Mesa redonda NARALO - Abuso de DNS e IA: combater e possibilitar ameaças

ICANN82 – 10 de março de 2025

Greg Shatan - NARALO / Moses Singer LLP: Obrigado a todos, e obrigado por virem à nossa mesa redonda sobre abuso de DNS e inteligência artificial. Um tema muito oportuno, uma combinação de dois tópicos muito oportunos, é claro. E sem mais delongas, já que temos um painel de luminares, deixe-me apresentá-los primeiro, diretamente à minha direita.

Jeff Bedser é um empreendedor experiente e líder em investigação de cibersegurança, inteligência de ameaças e mitigação de abuso de DNS. Ele é o CEO da CleanDNS, uma empresa que tem a missão de limpar a Internet de uma vez por todas, para melhor ou para pior, detectando e interrompendo atividades maliciosas de DNS. Em sua vida passada, ele foi detetive particular e usa essa expertise para proteger os usuários finais da Internet, as pessoas que nos preocupam aqui na At-Large. Ele participa de vários conselhos e comitês sobre governança da Internet, estabilidade e jurisdição, e tem 25 anos de experiência na área, fundou a iThreat, uma empresa de inteligência de ameaças, e tem servido no SSAC da ICANN desde 2007, além de ter sido membro do conselho da PIR. Então, Jeff, muito obrigado por estar conosco.

Tim Maurer está à sua direita. Tim é atualmente o Diretor de Política Global de Cibersegurança na Microsoft, onde colabora de perto com as equipes internas da Microsoft e partes interessadas externas. Antes da Microsoft, Tim trabalhou no governo dos Estados Unidos, primeiro como Conselheiro Sênior para Cibersegurança e

Tecnologias Emergentes no Departamento de Segurança Interna, e posteriormente no Conselho de Segurança Nacional da Casa Branca. Acredito que isso foi sob o governo do Presidente Biden, e ele passou uma década trabalhando em políticas de cibersegurança e tecnologia, além de ser autor do livro Cyber Mercenaries, the State, Hackers, and Power.

À sua direita, temos Ana Neves. Muitos de vocês provavelmente conhecem Ana como a representante do GAC de Portugal. Ana desempenha várias funções. Ela é membro do atual IGF MAG, que é um conselho de peso que mantém o IGF funcionando. Ela é a presidente do conselho consultivo do DNS.PT e lidera o Escritório de Governança da Internet na FCT, FCCN e UMIC em Portugal. Ela também é a Vice-Presidente da Comissão das Nações Unidas sobre Ciência, Tecnologia e Desenvolvimento. Ana tem mais de 30 anos de experiência em desenvolvimento de ciência e tecnologia digital e políticas públicas, e foi reconhecida em 2018 como CIO do Setor Público do Ano em Portugal e Líder Digital Europeia.

Então, temos um painel que me faz sentir obscuro e sem grandes realizações. Então, sem mais delongas, gostaria de iniciar a discussão.

Então, se pudermos ir aqui, estamos no primeiro slide. Antes de prosseguirmos, gostaria de mencionar que toda esta apresentação foi escrita por um Microsoft Copilot.

Não estou brincando.

E por alguma razão, lá está. Então, em vez de Deus ser meu copiloto, a Microsoft é meu Copilot. Espero que você aprecie isso, Tim.

Tim Maurer - Microsoft: Estou pronto. Estou pronto. O backup humano está aqui.

Greg Shatan - NARALO / Moses Singer LLP: Aí está. Então, de acordo com o Copilot, abuso de DNS refere-se ao uso indevido do sistema de nomes de domínio para fins maliciosos, como phishing, distribuição de malware e outras ameaças cibernéticas. A definição oficial da ICANN de abuso de DNS tem cinco categorias, talvez uma para cada região geográfica da ICANN. Malware, botnets, uso de botnets, phishing e farming, e spam, mas apenas quando o spam serve como um mecanismo de entrega para um dos outros quatro. Portanto, o spam por si só não é considerado abuso de DNS.

Aqueles de vocês que estão na ICANN há algum tempo podem lembrar que tivemos vários anos de discussão, é um bom termo para isso, sobre os limites e a definição de abuso de DNS. E, em vez de discutir mais sobre isso, estamos pelo menos vivendo com essa definição de abuso de DNS enquanto avançamos, já que isso certamente nos dá problemas suficientes.

Como

você sabe, e eu sei, e o Microsoft Copilot sabe, que a IA e o aprendizado de máquina estão sendo cada vez mais usados para combater o abuso de DNS, detectando e mitigando esses efeitos de forma mais eficaz.

Vou deixar você ler tudo isso no seu próprio tempo. Não precisamos ouvir isso agora. Prefiro ouvir o que nossos painelistas têm a dizer do que o que o Microsoft Copilot tem a dizer.

E o design, é claro, foi escolhido para mim pelo Microsoft PowerPoint. E a imagem na capa também foi escolhida pelo Copilot. Na verdade, sou uma pessoa muito criativa, mas agora decidi deixar o Copilot fazer todas essas coisas.

Então, de qualquer forma, gostaria de começar com o Tim. Vou dizer por mais um minuto, é claro, que o abuso de DNS também está sendo manifestado pela inteligência artificial. E há vários exemplos neste PowerPoint das maneiras pelas quais a IA está criando novas formas e mutando formas antigas de abuso de DNS. Então, temos meio que uma batalha da inteligência artificial. É para o bem e para o mal. E nossos três palestrantes discutirão tanto a cibersegurança geral

e interface de IA, como isso afeta o DNS e qualquer outra coisa que esteja em suas mentes.

Então, para dar uma visão geral, Tim, que é o único não-insider da ICANN em nosso painel, vai começar.

Tim Maurer - Microsoft: Muito obrigado, Greg. É um prazer estar com todos vocês aqui. Eu estava conversando com a Ana, acho que a última vez que tivemos a chance de nos encontrar foi antes da pandemia, que também foi a última vez que tive a oportunidade de participar de uma reunião da ICANN. E é um prazer especial estar aqui com todos vocês hoje porque esta é uma comunidade pela qual nós, da Microsoft, estamos muito entusiasmados, na esperança de que possamos usar a IA e maximizar seu potencial para a defesa da internet e garantir que ela seja usada para realmente ajudar a alcançar o que esperamos que a tecnologia desbloqueie, que é um maior progresso humano, e também garantir que a usemos de maneiras que nos ajudem a avançar nos objetivos e metas existentes que compartilhamos.

Para o ponto de Greg, eu acabei de me juntar à Microsoft há pouco mais de um ano, então tem sido uma experiência fascinante para mim estar agora na empresa e na vanguarda da inovação em IA. E a maneira como estamos pensando sobre IA de forma mais ampla, mas também especificamente em relação ao abuso de DNS, é que estamos cientes do fato de que a IA existe há um tempo, dependendo de como você a define, e que o aprendizado de máquina e a IA preditiva, assim como a IA analítica, têm sido usados de várias maneiras para já mitigar o abuso de DNS.

