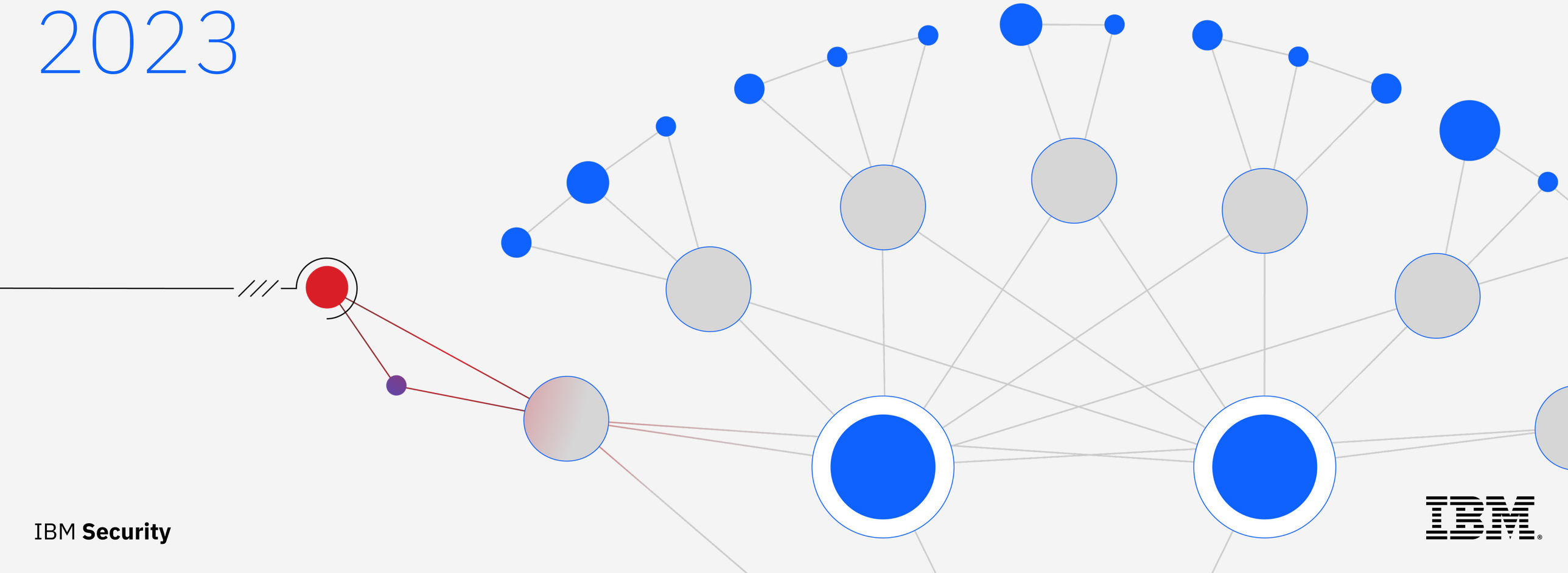
X-Force Threat Intelligence Index 2023

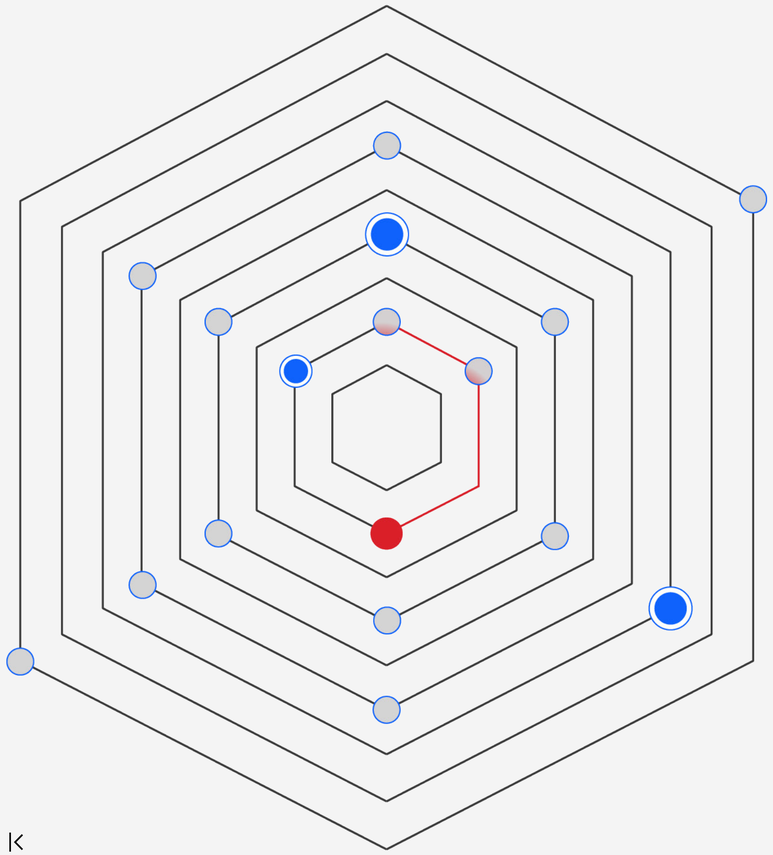


IBM **Security**

Índice

01

Resumo executivo



O ano de 2022 foi tumultuado na área de cibersegurança devido a vários eventos. Dentre os mais significativos, podemos destacar os efeitos da pandemia e o conflito militar na Ucrânia. A disrupção fez 2022 ser um ano de turbulência e custos econômicos, geopolíticos e humanos, criando exatamente o tipo de caos que propicia o crescimento do número de cibercriminosos.

E como esse número cresceu.

O IBM Security® X-Force® observou agentes de ameaça oportunistas que capitalizam com a desordem usando o cenário para se infiltrar em governos e empresas do mundo todo.

O IBM Security X-Force Threat Intelligence Index 2023 identifica tendências e padrões de ataque novos e existentes. Ele também inclui bilhões de pontos de dados, como dispositivos de terminal e rede, engajamentos de resposta a incidentes (RI), bancos de dados de exploração e vulnerabilidades e muito mais. Este relatório é uma coleção abrangente dos nossos dados de pesquisa de janeiro a dezembro de 2022.

Fornecemos essas descobertas como um recurso a clientes da IBM, pesquisadores de cibersegurança, criadores de políticas, profissionais da mídia e à grande comunidade de profissionais do setor de segurança e de líderes da indústria. A volatilidade do cenário atual, com ameaças cada vez mais sofisticadas e maliciosas, exige um esforço colaborativo para proteger empresas e cidadãos. Mais do que nunca, você precisa ter inteligência de ameaças e insights sobre segurança para prevenir ataques e proteger seus ativos críticos.

Para que você também possa crescer.

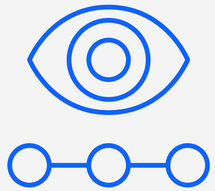
Como nossa análise de dados mudou em 2022

Em 2022, modificamos a forma como examinamos partes dos nossos dados. Com essas mudanças, podemos oferecer análises mais úteis e ficar mais alinhados com as estruturas padrão do setor. Assim, você tem mais dados para tomar decisões sobre segurança e pode reforçar a proteção da sua empresa contra ameaças.

Estas foram as mudanças na nossa análise em 2022:

- **Vetores de acesso inicial:** com a adoção da estrutura MITRE ATT&CK para rastrear vetores de acesso inicial, as descobertas das nossas pesquisas ficaram mais alinhadas com o setor de cibersegurança, e pudemos identificar tendências importantes em relação às técnicas.
- **Explorações e ataques de dia zero:** a extrapolação do nosso robusto banco de dados de vulnerabilidades, que inclui quase 30 anos de dados, ajuda a contextualizar nossas análises e identificar a ameaça criada pelas vulnerabilidades. Esse processo também contextualiza a proporção cada vez menor de explorações que podem ser usadas para atacar e de ataques de dia zero que causam impactos.
- **Métodos dos agentes de ameaça e seus impactos:** ao analisar as etapas de um ataque feito por agentes de ameaça e o seu impacto, conseguimos identificar os estágios críticos de um incidente. Esse processo identificou as áreas que podem precisar de suporte após um incidente.

Destaques do relatório



Principais ações sobre os objetivos: em quase um quarto de todos os incidentes remediados em 2022, a implementação de backdoors (21%) foi a principal ação sobre o objetivo. É importante observar que o aumento do uso do Emotet, um malware multifuncional, no início do ano contribuiu muito para um salto na ocorrência de backdoor na comparação anual. Apesar desse pico de ocorrência de backdoor, o ransomware, que ocupa a primeira posição no ranking desde pelo menos 2020, representou uma grande parcela dos incidentes (17%), reforçando que esse tipo de malware continua sendo uma ameaça.

A extorsão foi o impacto mais comum dos ataques nas empresas: com um percentual de 27%, esse foi o objetivo principal dos agentes de ameaça. As vítimas no setor de manufatura representaram 30% dos incidentes que resultaram em extorsão, porque os cibercriminosos continuaram a tendência de explorar um setor sob pressão.

O phishing foi o principal vetor de acesso inicial: identificado em 41% dos incidentes, o phishing continua sendo o principal vetor de infecção, seguido pela exploração de aplicações de uso público (26%). O número de infecções por macros maliciosas diminuiu, provavelmente porque a Microsoft decidiu bloquear macros por padrão. O uso de arquivos ISO e LNK como tática principal para enviar malware por meio de spam aumentou em 2022.

Aumento do hacktivismo e do malware destrutivo: a guerra da Rússia contra a Ucrânia possibilitou a demonstração de como o ambiente cibernético pode ser usado nas guerras modernas, o que era previsto por muitas pessoas na comunidade de cibersegurança.

Embora as piores previsões relacionadas ao ciberespaço não tenham se concretizado até a data desta publicação, houve um ressurgimento considerável do hacktivismo e dos malwares destrutivos. O X-Force também observou mudanças inéditas no mundo dos crimes cibernéticos devido ao aumento da cooperação entre os grupos de criminosos e à atuação de gangues que usam o Trickbot para atacar empresas ucranianas.

03

Principais estatísticas

27%

Percentual de ataques com extorsão

Os agentes de ameaça tentaram extorquir dinheiro das vítimas em mais de um quarto de todos os incidentes atendidos pelo X-Force em 2022. As táticas evoluíram na última década, e essa tendência deve continuar porque os agentes de ameaça estão buscando lucros de forma mais agressiva.

21%

Percentual de incidentes com implementação de backdoors

A implementação de backdoors foi a principal ação sobre o objetivo no ano passado, ocorrendo em mais de um a cada cinco incidentes informados no mundo todo. A intervenção dos recursos de proteção provavelmente impediu que os agentes de ameaça conseguissem alcançar outros objetivos, como o ransomware.

17%

Percentual de ataques de ransomware

Mesmo durante um ano caótico para alguns dos sindicatos de ransomware mais prolíficos, o ransomware foi a segunda ação sobre o objetivo mais comum, seguido pelas implementações de backdoor, e continua causando interrupções nas empresas. O percentual de ataques de ransomware caiu de 21% em 2021 para 17% em 2022.

41%

Percentual de incidentes envolvendo phishing para acesso inicial
As operações de phishing continuaram sendo a principal via de comprometimento em 2022. Dos incidentes remediados pelo X-Force, 41% usaram essa técnica para obter acesso inicial.

100%

Aumento no número de tentativas de interceptação de encadeamento por mês
Em comparação com os dados de 2021, o número de tentativas de interceptação de encadeamento por mês dobrou em 2022. Os e-mails de spam com Emotet, Qakbot e IcedID usaram muito a tática de interceptação de encadeamento.

52%

Diminuição dos kits de phishing que roubam dados de cartão de crédito
O objetivo de quase todos os kits de phishing analisados nos dados era coletar nomes (98%) e endereços de e-mail (73%), endereços residenciais (66%) e senhas (58%). As informações de cartões de crédito (o alvo em 61% dos ataques em 2021) deixaram de ser a opção preferencial dos agentes de ameaça. Dados mostram que apenas 29% dos kits de phishing tiveram essas informações como alvo em 2022, uma queda de 52%.

62%

Percentual de ataques de phishing que usam anexos de spear phishing
Os invasores preferiram atacar com anexos, que eram implementados por eles mesmos ou em combinação com links ou spear phishing via serviço.

26%

Percentual de vulnerabilidades de 2022 com explorações conhecidas
Em 2022, 26% das vulnerabilidades tiveram explorações conhecidas. De acordo com dados que o X-Force rastreia desde o início da década de 1990, essa proporção tem caído nos últimos anos, demonstrando o benefício da boa manutenção de um processo de gerenciamento de correções.

31%

Percentual de ataques globais na região Ásia-Pacífico
A região Ásia-Pacífico continuou sendo a mais atacada em 2022, concentrando 31% de todos os incidentes. Essa estatística representa um aumento de cinco pontos no percentual total de ataques atendidos pelo X-Force na região em 2021.

Principais vetores de acesso inicial

Em 2022, o X-Force substituiu o rastreamento de vetores de acesso inicial com categorias mais amplas, como phishing e credenciais roubadas, pelas técnicas de acesso inicial listadas na estrutura MITRE ATT&CK Matrix for Enterprise. Com essa mudança, o X-Force pode rastrear tendências importantes de forma mais detalhada e identificar as técnicas. Ele também gera dados mais fáceis de usar e comparar e está alinhado a esforços de padronização mais amplos do setor.

Principais vetores de acesso inicial em 2022

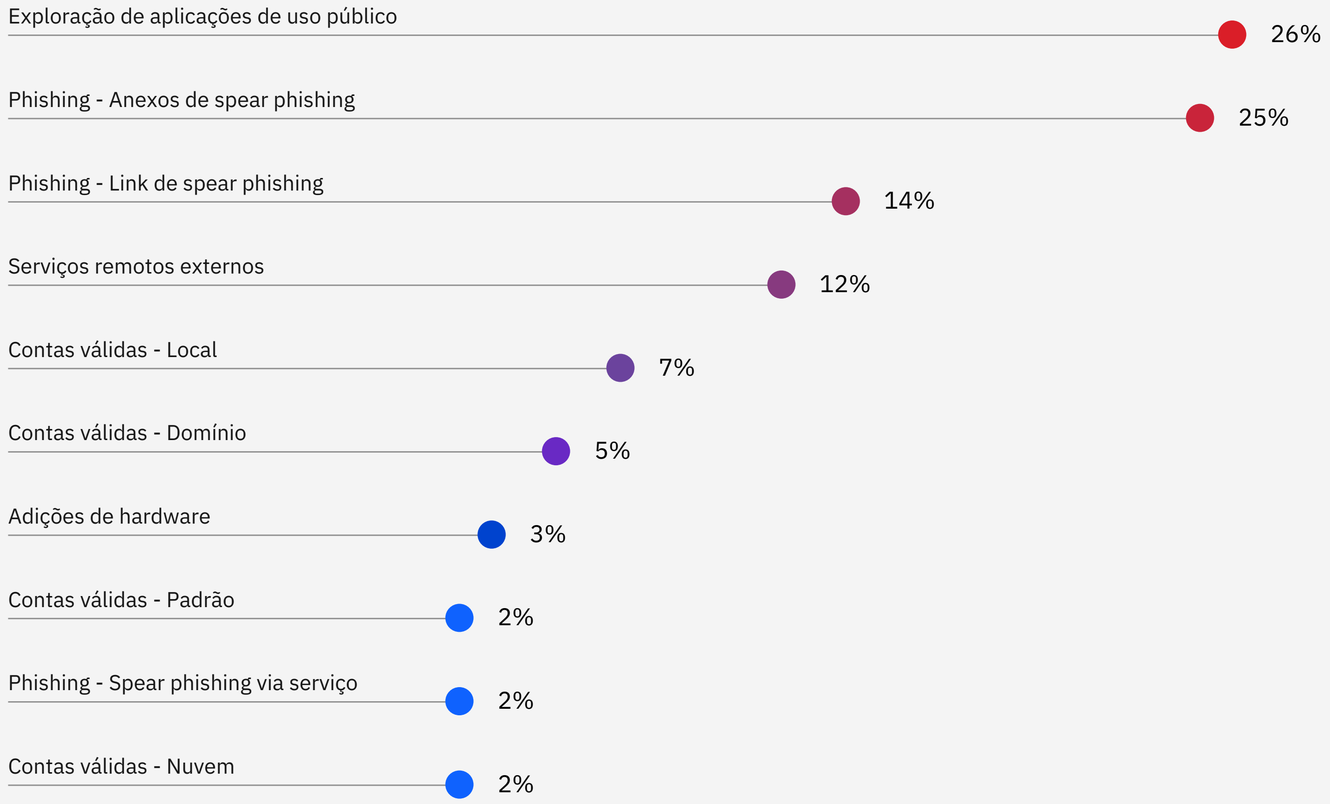


Figura 1: principais vetores de acesso inicial observados pelo X-Force em 2022. Fonte: X-Force

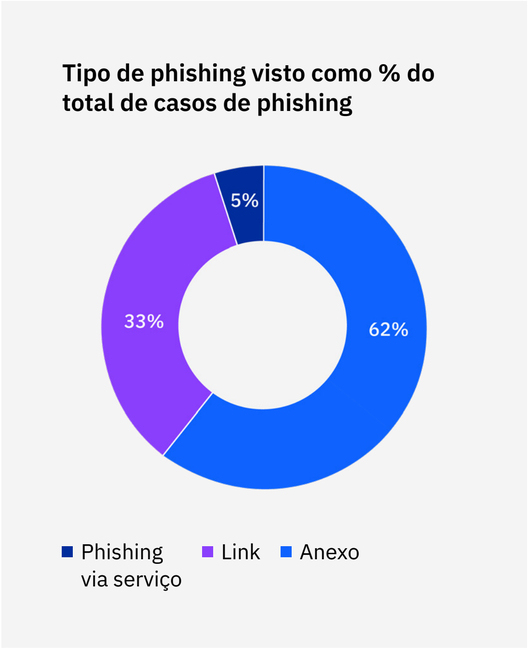


Figura 2: tipos de subtécnica de phishing como percentual do total de casos de phishing observados pelo X-Force em 2022. Fonte: X-Force

Phishing

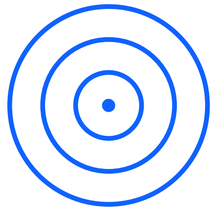
O phishing (T1566), seja por anexo, link ou como serviço, continua sendo o principal vetor de infecção e representou 41% de todos os incidentes remediados pelo X-Force em 2022. Esse percentual, que aumentou em relação aos 33% de 2020, se manteve estável em comparação com 2021. Se analisarmos todos os incidentes com phishing, os anexos de spear phishing (T1566.001) foram usados em 62% desses ataques, os links de spear phishing (T1566.002) em 33% e o spear phishing como serviço (T1566.003) em 5%.
O X-Force também observou que os agentes de ameaça usam anexos com phishing como serviço ou links em alguns casos.

