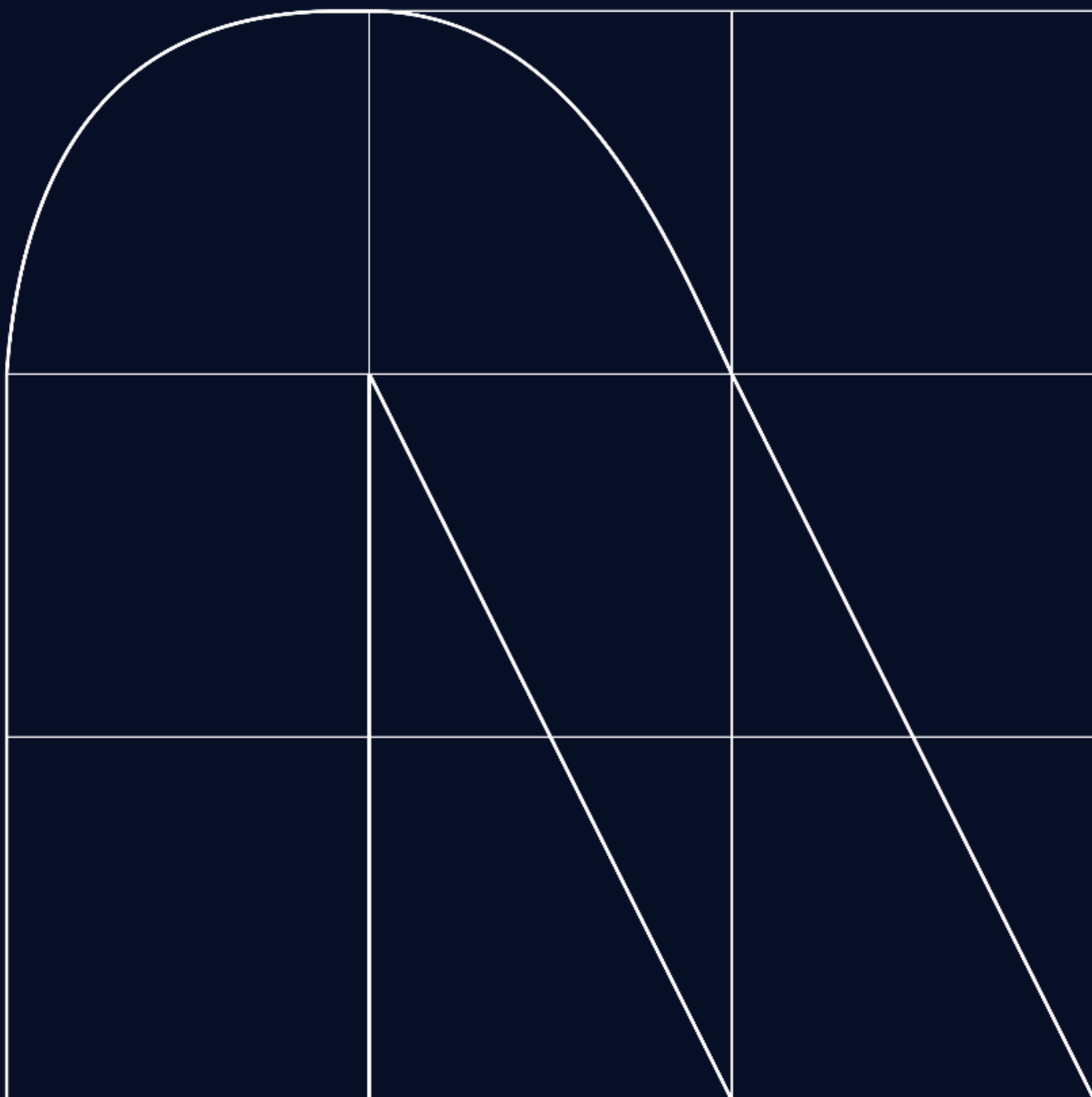
Número 84 | Novembro 2023

NTT DATA

Radar

A revista de cibersegurança



Cabos de comunicação submarinos, uma infraestrutura crítica que precisa de proteção.

