NÚMERO 81 | AGOSTO 2023

NTT DATA
Trusted Global Innovator

Radar

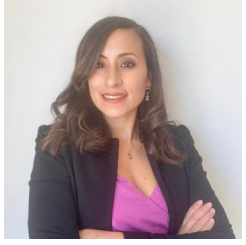
A revista de cibersegurança

CIBERSEGURIDAD, OBJETIVO ESTRATÉGICO.

Na era digital em que estamos vivendo, a cibersegurança se tornou um objetivo estratégico vital para pessoas, empresas e governos do mundo todo. Conforme a tecnologia avança e nossas vidas se tornam cada vez mais dependentes dos sistemas informáticos e das redes interconectadas, aumentam, também, os riscos associados à segurança da informação e à proteção de dados sensíveis. A cibersegurança passou a ser fundamental e estratégica, tanto a nível individual, quanto a nível global, por uma série de motivos:

1. Em primeiro lugar, devido ao crescimento exponencial das ameaças cibernéticas. Os cibercriminosos desenvolveram técnicas sofisticadas de infiltração em sistemas informáticos e redes, roubando informações confidenciais, causando danos à infraestrutura digital e interrupções significativas nas operações do nosso cotidiano. Esses ataques podem trazer consequências devastadoras, tanto econômicas como políticas. De roubos de identidade e fraudes financeiras até sabotagem de infraestruturas críticas ou espionagem cibernética. Consequentemente, os riscos são muitos e estão constantemente evoluindo. Portanto, deve-se prevenir e mitigar esses ataques, resguardando os interesses das organizações e das nações.
2. Em segundo lugar, devido ao aumento da interconectividade global. Atualmente, estamos mais conectados do que nunca graças à expansão da Internet e das redes digitais. Isso, obviamente, gerou novas oportunidades para o comércio, a colaboração e a comunicação, mas criou, também, uma superfície de ataque mais ampla, complexa e dinâmica para os cibercriminosos. As organizações e os governos dependem cada vez mais das tecnologias da informação e da comunicação para conduzir suas atividades diárias. Portanto, a cibersegurança se tornou um componente estratégico para proteger a integridade, confidencialidade e disponibilidade dos dados em um ambiente tão interconectado globalmente.
3. Em terceiro lugar, devido às implicações políticas e geopolíticas. Os ciberataques podem ter consequências para além do âmbito econômico, afetando a segurança nacional e as relações internacionais. É preciso que os governos e as organizações protejam suas infraestruturas críticas (redes elétricas, sistemas de transporte, redes de comunicação etc.) contra possíveis ataques cibernéticos que poderiam pôr em perigo a estabilidade e a segurança de um país. Além disso, os atores estatais e não estatais podem utilizar o ciberespaço como uma ferramenta para espionagem, desinformação e influência política. Portanto, a cibersegurança é necessária para proteger os interesses nacionais e garantir a estabilidade geopolítica.
4. Em quarto lugar, devido à proteção da privacidade e dos direitos individuais. À medida em que coletamos e compartilhamos cada vez mais informações pessoais on-line, é fundamental proteger a privacidade e garantir que os dados confidenciais não caiam em mãos erradas. As pessoas têm o direito de manter o controle sobre suas informações e de se protegerem contra o roubo de identidade, o assédio on-line, além de outras formas de abuso virtual. Portanto, a cibersegurança deve assegurar a confiança no mundo digital e proteger os direitos e liberdades fundamentais de todos.

Em suma, estamos diante de um panorama em que a cibersegurança se encontra incorporada dentro de nossas vidas, tanto no âmbito pessoal quanto no profissional, sendo essencial e estratégica em nossa sociedade digital. O crescimento das ameaças cibernéticas, a interconectividade global, as implicações políticas e geopolíticas, bem como a proteção da privacidade e dos direitos individuais têm impulsionado a necessidade de priorizá-la no âmbito digital. É por isso que tanto as organizações quanto os governos devem investir em medidas de cibersegurança efetivas para se proteger e proteger as pessoas contra os ciberataques, além de garantir a confiança e a estabilidade no mundo digital que está em constante evolução.



Andrea Isabel Muñoz Parreño
Manager de Cibersegurança en NTT DATA Ecuador

CIBERCRÔNICA

Nesta edição, falaremos sobre a ascensão dos novos vetores de entrada que estão surgindo a partir da criação de novas ferramentas baseadas em inteligência artificial e demais inovações. Focaremos nas extensões para navegadores já conhecidas.

Os vetores de entrada em cibersegurança se referem aos pontos de acesso a sistemas e redes que podem ser explorados por cibercriminosos para realizar ataques maliciosos.

Da inteligência artificial e o blockchain até a computação em nuvem, estas inovações vem transformando setores inteiros e abrem um leque de possibilidades sem precedentes. No entanto, com o progresso tecnológico, surgem também desafios relacionados à segurança.

> “El Instituto Nacional de Ciberseguridad de España advierten de que algunos usuarios malintencionados podrían utilizar ChatGPT con fines delictivos.”