Os dados do IBM X-Force Red de 2022 destacam ainda mais a importância do phishing e do gerenciamento incorreto de credenciais para os agentes de ameaça. Nos testes de penetração para clientes de 2022, o X-Force Red descobriu que aproximadamente 54% dos testes revelaram autenticação ou gerenciamento inadequado de credenciais. A equipe do X-Force Red Adversary Simulation fez spear phishing regularmente com códigos QR em tokens de autenticação de diversos fatores (MFA). Muitas empresas não tinham visibilidade das aplicações e dos endpoints expostos em portais de gerenciamento de acesso à identidade e conexão única (SSO), como o Okta.

Em segundo lugar, a exploração de aplicações de uso público (T1190), definida como invasores que se aproveitam de um ponto fraco em um computador ou programa para a internet, foi identificada em 26% dos incidentes atendidos pelo X-Force. Isso pode ser correlacionado com o que relatórios Threat Intelligence Index anteriores chamaram de “exploração de vulnerabilidade” e representa uma queda em relação aos 34% de 2021.

Em terceiro lugar, a violação de contas válidas (T1078) foi identificada em 16% dos incidentes observados. Nesses casos, adversários obtiveram e violaram credenciais de contas como meio de acesso. Esses incidentes incluíram contas na nuvem (T1078.004) e contas padrão (T1078.001) (2% cada), contas no domínio (T1078.002) (5%) e contas locais (T1078.003) (7%).

A coleta de informações de cartão de crédito pelos kits de phishing caiu consideravelmente, de 61% em 2021 para 29% em 2022.



Os kits de phishing estão durando mais tempo e priorizando PII em vez de dados de cartão de crédito

A IBM Security analisou milhares de kits de phishing do mundo todo pelo segundo ano consecutivo e descobriu que as implementações de kits estão funcionando por mais tempo e alcançando um número maior de usuários. Os dados indicam que a vida útil dos kits de phishing observada mais do que dobrou na comparação anual, e a implementação média no conjunto de dados permaneceu relativamente baixa, em 3,7 dias.

No geral, a implementação mais curta durou minutos e a mais longa, descoberta em 2022, funcionou por mais de três anos. Estes são os resultados da nossa investigação:

- Um terço dos kits implementados durou aproximadamente 2,3 dias no ano passado, mais do que o dobro da duração do ano anterior, quando a mesma proporção durou no máximo um dia.
- Aproximadamente metade de todos os kits informados impactou 93 usuários. Em 2021, cada implementação teve, em média, no máximo 75 vítimas em potencial.
- O total máximo informado de vítimas de um ataque de phishing foi pouco mais de 4.000, embora esse tenha sido um caso atípico.
- O objetivo de quase todos os kits de phishing analisados era coletar nomes (98%). Os outros objetivos observados foram a coleta de endereços de e-mail (73%), endereços residenciais (66%) e senhas (58%).
- A coleta de informações de cartão de crédito pelos kits de phishing caiu consideravelmente, de 61% em 2021 para 29% em 2022.
- Instâncias inferiores de kits de phishing com o objetivo de acessar dados de cartão de crédito indicam que os criadores de phishing estão priorizando informações pessoais identificáveis (PII), que oferecem opções mais variadas e nocivas. As PII podem ser coletadas e vendidas na dark web ou em outros fóruns ou usadas para realizar outras operações contra os alvos.

Principais marcas alvo de spoofing

As principais marcas que foram alvo de spoofing observadas incluem principalmente grandes nomes do setor de tecnologia. O X-Force acredita que essa mudança, em comparação com a lista mais diversificada de 2021, ocorreu devido à melhoria na capacidade de identificar as marcas que são alvo da configuração de spoofing de um kit, e não apenas a marca que ele ataca por padrão. Muitos kits de phishing são multifuncionais, e a marca que é alvo de spoofing pode ser mudada com a alteração de um parâmetro simples. Por exemplo, um kit pode fazer o spoofing do Gmail por padrão, mas uma atualização em uma linha pode transformá-lo em um ataque de spoofing à Microsoft.

As credenciais roubadas desses serviços são valiosas. O acesso a contas que as vítimas usam para gerenciar grande parte da presença on-line pode abrir a porta para o acesso a outras contas. O foco dos invasores nessa forma de acesso inicial é destacado no Cloud Threat Landscape Report de 2022. Esse relatório identificou que o número de contas vendidas na dark web triplicou (aumento de 200%) em comparação com 2021.

Comparação anual das principais marcas alvo de spoofing

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office 365	Hotmail

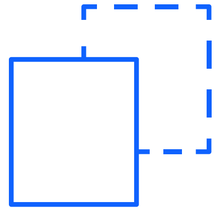
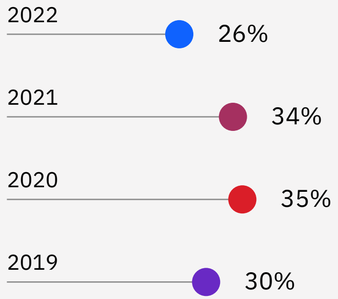


Figura 3: este gráfico identifica as principais marcas alvo de spoofing em 2021 e 2022 e demonstra que os agentes de ameaça estão priorizando, cada vez mais, grandes marcas de tecnologia. Fonte: dados sobre kits de phishing da IBM

Percentual de incidentes causados por exploração de vulnerabilidade nos últimos quatro anos



Vulnerabilidades

A exploração de vulnerabilidades, definida no relatório de 2022 como a exploração de aplicações de uso público (T1190), ficou em segundo lugar entre os principais vetores de infecção e tem sido o método preferencial dos invasores desde 2019. As vulnerabilidades foram exploradas em 26% dos ataques que o X-Force remediou em 2022, 34% em 2021, 35% em 2020 e 30% em 2019.

Nem toda vulnerabilidade explorada por agentes de ameaça resulta em um incidente de cibersegurança. O número de incidentes causados pela exploração de vulnerabilidades em 2022 diminuiu 19% em comparação com 2021, após aumentar 34% em comparação com 2020. O X-Force avaliou que essa mudança foi causada pela disseminação da vulnerabilidade Log4J no fim de 2021.

A exploração para acesso é uma área de pesquisa estratégica para a equipe do X-Force Red Adversary Simulation Services continuar simulando ameaças avançadas. A equipe aumentou o foco na pesquisa de vulnerabilidades para a exploração de sistemas operacionais (SO) e aplicações para ampliar o acesso e fazer a escalada de privilégios. Essa mudança de foco foi motivada por exercícios com clientes antigos que reforçaram a proteção de caminhos de ataque ao Active Directory tradicionais e pela necessidade de buscar novos caminhos de ataque.

Embora as vulnerabilidades sejam um vetor de acesso inicial comum, e o setor responda a várias ocorrências graves todos os anos, nem toda vulnerabilidade é igual. É importante que os tomadores de decisões façam uma análise abrangente do cenário de vulnerabilidades e garantam que têm o contexto necessário para entender a verdadeira ameaça que uma vulnerabilidade cria nas redes.

Há quase 30 anos e antes da criação do sistema Common Vulnerabilities and Exposures (CVE), o X-Force começou a criar um banco de dados de vulnerabilidades robusto. Agora esse banco de dados é um dos mais completos do setor de cibersegurança. Embora as vulnerabilidades representem um risco grande para a segurança, existem muito mais vulnerabilidades informadas do que explorações de ataque conhecidas. Além disso, apesar da atenção dada aos ataques de dia zero, o verdadeiro número desses ataques é menor do que o total de vulnerabilidades conhecidas.

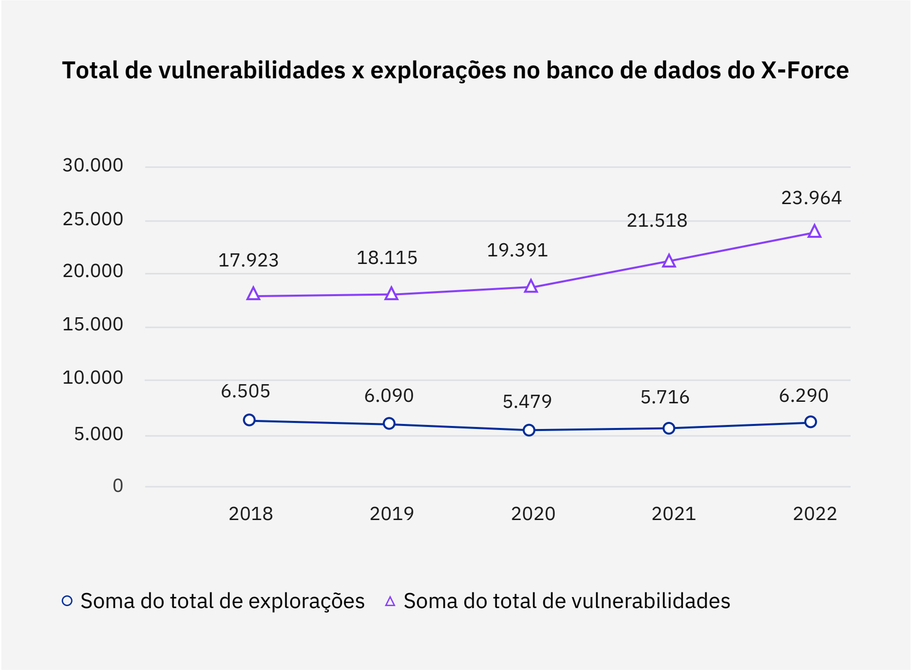


Figura 4: visualização do banco de dados de vulnerabilidades do X-Force que mostra vulnerabilidades e explorações nos últimos cinco anos.
Fonte: X-Force

Todos os anos, temos um novo número recorde de vulnerabilidades descobertas. O número total de vulnerabilidades rastreadas em 2022 foi de 23.964 em comparação com 21.518 em 2021. Essa tendência de crescimento ano após ano tem sido observada na última década. Para a satisfação dos profissionais de segurança cibernética, a análise do nosso banco de dados de vulnerabilidades mostra que a proporção de explorações conhecidas e viáveis em relação às vulnerabilidades informadas diminuiu recentemente: 36% em 2018, 34% em 2019, 28% em 2020, 27% em 2021 e 26% em 2022.

Esses números podem mudar com a exposição de ataques de dia zero e explorações desenvolvidas para vulnerabilidades mais antigas (às vezes anos após a identificação), e existem várias possíveis explicações para essa queda.

Em primeiro lugar, a criação de programas formais de identificação de bugs incentivou a descoberta proativa de vulnerabilidades nas aplicações. Além disso, diversas vulnerabilidades muito populares e conhecidas já são usadas pelos agentes de ameaça para explorar sistemas, reduzindo a necessidade de desenvolver novas explorações. Provavelmente a queda ocorreu devido a uma combinação de vários fatores, mas isso não indica que a exploração de vulnerabilidades seja uma ameaça menos grave.

Apesar da queda na proporção das explorações a vulnerabilidades, a gravidade dessas explorações que o X-Force rastreia aumentou nos últimos cinco anos. Em 2018, 58% das vulnerabilidades tiveram uma pontuação de gravidade “média” no Common Vulnerability Scoring System (CVSS),

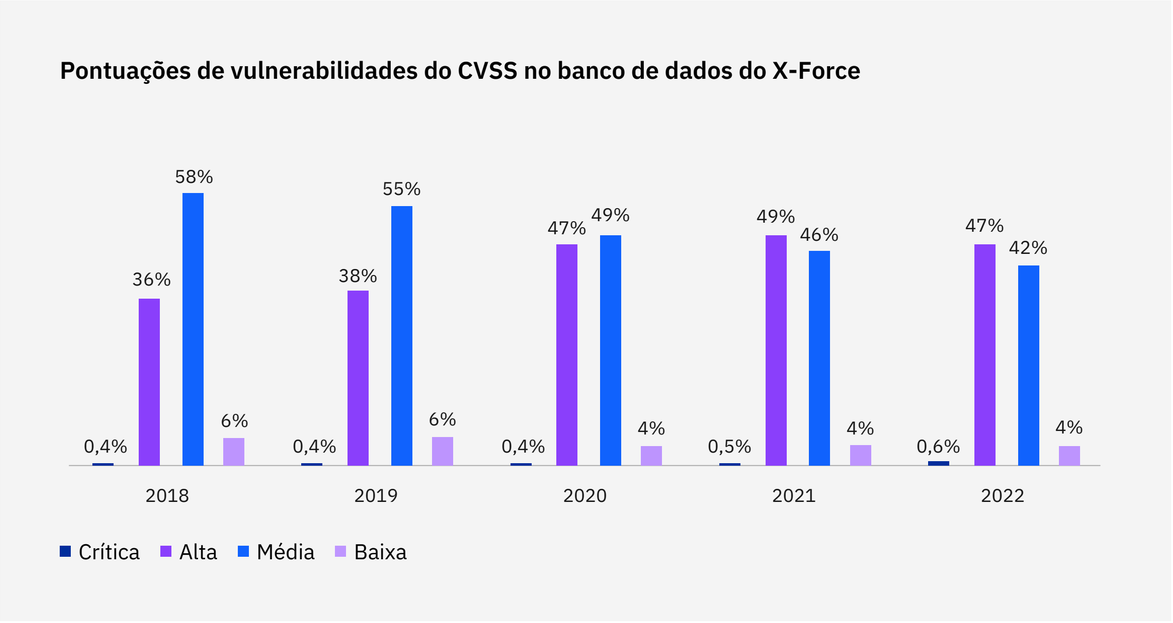


Figura 5: banco de dados do X-Force mostrando a gravidade das vulnerabilidades rastreadas no nosso sistema.
Fonte: X-Force

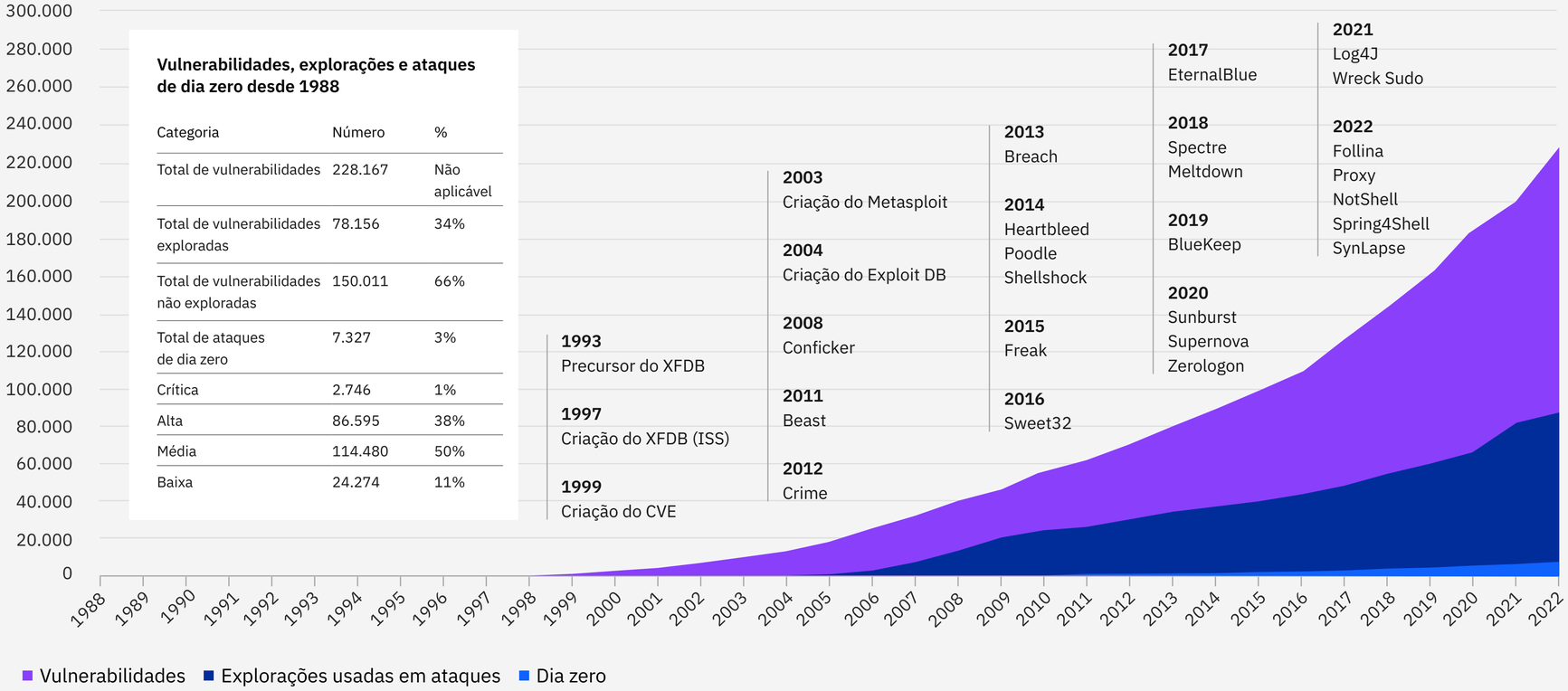
4,0 a 6,9 de 10, em comparação com pouco menos de 36% das vulnerabilidades com gravidade “alta”, de 7,0 a 9,9. A diferença entre essas duas pontuações se inverteu em 2021, e agora o número de vulnerabilidades de gravidade “alta” é 5% maior do que o número de vulnerabilidades com gravidade “média”.

