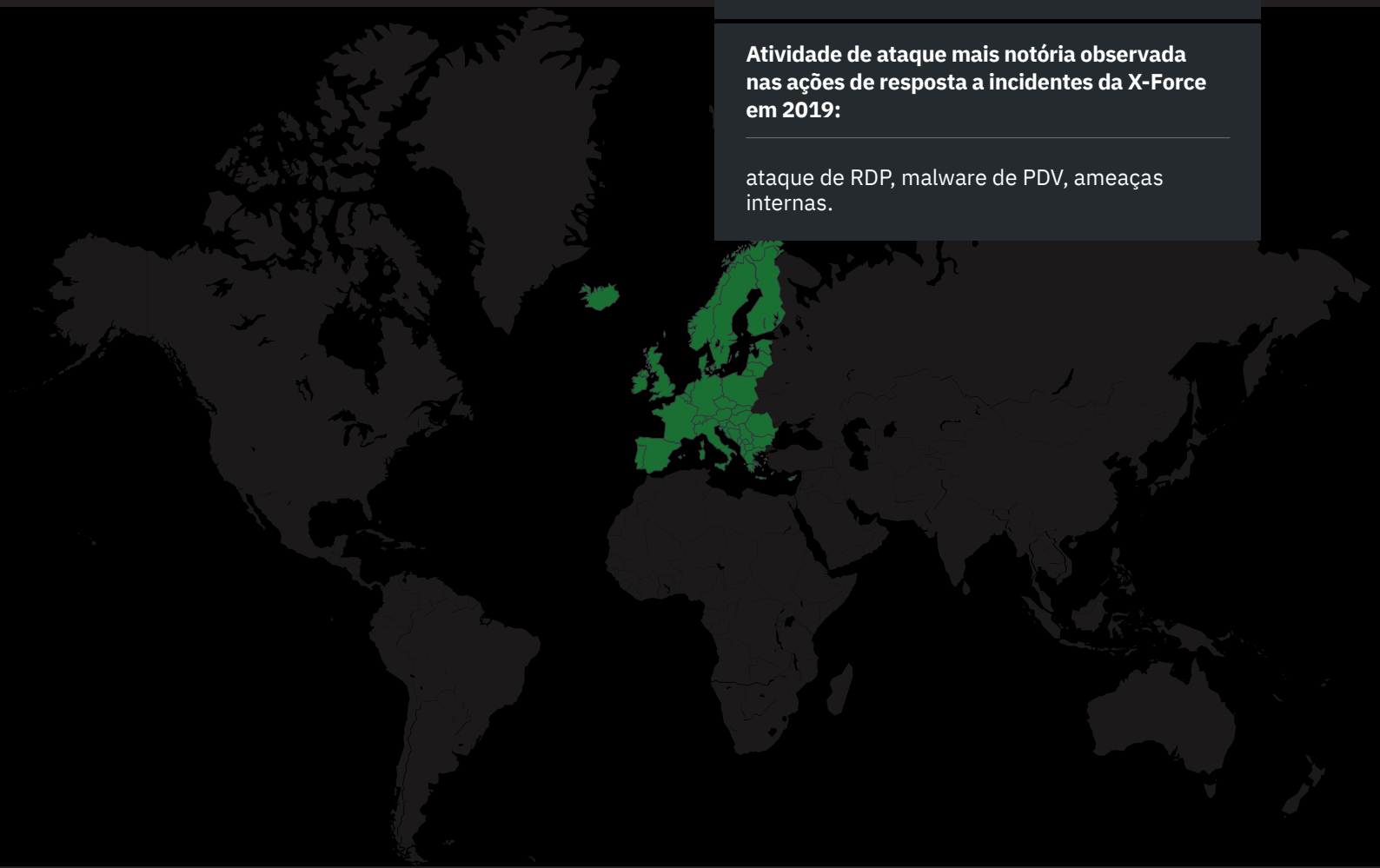
28 de junho
(Dia da Constituição da Ucrânia/aniversário de NotPetya).

Entre os grupos de ameaças que tiveram como alvo essa região estão:

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

Atividade de ataque mais notória observada nas ações de resposta a incidentes da X-Force em 2019:

ataque de RDP, malware de PDV, ameaças internas.



Oriente Médio

O X-Force IRIS observou vários incidentes afiliados a estados-nações que afetaram organizações no Oriente Médio em 2019, mas as métricas gerais para a atividade dos invasores foram relativamente baixas em 2019, com 7% dos incidentes nessa região.

Pode haver várias explicações para a atividade reduzida, como outras regiões geográficas que oferecem um maior retorno sobre o investimento em atividades de criminosos virtuais. No entanto, diferentemente de outras regiões, o Oriente Médio teve uma proporção maior de atividades hacktivistas e de estados-nações em comparação com outras partes do mundo.

A atividade hacktivista pode estar relacionada à agitação política na região em 2019, com vários incidentes importantes envolvendo o Irã. Da mesma forma, a atividade de estados-nações, como o ITG13, que busca os interesses do estado iraniano, seguiu os objetivos do estado ao visar organizações no setor de energia nessa região com ataques destrutivos.

A agitação política e a guerra cinética no Iêmen continuam a gerar o risco de atividades de ameaças virtuais, nas quais agentes de todos os lados do conflito estão usando ataques virtuais para espalhar sua mensagem e gerar receita. Esses riscos provavelmente continuarão em 2020, porque as diferentes partes continuam se ameaçando publicamente nesse conflito em andamento.