É nítida a ascensão que a inteligência artificial teve neste ano de 2023. A partir da aparição do ChatGPT, têm surgido diversas ferramentas que utilizam inteligência artificial (IA). Dentre elas, encontram-se as extensões para navegadores e aplicativos web que permitem a realização de tarefas de forma muito mais rápida, como a busca de informações, redações de textos específicos ou edição de fotos. Entretanto, esse aumento no surgimento de ferramentas supõe também um aumento no risco de que tais aplicativos contenham malware que consiga acessar as informações dos nossos dispositivos.

Recentemente, os especialistas em segurança da empresa Kolide conduziram um estudo que demonstrou que muitas dessas extensões IA foram desenvolvidas para roubar informações dos usuários. Isso não é nenhuma novidade, mas há uma enorme tendência atualmente sobre o uso deste tipo de ferramenta.

Em março de 2023, guard.io analisou e relatou uma ferramenta chamada “ uick access to Chat GPT”, que estava invadindo as contas dos usuários por meio de coleta de cookies de seus navegadores. A Google está reagindo no caso de seu navegador (Google Chrome), buscando filtrar e eliminar rapidamente essas ferramentas de seu Marketplace de extensões. No entanto, a grande demanda por essas ferramentas faz com que a detecção de todos os aplicativos mal-intencionados sendo lançados e disponibilizados aos usuários dia após dia seja uma tarefa complexa. O risco reside, também, no fato de que um grande número de usuários pode realizar o download, instalar e utilizar essas ferramentas enquanto os navegadores demoram para eliminar essas extensões.

Outro aspecto importante é a tentativa de desenvolver uma extensão ou ferramenta de forma rápida, a fim de que esta chegue primeiro ao mercado. Isso faz com que muitos aplicativos, embora não tenham sido desenvolvidos com más intenções, contenham muitas vulnerabilidades de código, já que, nesse processo rápido de desenvolvimento, é comum que não seja dada tanta importância à segurança, deixando diversas falhas em relação à privacidade.

Dito isso, ao adicionar uma extensão ao nosso navegador, é essencial nos certificarmos de que a fonte que desenvolveu essa ferramenta seja confiável e tenha sido aprovada pelas entidades que a distribuem.

Falando diretamente sobre o uso do ChatGPT, o Instituto Nacional de Cibersegurança da Espanha adverte que alguns usuários mal-intencionados poderiam utilizar o ChatGPT com fins ilegais, já que, como acontece com outras ferramentas, “existem vários vetores de ataque que os cibercriminosos podem aproveitar para explorar vulnerabilidades e atacar possíveis vítimas”.

Ainda que o ChatGPT possua protocolos de segurança que o impedem de atender a certas solicitações e responder a perguntas mal-intencionadas, ele pode permitir que alguém sem conhecimentos técnicos desenvolva roteiros e realize todo tipo de ataque, contornando as restrições existentes. Além disso, voltando às ferramentas e extensões, muitos destes aplicativos podem auxiliar o usuário com essas intenções, reformulando suas perguntas ou realizando testes que permitam tornar esses controles vulneráveis.

Segundo o INCIBE, os cibercriminosos poderiam obter, por meio da ferramenta, informações mais específicas sobre a empresa que desejam atacar. Dessa forma, fazem com que a mensagem seja mais crível e haja mais possibilidades de que a vítima “morda a isca”, referindo-se aos ataques de spoofing e phishing.

Em suma, como acontece a cada vez que uma nova tecnologia é disponibilizada no mercado, novas vulnerabilidades e vetores de ataque estão surgindo. Isso fará com que sejam criados novos requisitos de segurança para o desenvolvimento, análise e disponibilização de ferramentas que contenham essas tecnologias. Mais uma vez, inicia-se uma corrida entre os cibercriminosos, que tentam se aproveitar das vulnerabilidades, e os especialistas em cibersegurança, que tentam manter os usuários protegidos contra elas.

SEGURANÇA E MALWARE EM DISPOSITIVOS INTELIGENTES

Por: NTT DATA Europe & Latam

Na era da tecnologia conectada, os dispositivos inteligentes se tornaram parte integral de nossas vidas. Dos telefones e relógios inteligentes aos televisores e eletrodomésticos conectados à Internet, tais dispositivos nos oferecem conforto e eficiência para realizar nossas tarefas diárias. No entanto, apesar dos benefícios oferecidos, há também uma preocupação crescente: os dispositivos inteligentes se tornaram alvo para os cibercriminosos. Neste artigo, iremos explorar essa preocupação e analisar por que é tão importante nos conscientizarmos quanto aos riscos associados a estes dispositivos.