Mesmo assim, de todas as vulnerabilidades que o X-Force rastreou desde 1988, 38% foram classificadas com gravidade “alta”, e apenas 1% das vulnerabilidades foi classificado como de gravidade “crítica”, com a pontuação 10. Metade das vulnerabilidades rastreadas foi classificada como de gravidade “média”, e as outras 11% foram classificadas como de gravidade “baixa” (3,9 ou menos). Essas pontuações sozinhas não podem ser correlacionadas com a gravidade real de um CVE porque não mostram como a exploração é feita ou se uma exploração existe. No entanto, as pontuações ajudam as equipes de suporte a comparar as vulnerabilidades e priorizar as mais urgentes. O gráfico da Figura 6 na próxima página ajuda a entender a verdadeira natureza do problema de vulnerabilidade da indústria de cibersegurança.

Vulnerabilidades da tecnologia operacional (TO)

As vulnerabilidades dos sistemas de controle industriais (ICS) descobertas em 2022 diminuíram pela primeira vez em dois anos (457 em comparação com 715 em 2021 e 472 em 2020). A explicação para essa queda pode ser encontrada nos ciclos de vida do ICS e em como ele costuma ser gerenciado e corrigido. Os invasores sabem que com a demanda por tempo de inatividade mínimo, equipamentos com ciclo de vida mais longo e softwares mais antigos e com menos suporte, muitos componentes de ICS e de redes de TO ainda têm vulnerabilidades antigas. Geralmente, a infraestrutura é usada por muito mais tempo do que as estações de trabalho padrão de um escritório. Isso faz as vulnerabilidades do ICS terem uma vida útil mais longa em comparação com as vulnerabilidades que podem explorar a TI.

O problema da vulnerabilidade



Vulnerabilidades, explorações e ataques de dia zero desde 1988

Categoria	Número	%
Total de vulnerabilidades	228.167	Não aplicável
Total de vulnerabilidades exploradas	78.156	34%
Total de vulnerabilidades não exploradas	150.011	66%
Total de ataques de dia zero	7.327	3%
Crítica	2.746	1%
Alta	86.595	38%
Média	114.480	50%
Baixa	24.274	11%

Figura 6: gráfico mostrando o crescimento das vulnerabilidades, das explorações e dos ataques de dia zero desde 1988. Também inclui uma linha do tempo com os principais eventos envolvendo vulnerabilidades desde 1993. “XFDB” é o banco de dados do X-Force, e “Exploit DB” é o banco de dados de explorações. Fonte: X-Force

Principais ações sobre os objetivos

Anteriormente, o X-Force Threat Intelligence Index analisava os principais ataques com base em uma categoria mais ampla. Em 2022, o X-Force dividiu essa classificação em duas categorias: as ações específicas dos agentes de ameaça nas redes das vítimas, ou ação de adversário sobre o objetivo, e o efeito pretendido ou percebido dessa ação na vítima, ou impacto.

De acordo com os dados do X-Force Incident Response, a implementação de backdoors foi a ação sobre o objetivo mais comum e ocorreu em 21% de todos os incidentes informados. Essa ação foi seguida pelo ransomware (17%) e pelo comprometimento de e-mail corporativo (6%). Documentos maliciosos (maldocs), campanhas de spam, ferramentas de acesso remoto e acesso ao servidor foram descobertos em 5% dos casos (cada item).

Principais ações sobre os objetivos em 2022

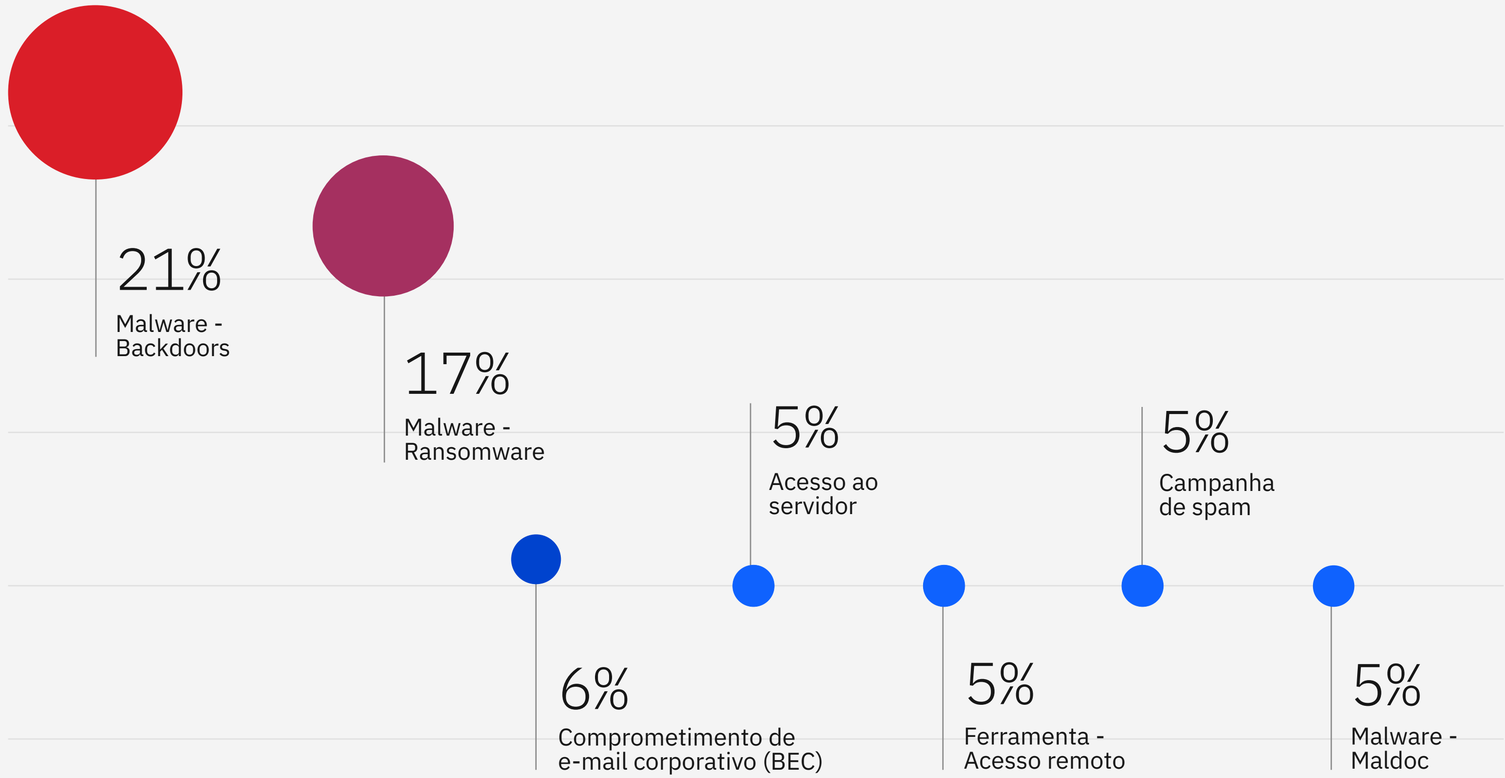


Figura 7: principais ações sobre os objetivos observadas pelo X-Force em 2022. Fonte: X-Force

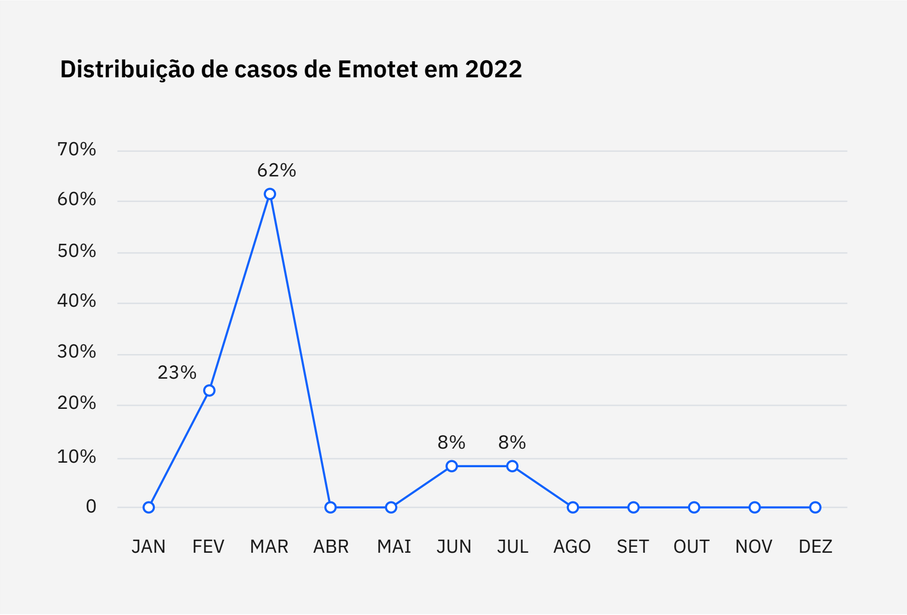


Figura 8: gráfico que mostra pico nos casos de Emotet no início de 2022. Fonte: X-Force

Nos casos em que uma implementação de backdoor foi classificada como uma ação sobre o objetivo, é provável que o agente de ameaça tivesse planos adicionais quando o backdoor foi operacionalizado. A intervenção bem-sucedida das equipes de segurança ou dos profissionais que resolvem incidentes provavelmente impediu que o agente de ameaça atingisse outros objetivos. Essa atividade maliciosa provavelmente incluiria ransomware, porque cerca de dois terços desses casos de backdoor tinham características de um ataque de ransomware.

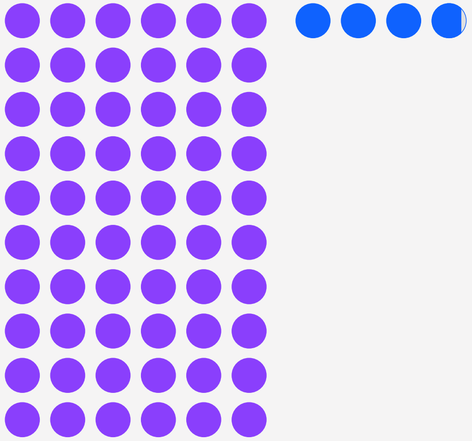
O aumento das implementações de backdoor também pode ser explicado pela quantidade de dinheiro que esse tipo de acesso pode gerar na dark web. O acesso a redes corporativas comprometidas por um invasor com acesso inicial geralmente é vendido por muitos milhares de dólares americanos. Esse tipo de acesso pode ser o objetivo de pessoas maliciosas que querem ter lucro rápido evitando problemas relacionados à manutenção do acesso e usando movimento lateral e exfiltração de dados de alto valor. Essas pessoas maliciosas que não têm acesso ao malware necessário para acessar a rede também podem recorrer aos backdoors.

Os invasores com acesso inicial geralmente tentam leiloar o acesso. Os valores observados pelo X-Force variam de USD 5.000 a USD 10.000, mas os preços finais podem ser inferiores. Outras pessoas informaram que o acesso pode custar de USD 2.000 a USD 4.000, sendo que um acesso foi vendido por USD 50.000. Esses valores podem ser comparadores ao preço muito menor de itens como um único cartão de crédito, que já foi visto sendo oferecido por menos de USD 10.

Os backdoors resultaram em um pico considerável nos casos de Emotet em fevereiro e março. Esse pico alterou muito o ranking de casos de backdoor. Os casos implementados nesse período representam 47% de todos os backdoors identificados no mundo todo em 2022. Após um hiato nos casos de Emotet de julho a novembro, seguido por um aumento nos casos durante quase duas semanas com um volume muito menor, o número de ocorrências de backdoor caiu consideravelmente.

Duração média do ataque de ransomware

2019	2021
Mais de 2 meses	Mais de 3 dias



Ransomware

Mesmo durante um ano caótico para alguns dos sindicatos de ransomware mais prolíficos, o ransomware foi a segunda ação sobre o objetivo mais comum, seguido pelas implementações de backdoor, e continua causando interrupções nas empresas. O percentual de ataques de ransomware caiu de 21% em 2021 para 17% em 2022.

Um estudo do IBM Security X-Force revelou uma redução de 94,34% na duração média dos ataques de ransomware de 2019 para 2021 (de mais de dois meses para pouco menos de quatro dias). Apesar disso, o ransomware é um perigo claro e presente que mostra sinais de expansão, e não de desaceleração.

Uma técnica particularmente prejudicial usada pelos operadores de ransomware para distribuir a carga útil em uma rede é comprometer os controladores de domínio. Um percentual pequeno (aproximadamente 4%) das descobertas dos testes de penetração de rede do X-Force Red revelou entidades com erros de configuração no Active Directory que poderiam resultar na escalada de privilégios ou no controle total do domínio. Em 2022, o X-Force também observou ataques de ransomware mais agressivos em infraestruturas subjacentes, como ESXi e Hyper-V. O possível alto impacto desses métodos de ataque reforça a importância de proteger os controladores de domínio e os hipervisores corretamente.

Variantes de ransomware

Como os grupos de ransomware e os invasores relacionados estão sempre mudando, o X-Force identificou uma rotatividade regular nos principais grupos ativos nesse espaço. O X-Force encontrou 19 variantes de ransomware em 2022, em comparação com as 16 de 2021. As variantes do LockBit representaram 17% do total de incidentes de ransomware observados, em comparação com os 7% de 2021. O Phobos ficou empatado com o WannaCry em segundo lugar (11%). Os principais grupos em 2022 tomaram o lugar do primeiro colocado de 2021, o REvil, também conhecido como Sodinokibi, que representou 37% dos casos em 2021, e do segundo colocado, o Ryuk, que representou 13% dos casos. O percentual dessas duas variantes caiu para 3%.

O LockBit 3.0 é a variante mais recente da família de ransomware LockBit, que faz parte de uma operação de ransomware como serviço (RaaS) associada ao LockerGoga e ao MegaCortex. O LockBit está em operação desde setembro de 2019, e o LockBit 3.0 foi lançado em 2022. Uma parte considerável do código-fonte do LockBit 3.0 parece ter sido aproveitada do ransomware BlackMatter.

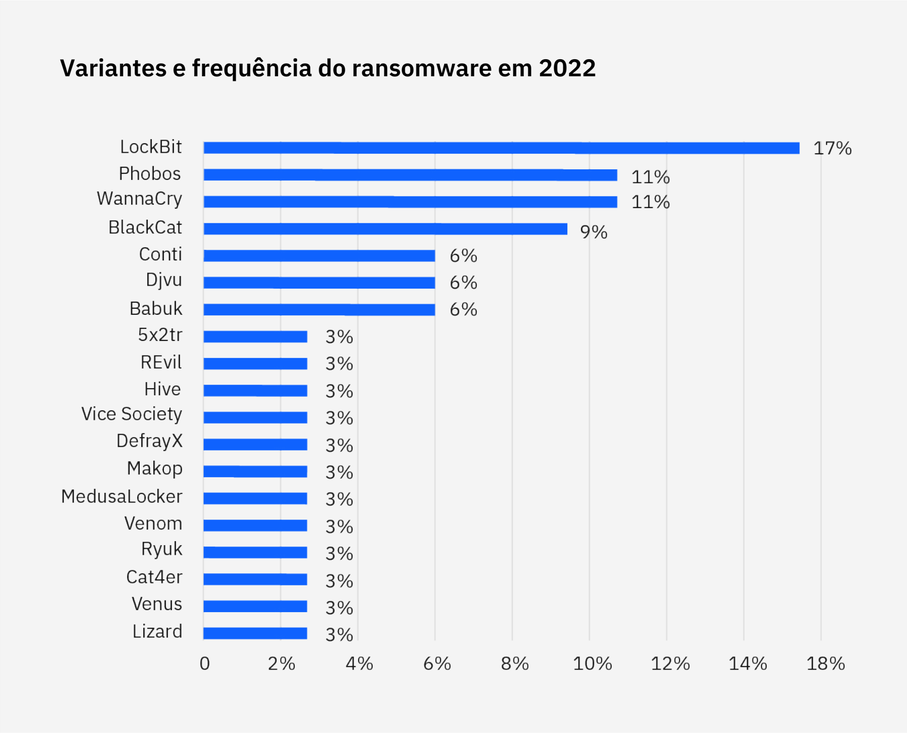


Figura 9: variantes de ransomware e a frequência de observação nas respostas a incidentes do X-Force em 2022. Fonte: X-Force

Os pesquisadores descobriram o ransomware Phobos no início de 2019. Com base em similaridades no código, nos mecanismos de entrega, nas técnicas de exploração e nas notas de resgate, o Phobos foi identificado como uma variante das conhecidas famílias de ransomware Crysis e Dharma. O Phobos tem sido muito usado em ataques de escala menor, que envolvem pedidos de resgate de valor mais baixo. As campanhas de phishing por e-mail e a exploração de portas do Remote Desktop Protocol (RDP) vulneráveis são os principais métodos de distribuição do Phobos.