Então, como Greg mencionou com o Copilot, a IA generativa vai, esperamos, nos ajudar a desbloquear mais potencial de várias maneiras e também tornar a forma como podemos ajudar a mitigar o abuso de DNS mais acessível a um conjunto mais amplo de defensores, quebrando barreiras que podem ter existido antes em relação ao nível de habilidades e usando IA generativa, em particular o Copilot, e outras ferramentas que temos para facilitar o uso de ferramentas pelos defensores para mitigar abusos.

Uma coisa que eu vou dizer logo de início, e depois espero tornar isso o mais interativo possível com os painelistas e todos vocês na sala, é que a empresa está olhando para a IA no contexto de segurança e no contexto de abuso de DNS através de três lentes.

A primeira é, como podemos maximizar o uso da IA para defesa? E isso significa, como mobilizamos clientes e a comunidade como a sua e a comunidade ICANN para adotar a tecnologia rapidamente? E a razão pela qual destaco a velocidade é que posso garantir que aqueles com propósitos nefastos estarão entre os mais rápidos a usar as novas ferramentas para descobrir como podem usá-las para avançar suas atividades maliciosas existentes. Então, quanto mais rápido todos nós pudermos tentar avançar a IA e usá-la para técnicas de defesa e mitigação, mais rápido podemos garantir que não apenas alcançaremos, mas também superaremos os atores de ameaça que estão atingindo organizações ao redor do mundo todos os dias.

A segunda peça que eu destacaria é que a empresa está, desde o início, muito focada em descobrir quais passos precisamos dar para que os atores mal-intencionados não possam tirar proveito de nossos produtos e serviços de IA. Então, há um ano, a empresa lançou uma política que deixou claro que, se detectarmos que um ator mal-intencionado que a empresa está monitorando, dos quais você pode imaginar que há muitos ao longo dos anos que no passado realizaram acesso não autorizado ou de outra forma chamaram nossa atenção. E notamos que eles estão usando produtos ou serviços de IA, tomaremos medidas para encerrar sua conta. Não importa se eles estão usando IA de forma produtiva. Não queremos que criminosos se tornem mais produtivos. Então, tomaremos medidas contra isso. E essa é uma política que veio da liderança, não em resposta a regulamentações ou pedidos do governo, mas foi um reflexo do compromisso de garantir que capacitamos o defensor e tentamos dificultar ao máximo a vida dos atores mal-intencionados envolvidos.

E então, a última peça, em termos de enquadramento geral, é que a empresa está focada no que precisamos fazer do nosso lado para garantir que a tecnologia não seja usada de forma indevida, considerando o Azure e nossos serviços de nuvem, e como também podemos proteger nossos produtos e serviços de IA, que, como você pode imaginar, estão sendo alvos de outros agentes mal-intencionados que gostariam de saber como os utilizamos internamente. Então, deixe-me usar isso como um enquadramento geral de três dimensões. Sei que há muito a discutir quando entrarmos nos detalhes do abuso de DNS.

Greg Shatan - NARALO / Moses Singer LLP: Muito obrigado, Tim. E eu percebi, claro, que você mencionou defesa de DNS ou defesa contra abuso de DNS várias vezes. Então, temos a sorte de ter conosco Jeff Bedzer, cuja vida é inteiramente definida pela defesa e limpeza do DNS. Não vou chamá-lo de novo xerife na cidade porque isso provavelmente é marca registrada de outra pessoa neste momento. Mas, de qualquer forma, Jeff, acho que... Ah, aí está. Você tem um distintivo. Não precisamos de distintivos fedorentos. Então, de qualquer forma, Jeff, gostaria que você aprofundasse um pouco mais. E sei que você tem um slide e provavelmente não foi escrito por um copiloto da Microsoft. Pode ter sido realmente escrito por você. Então, sem mais delongas, deixarei o slide e você falarem por si mesmos.

Jeff Bedser - SSAC / CleanDNS: Obrigado, Greg. E não, este não foi, mas não posso negar que já usei IA com sucesso para fazer muitos slides.

Vou aproveitar o fato de que falei com este grupo, parece que foi há uma semana, ontem, anteontem, sobre abuso de DNS em um sentido geral. E acho que esta apresentação que preparei é sobre como o CleanDNS está usando processos de IA para melhorar nessa luta, assim como Tim disse.

E mencionei, acho, na nossa apresentação, minha apresentação outro dia, que se você está pensando nisso agora, eles já pensaram, fizeram e provavelmente passaram para algo mais rápido porque estão muito à nossa frente. E se não usarmos as tecnologias emergentes na mesma velocidade e ritmo para defesa, vamos ficar tão para trás tão rápido que vai deixar todo mundo tonto.

Então, o que vou falar é sobre como temos implantado ativamente modelos de API no que fazemos porque, novamente, como eu disse outro dia, há um volume significativo de abusos que não conhecemos porque não estão sendo relatados. O que estamos vendo em todos esses relatórios ativos que estão sendo feitos são cerca de cinco a sete fontes que a maioria das pessoas usa para gerar os relatórios, mas isso é apenas a ponta do iceberg. E é literalmente, se você não vê, não é relatado. E a maioria das pessoas não relata o phishing ou o smishing ou qualquer outra coisa que estejam recebendo. Então, não sabemos sobre isso. Não podemos agir sobre isso.

Então, a melhor solução é detectar rapidamente. E quando você detecta rapidamente, pode mitigar rapidamente. E é nesse espaço que a CleanDNS atua. Estamos entre as empresas que detectam os abusos e a indústria ou nossa indústria entre os registros, registradores e empresas de hospedagem que precisam mitigá-los. E nosso objetivo é constantemente acelerar não apenas o relatório, mas a detecção. Para que possamos chegar ao ponto em que o processo entre detecção e mitigação leve segundos.

Enquanto isso, não sei se alguém leu aquele tomo do qual fui o presidente do grupo de trabalho do SSAC, SAC 115 sobre interoperabilidade e manejo ou gestão de abusos de DNS. Mas descobrimos nesse estudo, há vários anos, que o tempo médio era de 96 horas entre o relatório e a mitigação. E acho que todos podemos imaginar quantas

pessoas clicam em um link de phishing em 96 horas e quantas vítimas isso representa, e quantas menos se conseguirmos reduzir esse tempo para alguns segundos em vez de 96 horas. Então, vamos começar a apresentação.

Então, o SAC 115 foi o modelo a partir do qual decidi construir o CleanDNS porque muitas pessoas na indústria me apontaram que, embora fosse um ótimo artigo acadêmico, a menos que alguém construísse as soluções mencionadas no artigo, elas não iriam existir. E o CleanDNS foi construído para corresponder a isso. Eu gosto de chamar isso de ciclo virtuoso e darei crédito a quem merece. Byron Holland da CIRA usou esse termo comigo quando estávamos conversando sobre isso. Estamos tentando não apenas resolver um problema, mas também melhorar os relatórios e a indústria ao resolver o problema no meio do caminho. Agora, que tipo de evidência é necessária para agir sobre ele e, em seguida, encurtar o ciclo de eliminá-lo? Então, é um modelo de agregação para basicamente acelerar esse processo.