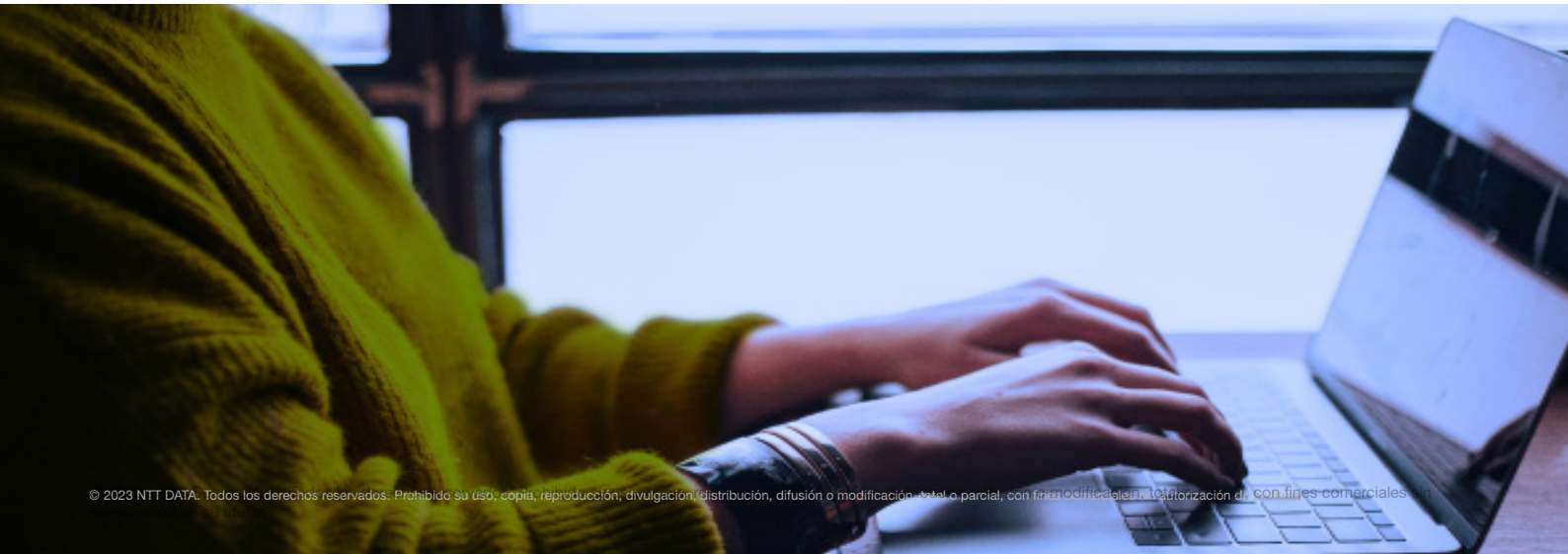
A ascensão dos dispositivos inteligentes:

A ascensão dos dispositivos inteligentes nos últimos anos impressiona. A conectividade dos dispositivos levou à ascensão de tecnologias como a internet das coisas (Internet of Things - IoT), que permite que múltiplos dispositivos se comuniquem e compartilhem informações entre si. Este avanço trouxe melhorias para nosso cotidiano, possibilitando um maior controle e acesso remoto aos nossos bens e serviços.

Os riscos de segurança:

Contudo, com um número cada vez maior de dispositivos inteligentes em nossos lares e vidas, presenciamos também um aumento nos riscos de segurança associados. Os cibercriminosos se aproveitam das vulnerabilidades presentes nesses dispositivos para obter acesso às nossas informações pessoais e financeiras, monitorar nossas atividades e, em alguns casos, até mesmo assumir o controle dos dispositivos.

Uma das principais preocupações é a falta de segurança no design e fabricação de tais dispositivos. Muitos fabricantes não dão atenção suficiente à proteção dos dados ou à implementação de medidas de segurança robustas, chegando a descumprir, em alguns casos, os padrões de segurança estabelecidos, o que expõe os usuários a ataques cibernéticos que podem ter consequências devastadoras.
Além disso, os dispositivos inteligentes frequentemente se conectam a redes Wi-Fi, que também podem estar vulneráveis a invasões. Senhas fáceis ou a falta de atualizações de segurança podem tornar as redes domésticas alvos fáceis para os cibercriminosos.
Isso pode levar à perda de informações pessoais muito sensíveis, desde localizações e rotas registradas no GPS, informações bancárias ou de saúde… podendo chegar à exposição e o monitoramento de hábitos pessoais.



Os últimos golpes identificados

O presente “surpresa”

Recentemente, um padrão preocupante foi detectado. Algumas pessoas recebem pacotes surpresa que contém aparelhos como fones de ouvido sem fio, smartwatches, smartbands, entre outros dispositivos similares. No entanto, por trás deste gesto aparentemente gentil, se esconde um segredo perigoso.

Estes dispositivos contêm malware, um software malicioso projetado para comprometer a privacidade e segurança dos usuários. Uma vez que estes dispositivos são vinculados a outros equipamentos, o malware é ativado silenciosamente, permitindo que os criminosos tenham acesso a informações pessoais e confidenciais, sem o conhecimento ou consentimento das pessoas afetadas.

Este malware pode conseguir acesso tanto à voz como às câmeras, o que permite aos golpistas acessar conversas e contas vinculadas aos relógios inteligentes (GPS, métodos de pagamento e mensagens).

Caso você receba um pacote indesejado contendo algum dispositivo eletrônico, as autoridades recomendam que esses dispositivos não sejam ativados e que você entre em contato ou entregue o pacote imediatamente à polícia.
Esses produtos também podem ser utilizados para a prática de brushing, que consiste no envio, por correio, de produtos não solicitados, geralmente falsificados, a pessoas aparentemente aleatórias, para permitir que as empresas escrevam críticas positivas em nome do destinatário, o que as permite competir com produtos já estabelecidos.