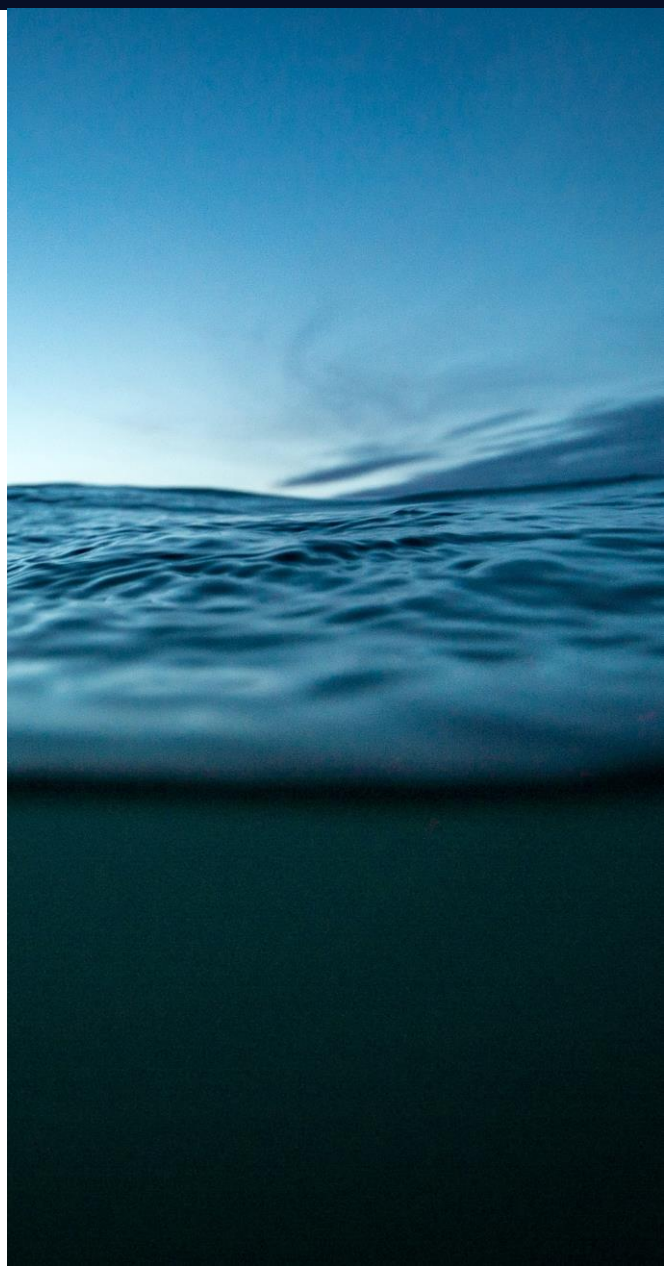
Por: Jorge Trujillo Ramirez

A comunicação global depende amplamente de uma infraestrutura crítica que frequentemente passa despercebida: **os cabos de comunicação submarinos.**

Estes cabos, que se estendem por milhares de quilômetros no fundo do oceano, são a coluna vertebral da conectividade mundial, permitindo a transmissão de dados, voz e vídeo através dos oceanos. No entanto, e ainda que sua localização exata seja secreta e sejam utilizadas técnicas de criptografia para proteger a informação, a crescente dependência destas redes submarinas **(99% das comunicações digitais do mundo transitam pela rede)** aumentou a preocupação sobre os riscos enfrentados em cibersegurança, e a segurança dos cabos foi um elemento pouco estudado na segurança internacional (segundo o que foi advertido por um relatório do parlamento europeu "***Security threats to undersea communications cables and infrastructure – consequences for the EU***", Junho de 2022), o que não é nada simples, já que afeta a governança dos oceanos, a soberania digital, a política de infraestruturas críticas e diversos aspectos da ação exterior, desde a política de defesa até a política de segurança.

No mundo todo, há cerca de 400 cabos, dos quais 250 passam pela Europa, sendo que a Espanha conta com 32 pontos de aterrissagem, que conecta 4 continentes (Europa, África, Ásia e América do Norte) e é o ponto estratégico da conexão global da União Europeia.

Todos os anos, ocorrem centenas de incidentes que causam cortes. A grande maioria ocorre por negligência nas operações pesqueiras próxima deles, mas o acúmulo de cortes nos últimos meses voltou a apresentar a possibilidade de outro tipo de ataque ou sabotagem aumentando o alerta sobre este tipo de infraestrutura, o que motivou a elaboração do mais recente relatório da ***ENISA, "SUBSEA CABLES - WHAT IS AT STAKE?*** publicado no final de julho deste ano, onde destaca-se que quase 40% das falhas nos cabos ocorrem por atracagem ou pesca, enquanto que no restante dos casos não há uma causa específica. No total, 87% dos incidentes são causados pela intervenção humana, sejam erros não intencionais ou ações maliciosas intencionais, sendo que apenas 4% das incidências são atribuídas a falhas do sistema (falhas da planta) e 5% ocorrem por fenômenos naturais.



Mesmo que este relatório reconheça que não existem muitos dados sobre incidentes de cabos submarinos provocados por ações maliciosas, ele recomenda aumentar o monitoramento das atividades marítimas civis e a identificação de comportamentos atípicos através de uma combinação de vigilância superficial e submarina para prevenir ataques nos seguintes cenários:

- **Ataques de sabotagem:** com o objetivo de alterar a conectividade, a destruição física intencional dos cabos pode ser realizada com dispositivos de corte improvisados como âncoras e dispositivos de dragagem, utilizando explosivos submarinos ou um veículo submergível, operado remotamente ou submarino.

- **Ataques de espionagem:** não há dúvidas de que a intervenção de cabos submarinos no fundo do mar pode ser considerada muito improvável (para acessar os dados que passam através do cabo no fundo do mar seria necessário cortar as fibras ópticas, o que geraria alarmes). A escuta de dados de comunicações através dos sistemas de gestão de redes de cabo ou nos pontos de aterrissagem é mais viável.

