ICANN81 | Assembleia Geral Anual – Encontro conjunto: GAC e SSAC
Domingo, 10 de novembro de 2024 – 16h30 às 17h30 TRT

JULIA CHARVOLEN: Oi. Bem-vindos a reunião do GAC e SSAC. Eu sou Julia, da equipe de apoio. A sessão está sendo gravada e é regida pelos padrões de comportamento da ICANN e pelas políticas anti-assédio.

As perguntas e comentários serão lidas em voz alta se forem inseridas no chat. Teremos interpretação simultânea dos seis idiomas da ONU e português. Levante a mão no Zoom para pedir a palavra, digam em que idioma forem falar se não for inglês. Passo a palavra a Nigel Hickson.

NIGEL HICKSON: Oi, boa tarde. Já me ouviram falar muitíssimo, mas nesta sessão vou falar menos e amanhã nada. O Nico se desculpou porque ele tem uma sessão no board da ICANN. A relação do GAC e SSAC, a proporção de sessões entre o GAC e o SSAC.

E como deve ser de participantes. É um prazer ter essa oportunidade aqui de encontrar-nos com o SSAC, como faz anos que fazemos e é muito interessante ouvir eles e eu vou moderar as perguntas. Mas eu passo a palavra a Ram.

RAM MOHAN: Obrigado por convidar o SSAC aqui no GAC, é sempre um prazer estar aqui. Eu sou presidente do SSAC, e antes de começar com a agenda, eu

vou aqui apresentar meus colegas para que cada um deles se apresente. São todos os membros do SSAC e vocês verão a diversidade em conhecimentos e experiência. Aqui a minha direita Rod Rasmussen, Merike Kaeo, Greg Aaron, Robert Guerra, Warren Kumari, John Levine, Steve Crocker, Tara Whalen.

TARA WHALEN: Tara Whalen, eu sou vice-presidente do SSAC.

BARRY LEIBA: Barry Leiba. Queria aqui advertir que o Warren tem um chapéu melhor do que o meu.

SUZANNE WOOLF: Sim, em geral tem muitos chapéus aqui.

RAM MOHAN: Tem outros membros que estão levantando a mão aqui no fundo da sala para participar dessa sessão, então muito obrigado aqui, Nigel, pelo convite. Aqui tem alguém que precisa ainda levantar a mão, mas tudo bem. Pensamos que primeiramente, considerando que nem todos vocês já nos conhecem, vamos dedicar uns minutos para apresentar e quem somos nós, o que fazemos e depois passaremos para os assuntos na pauta.

E, se observamos a missão da ICANN, fica claro que a SSAC tem a incumbência de cumprir a missão da ICANN, somos o Comitê Consultivo. Como vocês, não temos um poder formal na estrutura da ICANN e isso está muito bem, porque as recomendações devem ser algo natural, que aparecem, desaparecem e não são sujeitas a eleições ou votação.

E aqui nesses slides vemos que nos encontramos no mundo inteiro ou na maioria das partes desse mundo e estamos aumentando ainda mais a diversidade entre os membros. E este ano temos nove novos membros e dois deles da África e de outras partes do mundo. Isso é muito bom. E a razão fundamental de porque o pessoal que está no SSAC são selecionados para fazer parte do SSAC é porque eles têm uma experiência específica e profunda da área em que se especializam.

São especialistas ou tem experiência no seu campo de ação técnica. São pessoas que são especialistas em diferentes áreas e com muitos conhecimentos, muita expertise e isso é porque, principalmente, estamos focados em fazer recomendações técnicas à comunidade na qual os servimos. E temos um grupo então de pessoas do campo técnico.

Essa é a equipe de liderança do SSAC. Aqui a minha esquerda vemos os membros selecionados e eleitos para fazer parte da equipe de liderança e também vemos a equipe de apoio para políticas. E eu queria mencionar isso, especialmente porque a diferença de outras partes da ICANN é que a equipe de apoio... No SSAC temos Steve Cheng, entre outros, mas principalmente eles são especialistas qualificados por direito próprio e contribuem para as nossas discussões e não são apenas tomadores de notas, mas eles, contrariamente, oferecem e fazem contribuições muito úteis sobre os diferentes assuntos que nos interessam e vemos aqui vários deles.

E se observamos todo o SSAC, vemos que há ainda uma maior variedade de pessoas, pessoas da sociedade civil, centro acadêmico, empresas, governos, forças de policiamento, supervisão. E para entrar no SSAC é um processo aberto de solicitações. Há um comitê de membros no SSAC que classifica as solicitações, faz as entrevistas e também recomendam novos membros.

O SSAC, portanto, apoia essas pessoas, oferece uma lista de membros recomendados, diretorias. E a diretoria da ICANN, finalmente, designa essas pessoas. Eu vou pedir a Tara que fale sobre essa questão aqui, que está no centro do que o SSAC faz.