Prevenção e recomendações

Embora não exista uma segurança absoluta, há algumas medidas que os usuários podem tomar para que estejam protegidos dos cibercriminosos. Algumas recomendações essenciais são:

- Dispositivos atualizados: Certifique-se de instalar as atualizações de software e firmware mais recentes nos seus dispositivos inteligentes. Essas atualizações costumam conter correções de segurança importantes.
- Senhas sólidas: Utilize senhas fortes e únicas para seus dispositivos e redes Wi Fi. Evite senhas pré-definidas ou fáceis de serem descobertas.
- Redes seguras: Configure sua rede Wi-Fi doméstica com medidas de segurança adequadas, como criptografia WPA2 e um nome de rede único.
- Pesquisa prévia: Antes de comprar um dispositivo inteligente, pesquise sobre a reputação do fabricante com relação à segurança e privacidade. Escolha aqueles que levam esses aspectos a sério. Comprove as localizações e padrões de segurança reconhecidos e aplicados pelo fabricante.
- Proteção de dados: Certifique-se de ler e compreender as políticas de privacidade e os termos de serviço dos dispositivos e aplicativos utilizados. Considere limitar o acesso a informações pessoais somente às funções necessárias.

TENDÊNCIAS

A ascensão dos malwares em dispositivos móveis e outras preocupações

Na atual era digital, os dispositivos móveis se tornaram uma parte integral das nossas vidas, trazendo conectividade, comodidade e acesso a uma grande variedade de aplicativos e serviços. No entanto, essa crescente dependência também deu lugar a um aumento nos riscos e ameaças cibernéticas que afetam os dispositivos móveis.

Os especialistas preveem um aumento drástico em relação às ameaças à segurança móvel em 2023. Segundo um relatório recente da Cybersecurity Ventures, espera-se que o número de ameaças à segurança móvel cresça mais de 500% nos próximos três anos.

Os malwares para dispositivos móveis tem evoluído rapidamente. Normalmente, os cibercriminosos se concentravam na falta de controles de segurança dos sistemas operacionais e nos controles limitados dos mercados de aplicativos para praticar atividades maliciosas. Todavia, à medida que estas áreas evoluem, os agentes maliciosos estão aplicando técnicas e táticas do panorama geral de ameaças ao mundo dos dispositivos móveis.

O número de fraudes, roubos de identidade, interrupção de serviços e roubos de credenciais segue aumentando apesar dos esforços dos fornecedores de hardware e software em implementar contramedidas para combater esses ataques. Isso se deve, principalmente, à dificuldade em se manter o equilíbrio entre o humano e os sistemas durante a execução dos processos. Esse fator humano, inerente nesses dispositivos, sempre será o foco dessas atividades maliciosas nos vetores de entrada, permitindo o uso de técnicas mais sofisticadas que podem comprometer, entre outros aspectos, as chaves das identidades digitais armazenadas no dispositivo móvel.

Nos últimos anos, por exemplo, o malware Pegasus tem sido um tema recorrente nos portais de notícias, deixando a comunidade de segurança informática em alerta. Desenvolvido pela empresa israelense NSO Group, o Pegasus é um software espião avançado criado para dispositivos móveis que tem sido utilizado para investigar jornalistas, políticos, ativistas dos direitos humanos e pessoas de interesse no mundo todo.

Uma das características mais alarmantes do Pegasus é sua capacidade de infectar dispositivos sem o fator humano mencionado acima, se aproveitando de vulnerabilidades nos sistemas operacionais móveis. Uma vez instalado em um dispositivo, o malware pode coletar informações confidenciais, como mensagens de texto, e-mails, gravações de chamadas, localizações de GPS e senhas.

Embora seja difícil controlar esse tipo de ataque cibernético avançado patrocinado pelo Estado, sem dúvida há vetores de ataque que podem ser detidos, como o smishing ou o malware mais comum em dispositivos móveis. No vasto ecossistema dos aplicativos móveis, as lojas oficiais, como o Google Play, têm sido tradicionalmente consideradas como ambientes seguros e perfeitamente confiáveis para baixar aplicativos. No entanto, tem-se demonstrado nos últimos tempos que elas não utilizam métodos infalíveis para evitar o envio de aplicativos fraudulentos, havendo um crescimento alarmante da presença de malwares dentro dessas lojas.

Recentemente, o malware Clicker se infiltrou na Google Play se passando por ferramentas de utilidade como lanternas, leitores de código QR, câmeras, conversores de unidades ou gestores de tarefas. Esse tipo de cavalo de troia realiza fraudes publicitárias, por meio de conexões recorrentes a sites em segundo plano, permitindo que cibercriminosos obtenham acessos através de anúncios e cliques. Ao todo, esse cavalo de troia teria sido confirmado em 16 aplicativos considerados seguros e disponibilizados no Google Play, somando mais de 20 milhões de downloads.