- **Ataques contra estações de aterrissagem e sistemas de gestão de redes**: cada cabo submarino possui pelo menos duas estações de aterrissagem onde o cabo submarino se conecta à terra. As estações de aterrissagem são pontos fracos e relativamente vulneráveis a ataques físicos e cibernéticos. Os cenários que envolvem ataques a estações de aterrissagem vão desde cortar o abastecimento de energia até detonação de artefatos explosivos improvisados, inclusive ataques com mísseis.

- **Ataques a navios de manutenção:** também deveriam ser consideradas ações maliciosas contra navios de manutenção. Apenas dois barcos de cabo tem sua sede na União Europeia e outra no Reino Unido. Os barcos são vulneráveis a todo tipo de armas (por ex.: artefatos explosivos improvisados, mísseis) e os ataques aos navios de manutenção poderiam provocar longos apagões.

Resumindo, **os cabos submarinos de comunicações são uma parte fundamental da infraestrutura global de telecomunicações,** permitindo a comunicação a longa distância em todo o mundo. Sua segurança e confiabilidade são de suma importância para a economia global e a sociedade atual. Os riscos de cibersegurança são uma preocupação crescente em um mundo cada vez mais interconectado e, segundo o relatório do parlamento europeu, até o momento ainda não houve foco suficiente nesse quesito. Proteger esta infraestrutura crítica é essencial para garantir a segurança e a continuidade de nossas comunicações globais, por isso propomos que sejam acrescentadas nas análises de riscos as ameaças relacionadas a este tema e que, além disso, seja feito um acompanhamento e monitoramento meticuloso de sua evolução, para que seja possível detectar e alertar sobre elas o quanto antes.

Jorge Trujillo Ramirez
Project Leader de Cibersegurança na NTT Data Peru

Cibercrônica

Por: NTT DATA Europe & Latam

A inteligência artificial se transformou em uma ferramenta muito potente tanto para realizar ataques como para a defesa cibernética em grande escala.

Em conflitos recentes, vimos como táticas de guerra cibernética foram utilizadas para obter vantagens estratégicas. Estes ciberataques incluem a invasão de sistemas, a desinformação e a interrupção de serviços online.

A inteligência artificial (IA) foi uma ferramenta chave nestes ciberataques, já que permite automatizar e otimizar suas operações. A seguir, constam alguns exemplos do uso da IA em ciberataques:

Ataques de phishing avançados: A IA é utilizada para criar e-mails de phishing altamente personalizados e convincentes, projetados para enganar os destinatários e obter informações confidenciais.

> “A guerra cibernética nestes conflitos é um lembrete de como a tecnologia e a inteligência artificial estão sendo utilizadas no campo de batalha moderno.

Malware inteligente: Os cibercriminosos usam a IA para desenvolver malware capaz de invadir as defesas tradicionais e se adaptar às condições em tempo real.

Detecção de vulnerabilidades: Os agentes cibernéticos podem utilizar a IA para buscar constantemente vulnerabilidades em sistemas de informática e redes, o que lhes permite identificar e explorar pontos fracos.

Ataques de negação de serviço (DDoS): A IA é utilizada para coordenar e amplificar ataques DDoS, o que faz com que sejam mais difíceis de mitigar.

Desinformação e manipulação em redes sociais: A IA pode automatizar a criação e propagação de notícias falsas e desinformação em plataformas de redes sociais, o que pode influenciar na opinião pública.

Nestes casos, a inteligência artificial também é usada para fortalecer suas defesas cibernéticas. A IA é utilizada para detectar ameaças, identificar padrões atípicos e melhorar a segurança dos sistemas críticos.

A guerra cibernética nestes conflitos é um lembrete de como a tecnologia e a inteligência artificial estão sendo utilizadas no campo de batalha moderno. Estes desenvolvimentos apresentam desafios significativos para a cibersegurança e destacam a importância da cooperação internacional na prevenção e redução de ciberataques em tempos de conflito.

FraudeGPT

Falando de outros temas, no último radar falamos sobre algumas ferramentas novas no mercado, como a “FraudeGPT”. Estas ferramentas implementam a tecnologia de IA para a detecção e prevenção de fraudes, e muitas empresas espanholas já confiam nelas.

Estudos realizados na Espanha demonstram que a fraude continua sendo uma das maiores preocupações tanto para empresas como para consumidores. Um em cada cinco espanhóis admite ter sido vítima de fraude durante a realização de algum pagamento, sendo que a média do valor roubado é de 160 euros.

Outro estudo ressalta que as tentativas de fraude aumentaram ao longo destes últimos anos. Apesar disso, 60% dos comerciantes acreditam que seus sistemas de detecção de fraudes são eficazes, e apenas 24% deles afirmam ter investido em sistemas de prevenção e resposta no último ano.

Para combater esta crescente ameaça, a IA está sendo implementada em ferramentas de detecção de fraudes. Segundo as pesquisas realizadas, 53% dos comerciantes espanhóis utilizam a inteligência artificial para se defender de fraudes, além de softwares de gestão de chargeback para a gestão e redução do custo associado.