Então, ok, deixe-me explicar o que estamos fazendo com IA e isso.

Então, o primeiro é fácil e é um daqueles casos em que você pode ver rapidamente que a IA é melhor do que o humano. Todos aqui já foram vítimas de phishing. Alguém que não foi, por favor, explique por que está em uma conferência de tecnologia e não tem um telefone. Não? Ok.

Phishing é baseado em iscas. Uma isca é alguma empresa que faz você acreditar que está indo para algo que não é. Seja um banco, uma plataforma de e-commerce, sua operadora de telecomunicações, ou seu médico local, há uma isca envolvida. E essa isca é quase sempre uma imagem que faz você acreditar que é aquele banco, aquela plataforma de e-commerce, etc.

Bem, para os humanos que fazem a análise de phishing, eles não conhecem todos os bancos do planeta. Eles não conhecem todas as empresas do planeta. Eles não têm esse conhecimento. Eles têm feito isso por 30 anos. Eles nunca vão saber tudo. Os sistemas de IA podem acessar bancos de dados e sistemas que possuem esses arquivos de imagem para comparações rápidas.

Então, a análise de imagem pode lhe dar a capacidade de validar o logotipo. A análise de imagem pode verificar e ver se há uma tentativa de capturar credenciais. Há uma tentativa de capturar informações pessoalmente identificáveis? O que mais está dentro disso? E quando eu digo análise de imagem, é basicamente uma captura de tela. Então, a página de destino de um phishing, pharming, loja falsa ou smishing. Vou parar de usar todos os acrônimos. Mas você basicamente faz essa captura de tela e depois pode analisá-la pelo conteúdo. E então a IA é muito boa em dizer, sim, isso está estruturado de uma maneira que provavelmente é um phishing.

A análise de sentimento é baseada em olhar para o texto e outros componentes dele para dizer, cara, esse texto está pequeno na tela. Peço desculpas. Podemos compartilhar a apresentação depois, se todos quiserem.

Talvez eu possa ler na minha tela para você. Espere um momento.

Análise de relatórios de e-mails recebidos relacionados ao conteúdo e à intenção do remetente. Então, a indústria nos últimos 20 anos tem basicamente utilizado um mecanismo de relatório baseado em e-mail. E, claro, o problema com isso é que são dados não estruturados. Portanto, a análise de sentimento permite que você pegue esses dados de e-mail não estruturados e tente descobrir o que está acontecendo.

Os humanos são, por natureza, contadores de histórias. E quando algo acontece com você, você quer contar a história de como foi enganado e por que achou que essa pessoa pensava que você era tão atraente e que queria que você enviasse $50 para que ela pudesse te visitar. E as histórias são fascinantes de ler, mas levam muito tempo. E o que você realmente está procurando nesse texto é qual é o URL ou domínio envolvido? E do que você está acusando? Ah, você foi enganado e esse é o URL. Isso é tudo o que me importa. O resto da história é irrelevante para um esforço de mitigação. Então, a análise de sentimento nos ajuda a chegar lá.

E então uma relação contextual, novamente, colocando meus óculos, peço desculpas, é o vetor de incorporação das semelhanças entre os blocos de texto. Então estamos procurando padrões onde, por exemplo, spam ou phishing, é a mesma campanha do mesmo cibercriminoso porque eles estão usando a mesma estrutura, formato, etc. Assim, podemos desenvolver uma compreensão de grupos maiores. Não estamos derrubando um de cada vez. Podemos usar as relações contextuais para descobrir, ah, há 10.000 desses. Vamos derrubá-los todos de uma vez porque todos estão relacionados ao mesmo cibercrime com base no carimbo de data/hora, nas relações contextuais entre os dados.

Então, me adiantei um pouco, mas a detecção de logotipos é parte da análise de imagens. A detecção de PII é novamente. Uma das outras chaves é que muitos domínios que serão usados para abuso ou foram usados para abuso, eles colocam em uma página estacionada e colocam em uma página estacionada antes de usá-la para abuso. E às vezes eles a usam para abuso, voltam para uma página estacionada. Então, quando os bons estão olhando, eles pensam, ah, é apenas uma página estacionada. Não há nada lá. E então eles esperam que aquele tráfego vá embora e a ligam novamente. E agora é uma página de phishing novamente. Então, a detecção de se é uma página estacionada versus um phishing é um componente importante do uso da análise de imagens porque você não precisa de um humano para fazer isso novamente, o que encurta o tempo e acelera o processo.

Então, algumas possíveis futuras iniciativas que estamos considerando envolvem o ajuste fino de todo esse processo. É ótimo para phishing, mas que outros danos

podemos abordar aqui? Porque, novamente, o abuso de DNS, conforme definido sob as partes contratadas e suas obrigações, são aqueles que Greg mencionou. Mas todos nesta sala sabem que há muitos outros danos online e muitos outros danos online que precisam ser mitigados. E a maioria das partes que representam essas partes contratadas e a CCNSO agem sobre muitos outros tipos de danos que não são obrigados a agir, mas o fazem porque é a coisa certa a fazer. Então, como você ajusta um pacote de evidências que diz que esse tipo de dano, quando apresentado dessa forma, é um dano para que possa ser mitigado?

Detecção de código malicioso, certo? Isso é difícil porque, se você tiver que processar o código para determinar se é malicioso, estará colocando seus sistemas em risco de serem comprometidos. Então, usar a IA para analisar os padrões e identificar a qual família de malware isso pertence, quais partes estão envolvidas e como isso é direcionado é outro lugar onde a IA pode ser usada para combater isso.

E por fim, o componente de IA generativa disso, temos usado para estruturar as comunicações de saída para as partes afetadas. Se é um registro relatando a um registrador, usamos para gerar o texto explicando o que vimos, o que aconteceu, mas usamos para criar modelos, não para criar as comunicações reais porque qualquer um que tenha brincado com IA, como Greg apontou, e eu admito a história para ele, você tem que ser muito cuidadoso porque se a IA generativa sem restrições começa a fantasiar, e eu realmente tive que escrever um artigo para mim sobre todas as entidades trabalhando no abuso de DNS, e ela inventou algumas entidades ótimas que eu pesquisei, e pesquisei as notas de rodapé, e nenhuma dessas entidades existia. Os sites que eles referenciavam não existiam.

Então, você precisa ter muito cuidado com a IA generativa para controlar o ambiente a partir das restrições que você impõe a ela.

Então, armadilhas. Transparência. Não há ninguém que trabalhe comigo que não entenda que estamos usando essas tecnologias, e não queremos fingir que não estamos. Você precisa ficar atento aos vieses de dados, e isso também é uma preocupação legítima quando se trata de quais conjuntos de dados você aplica. Se eu começar a trazer conjuntos de dados de repórteres que têm muitos falsos positivos, mas não sabem que são falsos positivos, posso corromper todo o meu conjunto de dados na validação.