O WannaCry, identificado pela primeira vez em 2017, se espalha usando o EternalBlue para explorar a vulnerabilidade no servidor Microsoft Server Message Block 1.0 (SMBv1) (MS17-010). Vários casos de WannaCry ou Ryuk identificados pelo X-Force em 2022 foram causados por infecções de três a cinco anos atrás em equipamentos antigos e sem correções, o que destaca a importância de uma limpeza adequada após esses eventos.

Comprometimento de e-mail corporativo (BEC)

O BEC manteve a terceira colocação em 2022, representando 6% dos incidentes atendidos pelo X-Force. Essa colocação é um pouco inferior em comparação com 8% dos ataques em 2021 e 9% da quinta colocação em 2020. Esse ataque ficou na frente dos ataques de acesso ao servidor, que ficaram na segunda colocação em 2021. Esse tipo de ataque ocorre quando o invasor acessa um servidor com um objetivo desconhecido. Em 2022, isso foi classificado de forma mais detalhada com base no tipo de acesso obtido. Os links de spear phishing foram usados em metade dos casos de BEC atendidos pelo X-Force. Anexos maliciosos e violação de contas válidas foram as táticas usadas para viabilizar as tentativas de BEC em 25% dos casos (cada item).

06

Principais impactos

O X-Force também fez uma análise detalhada dos incidentes atendidos para identificar seus efeitos nas empresas e entender melhor o impacto que os agentes de ameaça queriam causar. Com essas informações, as empresas podem entender melhor os impactos mais comuns para planejar as respostas a possíveis incidentes com mais eficiência.

A análise descobriu que mais de um em cada quatro incidentes tinha o objetivo de extorquir as empresas. Esse foi o principal impacto observado nos incidentes remediados pelo X-Force. As técnicas mais usadas nos casos de extorsão foram ransomware ou BEC. Em muitos casos, a extorsão incluiu o uso de ferramentas de acesso remoto, mineração de criptomoedas, backdoors, assistentes de download e web shells.

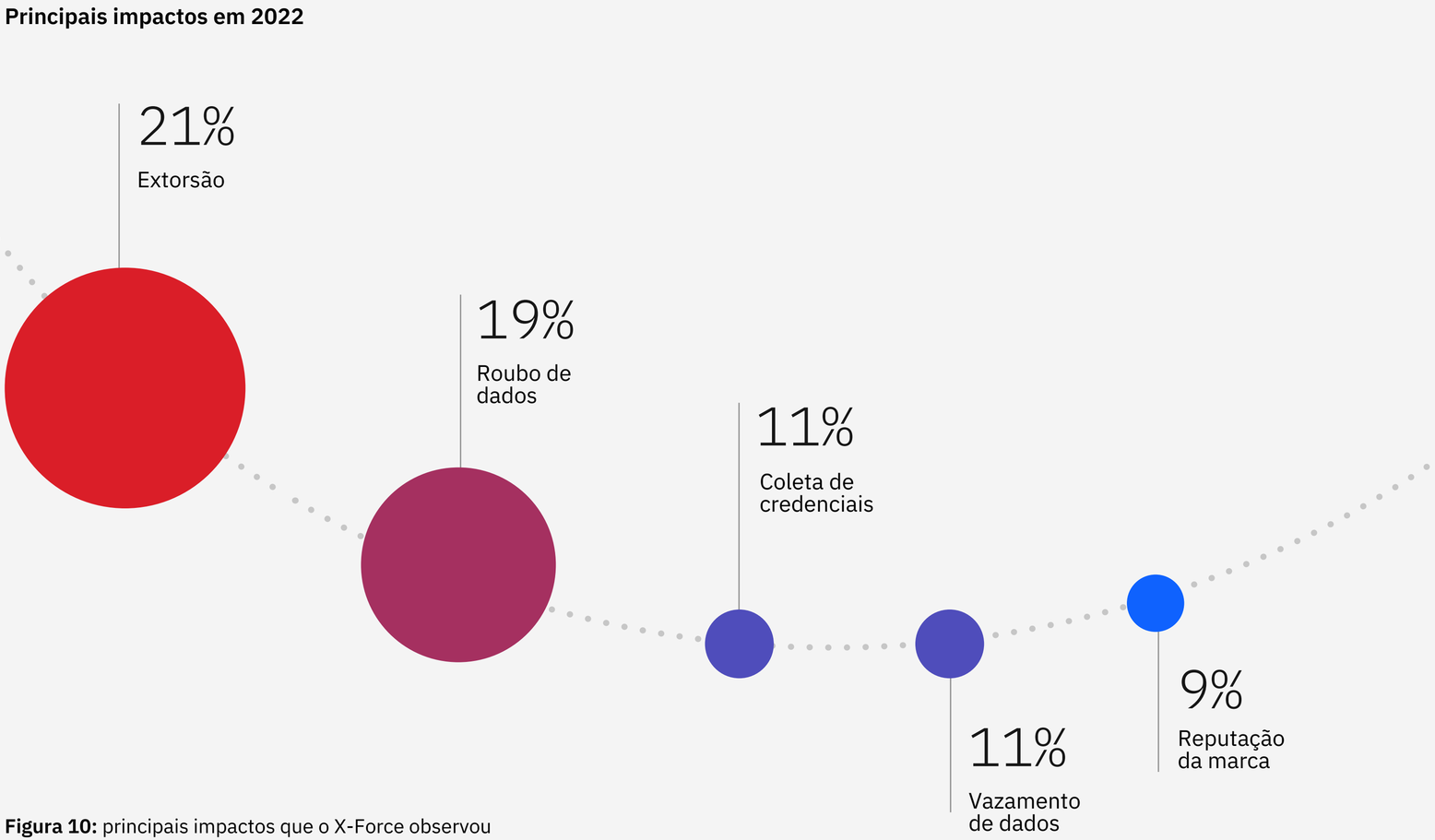


Figura 10: principais impactos que o X-Force observou na resposta a incidentes em 2022. Fonte: X-Force

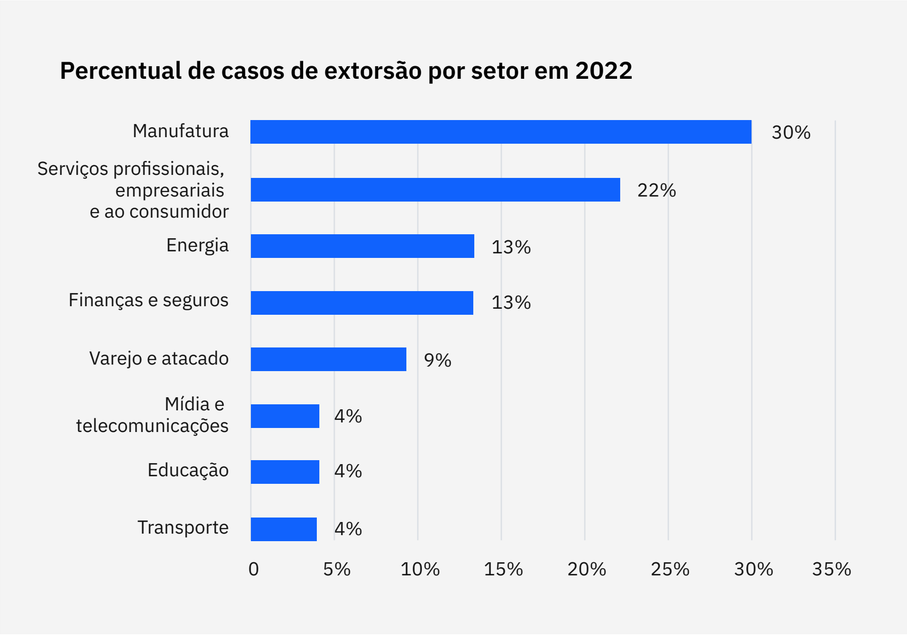


Figura 11: percentual de casos de extorsão por setor que o X-Force observou na resposta a incidentes em 2022. Os números não somam 100% devido ao arredondamento. Fonte: X-Force

O roubo de dados ficou em segundo lugar e representou 19% de todos os incidentes remediados pelo X-Force. A coleta de credenciais que resultou em roubo de nomes de usuário e senhas e exigiu mitigações correspondentes representou 11% dos casos. Os incidentes nos quais o X-Force identificou o vazamento de informações roubadas foram menos comuns do que o roubo de dados (11%). Os impactos na reputação da marca, como a disrupção nos serviços prestados pelos clientes, representaram 9% dos incidentes. No Apêndice, incluímos a lista completa dos impactos rastreados pelo X-Force.
Os incidentes que impactaram a reputação da marca das vítimas foram principalmente ataques de negação de serviço distribuída (DDoS), que são usados frequentemente para obrigar as vítimas a pagar para interromper o ataque.

Desenvolvimentos notáveis na extorsão on-line[1-9]

Ano	Evento	Tática
2013	Cryptolocker: um dos principais tipos de ransomware	Criptografia de dados
2014	DDoS 4 Bitcoin, Armada Collective	Ransom DDoS
2015	O ransomware Chimera adiciona a ameaça de vazar dados on-line roubados	Extorsão dupla
2017–18	BitPaymer e SamSam	Big game hunting
2020	Caso do ransomware Vastaamo	Extorsão tripla

Extorsão

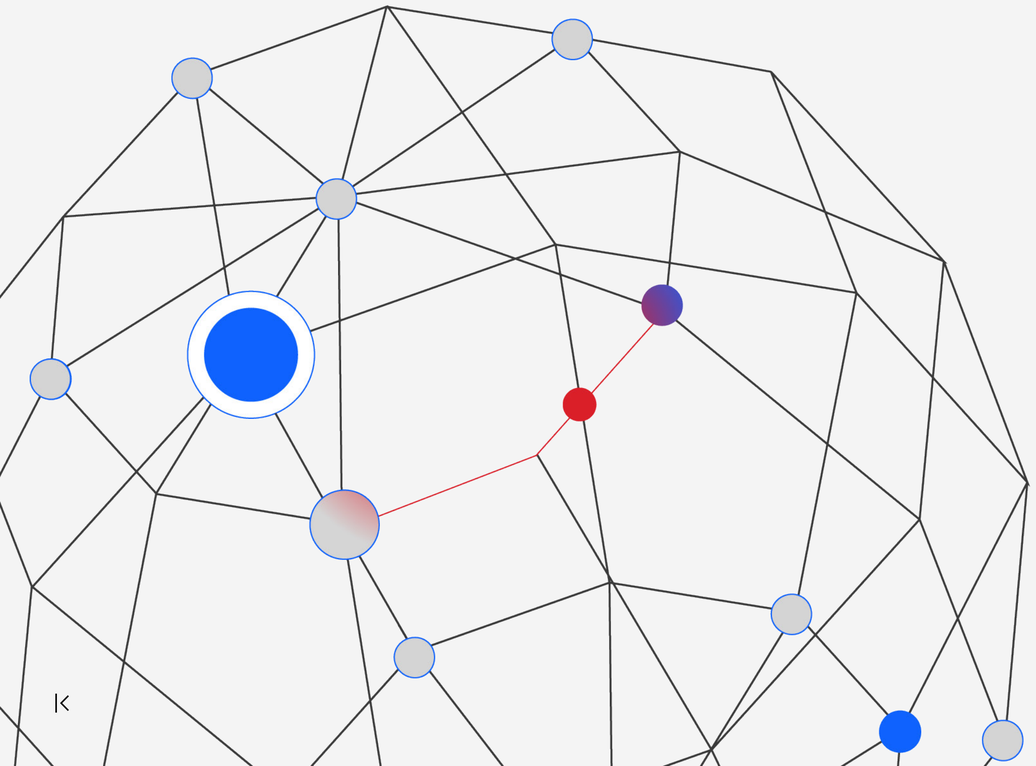
Embora a extorsão seja mais associada ao ransomware, as campanhas de extorsão incluíram diversos métodos de pressionar os alvos, como ameaças de DDoS, criptografia de dados e, mais recentemente, ameaças de extorsão duplas ou triplas que combinam vários dos elementos mencionados.

Outra tática usada por pelo menos um grupo de ransomware a partir de 2022 foi tornar os dados roubados mais acessíveis para outras vítimas. Ao facilitar que vítimas secundárias identifiquem os próprios dados em um vazamento, os operadores querem aumentar a pressão na empresa que é alvo do grupo de ransomware ou em uma afiliada. Em 2023, o X-Force prevê que os agentes de ameaça tentarão enviar notificações novas ou aprimoradas às vítimas para aumentar os possíveis custos legais e de reputação de uma invasão.

Muitas vezes, os profissionais de cibersegurança e as vítimas de ciberataques focam nos impactos dos agentes de ameaça em uma empresa. No entanto, é importante considerar as intenções dos agentes de ameaça, os recursos e como eles evoluem. Com essa abordagem, é possível entender como esses recursos vão evoluir. Como as opções de extorsão estão cada vez mais variadas e o principal objetivo dos agentes de ameaça que usam ransomware é o ganho financeiro, a equipe do X-Force avalia que eles vão continuar aperfeiçoando e ampliando as metodologias de extorsão para encontrar novas formas de pressionar as vítimas a fazer pagamentos.

07

Desdobramentos cibernéticos relacionados à guerra da Rússia contra a Ucrânia



Até a data desta publicação, a atividade cibernética da Rússia após a invasão da Ucrânia não resultou nos ataques generalizados e de alto impacto temidos por entidades de governos ocidentais. No entanto, a Rússia usou um número sem precedentes de wipers contra alvos na Ucrânia, o que comprova o investimento contínuo em malware destrutivo. Além disso, a invasão resultou no reaparecimento do hacktivismo feito por grupos simpatizantes da Rússia ou da Ucrânia e na reordenação do cenário de crimes cibernéticos do Leste Europeu.

Como a Rússia tem demonstrado recursos avançados para ataques cibernéticos a infraestruturas críticas desde 2015, agências de cibersegurança internacionais emitiram um aviso em abril de 2022. O aviso mencionou operações cibernéticas com potencial significativo e as disrupções relacionadas na Ucrânia e em outros países. O X-Force avaliou que as ameaças mais significativas que surgiram incluem o retorno do hacktivismo e do malware wiper, além de mudanças significativas no mundo dos crimes cibernéticos. A maioria dessas operações teve como alvo entidades da Ucrânia, da Rússia e de países vizinhos, mas algumas também afetaram outras áreas.

Para lidar com esse problema, os profissionais de cibersegurança estão empregando os avanços nas áreas de detecção, resposta e compartilhamento de informações obtidos nos últimos anos. Muitas das tentativas anteriores de ataque com wiper foram identificadas, analisadas e divulgadas rapidamente. Esses ataques incluíram pelo menos oito wipers identificados e a descoberta e desativação de um ataque cibernético russo na rede elétrica da Ucrânia em abril de 2022.

No ciberespaço, os efeitos mais sentidos da guerra foram as ações dos autoproclamados grupos de hacktivismo que atuam em defesa dos interesses nacionais da Rússia ou da Ucrânia. Embora muitos grupos tenham se formado desde a invasão da Rússia e estejam atuando contra redes da Rússia e da Ucrânia para marcar posicionamentos políticos, o Killnet é um dos grupos simpáticos à Rússia mais atuantes. Ele reivindicou ataques DDoS a serviços de utilidade pública, ministérios, aeroportos, bancos e empresas de energia de países membros da Organização do Tratado do Atlântico Norte (OTAN), países aliados na Europa e também ao Japão e aos Estados Unidos. As entidades que são possíveis alvos do Killnet devem garantir que têm meios para mitigar ataques DDoS. Uma boa opção é usar os serviços de um provedor de mitigação de DDoS externo.

Linha do tempo com eventos de hacktivismo específicos em 2022

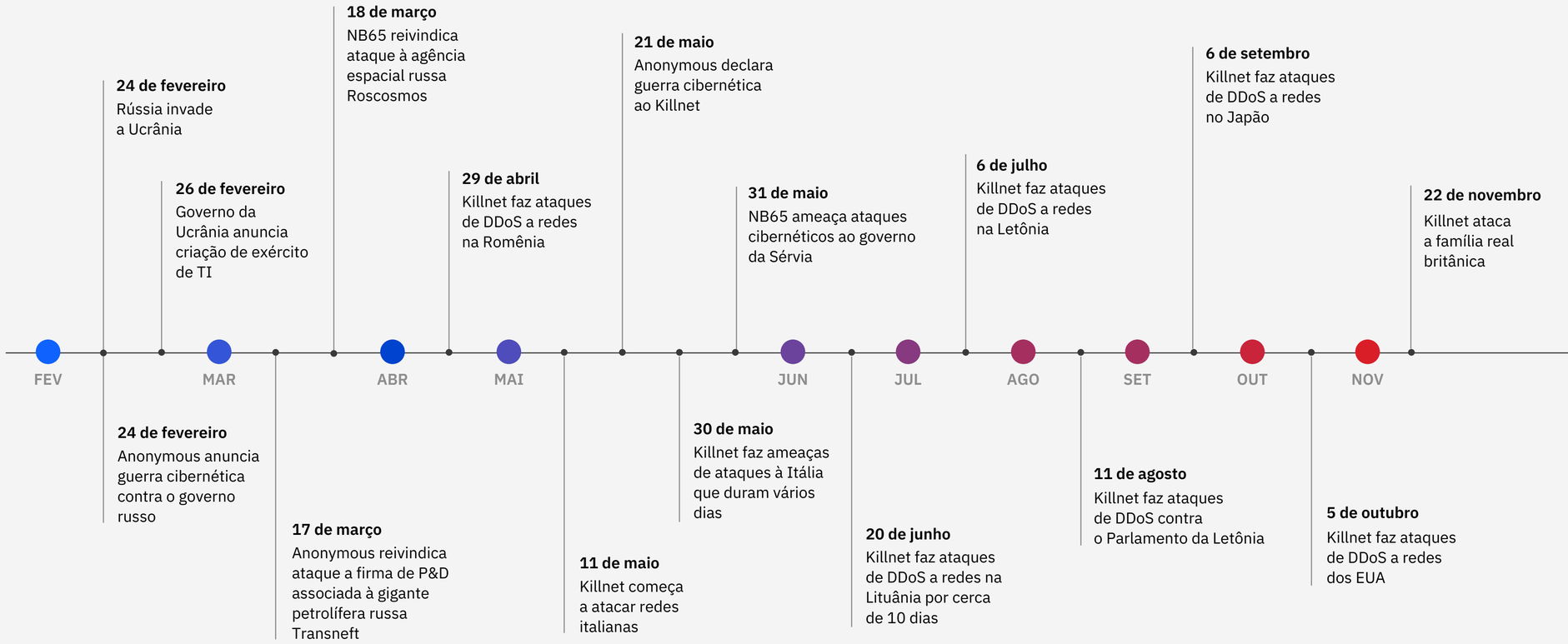


Figura 12: imagem mostrando eventos de hacktivismo observados até o momento durante o conflito na Ucrânia. Fonte: análise do X-Force de relatório de software livre

Wipers usados na guerra da Rússia contra a Ucrânia

A guerra da Rússia contra a Ucrânia se destaca pelo uso de várias famílias de wiper contra diversos alvos em sequência rápida e escala nunca vista, além do uso de malware com operações militares cinéticas.