Avaliando a situação e as previsões de futuro, recomenda-se que as empresas invistam não só em ferramentas de gestão e prevenção, como também em adaptá-las a suas necessidades específicas, aproveitar o aprendizado automático [*machine learning]* e trabalhar na diferenciação de compradores legítimos de outros agentes maliciosos.

Resiliência no blockchain: É necessário um plano de recuperação de desastres?

ANÁLISE

Um dos maiores desafios de uma companhia é estar preparada para uma interrupção que possa colocar em perigo a continuidade de seus processos críticos, e cujas respostas de recuperação diminuam o máximo possível os impactos negativos (reputacional, econômicos, operacionais, legais etc.) que a contingência tenha gerado ou possa gerar.

O contexto atual que temos mundialmente (efeitos extremos no meio ambiente, falta de energia, tensões políticas, aumento do cibercrime...) coloca em evidência o risco de as companhias sofrerem algum tipo de interrupção. As organizações estão adquirindo consciência e envidando esforços para identificar os riscos que possam afetar suas operações, a fim de traçar uma estratégia que reduza os riscos que possam colocar em perigo a disponibilidade dos serviços tecnológicos das companhias.

Uma das estratégias mais comuns e recorrentes das companhias são os planos de Recuperação de Desastres (em inglês, DRP). Tais planos são parte essencial da estratégia operacional e de segurança de qualquer negócio, já que foram projetados para assegurar que as operações sejam retomadas com rapidez caso ocorram interrupções inesperadas (desastres naturais ou causados por humanos). No entanto, com o surgimento do Blockchain e a decisão de algumas empresas de construir seus modelos baseados nesta tecnologia, ou inclusive de mudar seus modelos existentes para esta nova tecnologia, ocorre uma possível mudança nas práticas a respeito dos DRP.

Uma das principais características das redes Blockchain é a capacidade de resistir a falhas. Esta qualidade é derivada de sua arquitetura, que é formada a partir de nós independentes formados por redes descentralizadas e distribuídas. Diferentes dos sistemas tradicionais centralizados, nos quais uma falha pode paralisar todo o sistema, os sistemas Blockchain são fundamentalmente resistentes a este tipo de interrupções. Em uma empresa cujos sistemas sejam baseados em Blockchain, como por exemplo as dApps (aplicações que funcionam em uma rede Blockchain de forma descentralizada), o conceito da distribuição desempenha um papel muito importante em seu planejamento diante de um possível desastre. Para que uma rede Blockchain caia, é necessário que todos os nós que a compõe caiam, pois cada nó contém uma cópia inteira do Blockchain e é capaz de operar de forma independente.

A Ethereum, uma das maiores e mais populares redes Blockchain no mundo empresarial pela sua capacidade de guardar os denominados "Contratos Inteligentes" (programas autoexecutáveis armazenados em uma rede Blockchain que são ativados quando determinadas condições pré-definidas são cumpridas), possui milhares de nós distribuídos pelo mundo. Para forçar a queda desta rede Blockchain, seria necessário comprometer seus nós por meio de um dos seguintes métodos:

- Que ocorra um fenômeno natural em nível mundial que prejudicasse todos os nós. Este evento deve afetar todas as zonas geográficas que tenham nós e deve comprometer o abastecimento de energia elétrica ou a conexão à internet, ambos fatores essenciais para a rede Blockchain. Este fenômeno provocaria uma queda de serviço da rede Blockchain por não haver nós operacionais que possam sustentar a rede.
- A rede também poderia ser comprometida por meio de algum ataque que, em função do mecanismo de consenso da rede Blockchain, busque assumir o controle da rede. Mesmo que isso não afetasse necessariamente a disponibilidade do serviço, ainda assim comprometeria a confiabilidade dos dados, já que um agente mal-intencionado com controle suficiente sobre a rede poderia tentar manipular as transações ou inclusive reverter as já realizadas, quebrando a confiança inerente ao sistema. Mesmo que um único nó fosse comprometido com relativa facilidade (por ex.: Assumir o controle do nó fisicamente), para se comprometer a rede inteira, um grande número de nós (51% dos nós em um Proof of Work ou aqueles nós que somem 51% dos tokens da rede em um Proof of Stake) deveria ser comprometido. Este seria um processo extremamente caro e que certamente seria identificado pela comunidade, a qual poderia tomar medidas de prevenção.

Vale destacar que ambos os casos, tanto o desastre natural em nível global como o ataque massivo aos nós, são apresentados como uma hipótese de probabilidade muito baixa.

Outra questão para levar em consideração seria o tipo de rede. Se a rede Blockchain for pública (qualquer um pode se transformar em um nó), a resposta sobre como um DRP será administrado é muito simples: não será. Isso ocorre porque cada nó será administrado de forma independente e, ainda que possa ser definido um DRP, é impossível aplicá-lo em todos os nós. Se a rede Blockchain for privada (o acesso funciona mediante convite), funcionaria de forma diferente. As redes privadas possuem certo controle sobre os nós e, por tanto, podem estabelecer e difundir um DRP a todos os nós. O acompanhamento seria complicado devido ao número de nós existentes, pois cada um deles pode ter uma arquitetura diferente, mas poderia ser viável dependendo do quão maior for o controle sobre a rede.