Por exemplo, se houver um monte de arquivos de imagem que na verdade não são de e-commerce ou bancos, e eles entrarem nesse conjunto de dados, e agora estão sendo confirmados como tal, esse viés pode ser problemático. Falsos positivos e negativos ainda exigem, em que ponto você os envia para revisão humana? Aparentemente, isso é com o Tim. Então, vou precisar do seu endereço de e-mail para isso.

Mas, é claro, a gestão de casos sensíveis sobre os dados e os controles desses dados, especialmente para fins de privacidade, etc. Então, eu acho que isso é

o último slide. Então, vou devolver a palavra a você, Greg.

Greg Shatan - NARALO / Moses Singer LLP: Muito obrigado, Jeff. Muito interessante e oportuno.

Agora, vamos passar para Ana Neves. Ana, você pode dizer o que quiser.

Ana Cristina Amoroso da Neves - GAC / Portugal: Ok, muito obrigada. Então, o que eu quiser, bem, é muito bom estar aqui em Seattle, e em particular aqui no At-Large. É sempre uma grande honra estar aqui no At-Large, porque desde o início da minha vida no GAC, eu sempre defendi que o GAC e o At-Large deveriam realmente trabalhar juntos, porque devemos aumentar nossos esforços no setor público e nos sites dos usuários finais.

Então, o que posso dizer depois que a Microsoft e Jeffrey falaram e explicaram o abuso de DNS? O que posso dizer sobre a Microsoft é que é muito bom saber que vocês têm uma política para mitigar o abuso de DNS. Mas e as outras empresas que não têm essa política? E essa política

é previsto por quem? E podemos confiar que as empresas tenham essa política? Podemos confiar? Por quê?

Então, da perspectiva do setor público, é isso que eu acho que fui convidado a fazer parte desta mesa-redonda.

para fortalecer a colaboração entre os setores público e privado e ter mais parcerias e ver com os órgãos reguladores o que pode ser feito, sempre tendo em mente a cibersegurança, e os governos, ao regulamentar ou pensar em políticas públicas, sempre considerarem o abuso de DNS. Portanto, os esforços multissetoriais são realmente importantes para garantir o uso responsável da IA na segurança do DNS.

Outro ponto importante que eu gostaria de destacar aqui é o desenvolvimento de estruturas de governança de IA. Então, acho muito bom discutir isso aqui na ICANN e junto com o AtLarge, que poderia explorar políticas que garantam que a segurança impulsionada por IA esteja alinhada com os princípios de governança da internet global. E este é um ano muito bom para fazer isso, pois estamos refletindo sobre a revisão do WSIS+20, como agilizar esse processo com o pacto digital global e o que realmente devemos prever em todos esses processos e negociações.

E a última coisa que eu gostaria de destacar neste meu primeiro comentário é capacitar os usuários finais. A proteção impulsionada por IA deve ser projetada com transparência, permitindo que os indivíduos façam escolhas informadas sobre configurações de segurança e privacidade. Portanto, é sempre uma questão de bom senso, mas também de manter os usuários finais bem informados. Assim, a capacitação

é sempre importante, a privacidade é sempre importante de sublinhar em todos os nossos esforços.

Então, eu diria que fortalecer a colaboração, ter mais parcerias público-privadas, desenvolver estruturas de governança de IA e capacitar os usuários finais são meus três primeiros itens para esta discussão e para esta mesa-redonda.

Muito obrigado.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Ana. Podemos voltar no slide onde parei antes, que é basicamente o primeiro slide real aqui. Então

vamos para o próximo slide, por favor, só para cobrir algumas das coisas que nossos bons amigos do Copilot encontraram, apenas para colocar alguns fatos a mais em evidência.

Estamos vendo ataques de phishing impulsionados por IA, que usam IA para personalizar o phishing, tornando-o um pouco mais parecido com spearphishing, imitando contatos confiáveis, contornando filtros de segurança, melhorando a sintaxe e a gramática, a menos que os erros estejam lá para garantir que pessoas inteligentes não os leiam.

Então, inicialmente, a IA também pode ser usada para pré-julgar credenciais, testar milhares de credenciais roubadas em segundos, possibilitando ataques de força bruta e basicamente, você sabe, a natureza repetitiva desses ataques. Este é um negócio de volume e, portanto, a IA pode aumentar o poder do volume nas ameaças de atores mal-intencionados.

O próximo malware também pode ser aprimorado pela IA com código que se adapta dinamicamente para evitar a detecção e, você sabe, ajudando-o a se esconder do software antivírus, que, claro, está procurando por padrões que conhece e aprende. Então, também, é claro, usando IA, novamente, uma espécie de batalha dos bots.

Também podemos ver o reconhecimento usando ferramentas de varredura de rede com IA em alta velocidade e escala, identificando pontos fracos na infraestrutura de segurança, você sabe, ataques de penetração automatizados também, e então, a engenharia social novamente pode ser tornada mais dinâmica, mais real, mas ainda falsa, para contornar filtros tradicionais, novamente usando IA para ajustar as coisas de modo que pareçam menos ameaças óbvias.

Então, isso claramente indica por que precisamos usar recursos de defesa sofisticados e em constante aprimoramento para acompanhar tudo isso.

Então, algumas dessas soluções, é claro, são ferramentas de segurança DNS com inteligência artificial usando arquitetura de confiança zero com uma verificação mais rigorosa. Acho que todos nós notamos mais uso de autenticação multifator, mais uso de diferentes tipos de autenticação e camadas, mesmo nos últimos seis meses a um ano, apenas para tentar acompanhar os níveis de ameaça.

Então, você sabe, as plataformas de inteligência de ameaças precisam continuar se aprimorando e, você sabe, Tim já mencionou isso, ou melhor, Jeff já mencionou isso. Claro, sempre há o fator humano. Você ainda precisa treinar pessoas reais, funcionários e usuários finais, o público em geral, sobre como reconhecer ataques de phishing e engenharia social, a conscientização precisa ser mantida constantemente. Acabei de fazer o treinamento anual de cibersegurança da minha empresa e provavelmente já está desatualizado.

Você sabe, como advogado, eu posso apreciar a necessidade de continuar aprimorando os frameworks legais. A lei nunca avança tão rapidamente quanto a IA, é claro, mas, você sabe, tentar manter tanto as regras legais quanto éticas de maneiras que governem a IA de forma mais responsável. Uma das coisas sobre as quais estou curioso é se as empresas que estão trabalhando com IA estão suficientemente cientes do universo de abuso de DNS, em oposição a todos os outros universos que estão usando IA. Nosso espaço, embora importante, não é necessariamente a prioridade. Então, se as empresas de IA estão fazendo o suficiente para trabalhar com o restante do ecossistema.