Próximos eventos com importância histórica em segurança virtual:

21 de novembro
(Torneio de futebol Copa do Mundo de Clubes 2022, Catar)

Entre os grupos de ameaças que tiveram como alvo essa região estão:

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

Atividade de ataque mais notória observada nas ações de resposta a incidentes da X-Force em 2019:

Malware destrutivo, ataque de DDoS, script da Web.

América do Sul

A América do Sul enfrentou uma atividade crimes virtuais significativa em 2019, mas não recebeu o mesmo nível de foco das três principais regiões, representando apenas 5% dos incidentes. No entanto, a atividade continua aumentando nessa região em relação ao ano anterior, com a X-Force observando um aumento nas atividades significativas de resposta a incidentes, especialmente nos setores de serviços financeiros e de varejo.

Os incidentes observados nessa região incluíram atividades de ransomware, que continuaram crescendo em popularidade ao longo de 2019.

Próximos eventos com importância histórica em segurança virtual:

12 de junho
(Torneio de futebol Copa América 2020, Colômbia e Argentina).

Entre os grupos de ameaças que tiveram como alvo essa região estão:

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

Atividade de ataque mais notória observada nas ações de resposta a incidentes da X-Force em 2019:

Ataque de e-mail comercial, Ransomware, estado-nação visando o setor financeiro.

Preparação para resiliência em 2020

Com base nas descobertas da IBM X-Force neste relatório, acompanhar a inteligência de ameaças e desenvolver sólidos recursos de resposta são formas impactantes de mitigar ameaças no cenário em evolução, independentemente de em qual setor ou país se opera.

Nossa equipe recomenda várias etapas que cada organização pode seguir para se preparar melhor para as ameaças virtuais em 2020:

- Aproveite a inteligência sobre ameaças para entender melhor as motivações e táticas dos invasores e priorizar os recursos de segurança.
- Crie e treine uma equipe de resposta a incidentes na sua organização. Se isso não for possível, envolva um recurso eficaz de resposta a incidentes para garantir uma resposta imediata a incidentes de alto impacto. Em 2019, a IBM Security observou que a contenção de impactos reduz significativamente os custos associados, com a pronta intervenção da nossa equipe em uma infecção pelo MegaCortex, interrompendo o ataque de ransomware no meio do caminho e impedindo milhares de dólares em danos.
- Faça o teste de estresse do plano de resposta a incidentes da sua organização para desenvolver memória muscular. Exercícios de mesa ou experiências de alcance virtual podem fornecer à sua equipe uma experiência crítica para melhorar o tempo de reação, reduzir o tempo de inatividade e, finalmente, economizar dinheiro em caso de vazamentos.
- A implementação da MFA (autenticação multifator) continua sendo uma das prioridades de segurança mais eficientes para as organizações. Em 2019, o roubo ou a reutilização de credenciais foi um dos métodos de ataque mais comumente usados pelos invasores, e a MFA pode inibir efetivamente esse ataque antes que ele ocorra.
- Verifique se a organização tem uma solução para detectar e bloquear domínios falsificados, como Quad9, devido à prevalência de phishing como vetor de ataque.
- Faça backups, teste backups e armazene backups off-line. Não apenas garantir a presença de backups, mas também sua eficácia por meio de testes no mundo real faz uma diferença crítica na garantia da segurança da organização.

Seguir em frente com as conclusões mais importantes

Em 2020, as organizações precisarão se preocupar com ameaças novas e antigas.

— A superfície de risco continuará crescendo em 2020, com mais de 150 mil vulnerabilidades atuais e novas relatadas regularmente.

— Com mais de quatro vezes os registros vazados em 2019 do que em 2018, o ano de 2020 pode ver outro grande número de registros perdidos devido a invasões e ataques.

— Os invasores continuam mudando os vetores de ataque, visando mais os dispositivos de IoT, a TO (Tecnologia Operacional) e os sistemas industriais e médicos conectados, para citar alguns.

— O uso de malware por invasores continua flutuando, com ransomware, cryptominers e botnets, todos assumindo a liderança em diferentes pontos em 2019. Esperamos que essa tendência continue em 2020, o que significa que as organizações precisarão se proteger contra ameaças variadas que mudam ao longo do tempo.

— Altos níveis de inovação de código para ransomware e cryptominers provavelmente implicam que essas ameaças continuarão evoluindo em 2020, exigindo melhores recursos de detecção e contenção.

— A atividade de spam continua inabalável, exigindo lista de bloqueio diligente, correção de vulnerabilidades e monitoramento de ameaças pelas organizações.

— A mudança ano após ano na segmentação específica do setor destaca o risco para todos eles e a necessidade de avanços e maturidade significativos nos programas de segurança virtual em geral.

— As organizações podem usar sua localização para ajudar a identificar os invasores mais prováveis e as motivações de ataque para estimar e mitigar alguns dos riscos relevantes que elas possam enfrentar.

Sobre a X-Force

A IBM X-Force estuda e monitora as últimas tendências de ameaças, aconselhando os clientes e o público em geral sobre ameaças emergentes e críticas e fornecendo conteúdo de segurança para ajudar a proteger os clientes IBM.

Desde infraestrutura, proteção de dados e aplicativos a serviços de segurança gerenciados e em nuvem, o IBM Security Services tem o conhecimento necessário para ajudar a proteger seus ativos críticos. A IBM Security protege algumas das redes mais sofisticadas do mundo e emprega algumas das melhores mentes dos negócios.

Saiba mais sobre a IBM Security →

Colaboradores

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

IBM Security
New Orchard Rd
Armonk, NY 10504
Produzido nos Estados Unidos da América
Fevereiro de 2020

Produzido nos Estados Unidos da América
Fevereiro de 2020

IBM **Security**