Esses desenvolvimentos incluem pelo menos nove novos wipers: AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred e SoloShred. Esses wipers foram usados de forma predominante contra redes ucranianas desde antes da invasão inicial até o começo da guerra (principalmente de janeiro a março de 2022). Embora os wipers não sejam novidade, eles eram usados principalmente em campanhas específicas contra um conjunto limitado de alvos.

No entanto, as notáveis exceções WannaCry e NotPetya, que se espalham de forma indiscriminada após impactar as vítimas iniciais, são preocupantes porque esses wipers podem estar se espalhando de forma mais ampla ou sendo reprogramados para operações maliciosas em outros locais.

Na avaliação do X-Force, as ameaças cibernéticas patrocinadas pela Rússia continuam sendo um risco significativo para redes de computação e infraestrutura crítica no mundo todo. Essa avaliação é baseada no histórico de operações cibernéticas da Rússia que tiveram como alvo redes da Ucrânia, da Europa, da OTAN e dos EUA e nos ataques feitos por grupos russos desde 2015.

Mudanças nos grupos de cibercriminosos russos

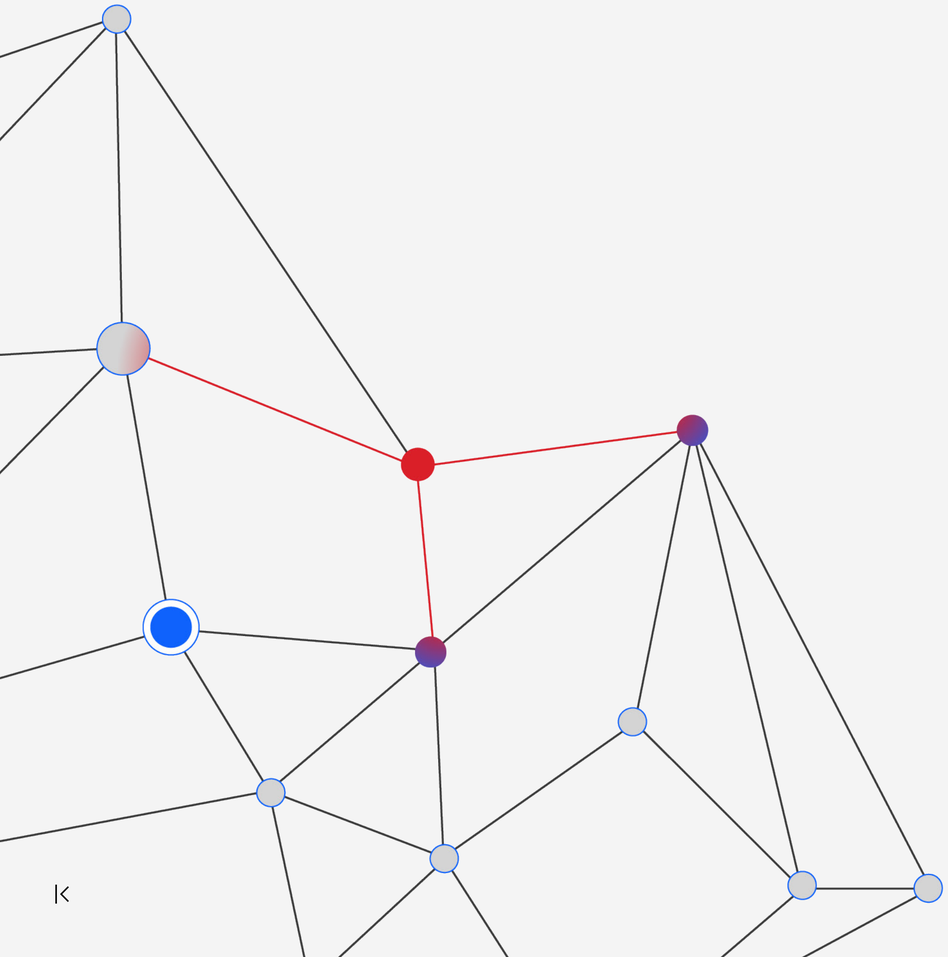
O ano de 2022 foi tumultuado para o ITG23, um dos sindicatos de cibercriminosos russos mais conhecidos e famoso por ter desenvolvido o Trickbot, um cavalo de Troia bancário, e o ransomware Conti. O grupo sofreu uma série de vazamentos importantes no início de 2022 após apoiar publicamente o envolvimento da Rússia na guerra. Chamados de ContiLeaks e TrickLeaks, esses vazamentos resultaram na publicação de milhares de mensagens de bate-papo e na revelação da identidade de vários membros do grupo. O X-Force encontrou indícios de que o ITG23 fez ataques sistemáticos de meados de abril até pelo menos meados de junho de 2022. Isso representa uma mudança inédita porque o grupo ainda não tinha atacado a Ucrânia.

Além disso, o grupo parece ter aposentado duas das principais famílias de malware, o Trickbot e o Bazar, e acabado com a operação do ransomware Conti. Vários relatórios sugerem que pode estar acontecendo uma mudança significativa na composição do grupo devido à divisão em diversas facções e à saída de alguns membros.

A desativação do Trickbot e do Bazar, responsáveis por um número considerável de infecções em 2021, gerou uma lacuna que foi preenchida rapidamente por famílias de malware como Emotet, IcedID, Qakbot e Bumblebee. Antes da desativação, o ITG23 ainda fazia muitas implementações do ransomware Conti, que representou um terço de todas as ocorrências de ransomware atendidas pelo X-Force no primeiro trimestre de 2022.

O grupo também lançou uma nova versão do malware Anchor, um backdoor secreto que o grupo implementava tradicionalmente contra alvos importantes. A nova versão descoberta pelo X-Force, que se chama AnchorMail, tem um mecanismo de comunicação de comando e controle (C2) atualizado e baseado em e-mail. O servidor C2 usa os protocolos Simple Mail Transfer Protocol Secure (SMTPS) e Internet Message Access Protocol Secure (IMAPS), e o malware se comunica com o servidor enviando e recebendo mensagens de e-mail criadas especificamente para essa finalidade.

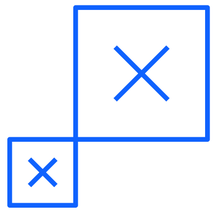
O cenário de malware



Aumento dos worms espalhados por USB

Depois que o X-Force observou tentativas de infecção com Raspberry Robin que impactaram empresas em meados de maio de 2022, o worm enigmático começou a se espalhar rapidamente nas redes das vítimas devido ao compartilhamento de dispositivos USB pelos usuários. As infecções atingiram um pico no início de junho. No começo de agosto, o Raspberry Robin chegou a representar 17% das tentativas de infecção observadas pelo X-Force. Esse pico foi identificado nos setores de petróleo e gás, manufatura e transporte. A taxa de tentativas de infecção de 17% nesses setores é significativa porque menos de 1% dos clientes do X-Force foram alvo da mesma variedade de malware.
O X-Force também observou um aumento na atividade do Raspberry Robin de setembro a novembro de 2022.

A disseminação de worms baseados em USB é viabilizada por engenharia social e exige algum acesso físico (de um usuário ou por outo meio) à rede ou ao endpoint.
A recomendação do X-Force é confirmar que suas ferramentas de segurança bloqueiam malwares baseados em USB conhecidos, fazer treinamentos de conscientização sobre segurança e desativar recursos de execução automática de qualquer mídia removível. Em ambientes com exigências de confidencialidade, como OT ou ambientes com isolamento físico, é mais seguro proibir o uso de unidades flash USB.
Se for necessário usar esses dispositivos, faça um controle rigoroso do número de dispositivos portáteis aprovados para uso no seu ambiente e implemente as sugestões anteriores.



Aumento do uso da Rust

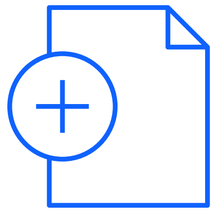
A linguagem de programação Rust ganhou popularidade entre os desenvolvedores de malware ao longo de 2022 devido à compatibilidade com várias plataformas e às taxas baixas de detecção por antivírus em comparação com outras linguagens mais comuns. Como a linguagem Go, ela também usa um processo de compilação mais complicado que pode fazer os profissionais de engenharia reversa terem mais trabalho para analisar o malware. Vários desenvolvedores de ransomware lançaram versões de malwares em Rust, inclusive BlackCat, Hive, Zeon e, mais recentemente, RansomExx. O X-Force também analisou um crypter do ITG23 em Rust, além da família CargoBay de backdoors e assistentes de download. O aumento da popularidade da Rust destaca o esforço de inovação contínuo do ecossistema de ransomware para enganar os mecanismos de detecção.

Vidar InfoStealer

O X-Force identificou um aumento repentino das ocorrências do malware Vidar InfoStealer, que começou em junho de 2022 e continuou até o início de 2023. Observado pela primeira vez em 2018, o Vidar é um cavalo de Troia para roubo de informações distribuído no formato de malware como serviço (MaaS). O cavalo de Troia é geralmente executado por usuários que clicam em links ou anexos de spam maliciosos (malspam). Como tem um conjunto variado de recursos, o Vidar pode ser usado para acessar diversas informações de dispositivos, como dados de cartão de crédito, nomes de usuário, senhas e arquivos, além de fazer capturas de tela da área de trabalho do usuário. O Vidar também pode roubar carteiras das criptomoedas Bitcoin e Ethereum.

Os ataques com um malware que rouba informações geralmente têm motivação financeira. Os dados roubados são analisados, e as informações valiosas são agrupadas e organizadas em um banco de dados. Esse banco de dados pode ser vendido na dark web ou por meio do Telegram, um aplicativo de mensagens privadas. Os agentes de ameaça podem usar as informações para cometer diversos tipos de fraude, como solicitar empréstimos bancários ou cartões de crédito, fazer compras on-line ou acionar um seguro de saúde de forma fraudulenta.

Eles também podem usar as credenciais de login comprometidas para acessar contas corporativas e serviços remotos. O custo médio do uso de um malware que rouba informações é de aproximadamente USD 250 por mês, e os usuários escolhem o malware preferencial. O X-Force observa com frequência tentativas de venda de acesso obtido por malware de roubo de informações. Os valores variam de USD 10 a USD 75. Quando o acesso é obtido, os agentes de ameaça podem usar facilmente os privilégios da conta invadida como um ponto de partida para outras atividades maliciosas.



Evolução dos mecanismos de entrega de malware

Está cada vez mais comum ver o envio de malware por meio de documentos maliciosos do Microsoft Office, geralmente anexados a e-mails de phishing. Os desenvolvedores de malware criaram esses documentos que contêm macros maliciosas criadas para executar malware quando o documento é aberto. O uso de macros com essa finalidade se tornou tão comum que os produtos do Microsoft Office começaram a incluir avisos de segurança ao abrir documentos com macros. Em julho de 2022, a Microsoft começou a bloquear a execução de macros por padrão em documentos recebidos por e-mail ou pela internet.

Como os responsáveis pela segurança cibernética melhoraram os recursos de detecção e prevenção, os agentes de ameaça começaram a substituir o Visual Basic Application (VBA) por um formato de macro mais antigo do Microsoft Excel conhecido como Macro 4.0. Os documentos maliciosos criados no Excel são usados há muito tempo. No entanto, a maioria dos mecanismos de segurança foi desenvolvida com base em macros VBA em um documento do Excel. Por algum tempo, as macros Excel Macro 4.0 foram uma boa forma de evitar as detecções. Nessa época, alguns agentes de ameaça começaram a enviar links de e-mail direcionando a vítima para um site de dropper para fazer o download de documentos maliciosos em vez de enviar esses itens anexados ao e-mail. Como a Microsoft fez mudanças para permitir que os administradores desativem a Macro 4.0 e também bloqueou a execução de macros baixadas da internet, os agentes de ameaça foram forçados a mudar de tática novamente.

Mesmo depois dessas mudanças, muitos criadores de malware ainda usam documentos do Microsoft Office com macros ativadas, mas grupos sofisticados adotaram uma cadeia de infecção mais intrincada e complexa. Essas novas táticas envolvem uma combinação de arquivos HTML com código binário incorporado ou um arquivo compactado protegido por senha. Esses arquivos também contêm uma imagem ISO que pode incluir um arquivo LNK, um arquivo CMD ou outros tipos de arquivo que provavelmente não seriam enviados para um destinatário de e-mail ou baixados da internet. Outras táticas incluem injeção de modelo remoto ou exploração de vulnerabilidades. O CVE-2021-40444, uma vulnerabilidade de execução remota de código no Microsoft HTML (MSHTML), é um exemplo de componente de software que renderiza páginas da internet no Microsoft Windows para executar o malware em vez de usar macros.

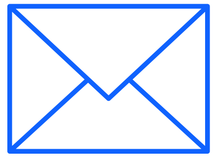
Os dados de spam destacam a ameaça do ransomware e ilustram tendências de macro

O X-Force analisou tendências de e-mail de spam e phishing para entender melhor a eficiência e o uso dessas táticas. A investigação descobriu que os e-mails de spam foram usados regularmente ao longo do ano para entregar malware, como Emotet, Qakbot, IcedID e Bumblebee, que em muitos casos resultou em infecções com ransomware.

Malware[10-18]	**Ransomware**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

Os dados nesta tabela cobrem um período que vai do final de 2021 até a publicação deste relatório. O itálico indica que o malware ou ransomware foi identificado em 2022, mas não é observado pelo X-Force desde pelo menos outubro de 2022.

O X-Force identificou um aumento da atividade do Qakbot em setembro de 2022 que usou contrabando de HTML para comprometer as vítimas. Essas infecções estão vinculadas a uma atividade abrangente pós-comprometimentos que inclui reconhecimento, reunião de informações e implementação de cargas úteis adicionais. As infecções com Qakbot não identificadas ao longo de 2022 resultaram em várias infecções com Black Basta. O X-Force identificou que os ataques de ransomware reivindicados no site de vazamentos do grupo de ransomware Black Basta diminuíram consideravelmente durante o intervalo na atividade de phishing do Qakbot, em meados de 2022. Com base nas previsões do X-Force, a retomada da atividade do Qakbot resultará em um número maior de vítimas de ransomware.



Enganando as macros

O uso de arquivos ISO e LNK passou a ser uma tática importante para infectar empresas devido às mudanças nas macros da Microsoft a partir de outubro de 2021. Essa tática inclui entregar cargas úteis diretamente por meio desses arquivos, que funcionam como um contêiner, e ofuscar arquivos com macros ativadas dentro desses arquivos.

- Arquivos ISO e arquivos compactados estão sendo usados para enganar o atributo Mark of the Web (MOTW) que a Microsoft está usando para ajudar os alvos a ativar macros maliciosas. Embora os arquivos ISO e compactados pareçam transferidos por download da internet, o anexo com macro ativada no arquivo não tem a mesma característica. Isso permite que os agentes de ameaça continuem o ataque.
- Outra forma de burlar as restrições a macros é incluir as cargas úteis diretamente nos arquivos LNK. Clicar nesses arquivos aciona comandos arbitrários usados principalmente para fazer download ou carregar os próximos estágios. Antes do início de 2022, apenas uma campanha, identificada em fevereiro de 2021, usava essa tática. O X-Force observou a recorrência dessa tática pela primeira vez entre fevereiro e março de 2022, mas agora ela está sendo usada com frequência.

Outras tendências que o X-Force detectou nas campanhas de spam dos agentes de ameaça incluem o aumento do uso de arquivos compactados criptografados como anexos e a interceptação de encadeamento, como explicado aqui.

- As extensões compactadas criptografadas, que são mais difíceis de ser detectadas por softwares antivírus e sinalizadas como maliciosas, foram descobertas com mais frequência em 2022. Em comparação com dados desde abril de 2021, o número médio de e-mails de spam com esses anexos entregues por semana aumentou nove vezes em 2022.
- A interceptação de encadeamento, ou seja, quando os agentes de ameaça se inserem em conversas por e-mail, é uma tática usada há muito tempo para aumentar a legitimidade do spam e conseguir o engajamento das vítimas de forma mais eficiente. O uso dessa tática aumentou consideravelmente em 2022, em comparação com a maioria dos meses de 2021, e se estabilizou no segundo trimestre, uma tendência que o X-Force vincula em grande parte ao envio de spam com Emotet.