Por último, mas não menos importante, é claro, continuar com medidas de segurança mais proativas, uma maior paranoia também é crucial. Próximo slide, por favor.

Esta é a biografia do Jeff, pelo menos a que foi fornecida a mim pelo Microsoft Copilot. Você pode lê-la quando quiser. Parece bastante precisa, não inventou muita coisa.

Primeiro pedi a do Tim. Houve uma área que você deveria destacar. Ah, não. O que foi?

Jeff Bedser - SSAC / CleanDNS: Volte um slide. Volte um slide.

Greg Shatan - NARALO / Moses Singer LLP: Olhe o ano na parte inferior do segundo parágrafo.

Jeff Bedser - SSAC / CleanDNS: Ah, o ano 2071.

Greg Shatan - NARALO / Moses Singer LLP: Bem, na verdade, isso aconteceu porque havia uma nota de rodapé que eu não removi. Então, foi um erro humano.

Esta foi a primeira tentativa usando IA para obter a biografia do Tim. Não mencionou a Microsoft de forma alguma. Novamente, espero que seja mais ou menos precisa, mas, novamente, não está atualizada.

Coloquei Microsoft no prompt.

Adicionei Microsoft ao prompt e, voilà, descobrimos que ele é o Diretor Sênior de Política Global de Cibersegurança na Microsoft. Mas eu não teria sabido disso se não tivesse colocado no prompt. Então, o Microsoft Copilot ainda não conhece bem o Tim. Mas vejo que ele está tomando notas, então isso provavelmente será corrigido.

Eu queria saber mais sobre Tim e seus hobbies. Então, caminhadas, ciclismo, fotografia, leitura. Ele tem interesses diversos e um compromisso com o crescimento pessoal e bem-estar. Pelo menos é isso que o Microsoft Copilot diz.

Esta é a biografia da Ana. Novamente, não chega aos pés da biografia que ela nos deu, mas não parece estar completamente fora do tópico. Mas, próximo slide. Minha primeira tentativa resultou em uma Ana Neves completamente diferente, Ana Luisa Neves. Eu não usei o nome do meio dela nisso, mas essa pessoa também está muito no nosso mundo, de certa forma. Ela é Diretora de Saúde Digital Global no Imperial College em Londres. E espero que vocês duas se encontrem em algum momento. E se não, talvez devessem se procurar. Provavelmente têm muitas coisas interessantes para discutir sobre o nosso futuro digital. Próximo slide, por favor.

Este sou eu, se você quiser saber algo sobre mim. Isso está um pouco desatualizado. Como eu disse, já participei de mais de 10 reuniões da ICANN. A resposta real é mais de 35 reuniões da ICANN. E eu não sou mais o Presidente da ISOC Nova York. Eu me rebaixei para Secretário, ainda estou no conselho. Todo o resto é mais ou menos verdade. Próximo slide, por favor.

É isso. Esta é outra foto de Seattle na neblina, escolhida pelo Microsoft Copilot. Então, vamos nos afastar dos slides. Você pode deixar esta aqui. É meio bonita, embora um pouco apocalíptica.

Vamos entrar na discussão sobre a ofensiva e defensiva da IA. E estou me perguntando, vou começar com você, Jeff. O que você espera nas próximas etapas? E quando você olha para como a IA está mudando, o que isso vai fazer na área de abuso de DNS em que estamos?

Jeff: Essa é uma ótima pergunta, Greg. Cara, espero que ninguém esteja ouvindo isso e tirando ideias de mim.

Então, acho que o espaço onde veremos mais isso é na gestão de identidades e identidades falsas. A capacidade da IA de criar cartões de identidade nacionais e locais

quase perfeitos, com as identidades de pessoas reais, mas talvez com uma foto alternativa e tal, tornando quase impossível distinguir uma pessoa real de uma falsa, é uma grande preocupação.

Vou reformular a transcrição com a devida atribuição dos falantes e estrutura de parágrafos:

E então, quando você pensa no fato de que agora pode dizer, ok, IA, não a IA dele, porque está impedindo essas coisas, e não estou sendo sarcástico. A dele realmente impede essas coisas. IA, eu quero um número de cartão de crédito que ainda não foi usado e que foi roubado de uma violação. Quero combiná-lo com um ID da mesma pessoa com o endereço residencial real dela. E se ela estiver domiciliada no estado da Pensilvânia, nos EUA, quero uma carteira de motorista que corresponda ao modelo da carteira de motorista da Pensilvânia. E quero colocar minha foto nela de uma maneira que pareça uma foto de carteira de motorista. Então, acho que sem sorrir. E depois gerar essa imagem para que, quando eu quiser comprar um domínio, comprar alguns serviços com esse cartão de crédito roubado, ele passe por todas as verificações de conheça seu cliente. O cartão de crédito não foi sinalizado antes. Há um ID perfeito para combiná-lo. E tudo isso foi gerado em, não sei o que você acha, quatro ou cinco segundos.

Que quando se trata de cibercrime, o cibercrime precisa ser alimentado por algo. É principalmente alimentado por cartões de crédito roubados e contas bancárias comprometidas. E você chega a esse dinheiro basicamente com credenciais roubadas modificadas. E a maneira de obter essas credenciais é basicamente através dessas credenciais sólidas que validam quem uma pessoa real é. Acho que essa é uma das maiores questões que veremos emergir e que realmente vai mudar o cenário rapidamente.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Jeff. Tim, vou fazer uma pergunta semelhante, mas também vou pedir que você pense na pergunta anterior que fiz, que é o que os desenvolvedores de IA estão fazendo em particular? Eles estão cientes do nosso espaço de abuso de DNS em comparação com todas as outras coisas potenciais que a IA pode ser usada para o bem e para o mal?

Tim: Sim, a resposta é sim, em parte porque é do interesse da Microsoft, dado que também operamos uma infraestrutura de nuvem significativa e dependemos de garantir que, no geral, a internet funcione de uma maneira que não seja abusada por agentes mal-intencionados.

Para apenas expandir o exemplo que ouvimos sobre a maneira como os atacantes estão usando isso, acho que há algumas boas notícias nisso. Desde o advento da IA generativa e dos vários modelos que foram lançados, houve alguns que previram um cenário muito mais apocalíptico e o que poderia acontecer. Não vimos o ressurgimento de worms que vimos no início dos anos 2000, que você poderia imaginar que a IA

generativa escreveria novos códigos que teriam evitado os mecanismos de detecção existentes ou apenas os filtros. O que vimos principalmente é que os atores de ameaças existentes adotam incrementalmente a IA para TTPs conhecidos e avançam seus objetivos. Isso não é ótimo, obviamente, mas em termos do espectro de possibilidades, acho que há algumas boas notícias aqui em termos do que vimos.