TARA WHALEN: Muito obrigada. Nós produzimos muito material técnico. Já faz anos que fazemos isso com assuntos variados como segurança, estabilidade, identificadores únicos, todo um feixe de assuntos e sempre voltamos aos nossos assuntos de base com foco e neles disponibilizamos esses materiais para a comunidade e vocês podem recorrer ao SSAC para também fazer consultas, aqui estão os assuntos principais.

O principal é o abuso ao DNS, porque o DNS é um sistema muito importante com muito abuso online e é uma ferramenta muito útil para os maliciosos. E também é importante o que nós fazemos para mitigar esses atos criminosos.

E uma segunda área que para aqueles que estão esperando para a nova rodada, estão os novos gTLDs, que sempre são agregados novos nomes no sistema. E aqui surgem problemas de segurança e estabilidade

como a coalizão de nomes. É feita uma análise pela qual estudamos que acontece quando há uma expansão para evitar confusão entre as cadeias de caracteres e sempre recebemos consultas para oferecer recomendações sobre esse assunto.

E terceiro, DNSSEC que tem a ver com a segurança, a tecnologia da segurança, já trabalhamos faz tempo nisso com uma tecnologia que estamos tentando implementar e é um assunto complexo, é uma tecnologia complexa. É necessário um tempo para entender como funciona. E há coisas como ter uma melhor automação para que haja uma melhor funcionalidade do DNSSEC.

Também estão os espaços de nomes altamente. Essa é uma questão que surgiu já faz uns anos com o aparecimento dos blockchain, mas há outros sistemas de espaços de nomes, como pessoas, como a criptomoeda, que permitem que você compre diferentes domínios. Com isso traz problemas e isso coexiste também e interage com o DNS. E por último, um assunto que está muito presente aqui é a governança da internet, especificamente sobre os assuntos da segurança e estabilidade, são muito importantes aqui.

Há muitos problemas na internet quanto a segurança, estabilidade e para tomar decisões num espaço é muito útil que vocês tenham uma orientação muito clara e muito útil dos especialistas, os experts técnicos. E também sabemos que o nosso trabalho se torna mais forte quando recebemos o input daqueles que estão trabalhando, que fazem essas consultas. Isso nos permite dar respostas detalhadas.

É importante interagir com aqueles que consultam e nós chamamos os especialistas, os assuntos são consultados, por exemplo, no espaço das políticas e trabalhamos de forma colaborativa para elaborar o tipo de recomendação certa. E agora temos alguns grupos de trabalho que estão produzindo materiais e duas das iniciativas atuais são as de um grupo de software de código aberto e gratuito.

A infraestrutura do DNS, alguns de vocês sabem que muitos dos componentes são implementados na infraestrutura do DNS e muitos são iniciativas de código aberto que podem ser grupos grandes ou pequenos, com diferentes montantes de fundos de financiamento, como contratos, seguros, relações em diferentes partes e essa é uma parte da infraestrutura crítica do funcionamento do DNS.

Seria útil que mostrar algumas das dependências nesse sentido. E também fazer perguntas ou premissas sobre o software das pessoas, sobre o que pode ser feito ou não pensando na confiabilidade e a solidez desses softwares. Então, aqui, não sei se meus colegas querem mencionar alguma coisa ou não. Esse é o meu resumo. Se está faltando ou alguma coisa no meu resumo? Não? Está tudo bem?

Se estiverem interessados num software de código aberto, pode perguntar. E também estamos trabalhando na filtragem e bloqueamento do DNS e um dos mecanismos de fazer o bloqueamento de bloqueio de conteúdo online tem a ver com o DNS para gerenciar o bloqueamento de conteúdo entre usuários finais e os recursos, já faz

um tempo que fazemos isso. É uma tecnologia que utilizamos e já faz as últimas recomendações que foram publicadas faz mais de uma década e muita coisa já mudou desde então no campo tecnológico e regulatório.

Quanto ao tecnológico, muitas consultas do DNS vão passando por vias que são menos óbvias e que as pessoas talvez não podem olhar como são utilizadas, é uma área em que temos inputs e estamos falando com as pessoas no setor das políticas. E recentemente falamos bastante com o pessoal encarregado das políticas na ICANN, o que eles estão fazendo no espaço de política e realmente isso é muito positivo para nós. São questões prementes e gostamos muito desse processo colaborativo.

Então, essa é uma visão geral de todos os tópicos, mas temos um nível mais detalhado. Não sei quem quer falar aqui no próximo slide.

RAM MOHAN: Antes de passar para o próximo. Nigel, você pode verificar se há alguma pergunta ou intervenção?

NIGEL HICKSON: Sim, pensava fazer isso porque é muita informação. É interessante como vocês têm estão apresentando os temas aqui. Mais alguma pergunta, observação antes de passarmos aos problemas com o blockchain? E a inteligência artificial também. Desculpem, não sei se tem alguém aqui online que queira perguntar. Os nossos amigos da União Europeia.