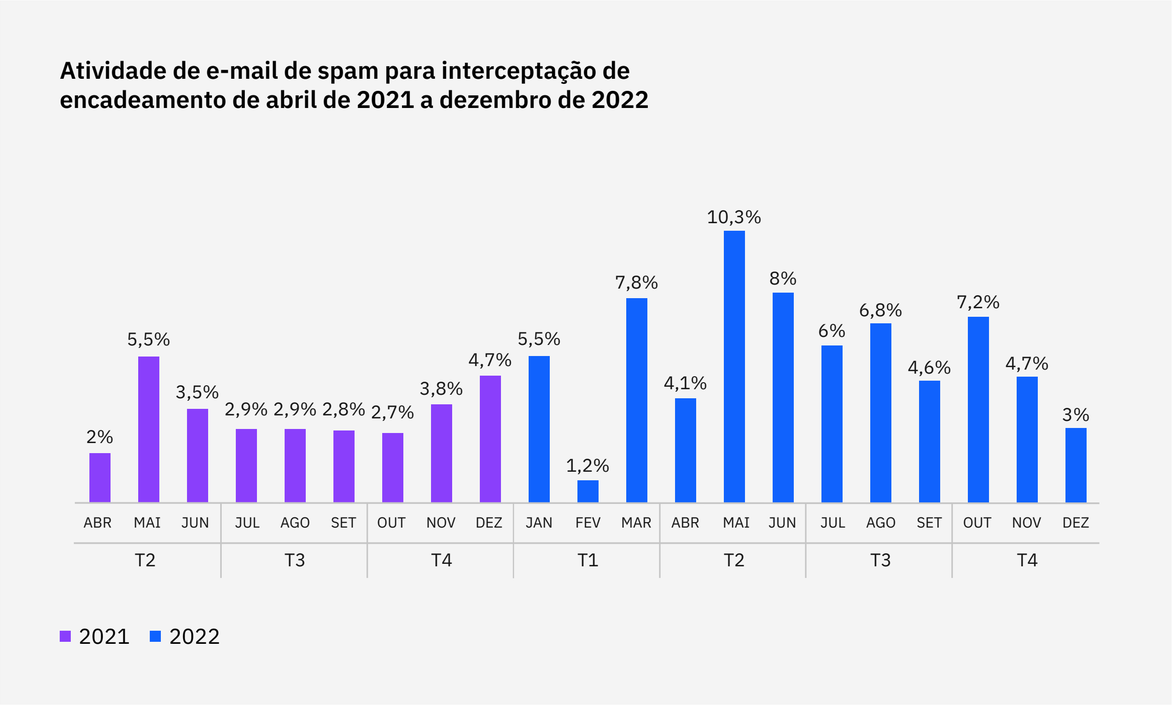
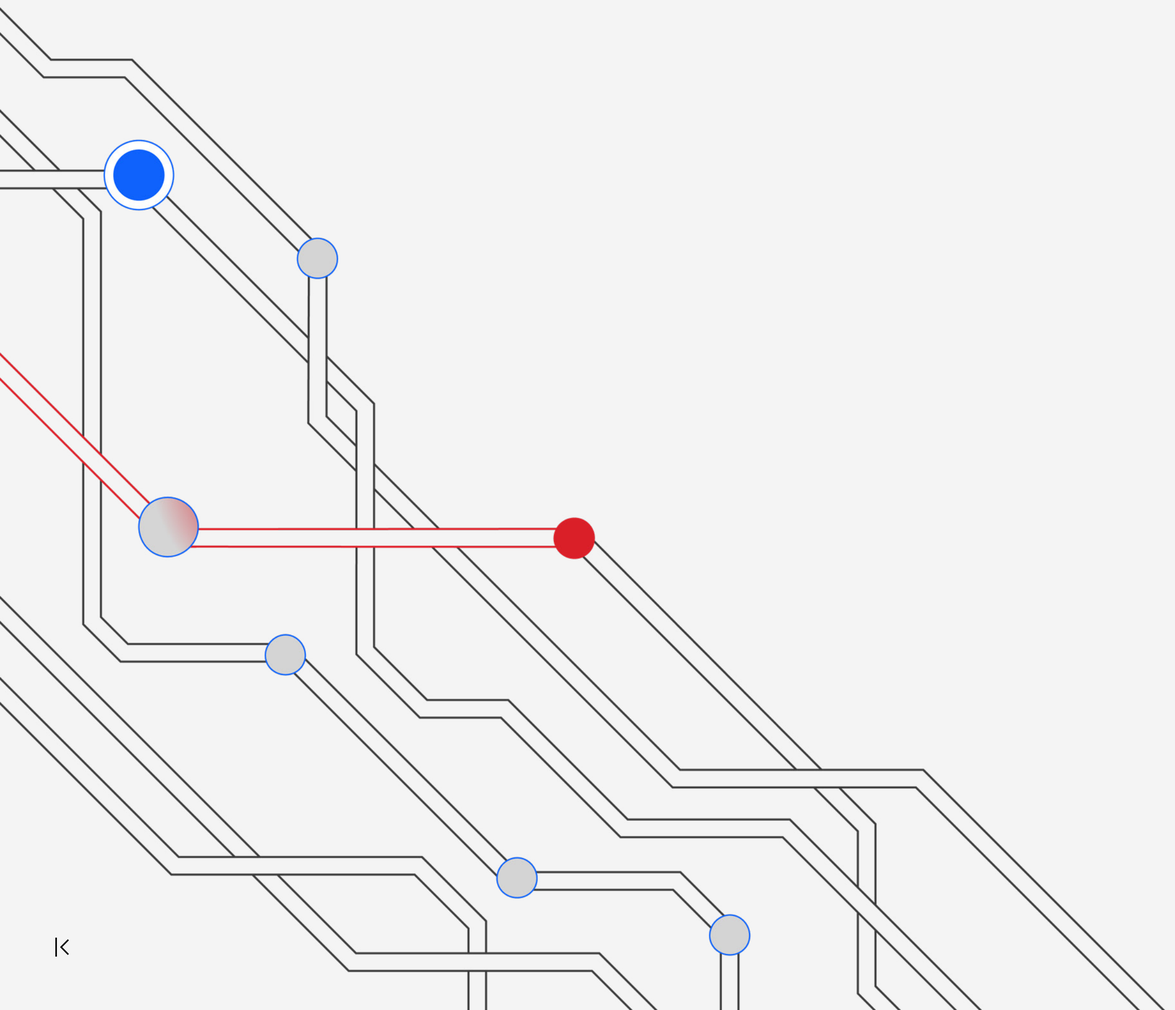


Figura 13: os números mostram o percentual por mês do total de tentativas de interceptação de encadeamento detectadas nos dados do X-Force desde abril de 2021.
Fonte: X-Force

- O Emotet voltou a ser usado em 2021 depois que o botnet foi interrompido em janeiro de 2021. Ele continuou sendo usado em 2022, teve um hiato de quase quatro meses a partir de meados de julho, e voltou a ser usado por quase duas semanas em novembro do mesmo ano.
- Os dados mostraram mais ou menos o dobro de tentativas frequentes por mês em 2022 em comparação com os dados desde abril de 2021. A interceptação de encadeamento aumentou de forma irregular até maio de 2022, e a queda no uso dessa tática no segundo semestre está relacionada em parte à inatividade do Emotet.
- Os e-mails de spam com Emotet, Qakbot e IcedID usaram muito a tática de interceptação de encadeamento. O retorno do Emotet em novembro de 2021 contribuiu para o aumento com oscilações até maio de 2022. A queda geral no segundo semestre está relacionada ao hiato no uso do Emotet de julho a outubro e a um breve retorno em novembro de 2022.
- Rastrear interceptações de encadeamento e distinguir essas ocorrências com precisão de outros casos nos quais os invasores apenas adicionam uma linha de assunto de resposta a um e-mail de spam é uma tarefa difícil que deve ficar ainda mais complicada. Por exemplo, alguns agentes de ameaça começaram a remover “Re:” da linha de assunto, provavelmente porque sabem que esse cabeçalho pode ser usado para rastrear a atividade deles.

09

Ameaças à TO e aos sistemas de controle industrial



Ameaças à tecnologia operacional

Em 2022, foram descobertos dois tipos de malware específicos da TO, o Industroyer2 e o INCONTROLLER, também conhecido como PIPEDREAM, e também houve a divulgação do OT: ICEFALL, um conjunto de vulnerabilidades de TO. O cenário de ameaças cibernéticas de TO está crescendo consideravelmente, e os proprietários e operadores de ativos de TO precisam estar cientes das mudanças.

O X-Force analisou com mais atenção dados de resposta a incidentes e ataques a redes específicos da TO para gerar insights sobre como os agentes de ameaça estão tentando comprometer os clientes em setores relacionados à TO. Os dados de ataques a redes mostram que os ataques de força bruta, o uso de padrões de criptografia fracos e desatualizados e senhas fracas ou padrão são alertas comuns nos ambientes de TI e TO desses setores.

Os alertas de prováveis tentativas de ataque de força bruta foram os mais comuns nos dados de ataques a redes do Sistema de Comando de Incidentes (SCI), seguidos de perto pelos alertas de criptografia fraca. Os alertas mais comuns de criptografia fraca estavam relacionados ao uso contínuo do Transport Layer Security (TLS) 1.0, um método de criptografia obsoleto e inseguro que deixou de ser usado em março de 2021. Embora o governo dos EUA recomende a reconfiguração para usar o TLS 1.2 ou o 1.3, as diretrizes do National Institute of Standards and Technology (NIST) analisam a realidade de forma mais detalhada. A realidade é que sistemas mais antigos talvez precisem continuar usando versões mais fracas da criptografia para garantir a continuidade das funcionalidades. Também é importante mencionar os alertas de senha fraca ou padrão, principalmente porque essas são vulnerabilidades

básicas que facilitam os ataques de força bruta. A verificação de vulnerabilidades internas e externas de forma generalizada e possivelmente indiscriminada foi a tentativa de ataque mais comum nos setores relacionados à TO. Os dados revelaram que vulnerabilidades e ameaças antigas ainda são relevantes. Um grupo de vulnerabilidades descoberto em 2021 pelo Cisco Talos no software de monitoramento Advantech R-SeeNet gerou uma pequena maioria de alertas de verificação de vulnerabilidade nos setores de TO em 2022. Essas vulnerabilidades podiam permitir que invasores executassem código ou comandos arbitrários.

No entanto, a segunda vulnerabilidade mais comum foi identificada em 2016. A CVE-2016-4510, que ignora filtros no aplicativo VTScada da Trihedral, pode permitir que usuários não autenticados enviem solicitações HTTP para acessar arquivos. Ataques como WannaCry e Conficker, que continuam sendo ameaças significativas à TO, reforçam ainda mais os riscos das ameaças antigas.

Manufatura continua sendo o setor de TO mais visado

Os dados da análise do subconjunto de incidentes nos setores relacionados à TO mostram que o setor de manufatura foi o mais atacado em 2022. O setor foi alvo de 58% dos incidentes que o X-Force ajudou a remediar. A implementação de backdoors foi a principal ação sobre o objetivo e foi identificada em 28% dos casos no setor de manufatura. Esse setor é muito interessante para os invasores que usam ransomware, provavelmente porque as empresas têm baixa tolerância ao tempo de inatividade.

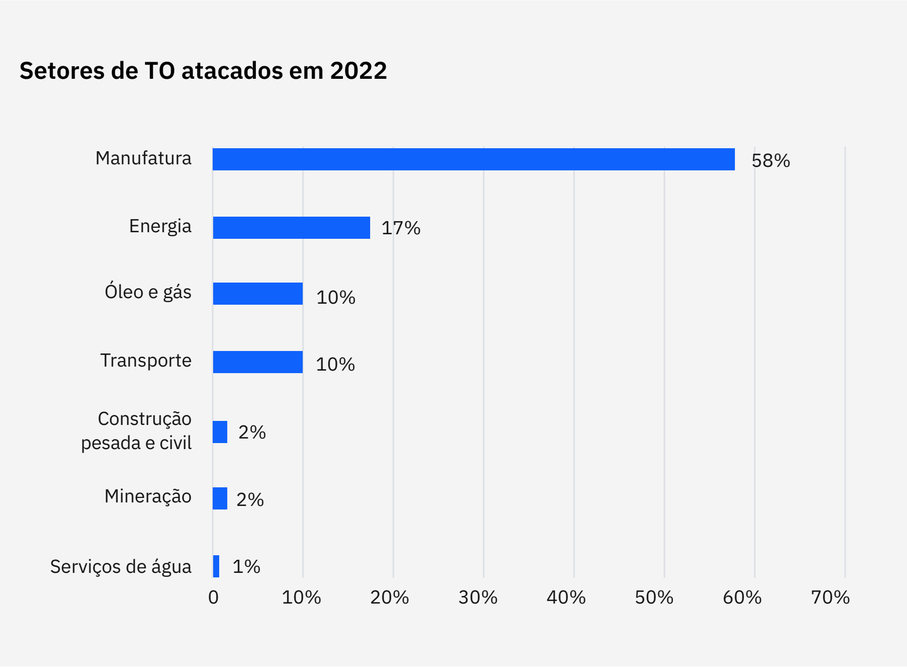


Figura 14: proporção de casos de resposta a incidente por setor relacionado à TO atendidos pelo X-Force em 2022. Fonte: X-Force

A análise dos vetores de acesso inicial nos setores relacionados à TO identificou que o spear phishing foi responsável por 38% dos casos, incluindo o uso de anexos em 22% dos casos, o uso de links em 14% dos casos e de spear phishing como serviço em 2% dos casos. A exploração de aplicações de uso público (24%) ficou com o segundo lugar, seguindo a tendência mais ampla do setor. A detecção de backdoors também foi um dos principais incidentes nesses setores (20% dos casos), seguida pelo ransomware (19%). A extorsão também continua ocupando a primeira posição dentre os impactos (29%), e o roubo de dados ficou logo atrás (24%).

Outra vulnerabilidade importante explorada na TO é a falta de segmentação adequada entre as redes de TO e TI. A equipe do X-Force Red Adversary Simulation Services explora regularmente a segmentação fraca para acessar ambientes de TO isolados. Esses ambientes incluem servidores de salto, estações de trabalho com operador do tipo dual-homed e servidores de relatórios, como historiadores de dados que expõem serviços da web e SQL de redes de TO para redes de TI corporativas. Segmentar essas partes das suas redes de forma adequada e monitorar a comunicação entre as partes com atenção pode manter os ativos protegidos.

Tendências geográficas

Em 2022, a região Ásia-Pacífico foi a mais atacada pelo segundo ano consecutivo, concentrando 31% dos incidentes atendidos pelo X-Force IR. A Europa ficou logo atrás com 28% dos ataques, e a América do Norte teve 25% dos incidentes. A região Ásia-Pacífico e a Europa tiveram proporções mais altas de casos, aumentando cinco e quatro pontos percentuais, respectivamente, em comparação com os números de 2021, e houve uma queda considerável no Oriente Médio (de 14% para 4%).

Incidentes por região 2020 – 2022

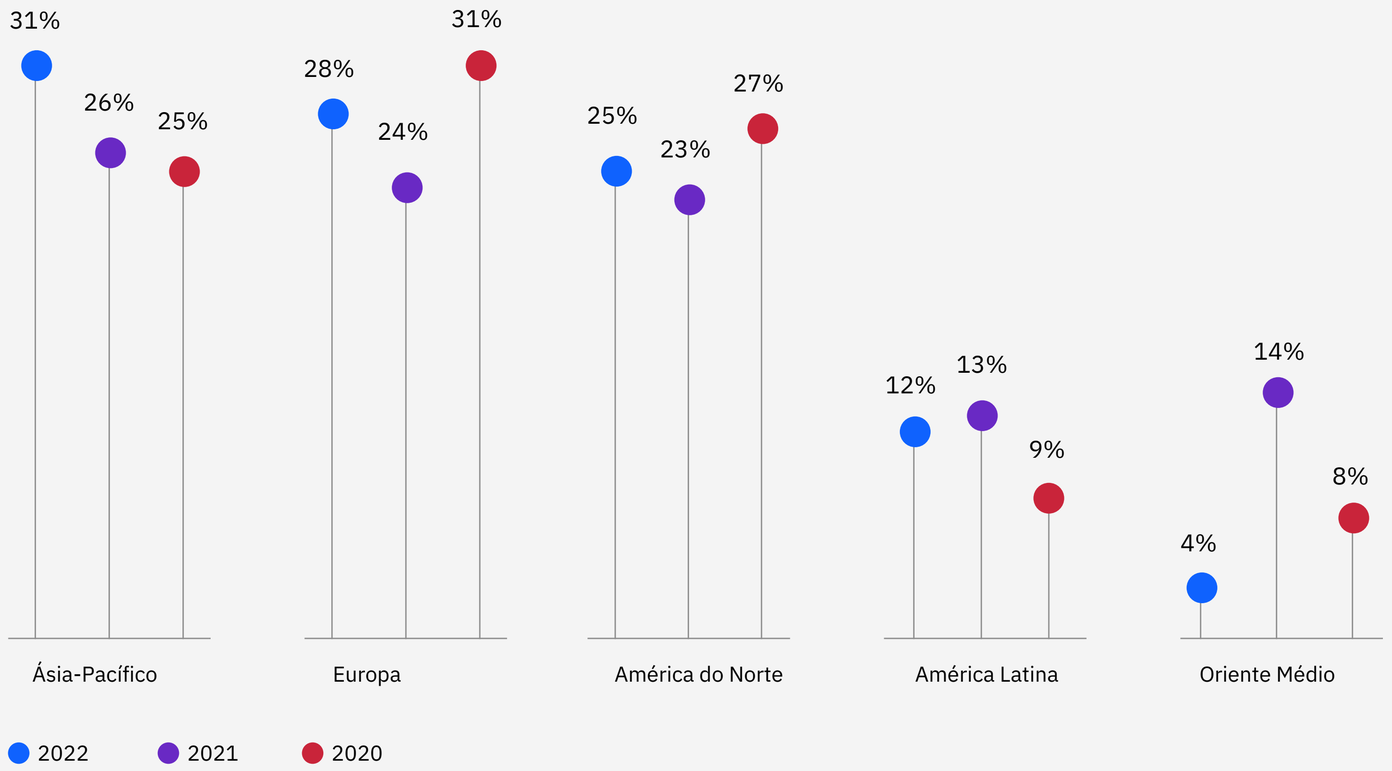


Figura 15: proporção de casos de resposta a incidente por região atendidos pelo X-Force de 2020 a 2022. Fonte: X-Force

1 | Ásia-Pacífico

A região Ásia-Pacífico, mais especificamente o Japão, foi o epicentro do pico do Emotet em 2022. Embora não esteja diretamente relacionado à guerra na Europa, o aumento dos casos de Emotet no Japão ocorreu em paralelo à invasão da Ucrânia pela Rússia. Como observado por outros pesquisadores da comunidade de cibersegurança, essa invasão ajudou a aumentar muito o uso do Emotet na época. As campanhas de spam foram identificadas em vários setores, mas a maioria dos casos ocorreu no setor de serviços financeiros e de seguros. O Emotet é entregue principalmente por campanhas de spam que usam títulos chamativos.