A pergunta chave neste caso é se realmente é necessário que uma organização cujo sistema esteja em uma rede Blockchain invista recursos na criação de um DRP. A priori pareceria que não, já que, devido às características básicas de resiliência destas redes, este trabalho não é necessário por não fornecer capacidade de resiliência adicional. Além disso, se todos os nós caírem de forma simultânea, provavelmente será por algum desastre do qual a recuperação é impossível. Por tanto, podemos considerar o uso da tecnologia Blockchain como uma estratégia em si para reduzir os riscos citados no início deste artigo.

Vale destacar que, no mundo da segurança, sempre são citados os três pilares: disponibilidade, integridade e confidencialidade. A disponibilidade é a garantia de acesso à informação no momento necessário, a integridade é a proteção das informações diante de manipulações não desejadas e a confidencialidade trata-se de assegurar que o acesso seja permitido apenas para pessoas autorizadas. Levando isso em consideração, podemos comprovar que as características básicas do Blockchain protegem a disponibilidade por meio da distribuição de nós e a integridade da informação, já que cada nó contém uma cópia inteira do Blockchain criptograficamente protegida (para assegurar sua imutabilidade). A confidencialidade, no entanto, é um desafio maior devido à transparência inerente das redes Blockchain (existem medidas alternativas para assegurar a confidencialidade, mas essas costumam ter uma maior complexidade). Por tanto, as empresas que optem por dar especial importância à disponibilidade e a integridade da informação deveriam considerar a possibilidade de incorporar a Blockchain em suas operações ou mudar seu modelo para esta tecnologia.

María Lezana Juberías
Cybersecurity Expert NTT DATA Europe & Latam

Óscar Marimon Rius
Cybersecurity Consultant NTT DATA Europe & Latam

A preocupante sofisticação do vishing com a Inteligência Artificial Generativa.

TENDÊNCIAS

O phishing e suas diversas mutações continuam sendo uma das estratégias mais utilizadas por cibercriminosos atualmente. Apesar dos esforços crescentes das empresas para instruir seus funcionários sobre estes ataques, ainda presenciamos inúmeros exemplos desta técnica em ação.

Durante este ano, fomos testemunhas de campanhas de phishing que roubam a identidade de instituições respeitadas como a Agência Tributária Espanhola [Receita] e a Dirección General de Tráfico (DGT) da Espanha [órgão semelhante ao *DETRAN]*, usando envios massivos de sms fraudulentos que alegam sanções monetárias inexistentes e direcionam os usuários a sites maliciosos.

Particularmente, nos últimos meses, as técnicas de **vishing** ganharam notoriedade. O vishing é um tipo de golpe de engenharia social por telefone no qual, por meio de uma ligação, é roubada a identidade de uma empresa, organização ou pessoa de confiança, com a finalidade de obter informações pessoais e sensíveis da vítima. Um exemplo disso é uma campanha que se passava pelo Instituto Nacional de Ciberseguridad de España (INCIBE) [Instituto Nacional de Cibersegurança da Espanha] com o objetivo de roubar dados pessoais de usuários. Esta manobra de fraude combinava vishing e phishing, começando com ligações telefônicas nas quais os hackers se passavam por representantes do INCIBE e tentavam persuadir os usuários para que fornecessem informações, incluindo seus endereços de e-mail, como parte de seu esquema fraudulento.

Outro incidente de destaque é o *hacking* da MGM Resorts International, um conglomerado que administra alguns dos maiores cassinos de Las Vegas. O grupo de hackers, conhecido como "Scattered Spider", investigou os funcionários da MGM no LinkedIn e utilizou a identidade de um deles para ligar para o serviço de assistência técnica e solicitar uma redefinição de senha. Em apenas 10 minutos, os cibercriminosos tinham conseguido acessar a rede.

O uso da voz e imagens de indivíduos para finalidades fraudulentas não é novidade, mas é surpreendente a facilidade com a qual os hackers podem manipular estas tecnologias para seus próprios objetivos. Ao longo deste ano, fomos testemunhas de diversas campanhas de manobras de fraude que usavam a voz e imagem de celebridades, como Elon Musk, que foram objeto frequente destes golpes, especialmente no âmbito das criptomoedas. Alguns dos ataques mais notórios envolvem a invasão de canais do YouTube com uma ampla audiência que, da noite para o dia, começam a espalhar conteúdo fraudulento.

Recentemente, uma campanha falsa se tornou viral, utilizando a identidade de Jimmy Donaldson, conhecido como MrBeast, para supostamente sortear um iPhone 15 Pro entre 10.000 pessoas. O mais impactante destas campanhas é a rapidez com a qual um cibercriminoso pode executá-las utilizando ferramentas como HeyGen.