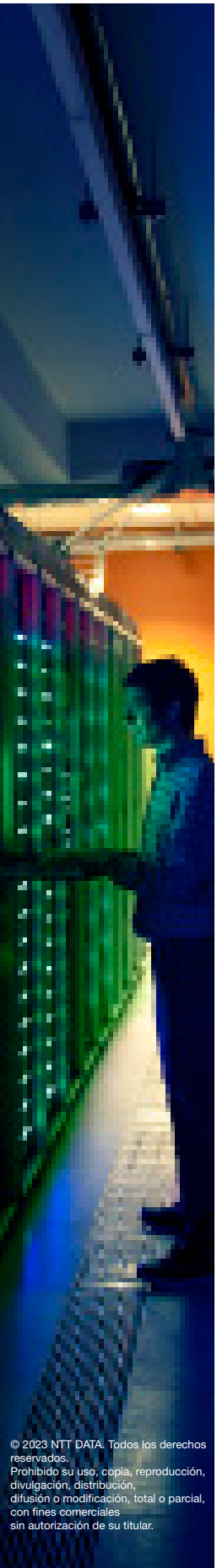
Embora os usuários precisem se conscientizar quanto aos riscos potenciais e adotar medidas para proteger seus dispositivos, também é essencial que os desenvolvedores assumam a liderança na hora de garantir a segurança de seus aplicativos. Isso pode incluir a aplicação de melhores medidas de segurança, como a autenticação de dois fatores ou a criptografia, visando manter os usuários protegidos. Além disso, é necessário considerar sempre esse fator humano e buscar implementar medidas adicionais que evitem maiores danos em caso de falhas.

Esse aumento das ameaças à segurança móvel se deve ao maior uso dos dispositivos móveis para atividades sensíveis, como operações bancárias e compras. Com o passar dos anos e as melhorias desse tipo de dispositivo, há cada vez mais pessoas que utilizam exclusivamente o aparelho móvel e não possuem um computador pessoal. Por outro lado, a ascensão do mundo da IoT vem aumentando exponencialmente o potencial das ameaças cibernéticas voltadas aos dispositivos móveis, visto que, inicialmente, eram sistemas que tinham por objetivo oferecer esse tipo de tecnologia ao menor custo, abrindo mão da segurança para torná-los mais baratos e favorecendo o desenvolvimento de diversos vetores de entrada.

Essas previsões evidenciam a necessidade de aumentar as medidas de segurança móvel. Por isso, é essencial compreender as ameaças potenciais e adotar medidas para se proteger com a colaboração de usuários e desenvolvedores, mantendo seus dispositivos seguros e protegidos. Como em qualquer âmbito da cibersegurança, a defesa está sempre um passo atrás do ataque. Por isso, é extremamente importante cobrir o maior número possível de gaps que possam servir como vetor de entrada.

VULNERABILIDADES

Receba nosso boletim completo de correções e vulnerabilidades assinando nosso boletim informativo **aquí**.



Linux

CVE-2023-3269
Data: 11/07/2023

Descrição. No último 11 de julho, foi divulgada uma vulnerabilidade que afeta o subsistema de gestão de memória do kernel do Linux.

A vulnerabilidade ocorre pois a gestão de bloqueios para acesso e atualização de áreas de memória virtual (VMA) é incorreta, o que pode causar problemas após a liberação da memória. Esta vulnerabilidade pode ser explorada para executar código arbitrário do kernel, escalar contêineres e, além disso, obter privilégios de root.

Link: https://my.f5.com/manage/s/article/K000135446?utm_source=f5support&utm_medium=RSS
https://www.ccn-cert.cni.es/component/vulnerabilidades/view/34489.html
https://www.cve.org/CVERecord?id=CVE-2023-3269

Produtos envolvidos. Kernel do Linux para distribuição do Fedora, todas as versões foram afetadas

Solução: Atualizar para a versão mais recente.

FortiOS/FortiProxy

CVE-2023-33308
Data: 11/07/2023

Descrição. Uma vulnerabilidade crítica no FortiOS e FortiProxy foi divulgada. Esta vulnerabilidade de transbordamento baseada em pilha permite que um invasor remoto execute códigos ou comandos arbitrários por meio de pacotes especificamente preparados para alcançar políticas de proxy ou de firewall com modo proxy junto a uma inspeção profunda de pacotes SSL.No mesmo dia em que a vulnerabilidade crítica foi detectada, patches de segurança foram lançados para que as correções necessárias no FortiOS y FortiProxy fossem implementadas

Link: https://www.cisa.gov/news-events/alerts/2023/07/11/fortinet-releases-security-update-fortios-and-fortiproxy
https://www.fortiguard.com/psirt/FG-IR-23-183

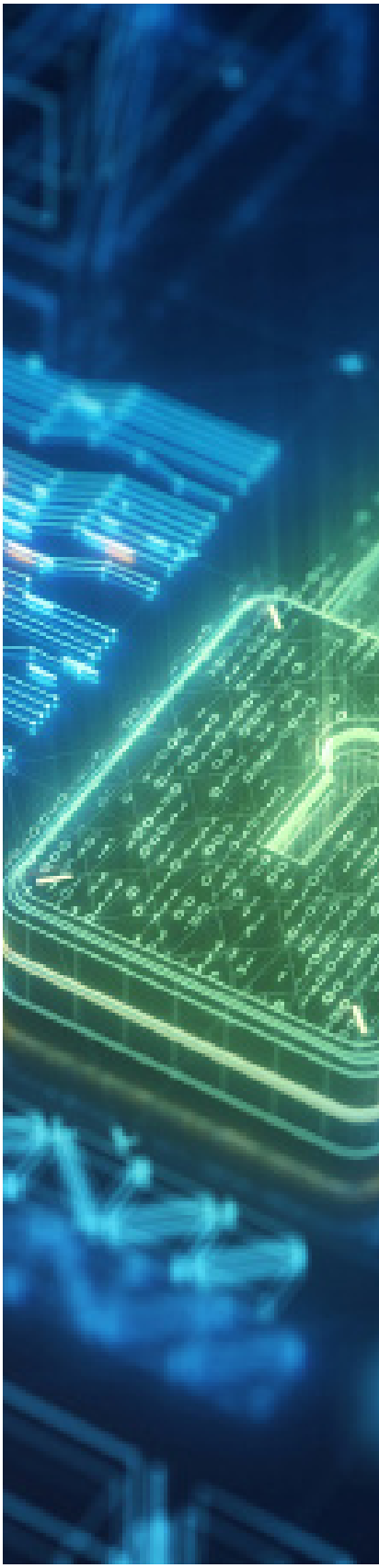
Produtos envolvidos. Os recursos afetados por esta vulnerabilidade são os seguintes:

- FortiOS versão 7.2.0 a 7.2.3.
- FortiOS versão 7.0.0 a 7.0.10.
- FortiProxy versão 7.2.0 a 7.2.2.
- FortiProxy versão 7.0.0 a 7.0.9.

Solução: Os seguintes patches foram disponibilizados pelo fabricante:

- Atualizar a FortiOS versão 7.2.4 ou superior.
- Atualizar a FortiOS versão 7.0.11 ou superior.
- Atualizar a FortiProxy versão 7.2.3 ou superior.
- Atualizar a FortiProxy versão 7.0.10 ou superior.

PARCHES



Adobe

Data: 11-07-2023

Descrição. A Adobe publicou uma atualização de segurança para o Adobe ColdFusion, a fim de corrigir vulnerabilidades críticas e altas encontradas em abril de 2023.Confira abaixo os detalhes das vulnerabilidades de segurança crítica:

- CVE-2023-29298: By-pass do controle de acesso no qual se permite a passagem para diferentes rotas de administrador a partir de origens não autorizadas.
- CVE-2023-29300: Desserialização de dados não confiáveis que acaba gerando uma execução arbitraria de código.
- CVE-2023-29301: Vulnerabilidade relacionada com pouca restrição ou tentativas de autenticação em excesso.

Link:
https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

Produtos envolvidos:

- ColdFusion 2018: atualização 16 e versões anteriores.
- ColdFusion 2021: atualização 16 e versões anteriores.
- ColdFusion 2023: GA Release (2023.0.0.330468).

Solução:

- ColdFusion 2018: atualização 17.
- ColdFusion 2021: atualização 17.
- ColdFusion 2023: atualização 1.

Microsoft

Data: 06-06-2023

Descrição.

No último dia 11 de julho, foram divulgadas diversas vulnerabilidades 0-day que atualmente são passíveis de exploração em produtos da Microsoft.

- CVE-2023-32046: Vulnerabilidade de elevação de privilégios na plataforma Windows MSHTML. Esta vulnerabilidade era explorada ao abrir um arquivo especialmente desenvolvido por e-mail ou sites maliciosos.
- CVE-2023-32049: Vulnerabilidade de by-pass de recursos de segurança do Windows SmartScreen.
- CVE-2023-36874: Vulnerabilidade de elevação de privilégios no serviço de notificação de erros do Windows: esta falha de elevação de privilégios ativamente explorada permitia aos invasores obterem privilégios de administrador no dispositivo Windows.
- CVE-2023-32057: Vulnerabilidade de execução remota de código em filas de mensagens da Microsoft.
  Além das vulnerabilidades 0-day, foram encontradas as seguintes vulnerabilidades em produtos da Microsoft:

- 33 vulnerabilidades de elevação de privilégios
- 13 vulnerabilidades de by-pass de recursos de segurança
- 37 vulnerabilidades de execução remota de código
- 19 vulnerabilidades de divulgação de informação
- 22 vulnerabilidades de negação de serviço
- 7 vulnerabilidades de roubo de identidade

Link: https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2023-patch-tuesday-warns-of-6-zero-days-132-flaws/

Produtos envolvidos: Diversos produtos de Microsoft.

Solução: Atualizar com os patches indicados para cada produto da Microsoft

EVENTOS

Cybersecurity Summer BootCamp

03 - 13 de julho de 2023 |

O Instituto Nacional de Cibersegurança (INCIBE) e a Organização dos Estados Americanos (OEA) organizam anualmente o Cybersecurity Summer BootCamp, um programa internacional de capacitação especializado em cibersegurança destinado às Forças e Órgãos de Segurança, Ministério Fiscal, Juízes e Magistrados, Formuladores de Políticas e Especialistas de Centros de Resposta a Incidentes Cibernéticos.

Link: https://www.incibe.es/eventos/summer-bootcamp

Congresso de Transformação Digital do Terceiro Setor Social da Catalunha

11 de julho de 2023 |

No próximo dia 11 de julho, será organizado, no Hub Social (c/ Girona, 34, 08010 - Barcelona), o Congresso de Transformação Digital do Terceiro Setor Social da Catalunha pela Taula D'entitats del Tercer Sector Social de Catalunya, por meio do projeto m4Social e em colaboração com a Fundación Telefónica.

Link: https://m4social.org/es/esdeveniment/congres-de-transformacio-digital-del-tercer-sector-social-de-catalunya/

Cybersecurity Financial & Government Edición Ecuador

6 de julho 2023 |

O Cybersecurity Financial & Government Edición Ecuador será realizado no Swissotel Quito, em 6 de julho de 2023, mostrando a atualidade empresarial de Ecuador e internacional em relação aos setores de Tecnologias digitais e Tecnologia de segurança.