O setor de manufatura encabeça a lista dos setores atacados nessa região com 48% dos casos, e o setor de serviços financeiros e de seguros ocupa o segundo lugar com 18%.

O spear phishing por meio de anexos foi o principal vetor de infecção (40%) na região, seguido pela exploração de aplicações de uso público (22%). Os casos de serviços remotos externos e links de spear phishing empataram em terceiro lugar com 12% dos casos.

As implementações de backdoors foram a ação sobre o objetivo mais comum em 31% dos casos na região. O ransomware ficou em segundo lugar (13%), e os maldocs ficaram em terceiro lugar (10%). A extorsão foi o impacto mais comum, observada em 28% dos casos. O impacto na reputação da marca ficou em segundo lugar (22%), e o roubo de dados ficou em terceiro lugar (19%).

O Japão concentrou 91% dos casos na região Ásia-Pacífico, as Filipinas tiveram 5% dos casos, e Austrália, Índia e Vietnã tiveram 1,5% dos casos (cada).

Na região Ásia-Pacífico, o setor de manufatura foi o mais atacado com 48% dos casos.

2 | Europa

A Europa teve um aumento significativo na implementação de backdoors a partir de março de 2022, logo depois que a Rússia invadiu a Ucrânia. As implementações de backdoors representaram 21% dos casos na região, e o ransomware representou 11% dos casos. As ferramentas de acesso remoto foram identificadas em 10% dos casos atendidos pelo X-Force. Em termos de impactos para os clientes, 38% dos casos observados pelo X-Force na Europa envolviam extorsão, 17% resultaram em roubo de dados e 14% fizeram a coleta de credenciais. A Europa foi a região mais atingida por extorsões, concentrando 44% de todos os casos observados.

A exploração de aplicações de uso público foi o principal vetor de infecção usado contra empresas europeias, representando 32% de todos os incidentes remediados pelo X-Force na região, e muitas dessas explorações resultaram em infecções com ransomware. A violação de contas locais válidas ficou em segundo lugar com 18% dos casos, e os links de spear phishing representaram 14% dos casos, uma queda considerável em relação aos 42% de 2021. Essa diminuição do uso de links de spear phishing pode ser resultado do aumento da conscientização dos usuários, da melhoria dos recursos de segurança de e-mail ou de proteções mais eficientes que identificam malware após a instalação.

O setor de serviços profissionais, corporativos e para consumidores empatou com o de serviços financeiros e de seguros como o mais atacado. Cada um desses setores concentrou 25% dos casos atendidos pelo X-Force. O setor de manufatura ficou em segundo lugar com 12% dos casos, e os setores de energia e saúde empataram em terceiro lugar com 10% dos casos.

O Reino Unido foi o país mais atacado da Europa, concentrando 43% dos casos. A Alemanha teve 14%, Portugal teve 9%, a Itália teve 8% e a França teve 7%. “O X-Force também atendeu a um número menor de casos nos seguintes países: Noruega, Dinamarca, Suíça, Áustria, Grécia, Groenlândia, Espanha e Sérvia.

O Reino Unido foi o país mais atacado da Europa, concentrando 43% dos casos.

3 | América do Norte

O X-Force observou um pequeno aumento no número de incidentes na América do Norte, que passaram de 23% de todos os casos em 2021 para 25% em 2022.

As empresas de energia foram para o topo da lista de vítimas na América do Norte, concentrando 20% de todos os ataques atendidos pelo X-Force em 2022. Os setores de manufatura e de varejo e atacado empataram em segundo lugar com 14% dos casos cada um. O setor de varejo e atacado ocupou uma posição similar em 2021, mas os números do setor de manufatura representaram uma queda de 50% em relação a 2021. O setor de serviços profissionais, corporativos e para consumidores ficou em terceiro lugar em 2022 (12%) devido ao aumento dos casos de ransomware e outros casos relacionados a malware.

Os principais vetores de infecção identificados foram a exploração de aplicações de uso público (35%) e os anexos de spear phishing (20%). Os incidentes de ransomware representaram 23% dos casos. Alguns deles foram o resultado de detecções de infecções com WannaCry ou Ryuk ocorridas em 2018 ou 2019. Isso reforça a importância de uma limpeza adequada após esses eventos. Na região, 12% dos casos foram botnets, com backdoors e BEC empatados em terceiro lugar (10% cada).

Ao analisar o principal impacto dos agentes de ameaça, a coleta de credenciais ficou com a primeira posição, representando 25% dos incidentes remediados pelo X-Force na América do Norte. O vazamento e o roubo de dados ficaram empatados em segundo lugar (17% cada), e a extorsão representou 13% dos casos.

Os Estados Unidos concentraram 80% dos ataques na região, e o Canadá teve apenas 20%.

As empresas do setor de energia foram as mais atacadas na América do Norte (20% dos casos).

4 | América Latina

Para fins de relatório, a IBM considera que a América Latina inclui México, América Central e América do Sul.

Os incidentes na América Latina seguiram as tendências globais. O setor de varejo e atacado, que foi o segundo mais visado em 2021, subiu para o primeiro lugar com 28% dos casos remediados pelo X-Force. O setor de serviços financeiros e de seguros foi o segundo mais atacado com 24% dos casos, seguido pelo setor de energia (20%).

O ransomware cresceu mais do que outros ataques na América Latina, representando 32% dos casos atendidos pelo X-Force. A implementação de backdoors foi a segunda ação sobre o objetivo mais identificada (16%), e BEC e interceptação de encadeamento de e-mail ficaram empatadas em terceiro lugar (11% cada). A extorsão e o roubo de dados foram os impactos mais comuns na região (27% dos casos), com perda financeira em 20% dos casos. Os vazamentos e a destruição de dados empataram em terceiro lugar com 13% dos casos cada.

Os principais vetores de acesso inicial incluíram os serviços remotos externos (30%) e a exploração de aplicações de uso público (20%). Drive-by compromise, adições de hardware, contas de domínio válidas, contas locais válidas e anexos de spear phishing representaram 10% dos casos cada.

De todos os casos atendidos pelo X-Force na América Latina, o Brasil concentrou 67%, a Colômbia teve 17% e o México teve 8%. Peru e Chile dividiram os outros 8%.

Na América Latina, o Brasil concentrou 67% dos casos atendidos pelo X-Force.

5 | Oriente Médio e África

Para fins de relatório, a IBM considera que Oriente Médio e África incluem o Levante, a Península Arábica, o Egito, o Irã e o Iraque e todo o continente africano.

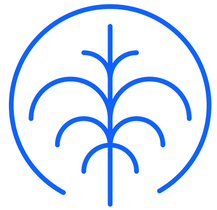
A implementação de backdoors foi detectada em 27% dos casos atendidos pelo X-Force nessa região em 2022. Ransomware e worms empataram como o segundo tipo de ataque mais comum (18% cada). Os ataques com extorsão e perda financeira representaram metade dos impactos identificados nos incidentes na região em 2021 (cada).

Os links de spear phishing foram usados para acesso inicial em dois terços dos casos, e a mídia removível foi responsável por um terço dos incidentes que o X-Force remediou no Oriente Médio e na África.

O setor de serviços financeiros e de seguros foi o mais atacado no Oriente Médio e na África em 2022, concentrando 44% dos incidentes. Esse percentual indica uma pequena queda em relação aos 48% de 2021. O setor de serviços profissionais, corporativos e para consumidores concentrou 22% dos ataques, e os setores de manufatura e energia empataram em terceiro lugar com 11%.

A Arábia Saudita teve dois terços dos casos na região atendidos pelo X-Force. Os outros casos ocorreram no Catar, nos Emirados Árabes Unidos e na África do Sul.

O ataque mais comum nessa região foi a implementação de backdoors (27% dos casos).



Tendências do setor

Pelo segundo ano consecutivo, o setor de manufatura foi o mais atacado, de acordo com os dados de resposta a incidentes do X-Force. O setor de serviços financeiros e de seguros perdeu o primeiro lugar por apenas um ponto percentual em 2021, após ocupar essa posição por cinco anos consecutivos. Em 2022, o setor ficou em segundo lugar novamente com uma grande margem de quase seis pontos percentuais.

Percentual de ataques por setor de 2018 a 2022

Indústria	2022	2021	2020	2019	2018
Manufatura	24,8%	23,2	17,7	8	10
Serviços financeiros e de seguros	18,9%	22,4	23	17	19
Serviços profissionais, corporativos e para consumidores	14,6%	12,7	8,7	10	12
Energia	10,7%	8,2	11,1	6	6
Varejo e atacado	8,7%	7,3	10,2	16	11
Educação	7,3%	2,8	4	8	6
Setor de saúde	5,8%	5,1	6,6	3	6
Governo	4,8%	2,8	7,9	8	8
Transportes	3,9%	4	5,1	13	13
Mídia e telecomunicações	0,5%	2,5	5,7	10	8

24,8%

dos casos de resposta a incidentes do X-Force ocorreram no setor de manufatura.

1 | Manufatura

O setor de manufatura foi o mais atacado e com uma margem um pouco maior em comparação com 2021. Em 2022, os backdoors foram implementados em 28% dos incidentes, superando o ransomware, que apareceu em 23% dos incidentes remediados pelo X-Force. O percentual de implementações de backdoor também foi resultado do pico de infecções com Emotet. Alguns desses casos poderiam ter resultado em ataques de ransomware, entre outras atividades maliciosas, mas foram identificados a tempo de serem remediados.

Os anexos de spear phishing e a exploração de aplicações de uso público ficaram empatados como os dois principais vetores de infecção (28% cada). Os serviços remotos externos ficaram em segundo lugar (14%), e os links de spear phishing e as contas padrão válidas empataram em terceiro lugar como acesso inicial em 10% dos casos.

A extorsão, vista em 32% dos casos, foi o principal impacto nas empresas de manufatura. O setor de manufatura é conhecido por ter pouca ou nenhuma tolerância ao tempo de inatividade, e essa intolerância faz a extorsão ser uma estratégia lucrativa para os invasores. O roubo de dados foi o segundo impacto mais comum (19%), seguindo pelos vazamentos de dados (16%). A região Ásia-Pacífico concentrou a maioria dos incidentes do setor de manufatura (aproximadamente 61% dos casos). A Europa e América do Norte ficaram empatadas em segundo lugar com 14%, a América Latina teve 8% e o Oriente Médio e a África tiveram 4%.

18,9%

dos casos de resposta a incidentes do X-Force ocorreram no setor serviços financeiros e seguros.

2 | Serviços financeiros e de seguros

As empresas de serviços financeiros e de seguros ficaram em segundo lugar e tiveram menos de um em cada cinco ataques atendidos pelo X-Force em 2022. Esse percentual indicou uma ligeira queda em relação aos anos anteriores porque outros setores, principalmente o de manufatura, começaram a ser atraentes para os invasores.

As empresas de serviços financeiros e de seguros costumam ser pioneiras em transformações digitais e adoção da nuvem em comparação com outros setores. Por isso, talvez os invasores precisem se esforçar mais para atacar essas empresas.

Os ataques de backdoor foram a ação sobre o objetivo mais observada (29%), seguidos por ransomware e maldocs (11% cada). O principal vetor de infecção foram os anexos de spear phishing, usados em 53% dos ataques a esse setor. A exploração de aplicações de uso público ficou em segundo lugar em 18% dos ataques, e os links de spear phishing foram o vetor de acesso inicial em 12% dos casos.

A Europa teve o maior volume de ataques a empresas do setor de serviços financeiros e de seguros (aproximadamente 33% de todos os ataques), e a região Ásia-Pacífico ficou logo atrás com cerca de 31%. A América Latina teve aproximadamente 15% dos incidentes atendidos pelo X-Force, e América do Norte, Oriente Médio e África tiveram cerca de 10% (cada).

14 , 6%

dos casos de resposta a incidentes do X-Force ocorreram no setor de serviços profissionais, corporativos e para consumidores.

3 | Serviços profissionais, corporativos e para consumidores

O setor de serviços profissionais inclui empresas de consultoria, empresas de gestão e escritórios de advocacia. Esses serviços concentram 52% das vítimas nesse segmento. Já os serviços corporativos incluem firmas, como serviços de TI e tecnologia, relações públicas, publicidade e comunicações. Esses serviços representam 37% das vítimas. Os serviços para consumidores, que incluem construtores, imobiliárias, artes, entretenimento e recreação, representaram 11% dos casos. Juntos, eles formam a categoria “Serviços profissionais, corporativos e para consumidores” do X-Force Threat Intelligence Index 2023.

Os serviços profissionais, corporativos e para consumidores foram alvo de ataques de ransomware e backdoor mais frequentemente (18% dos casos em cada serviço). Os dois principais vetores de infecção foram a exploração de aplicações de uso público e os serviços remotos externos (23% cada). Os anexos de spear phishing e as contas locais válidas foram a causa de 15% dos casos (cada).

A extorsão foi o impacto mais comum em 28% dos casos, e o roubo de dados, a coleta de credenciais e os vazamentos de dados representaram 17% (cada). O X-Force atendeu a 47% dos casos na Europa, 33% na América do Norte, 10% na região Ásia-Pacífico, 7% no Oriente Médio e na África e 3% na América Latina.

10,7%

dos casos de resposta a incidentes do X-Force ocorreram no setor de energia.

4 | Energia

As empresas de energia, que incluem empresas de fornecimento de energia elétrica e petróleo e gás, foram o quarto setor mais atacado (mesma colocação de 2021), com 10,7% dos ataques. A exploração de aplicações de uso público foi o vetor de infecção mais comum em 40% dos casos. Os links de spear phishing e os serviços remotos externos foram responsáveis por 20% dos casos (cada). Os botnets foram a ação sobre o objetivo mais frequente em 19% dos casos, e ransomware e BEC ficaram empatados em segundo lugar (15%).

Roubo de dados e extorsão foram identificados em 23% dos casos, seguidos pela coleta de credenciais e pelas infecções com botnet (15% cada). De todos os casos atendidos pelo X-Force no mundo inteiro, as empresas da América do Norte foram as vítimas mais comuns (46%) em comparação com a Europa e a América Latina (23% cada). Pouco menos de 5% dos casos ocorreram nas regiões Ásia-Pacífico e Oriente Médio e África.

O setor de energia continua sendo pressionado por várias forças internacionais, principalmente pelas que foram exacerbadas devido à guerra da Rússia contra a Ucrânia e aos reflexos no já tumultuado comércio de energia global.

8,7%

dos casos de resposta a incidentes do X-Force ocorreram no setor de varejo e atacado.

5 | Varejo e atacado

Os varejistas são responsáveis pela venda de produtos para consumidores e atacadistas. Os atacadistas geralmente são responsáveis pelo transporte e pela distribuição desses produtos das empresas de manufatura para os varejistas ou direto para os consumidores. O setor de varejo e atacado foi o quinto mais visado, de acordo com dados do X-Force IR, mantendo a posição do ranking de 2021.

O vetor de acesso inicial mais comum nos ataques ao setor de varejo e atacado foi e-mails de spear phishing com um link malicioso (33%). Serviços remotos externos comprometidos, spear phishing com anexos maliciosos e adições de hardware representaram 17% dos casos (cada).

Ransomware, backdoors e BEC foram as ações mais comuns dos invasores, sendo que cada uma representou 19% das atividades. Worms foram identificados em 10% dos casos. A extorsão das vítimas ocorreu em 50% dos casos, e coleta de credenciais e perda financeira ocorreram em 25% dos casos (cada). A América do Norte e a América Latina concentraram a maioria dos casos (39% em cada região) em comparação com a Europa (22%).

7,3%

dos casos de resposta a incidentes do X-Force ocorreram no setor de educação.