Esta tecnologia, quando está nas mãos de agentes maliciosos com mais conhecimentos e recursos, pode ser utilizada para causar influência em conflitos internacionais. Um exemplo ocorreu na Rússia, onde emissoras de rádio e canais de televisão foram hackeados para disseminar deepfakes de Vladimir Putin, espalhando informações falsas sobre retiradas e mobilizações massivas.

O vishing, combinado com ferramentas de inteligência artificial generativa, evoluiu rapidamente e se transformou em uma ameaça significativa. Estes ataques aproveitam o roubo de identidade, o uso de figuras públicas e a manipulação da voz para enganar as vítimas. A facilidade de criação de deepfakes e campanhas fraudulentas gera desafios adicionais para a cibersegurança.

A UE tomou a iniciativa, em meados deste ano, de impulsionar a primeira lei europeia sobre inteligência artificial, prevista para o final do ano e que regula vários aspectos dos usos desta tecnologia e inclui sob vigilância sistemas como o ChatGPT. Nos termos desta lei, os provedores deverão identificar e reduzir os potenciais riscos e cumprir os requisitos de transparência avisando que o conteúdo foi gerado por meio da IA, ajudando a distinguir as imagens reais das “Deepfake”.

Além disto, como reação ao aumento do volume de conteúdo gerado por meio da IA, surgiram cada vez mais ferramentas para detectá-lo. O Twitter já lançou ferramentas para combater a desinformação em sua plataforma e o Google lançou o SynthID, outra ferramenta especialmente focada na detecção de imagens geradas por IA.

Além das implicações na segurança pessoal, o vishing pode ser utilizado para causar influência em conflitos internacionais ao espalhar informações falsas. Isso ressalta a necessidade de ficar alerta e adotar medidas de segurança sólidas para se proteger contra estas ameaças em constante evolução. A educação sobre a identificação de manobras de fraude e a implementação de medidas de segurança cibernética robustas são cruciais em um mundo onde a tecnologia de manipulação de voz e imagens está ao alcance dos cibercriminosos.

Vulnerabilidades

Receba nosso boletim informativo completo sobre patches e vulnerabilidades inscrevendo-se aqui.

Vulnerabilidade crítica na Cisco Emergency Responder

Data: 4 de outubro de 2023
Gravidade**: CRÍTICA**
CVE: CVE-2023-20101

Descrição:

No dia 4 de outubro, a Cisco fez uma publicação sobre uma vulnerabilidade crítica na aplicação Cisco Emergency Responder devido à existência de credenciais estáticas do usuário root que não podem ser alteradas ou eliminadas; normalmente estas credenciais são utilizadas durante o desenvolvimento.

Com a exploração desta vulnerabilidade, um hacker não autenticado seria capaz de iniciar sessão no dispositivo afetado com o usuário root, permitindo, assim, a execução de comandos com permissões elevadas.

A Equipe de Resposta a Incidentes de Segurança de Protocolos (PSIRT) da Cisco informou que não encontrou divulgações públicas sobre esta vulnerabilidade.

Link

Produtos afetados:

Esta vulnerabilidade afeta somente a versão 12.5(1)SU4 da Cisco Emergency Responder.

Resolução:

A solução recomendada para lidar com esta vulnerabilidade consiste em atualizar as instalações vulneráveis; sendo a primeira versão fixa a versão 12.5(1)SU5.

Vulnerabilidade no Google Chrome

Data: 3 de outubro de 2023
Gravidade**: ALTA**
CVE: CVE-2023-5346

Descrição:

Na última terça-feira, dia 3 de setembro [sic], o Chrome lançou uma atualização para a aplicação de desktop do Google Chrome. Nesta atualização constam informações sobre a correção de uma vulnerabilidade alta. Esta vulnerabilidade permitiria que um hacker executasse um código de forma remota para explorar a corrupção da memória na pilha de execução do navegador utilizando uma página HTML especialmente projetada.

Trata-se de uma vulnerabilidade gerada devido a um problema no interpretador JavaScript do Google Chrome (V8), dado que interpreta incorretamente o tipo de dados.

Outros navegadores como o Microsoft Edge, por serem baseados no Chromium, também foram afetados por esta vulnerabilidade e, na Microsoft, uma atualização de segurança para ele já foi lançada.

Link
Link

Produtos afetados:

Os recursos afetados por esta vulnerabilidade são os seguintes:

- Google Chrome, versões anteriores à versão 117.0.5938.149.
- Microsoft Edge, versões anteriores à versão 117.0.2045.55.

Resolução:

A solução consiste na atualização dos navegadores Google Chrome para a versão 117.0.5938.149 e Microsoft Edge para a versão 117.0.2045.55.

Patches

Boletim de segurança mensal da Android
Data: 2 de outubro de 2023
Gravidade**: CRÍTICA**

Descrição:

A Android publicou, no último dia 2, seu boletim de segurança correspondente ao mês de outubro. Nele, um total de 51 vulnerabilidades foi informado, entre as quais 5 são vulnerabilidades críticas e 46 são altas.