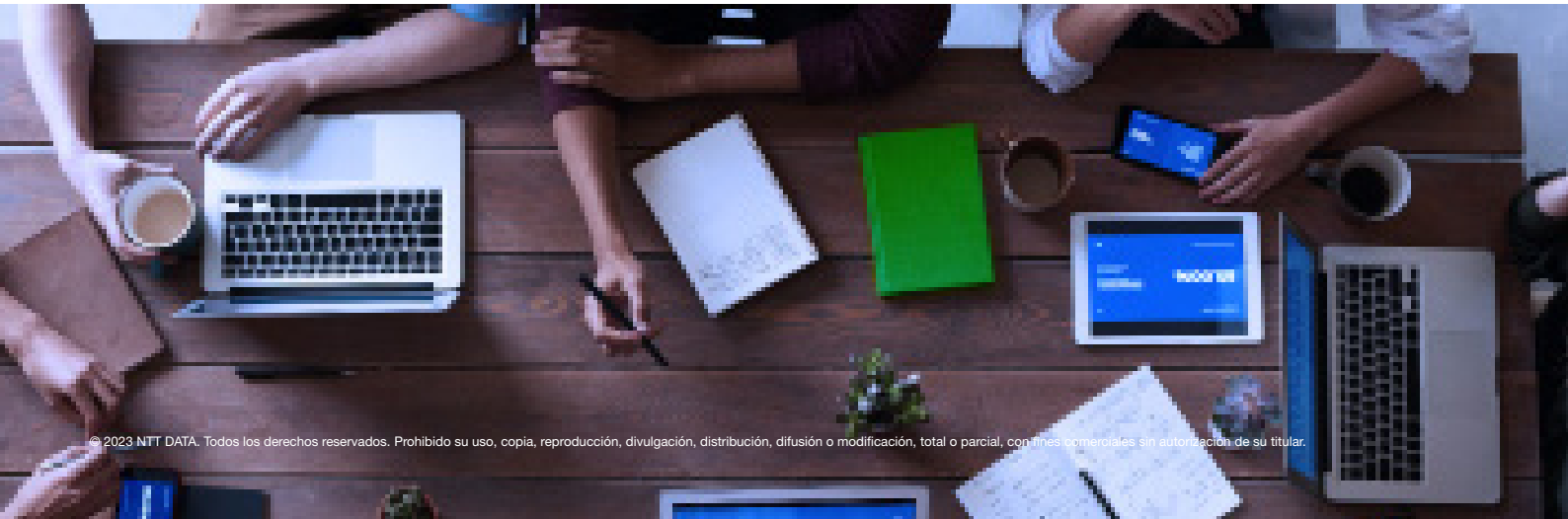
Link: https://www.neventum.es/ferias/cybersecurity-financial-government-edicion-ecuador

Cyber Security EXPO

5 - 10 de julho de 2023 |

A EXPO de Cibersegurança é o único evento dedicado a contratações, desenvolvido para clientes e agências de recrutamento em operação no setor de cibersegurança, considerando natureza sensível de alguns postos de trabalho e a possibilidade de os candidatos desejarem manter a discrição.

Link: https://www.cybersecurityexpo.co.uk/manchester



RECURSOS

RULES_OCI CON BAZEL

A Google lançou recentemente a Rules_oci, uma extensão de código aberto para Bazel que visa facilitar e melhorar a segurança na criação de imagens de contêineres. Este complemento, conhecido como um "conjunto de regras", oferece suporte tanto à comunidade de contêineres quanto à segurança das imagens de contêineres.

Link: https://noticiasseguridad.com/tutoriales/proteger-las-imagenes-de-los-contenedores-con-la-herramienta-gratis-de-google-rules_oci-con-bazel/

Cisco anuncia Extended Detection and Response (XDR)

A Cisco está desenvolvendo uma solução XDR que combina a experiência em redes e em terminais para uma detecção e resposta baseada em riscos. A Cisco XDR, em fase beta, estará disponível em julho de 2023. A solução cloud native utiliza dados analíticos para priorizar detecções e automatizar respostas, reduzindo as pesquisas intermináveis nos centros de operações de segurança.

Link: https://bitlifemedia.com/2023/05/cisco-presenta-nuevas-soluciones-ciberseguridad-xdr/