Então, acho que já há algumas lições interessantes aprendidas olhando para os últimos meses em termos de como os defensores estão usando isso. Como você demonstrou com seus prompts, a IA pode ser divertida ao ver o que ela produz, mas também destaca a importância de como você realmente usa a tecnologia, quais prompts você está usando, quão específicos são os prompts, e traduzir isso agora em técnicas defensivas. Se você, por exemplo, usar um Copilot ou um Copilot para segurança ou qualquer um dos outros produtos e serviços de IA para produzir relatórios específicos quando uma anomalia é detectada e apenas usá-lo para automatizar mais, por exemplo, sinalizando que uma anomalia específica foi detectada, produzindo um resumo executivo.

Também queremos garantir que instruímos o modelo a errar pelo lado de incluir mais, em vez de menos, potenciais anomalias para que capturemos os falsos positivos, porque o que os humanos devem fazer é revisar o que é sinalizado, e preferimos capturar mais falsos positivos que podemos descartar do que o modelo potencialmente reduzir o número de sinalizações que podem incluir mais falsos negativos do que qualquer outra coisa. Então, eu realmente acho que, primeiro, o humano continua sendo importante. A maneira como podemos aproveitar a IA é idealmente usada de uma forma que nos ajude a usar os humanos de maneira mais eficaz, e o que, em relação ao seu ponto sobre escala, me deixa um pouco otimista é, apesar das preocupações que você mencionou, especialmente sobre a questão da identidade, com a qual concordo completamente, que um dos principais desafios que tivemos no lado defensivo tem sido a falta de habilidades e pessoas suficientes treinadas para realizar certas tarefas, o que, se conseguirmos usar a IA em escala para reduzir essas barreiras de entrada e usá-la para produzir relatórios que sejam mais facilmente consumíveis até mesmo para pessoas menos habilidosas em cibersegurança, então podemos ter um efeito positivo em termos da avaliação geral de se a IA está ajudando a avançar na defesa ou no ataque.

Só uma rápida observação sobre o ponto da Ana que eu não queria deixar sem comentar sobre a importância do engajamento entre o setor privado e o setor público. Acho que, olhando para os últimos três anos, tem sido fascinante ver como, após o lançamento do chat GPT e a manchete do New York Times, quão rapidamente os reguladores, como com o Ato de IA da UE ou no governo dos EUA, com as várias políticas em vigor, implementaram rapidamente novas regulamentações, leis e políticas, a ponto de as empresas terem que se certificar de que estavam acompanhando. E com o surgimento dos institutos de segurança de IA, que, novamente, têm o objetivo de garantir que temos mitigadores em vigor para que você não possa simplesmente digitar, oh, me diga este número de cartão de crédito. Tenho ficado bastante

impressionado com a rapidez com que governos e reguladores colocaram estruturas em prática em um período muito curto de tempo e como eles se engajaram com o setor privado, seja a Microsoft, seja muitas outras empresas, para tentar colocar algumas estruturas em prática que são baseadas em riscos e focadas no que devemos prestar atenção.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Ana. Gostaria de obter sua perspectiva e, particularmente, vou pedir uma perspectiva europeia porque nós três, entre outras coisas que temos em comum, estamos sempre nos Estados Unidos, o que, claro, também está mudando massivamente. Mas precisamos, eu estaria interessado em colocar algumas perspectivas diferentes na discussão aqui.

Ana Cristina Amoroso da Neves - GAC / Portugal: Sim, absolutamente. Então, na Europa, acho que entendemos que o cenário de ameaças para abusos de DNS está evoluindo rapidamente com a IA e o aprendizado de máquina. Então,

estamos tentando desenvolver diretrizes para o uso ético da IA na prevenção de abusos de DNS, ao mesmo tempo em que abordamos preocupações de privacidade relacionadas à análise de tráfego de DNS impulsionada por IA.

Então, temos este relatório feito na União Europeia. O estudo abrangente da União Europeia sobre DNS

abuso, que fornece recomendações para registros e registradores. É de, eu acho, dezembro de 2022. E é interessante ver que domínios como .de e .eu

são os domínios que são menos abusivos. Então, onde o abuso de DNS não é

tão forte. Então, isso é uma evidência de que algum trabalho e a implementação técnica e esse tipo de colaboração entre os setores público e privado são muito importantes.

É muito importante também trabalhar em conjunto com pesquisadores em IA, porque são eles que podem nos ajudar na prevenção. E, portanto, ter esses componentes de prevenção antes do que pode acontecer é muito importante. Então, novamente, a participação de múltiplas partes interessadas é tão importante em todos esses processos digitais e o abuso de DNS é mais um. Portanto, a importância de incluir a academia, pesquisadores e desenvolvedores de IA em todos esses processos é

tremendamente importante. E assim, somente com esse tipo de envolvimento e ouvindo todas essas pessoas e entidades e diferentes partes interessadas envolvidas, podemos alcançar diferentes camadas de políticas, sejam políticas para empresas, sejam políticas públicas para abordar o abuso de DNS. Essa é a minha opinião por enquanto.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Ana. Temos muitas pessoas na sala e também virtualmente. Então, gostaria de passar para a sessão de perguntas e respostas. Se você estiver remoto, por favor, coloque suas perguntas no pod de Q&A e elas serão lidas em voz alta por Michelle DeSmyter. E se você estiver na sala e estiver no Zoom, por favor, levante a mão e vejo que a mão de Joanna está levantada. E se você não estiver no Zoom, apenas levante a mão. E se você não estiver na mesa, temos um microfone móvel que virá até você. Então, não seja tímido se não estiver sentado perto de um microfone. O microfone virá até você. Então, começaremos com Joanna Kulesza.

Joanna Kulesza - ALAC / University of Lodz: Obrigada. Muito obrigada, Greg. Esta é Joanna Kulesza para fins de transcrição. Obrigada por todas as apresentações. É maravilhoso ouvir sobre a ligação entre IA e DNS.

Eu tenho uma pergunta que se baseia na intervenção da Ana e naquele último comentário. Acho que faz sentido direcioná-la ao Tim. Muito obrigado por essa revisão tão abrangente. Você meio que abordou isso. Não sei se você se sente à vontade para responder com seu chapéu da Microsoft. Então, sinta-se à vontade para escolher como abordar isso. Temos um histórico de pesquisa, um histórico de pesquisa compartilhado. Portanto, se você quiser falar sobre políticas globais de cibersegurança, isso também é perfeitamente aceitável.

Vou começar com um pouco de contexto para essa pergunta, mas depois gostaria de ouvir seu feedback. Por um lado, a Microsoft foi vital no apoio à Ucrânia após a agressão russa sem precedentes. A inteligência, cibersegurança e análise de ameaças da Microsoft foram essenciais para os ucranianos prepararem suas defesas. A situação pode mudar em breve. Parece que o compartilhamento de informações foi interrompido. Agora pode estar voltando. Acho que isso é uma indicação muito clara de como a regulamentação nacional pode visar tentativas de garantir a cibersegurança, seja no nível de abuso de DNS ou, de forma geral, no que diz respeito ao compartilhamento de informações.