Entre as vulnerabilidades críticas constam as seguintes:

- CVE-2023-40129 e CVE-2023-4863: São duas vulnerabilidades críticas que permitiriam que um hacker executasse um código de forma remota. Ambas as vulnerabilidades afetam o componente system.
- CVE-2023-24855: Esta vulnerabilidade crítica ocorre pela corrupção de memória no modem durante o processo de configuração de segurança prévio ao AS Security Exchange.
- CVE-2023-28540: Esta vulnerabilidade ocorre por uma autenticação incorreta durante o protocolo de ligação TLS que provoca problemas criptográficos no modem de dados.
- CVE-2023-33028: Trata-se de uma vulnerabilidade gerada pela corrupção de memória no firmware WLAN durante o processo de realização de uma cópia de memória de cachê pmk.

As três últimas vulnerabilidades afetam o componente Qualcomm closed-source.

Link

Produtos afetados:

As vulnerabilidades corrigidas neste boletim afetam os seguintes recursos:

- Android Open Source Project (AOSP) versões 11, 12, 12L e 13.
- Componentes: framework, system, sistema de atualizações do Google Play, Arm, MediaTek, Qualcomm (incluindo closed-source)

Atualização:

Atualizar os dispositivos afetados com os patches de segurança publicados pelo fabricante.

Atualização de uma vulnerabilidade 0 day na Apple
Data: 4 de outubro de 2023
Gravidade**: ALTA**

Descrição:

A Apple publicou uma atualização de segurança para iOS e iPadOS que corrige uma vulnerabilidade zero-day CVE-2023-42824.

A vulnerabilidade identificada como CVE-2023-42824 afeta o kernel e poderia dar a um hacker local a capacidade de aumentar seus níveis de privilégios nos dispositivos afetados. A Apple informa que esta falha de segurança pode ter sido utilizada contra as versões de iOS vulneráveis.

Esta atualização de segurança também abrange a vulnerabilidade CVE-2023-5217, uma falha de segurança zero-day do Google Chrome do dia 28 de setembro. Esta vulnerabilidade ocorre devido a um transbordamento de buffer de pilha na codificação vp8, presente na libvpx, uma biblioteca de codecs de vídeo desenvolvida em conjunto pela Google e a Alliance for Open Media (AOMedia). Este problema foi resolvido por meio da atualização para a libvpx 1.13.1.

Link
Link

Produtos afetados:

A vulnerabilidade afeta todas as versões anteriores à versão 16.6. Definitivamente, afeta os seguintes produtos:

- iPhone XS e posteriores.
- iPad Pro-12.9 polegadas, segunda geração e posteriores.
- iPad Pro-10.5 polegadas
- iPad Pro-11 polegadas, primeira geração e posteriores.
- iPad Air terceira geração e posteriores.
- iPad sexta geração e posteriores.
- iPad mini quinta geração e posteriores.

Atualização:

iOS 17.0.3 and iPadOS 17.0.3

Eventos

Black Hat MEA
14 a 16 de Novembro

A edição de Black Hat MEA (Oriente Médio e África) ocorrerá em Riad, Arábia Saudita, de 14 a 16 de novembro. Este evento líder na região promoverá a troca de conhecimentos e a divulgação de novas tecnologias através de conferências e oficinas ministradas por especialistas da indústria.

Link

National Cyber League España
25 de Outubro a 16 de Novembro

A National Cyber League é uma competição organizada na Espanha pela Guardia Civil [corporação policial militarizada] realizada de 22 de outubro até 16 de novembro. Esta competição tem como objetivo potencializar o talento dos jovens através de uma perspectiva multidisciplinar, abordando aspectos técnicos, legais e de comunicação.

Link

Cyber Security & Cloud Expo
30 de Novembro a 1 de Dezembro

O Cyber Security & Cloud Expo é um evento que ocorre em Londres de 30 de novembro a 1º de dezembro, onde são abordados diversos temas, tais como a inteligência artificial, blockchain e a Internet das Coisas (IoT), focados em diversos setores, incluindo a cibersegurança.

Link

Recursos

Novos Métodos de engenharia social por meio da IA

Atualmente, a inteligência artificial oferece a capacidade de assumir a identidade de outra pessoa em tempo real. Isso ocorre por meio de aplicações como VoiceX, que nos permite modificar nossa voz, e DeepfakeVFX, que nos permite alterar nosso rosto de maneira convincente. Graças a estas tecnologias, é possível roubar a identidade de alguém e, assim, obter informações que podem ser usadas de forma maliciosa.

Link

A RNS compartilha mais de 30 alertas diários sobre ciberameaças ativas

A Red Nacional de Operaciones de Ciberseguridad (RNS) [Rede Nacional de Operações de Cibersegurança], sob a direção do Centro Criptológico Nacional (CCN), informa sobre mais de 30 ciberameaças diárias em andamento, oferecendo às entidades participantes a oportunidade de tomar medidas para reduzir possíveis riscos.

Link

Raspberry Pi5

No final de outubro, estará disponível para venda o Raspberry Pi 5, um computador de placa única com um rendimento substancialmente melhorado em comparação ao seu anterior. Este avanço tecnológico permitirá aos entusiastas e profissionais de TI realizar uma ampla gama de projetos com maior eficiência e versatilidade.