6 | Educação

Os incidentes no setor de educação envolveram casos de backdoor em 20% dos ataques atendidos pelo X-Force. Ransomware, adware e spam representaram 13% (cada). A exploração de aplicações de uso público foi o acesso inicial mais observado em 42% dos casos, seguida pelos anexos de spear phishing (25%). Phishing por meio de serviço ou link e violação de conta local e nuvem válida representaram 8% dos vetores de acesso inicial (cada). Roubo de dados, vazamento de dados, extorsão e reconhecimento foram os impactos em 25% dos casos (cada). A região Ásia-Pacífico concentrou 67% dos casos, a América do Norte teve 27% e a América Latina teve 6%.

5,8%

dos casos de resposta a incidentes do X-Force ocorreram no setor de saúde.

7 | Setor de saúde

O setor de saúde caiu para o sétimo lugar entre os 10 principais setores, em comparação com o sexto lugar em 2021. A proporção de casos do setor de saúde atendidos pelo X-Force manteve o percentual de 5% a 6% nos últimos três anos. Ataques de backdoor ocorreram em 27% dos casos, e web shells em 18%. Adware, BEC, mineração de criptomoedas, carregadores, ferramentas de reconhecimento e verificação e ferramentas de acesso remoto representaram 9% dos casos (cada). O reconhecimento foi responsável pela maioria dos impactos observados (50%), e o roubo de dados e a mineração de moedas digitais foram identificados em 25% dos casos (cada).

Os alvos na Europa concentraram 58% dos incidentes, e os casos na América do Norte foram responsáveis pelos outros 42%.

4,8%

dos casos de resposta a incidentes do X-Force ocorreram no setor de governo.

8 | Governo

Os governos também foram um dos principais alvos dos backdoors, representando 25% dos casos do X-Force IR. Esse percentual ficou empatado com os ataques DDoS, que também representaram um quarto dos casos. As variadas informações confidenciais nas redes do setor público são um alvo comum das campanhas de espionagem cibernética. Essas informações podem incluir bancos de dados de PII abrangente e outras informações que podem ser usadas por grupos patrocinados por governos ou vendidas por cibercriminosos para fins lucrativos. Maldocs foram identificados em 17% dos casos, e mineração de criptomoedas, ferramentas de aquisição de credenciais, ransomware e web shells foram responsáveis pelos outros 83%.

De todos os casos nesse setor, o X-Force conseguiu vincular incidentes a cibercriminosos, ameaças internas que levaram à destruição de dados, hacktivismo e grupos de ameaças que conduzem espionagem patrocinados por governos (na mesma proporção).

A exploração de aplicações de uso público e os anexos de spear phishing foram os principais vetores de infecção (40% cada), e a violação de contas padrão válidas representou 20% dos casos. As entidades governamentais na região Ásia-Pacífico foram as mais atacadas (50% dos casos). Na Europa, esse percentual foi 30%, e na América do Norte foi 20%.

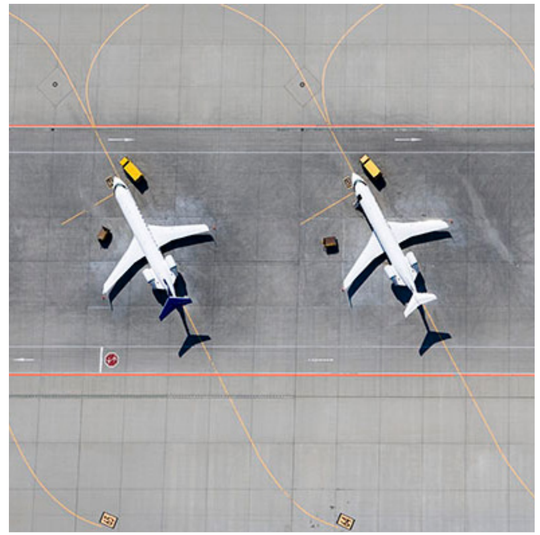
3,9%

dos casos de resposta a incidentes do X-Force ocorreram no setor de transportes.

9 | Transportes

Após ocupar a sétima posição em 2021, o setor de transportes voltou à nona posição de 2020. No entanto, o setor ainda concentrou o mesmo percentual de incidentes atendidos pelo X-Force. O phishing foi o vetor de acesso inicial mais comum em 51% dos casos (distribuídos de forma igualitária entre links, anexos e spear phishing como serviço). A violação de contas locais válidas representou 33% dos vetores de acesso inicial, e as contas de nuvem válidas serviram como ponto de entrada em 17% dos casos. As principais ações sobre os objetivos foram acesso ao servidor e implementação de ferramentas de acesso remoto (25% cada), seguidas por campanhas de spam, ransomware, backdoors e deface em 13% dos casos (cada).

O roubo de dados foi mais comum em 50% dos casos, e a extorsão e os impactos na reputação da marca representaram 25% dos casos (cada). As entidades de transporte na Europa foram as mais atacadas, concentrando 62% dos casos, e a região Ásia-Pacífico ficou em segundo lugar com pouco mais de 37% dos casos.



0,5%

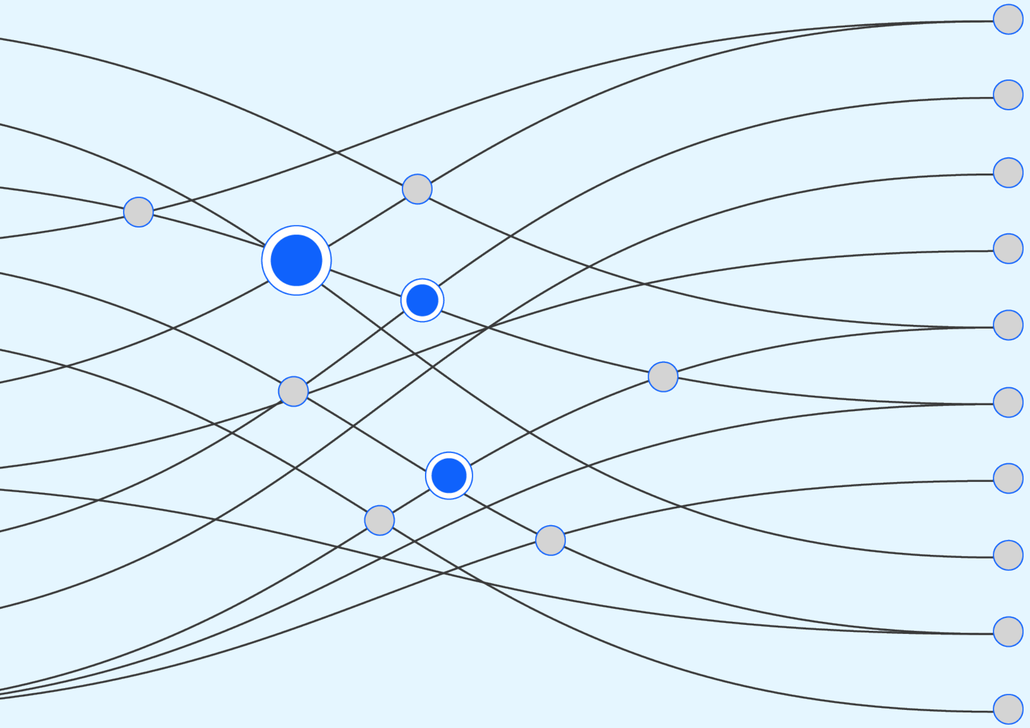
dos casos de resposta a incidentes do X-Force ocorreu no setor de mídia e telecomunicações.

10 | Mídia e telecomunicações

O setor de mídia e telecomunicações representou uma pequena fração dos incidentes atendidos pelo X-Force, ficando em último lugar pelo segundo ano consecutivo. As violações de serviços remotos externos, como VPNs e outros mecanismos de acesso, e de contas de domínio válidas foram os vetores de infecção observados. Esses vetores facilitaram ataques de ransomware. As ações observadas nesses casos incluíram a implementação de ransomware e de ferramentas de exfiltração de dados. Essas ações resultaram em roubo, vazamento, destruição e extorsão de dados.

12

Recomendações



Siga as recomendações abaixo para proteger sua empresa contra ameaças maliciosas, incluindo as apresentadas neste relatório.

Gerencie seus ativos: o que temos? O que queremos proteger? Quais dados são críticos para nosso negócio? Essas são as primeiras perguntas que uma equipe de segurança deve responder para criar uma proteção eficiente. Priorizar a descoberta de ativos no seu perímetro, entender sua exposição a ataques de phishing e reduzir essas superfícies de ataque também contribui para uma segurança holística. Além disso, as empresas precisam ampliar os programas de gerenciamento de ativos para incluir código-fonte, credenciais e outros dados que talvez já existam na internet ou na dark web.

Conheça seu adversário: embora muitas empresas tenham um panorama abrangente do cenário de ameaças, o X-Force recomenda adotar uma visão que coloque em evidência os agentes de ameaça com mais probabilidade de atacar seu setor, sua empresa ou sua região. Essa perspectiva inclui entender como esses agentes de ameaça operam, identificar o nível de sofisticação e conhecer as táticas, as técnicas e os procedimentos com mais probabilidade de serem empregados.

Gerencie a visibilidade: após entender mais sobre os adversários com maior probabilidade de realizar ataques, as empresas precisam confirmar que têm visibilidade apropriada das fontes de dados que podem indicar a presença de um invasor. Manter a visibilidade em pontos estratégicos da empresa e garantir que alertas sejam disparados e resultem em ações rápidas são medidas críticas para interromper a ação dos invasores antes que eles causem disrupções.

Conteste suposições: as empresas precisam admitir que já sofreram algum comprometimento. Dessa forma, as equipes podem fazer novas análises continuamente para identificar o seguinte:

- Como os invasores se infiltram nos sistemas
- Como os recursos de detecção e resposta estão protegendo contra as mudanças nas táticas, nas técnicas e nos procedimentos
- O nível de dificuldade para um provável adversário comprometer seus dados e sistemas mais críticos

As equipes de segurança mais eficientes fazem testes de ataque frequentes que incluem busca de ameaças, teste de penetração e teste red teaming com base em objetivos para detectar ou validar caminhos de ataque oportunistas nos ambientes.

Use a inteligência: aplique a inteligência de ameaça a tudo que você fizer. Com a aplicação eficiente da inteligência de ameaça, você pode analisar caminhos de ataque comuns e identificar as principais oportunidades para mitigar ataques muito utilizados. Isso também ajuda a desenvolver oportunidades de detecção de alta fidelidade. A aplicação da inteligência de ameaça deve ser combinada com o entendimento dos seus adversários e de como eles operam.

Prepare-se: os ataques são inevitáveis, mas as falhas podem ser evitadas. As empresas devem desenvolver planos de resposta a incidentes personalizados para o ambiente. Esses planos devem ser testados e modificados regularmente sempre que houver mudanças para melhorar o tempo de resposta, remediação e recuperação.

Trabalhar com um fornecedor de resposta a incidentes confiável reduz o tempo necessário para conseguir profissionais com qualificação para mitigar um ataque. Além disso, incluir seu fornecedor de resposta a incidentes no desenvolvimento e no teste do plano de resposta é essencial e contribui para uma resposta mais eficiente.
Os melhores planos de resposta a incidentes envolvem vários departamentos, incorporam stakeholders fora do departamento de TI e testam as linhas de comunicação entre as equipes técnicas e a equipe de liderança sênior. Por fim, testar seu plano em um exercício de cyber range imersivo e de alta pressão pode melhorar muito a capacidade de reagir a um ataque.

Reforce a segurança com estas ações:

- [ ] Gerencie seus ativos
- [ ] Conheça seu adversário
- [ ] Gerencie a visibilidade
- [ ] Conteste suposições
- [ ] Use a inteligência
- [ ] Prepare-se

Sobre

IBM Security X-Force

O IBM Security X-Force é uma equipe de hackers, agentes de resposta, pesquisadores e analistas centrados em ameaças. O portfólio do X-Force inclui produtos e serviços de ataque e defesa, alimentados por uma visão de 360 graus das ameaças.

Nesta era de sucessivos ataques cibernéticos, em que tudo está conectado e as regulações continuam aumentando, as empresas precisam de uma abordagem de segurança focada. O X-Force acredita que a ameaça deve ser o ponto focal. Por meio de serviços de teste de penetração, gerenciamento de vulnerabilidades e simulação de adversários, a equipe de hackers do X-Force Red se coloca no lugar dos agentes de ameaça para encontrar as vulnerabilidades que expõem seus ativos mais importantes. Com a preparação, a detecção e a resposta aos incidentes, além dos serviços de gerenciamento de crise, a equipe do X-Force Incident Response sabe onde as ameaças se escondem e como elas podem ser interrompidas. Os pesquisadores do X-Force criam técnicas ofensivas para detecção e prevenção de ameaças, e os analistas do X-Force coletam e transformam dados de ameaças em informações práticas para reduzir os riscos.

O X-Force entende profundamente como os agentes de ameaça pensam, planejam e atacam, o que ajuda você a prevenir, detectar, responder e se recuperar de incidentes para focar nas suas prioridades de negócios.

Se sua organização precisar de suporte para fortalecer a abordagem de segurança, agende uma conversa individual com um especialista do IBM Security X-Force.

Marque uma consultoria →

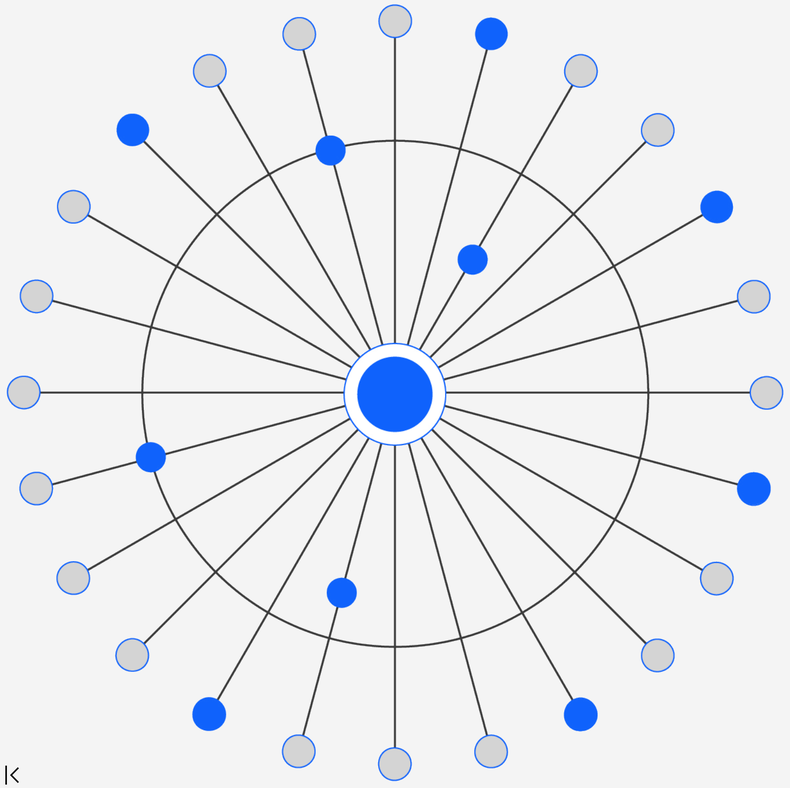
IBM Security

O IBM Security se adapta à sua área de cobertura e trabalha com você para encontrar o caminho mais adequado. Com nossos recursos dinâmicos de IA e automação, ajudamos você a ficar sempre um passo à frente com mais velocidade e precisão. Tenha a certeza de que você está tomando as medidas certas para as necessidades atuais e futuras com os insights da nossa equipe confiável que inclui os melhores especialistas do setor. Da previsão de ameaças à proteção de dados, trabalhando com vários fornecedores ou em diversas partes do mundo, seja quais foram os objetivos da sua empresa, o IBM Security pode ajudar você a alcançar metas de negócios ambiciosas, explorando novas tecnologias inovadoras e minimizando ameaças inesperadas.

Saiba mais →

14

Colaboradores



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

15

Apêndice

Lista de impactos

Impactos	Impactos
Botnet	Mineração de moedas digitais
Reputação da marca	Espionagem
Coleta de credenciais	Extorsão
Destruição de dados	Perda financeira
Vazamento de dados	Produção interrompida (TO)
Roubo de dados	Reconhecimento

1. “A timeline of the biggest ransomware attacks”, CNET, 15 de novembro de 2021
2. “International action against DD4BC cybercriminal group”, Europol, 12 de janeiro de 2016
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion”, Recorded Future, 7 de dezembro de 2015
4. “A Brief History of Ransomware.” Varonis, 10 de novembro de 2015
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild”, MalwardBytes Labs, 8 de dezembro de 2015
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware”, Crowdstrike, 14 de novembro de 2018
7. “Operators of SamSam Continue to Receive Significant Ransom Payments”, Crowdstrike, 11 de abril de 2018
8. “Triple Extortion Ransomware: The DDoS Flavour”, PacketLabs, 12 de maio de 2022
9. “They Told Their Therapists Everything. Hackers Leaked It All”, Wired, 4 de maio de 2021
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike”, The DFIR Report, 1º de agosto de 2021
11. “Diavol Ransomware”, The DFIR Report, 13 de dezembro de 2021
12. “Quantum Ransomware”, The DFIR Report, 25 de abril de 2022
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks”, Kroll, 6 de junho de 2022
14. “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming”, Proofpoint, 28 de abril de 2022
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated)”, Unit 42, 3 de junho de 2022
16. “AdvIntel’s State of Emotet aka “SpmTools” Displays Over Million Compromised Machines Through 2022”, AdvIntel, 13 de setembro de 2022
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack”, NCC Group, 19 de agosto de 2022
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack”, NCC Group, 19 de agosto de 2022

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP

Produzido nos Estados Unidos da América
Fevereiro de 2023