Por outro lado, Ana mencionou, e você também indicou isso, que há uma regulamentação aprimorada sobre IA, incluindo o AI Act. O senador Cruz, em dezembro do ano passado, disse que o AI Act atrasa a inovação e poderia ser considerado uma interferência estrangeira no desenvolvimento de IA nos EUA. Agora, isso me leva ao meu último ponto e à pergunta em si. Nossa boa amiga, Marietje Schaake, publicou um livro, o Tech Coup, você deve estar ciente do conceito. E recentemente, ao falar sobre isso, ela mencionou que este poderia ser o momento quântico para pesquisadores que não se sentem muito confortáveis pesquisando nos EUA se mudarem para a UE.

A UE, disse ela, deveria estender o tapete vermelho, meio que em um cenário reverso ao que testemunhamos em meados da década de 1930. Então, com seu chapéu de pesquisador, não tenho certeza se é uma pergunta confortável para a Microsoft responder, e eu não a faria neste contexto. Qual você acha que é o papel da regulamentação no desenvolvimento de IA para a cibersegurança? E vou transformar

isso em uma pergunta relacionada à política antes que Jonathan me coloque no meu lugar. O que a comunidade de usuários finais pode fazer, talvez trabalhando junto com o comitê consultivo governamental, para garantir que usamos a IA para proteger os indivíduos dos cibercriminosos? Acredito que seja uma maneira diplomática de fazer uma pergunta. E sei que você pode identificar claramente o desafio geopolítico que estou tentando abordar. Quaisquer pensamentos que você possa compartilhar serão apreciados. Muito obrigado.

Tim Maurer - Microsoft: Obrigado, Joanna. E também é bom vê-la novamente, o que acho que remonta aos dias pré-pandemia e antes do meu tempo no governo.

Estou feliz em responder a isso em nome da Microsoft, porque a empresa tem sido muito clara em relação a alguns dos desafios geopolíticos que enfrentamos e está muito comprometida com a cibersegurança, tanto para a empresa quanto para os clientes. Existe a iniciativa de futuro seguro, que colocou a segurança de volta no centro das atenções para toda a empresa.

Deixe-me abordar o último ponto primeiro sobre o que esta comunidade pode fazer. Acho que estamos em um momento realmente crucial de inovação tecnológica, onde o progresso que estamos fazendo com a inteligência artificial e a Microsoft tem lançado novos produtos e serviços de forma bastante regular e planeja continuar fazendo isso, é para que esta comunidade nos ajude a descobrir a melhor forma de usar a tecnologia para o bem e, neste contexto, particularmente para a defesa. E isso realmente depende de vocês, podem apostar que as pessoas focadas em monetizar ações nefastas serão rápidas em testar como essas novas ferramentas podem ajudar a avançar seus objetivos. Então, precisamos garantir que sejamos tão rápidos na adoção da tecnologia. E se vocês identificarem áreas onde vejam vulnerabilidades, onde considerem haver questões de pesquisa nas quais uma empresa como a Microsoft deveria se concentrar, por favor, compartilhem isso conosco, porque estamos no mesmo barco tentando garantir que maximizamos o potencial da tecnologia para o bem. Portanto, definitivamente, acolhemos, seja através do GAC ou de outros mecanismos, contribuições desta comunidade e queremos ouvir todos vocês.

Sobre o último ponto, sobre o primeiro ponto apenas sobre a UE e a regulamentação, a empresa tem sido muito clara ao afirmar que acreditamos que há certas áreas onde a regulamentação será útil. Acho que onde a empresa e a Microsoft começam a se preocupar mais é se a regulamentação for muito prescritiva e não focada em resultados, dado o ritmo acelerado da tecnologia. E quando começamos a ver diferentes estruturas regulatórias surgindo em muitos países e jurisdições diferentes que às vezes são divergentes ou até mesmo conflitantes entre si, porque então rapidamente entra no território de se tornar um desafio para nós navegar e implementar. Portanto, acreditamos que agora estamos à beira de fazer avanços significativos onde, conforme meu comentário anterior sobre o talento, podemos ser capazes de inclinar a balança em nível sistêmico a favor da defesa. Então queremos garantir que alcancemos esse potencial.

Greg Shatan - NARALO / Moses Singer LLP: Muito obrigado, Tim. E obrigado, Joanna, pela pergunta muito abrangente. Se pudermos passar para a seção de perguntas e respostas a seguir, e depois disso, iremos para Hadia.

Michelle DeSmyter - ICANN: Obrigada, Craig. E aqui é Michelle para o registro. Temos uma pergunta de Saeed Najeeb. Qual método está sendo usado para encontrar IA no CleanDNS?

Jeff Bedser - SSAC / CleanDNS: Bem, os métodos que usamos estão na apresentação. Eu sei que internamente usamos o Copilot para usos internos. Mas na plataforma, acho que isso é provavelmente proprietário. Estamos usando um disponível comercialmente, mas não tenho permissão para divulgar qual.

Michelle DeSmyter - ICANN: Tudo bem. Nossa próxima pergunta vem de Siva Subramanian. Por outro lado, a IA não pode ser usada para projetar sites de phishing que pareçam mais autênticos a tal ponto que o site de phishing esteja livre dos padrões e elementos típicos?

Jeff Bedser - SSAC / CleanDNS: Vou responder essa pergunta.

Então, sim. Mas um site de phishing não é apenas a página de destino. E os outros detalhes sobre a infraestrutura ao redor desse site. Então, por exemplo, a maioria dos sites de phishing foi criada com o propósito de phishing. Quero dizer, há alguns hosts comprometidos, mas a maioria é um registro malicioso para criar esse site. Portanto, a idade do domínio é um fator chave, assim como a estrutura, os servidores de nomes subjacentes, IPs, a reputação deles. Muitas vezes você descobrirá que o endereço IP subjacente e os hosts são hosts à prova de bala, e hosts à prova de bala são aqueles, o nome à prova de bala vem do fato de que eles não respondem a intimações ou qualquer tipo de processo e não registram nada. Isso realmente não é uma prática comercial legítima. Então, se você está fazendo isso, basicamente significa que está facilitando atividades criminosas. Portanto, há muitos fatores a considerar além da página de destino. Mas sim, as páginas de destino estão ficando cada vez melhores usando IA. Não há dúvida sobre isso.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Jeff. Em seguida, vou passar para Hadia Elminiawi na sala.

Hadia está se aproximando do microfone.

Hadia Elminiawi - SSAC / AFRALO: Obrigada, Greg. E aqui é Hadia, para constar. Minha pergunta é para Ana. Então, Ana, você falou sobre transparência na IA. E minha pergunta para você é: o que transparência significa em termos práticos? Isso significa

IA de código aberto? Sabemos, por exemplo, que a IA de código aberto ainda não desmistifica como a IA toma suas decisões. E sistemas de caixa preta continuam sendo caixas pretas, mesmo com código aberto. Então, em termos práticos, o que isso realmente significa? Obrigada.