Link

Vazamento do ransomware HelloKitty

No dia 9 de outubro de 2023, o ransomware HelloKitty vazou em um fórum de hackers - este malware provocou muitas dores de cabeça para empresas como CD Proyect em 2021 e Cloudflare em 2022. Graças a este vazamento, muitos cibercriminosos poderão se aproveitar para poder desenvolver seu próprio malware sem ter tantos conhecimentos avançados, podendo provocar um aumento nos ataques desta natureza.

Link

Responsables Ciber

María Pilar Torres Bruna

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

Carla Passos Schawarzer

Directora de Ciberseguranç a na NTT DATA Brasil
carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzón Ramírez

Manager de Ciberseguranç a na NTT DATA Colombia
miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis Rivero

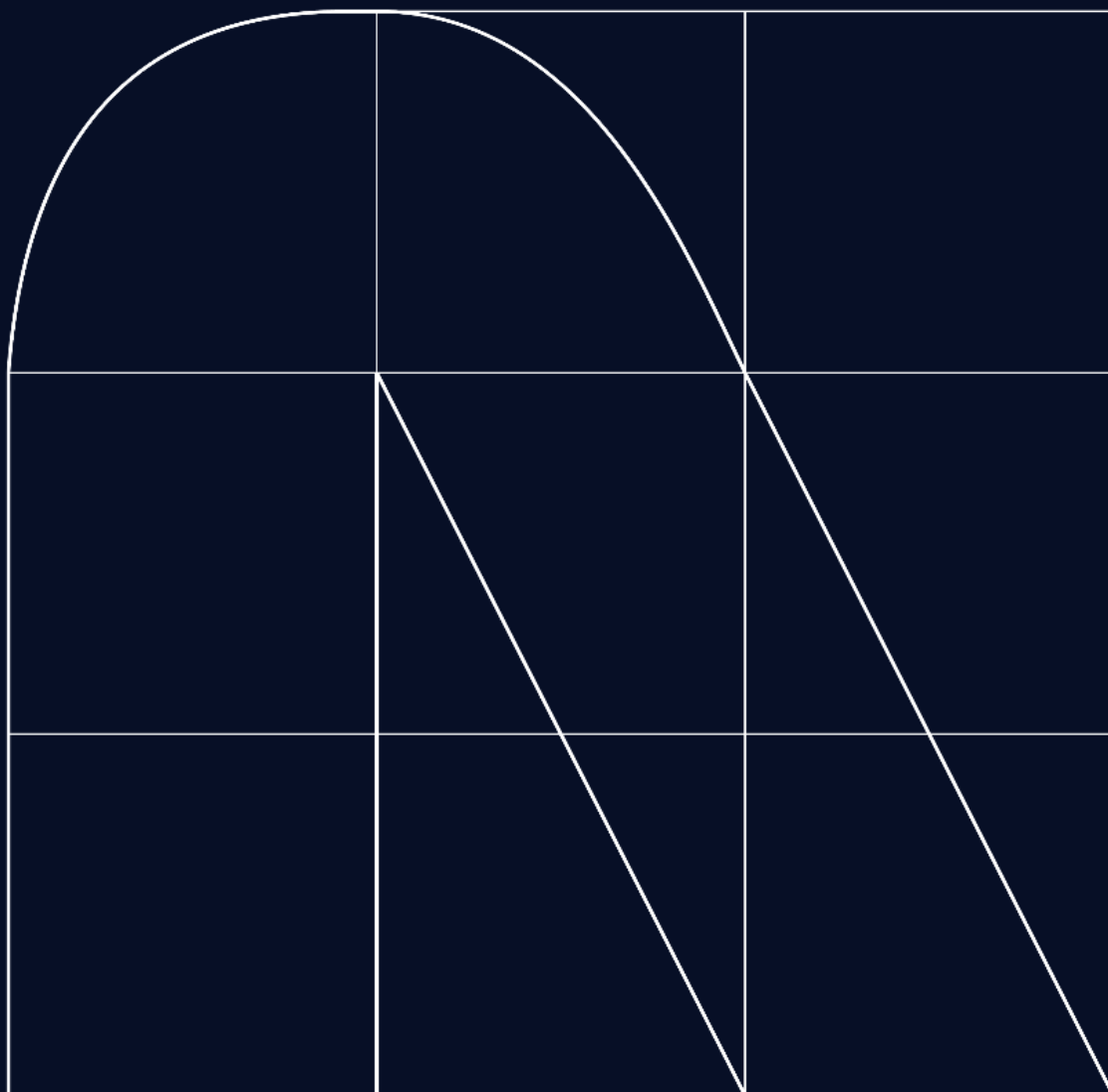
Manager de Ciberseguranç a na NTT DATA México
fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Ciberseguranç a na NTT DATA USA
nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Manager de Ciberseguranç a na NTT DATA Chile
jose.uzcategui@emeal.nttdata.com



Powered by the cybersecurity NTT DATA team

es.nttdata.com