Google Cloud combate a lavagem de dinheiro em entidades financeiras com IA

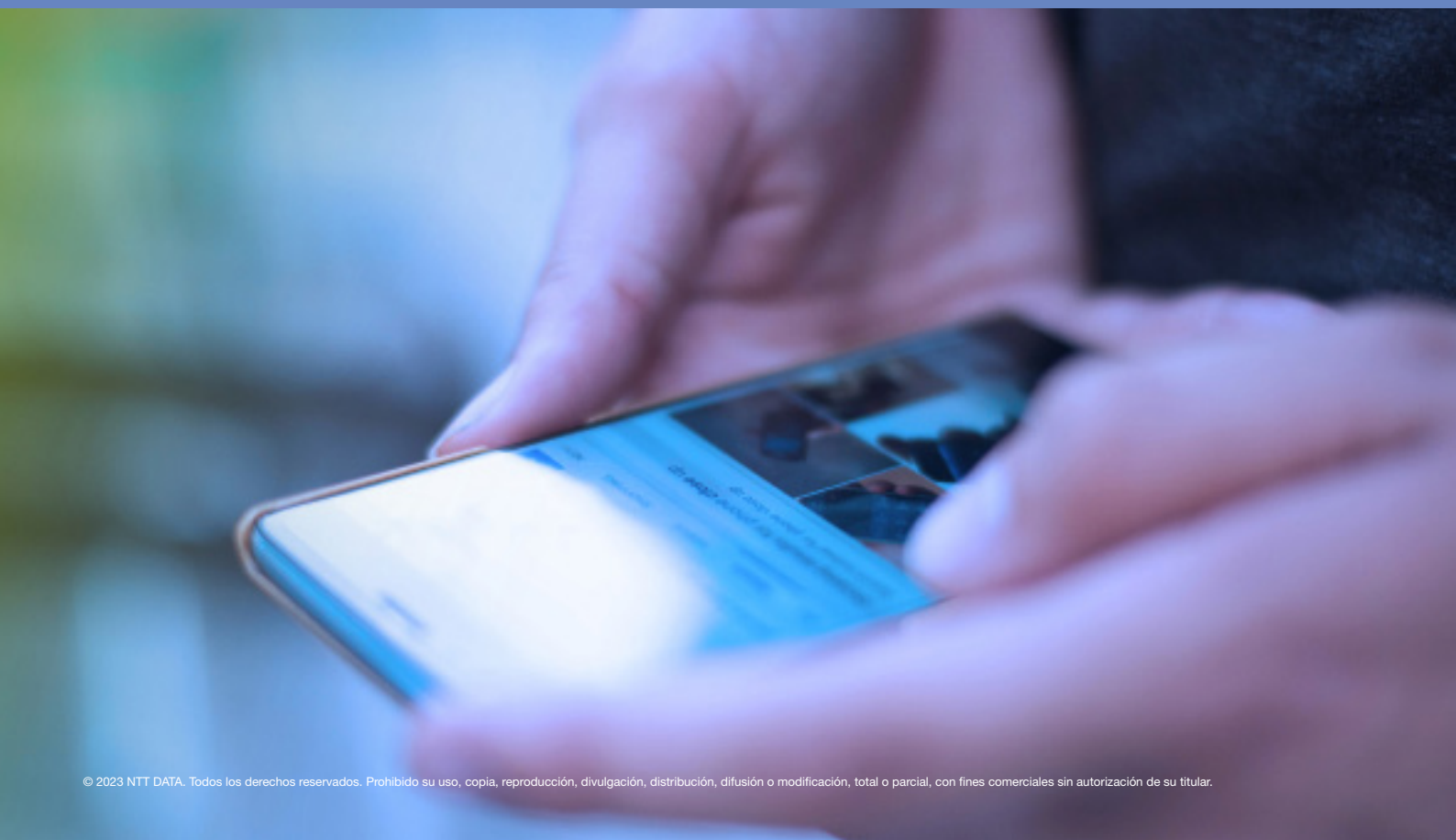
A Google Cloud apresentou a AML AI (Anti Money Laundering AI), um produto orientado por inteligência artificial (IA) que visa melhorar a detecção de lavagem de dinheiro em entidades financeiras. Esta solução, desenvolvida especificamente para combater este tipo de delito de maneira mais eficaz e eficiente, aproveita a potência da IA para oferecer análises avançadas e precisas. Com a AML AI, as entidades financeiras podem fortalecer sua capacidade de detectar e prevenir atividades ilícitas relacionadas à lavagem de dinheiro, possibilitando uma maior proteção e segurança em sua operação.

Link: https://cybersecuritynews.es/google-cloud-lanza-un-producto-para-luchar-contra-el-blanqueo-de-capitales-asistido-por-ia-para-entidades-financieras/

Novo método de phishing detectado no Microsoft Teams: Roubo de identidade de usuários internos e envio de mensagens falsas

Um novo método de phishing foi detectado no Microsoft Teams, permitindo aos invasores roubarem a identidade de usuários internos de uma organização e enviarem mensagens falsas a outros usuários. Como resultado, o pesquisador de segurança Alex Reid criou uma ferramenta chamada "TeamsPhisher", utilizando Python, que automatiza completamente esse tipo de ataque. O software combina as estratégias de ataque desenvolvidas pelos pesquisadores da Jumpsec, as técnicas de Andrea Santese e as funções de autenticação e assistência da ferramenta "TeamsEnum", criada por Bastian Kanbach.

Link: https://github.com/Octoberfest7/TeamsPhisher



RESPONSÁVEIS CIBER

María Pilar Torres Bruna

Directora de Cibersegurança na NTT DATA Latam y Perú maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schwarzer

Directora de Cibersegurança na NTT DATA Brasil

carla.passosschwarzer@emeal.nttdata.com

Javier Mauricio Albarracin

Director de Cibersegurança na NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

Fernando Vilchis

Director de Cibersegurança na NTT DATA México fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Ciberseguridad na NTT DATA EE.UU

nestor.ordonez.ramirez@emeal.nttdata.com

Carolina Pizarro

Director de Ciberseguridad na NTT DATA Chile

carolina.pizarrodiaz@emeal.nttdata.com


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com