Ana Cristina Amoroso da Neves - GAC / Portugal: Obrigado por essa pergunta. Muito interessante. Acho que quando mencionei a transparência da IA, estava falando sobre transparência e responsabilidade. Então, os modelos de IA devem ser explicáveis. Isso permite que os operadores da NES e os profissionais de cibersegurança entendam os processos de tomada de decisão. Se você não entende pelo que está lutando, fica muito difícil. Portanto, se os modelos de IA puderem ser explicáveis, é muito mais fácil abordar o que pode estar errado. Então,

é isso em poucas palavras. Obrigado.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado. Jonathan, você tinha uma pergunta?

Jonathan Zuck - ALAC: Sim, Jonathan Zuck para constar.

Eu só tenho minha própria IA, que acho que vou chamar de inteligência antiga, para detectar tentativas de phishing e coisas assim. Mas parece que a maioria dos e-mails de phishing está de alguma forma ligada a entidades com marcas registradas ou a grandes nomes reconhecíveis. E em algum lugar embutido nesse e-mail há um link para um site de farming. E acho que estou curioso sobre o grau em que um gerenciador de e-mails poderia olhar e detectar de quem isso deveria ser e verificar os links que estão embutidos no e-mail e ver se eles são de propriedade da entidade que o e-mail parece ser. Parece uma tarefa bastante simples para uma IA, mas acho que não vi nada assim até hoje. Quero dizer, lembro-me de ficar realmente surpreso um dia quando cliquei em enviar no Gmail e ele disse: "Ei, parece que você quis anexar um arquivo". E fiquei realmente empolgado e depois um pouco assustado, mas, você sabe, ok, eles estão lendo a mensagem. Quero dizer, na entrada, parece que esse tipo de análise diz: "Ei, isso parece ser da Norton Utilities, mas os links embutidos nele, então tenha cuidado" ou algo assim.

Tim Maurer - Microsoft: Acho que isso remonta ao que discutimos no início sobre quando falamos de IA, muito disso não é novo e que na verdade já temos uma boa quantidade de sistemas em vigor que são baseados em aprendizado de máquina e algoritmos que, para o seu ponto, são as razões pelas quais muitos e-mails vão diretamente para a pasta de spam, porque existem filtros que agora estão em vigor em comparação com 15, 20 anos atrás, que tornam sua caixa de entrada mais limpa do que costumava ser. É aqui que eu acho que, para o seu ponto e também o que você levantou, o verdadeiro potencial que esperamos ver com a IA no futuro é conectar melhor alguns dos pontos que não foram capazes de se conectar e trazer diferentes fontes de dados e insights juntos para que você possa detectar se um site foi registrado

de uma maneira onde temos preocupações sobre a identidade por causa do comprimento da página. E é aí que pensamos que o verdadeiro potencial pode estar, além de torná-lo mais amigável e consumível e, no ponto sobre explicabilidade, descobrir o que é que o humano realmente precisa saber e ler para então agir sobre isso. Então, espero que isso responda à sua pergunta.

Greg Shatan - NARALO / Moses Singer LLP: Estamos além do tempo, mas vou aceitar uma última pergunta. Amrita, por favor.

Amrita Choudhry - CCAOI: Muito obrigada, Greg. Amrita, para constar, tenho duas perguntas. Uma é, eu gostaria de entender basicamente de Tim, você e Jeffrey, temos falado sobre o abuso da língua inglesa e como a IA pode ou não pode usá-la ou agravá-la. E quanto aos falantes de outras línguas? Porque essa é a maioria global, o que está acontecendo lá. A segunda é que estamos vendo que o abuso de nomes de domínio está crescendo. Conteúdo, obviamente, mas o efeito financeiro e de reputação em todos os lugares. E especialmente vindo de países da maioria global onde você tem novos usuários que não são tão alfabetizados digitalmente ou mesmo alfabetizados até certo ponto. Então, o que vocês estão fazendo para esses usuários finais, com vídeos ou tutoriais de treinamento, etc? Como vocês estão fazendo, especialmente quando a Microsoft, há cerca de 10 anos, tinha cursos de alfabetização digital para as pessoas. Então, para esse tipo de segurança, o que vocês estão fazendo? Porque as pessoas também estão perdendo dinheiro. Obrigada.

Tim Maurer - Microsoft: Vou começar e depois...

Então, a Microsoft, com seus negócios ao redor do mundo, está lançando produtos, serviços e modelos em vários idiomas, incluindo questões de segurança em relação aos nossos esforços de red teaming, que não ocorrem apenas em inglês, mas também em outros idiomas. Estamos muito comprometidos em garantir que a tecnologia seja acessível para pessoas em todo o mundo e que as medidas de mitigação de segurança e proteção sejam refletidas de acordo com os usuários que as utilizam.

Com relação à capacitação e treinamento, fizemos um grande anúncio no ano passado em relação ao Quênia e com um foco específico no sul global, porque estamos muito conscientes de que queremos usar a tecnologia para trazer novos usuários online e garantir que eles saibam como usar a tecnologia. Também temos muito treinamento interno onde todos somos incentivados a usar a tecnologia. Então, não é apenas focado em grupos de usuários específicos ou países. Acho que é um esforço geral para garantir que forneçamos o treinamento junto com o lançamento de novos produtos e serviços, para que possamos maximizar o impacto da tecnologia.

Jeff Bedser - SSAC / CleanDNS: Então, obrigado por esse ponto importante, porque eu realmente esqueci de mencionar na minha apresentação que não se trata apenas de inglês. Mas sim, as ferramentas utilizadas são feitas para qualquer idioma em que a ameaça apareça, seja na análise de imagem, seja no texto. E isso, novamente, é uma

das razões pelas quais a IA é tão eficaz para nós, porque eu não preciso ter alguém na equipe que fale e leia todos os idiomas do mundo. A IA pode fazer a avaliação do idioma, determinar o que está acontecendo e extrair os componentes relevantes.

Então, sim, um componente muito importante é garantir que lidamos não apenas com os idiomas majoritários, mas com todos os idiomas, porque, como estamos fornecendo serviços ao redor do mundo, vemos phishing, malware, etc., sendo entregues em todos os idiomas. Portanto, usamos a IA de forma eficaz para nos ajudar com o fato de que eu não poderia arcar com uma equipe tão grande que gerenciasse todos esses idiomas.

Greg Shatan - NARALO / Moses Singer LLP: Obrigado, Jeff. Chegamos ao fim do nosso tempo. Infelizmente, ainda temos algumas perguntas interessantes. Desculpe, Dana e Atif. Mas esta é, claro, uma discussão contínua. Gostaria de agradecer a todos os nossos palestrantes, Jeff Bedser, Tim Maurer, Ana Neves, por estarem aqui. Gostaria de agradecer a todos por ouvirem e fazerem deste um debate memorável da NARALO. Voltaremos a esta sala daqui a meia hora para a assembleia da NARALO. Obrigado. E esta reunião está encerrada.