GEMMA CAROLILLO: Gemma Carolillo, da Comissão Europeia. Um comentário breve. Primeiro, é muito bom ver que... (inint) [00:18:20] do que vocês estão fazendo são coisas que coincidem muito com o que nós estamos fazendo. E isso é frequente, sim, mas há uma outra pergunta importante que, pelo que entendi, é sobre o trabalho, a segurança no código aberto é algo que acabou de começar agora? E é muito interessante e de grande interesse para nós. E é importante que entremos em contato com vocês para obter mais informação sobre esse trabalho.

BARRY LEIBA: Fala Barry Leiba, co-presidente do grupo de trabalho produzindo esses documentos. Vai ser muito bom apresentar esses relatórios periodicamente à medida que formos avançando, vai rapidamente talvez que possamos apresentar uma atualização de onde nós nos encontramos.

RAM MOHAN: E uma coisa que eu gostaria de agregar aqui, além do que o Barry mencionou, é que também é a oportunidade de que as partes dos grupos convidem especialistas ou aquelas que têm informação para informar aqui sobre o que os grupos de trabalho estão fazendo no SSAC. Podemos fazer isso nas próximas sessões.

NIGEL HICKSON: Podemos então falar mais sobre isso depois.

RAM MOHAN: Jeff Bedser deveria estar aqui, mas infelizmente ele não está se sentindo muito bem, então eu vou apresentar essa parte. Eu achei que seria útil explicar algumas perspectivas dos nossos membros sobre

abuso do DNS. O SSAC não tem um grupo de trabalho que precisa fazer uma recomendação de consenso. E o que vocês verão aqui é baseado no conhecimento dos nossos membros.

Nós estamos falando como SSAC, mas baseados no conhecimento e expertise de alguns dos nossos membros. Então a gente, a aprendizagem de máquina e inteligência artificial. A aprendizagem de máquina é um subconjunto em que os algoritmos aprendem dos dados e predizem ou tomam decisões. Então, essa aprendizagem de máquina é uma parte da inteligência artificial.

O abuso do DNS pode ser uma excelente aplicação de IA. Então, os criminosos que já são ou desejam podem utilizar, porque a inteligência artificial, especialmente a generativa, é uma boa forma de criar novo texto, imagens, vídeos, outros artefatos como logotipos de banco, por exemplo. Utilizando então esse aprendizado de máquina aplicada a IA pode criar e-mails e mensagem de texto que parecem ter sido criados por um humano. Então, quanto mais autêntico for, maior a probabilidade de que os alvos sejam vítimas.

E então a IA generativa. No passado, quando recebia um e-mail de phishing sempre se notava alguma coisa errada ou as maiúsculas não estavam certas, a ortografia errada, mas isso pode ser traduzido automaticamente de um idioma para vários outros, e isso significa que a escala e o escopo do problema se amplia drasticamente.

Então, quando olharmos o lado o combate ao abuso de DNS usava reconhecimento de padrões como mecanismo primário para combater o abuso em escala. Então, por exemplo, se vê as informações subjacentes ao nome de domínio, os endereços de IP associados, qual é o recurso, o nome registrado por um registrador.

Então esses templates padrões, esses modelos são reutilizados e valores de (hash) [00:24:44], porque no passado, quando isso era feito por humanos havia... então padrões acessíveis e repetitivos com a IA generativa, cada domínio específico pode ser completamente copiado e são gerados em quatro horas, por exemplo, e agregados ao arquivo da zona. Antes, o phishing era uma mensagem para 400 pessoas e agora são 100.000 mensagens para 100.000 indivíduos diferentes.

Quais são os outros usos de IA para abuso? Estamos vendo que a IA está sendo usada recente por sock puppeting, que é a criação e o uso de identidades falsas que combinadas então para o registro de domínios e contas de hospedagem. Há uso também para imagens íntimas não consensuais, material de abuso infantil, abuso sexual infantil e falsificação, especialmente, que se pode criar documentos de identidade em alguma jurisdição. Por exemplo, tem códigos de país que você precisa fornecer uma identidade para registrar o nome, mas agora você pode criar uma identidade falsa.

Então, essa medida de segurança pode ser superada facilmente. As imagens geradas por IA estão ligadas ao conteúdo e se algumas imagens são mais realistas, outras menos, mas estão ficando cada vez

melhores. Então, os mesmos prompts de anos atrás, produziam imagens que não pareciam ser geradas por um designer gráfico.

É difícil ler o que está nesse slide, mas são dados de um relatório de pesquisa que mostra a frequência de táticas para o mau uso da IA generativa, então (inint) [00:28:09] identidade, amplificação. O slide anterior mostrava de forma geral e aqui mostra cada mau uso dessa inteligência artificial generativa.

Como foi dito anteriormente, as imagens de IA parecem estar gerando imagens cada vez mais escuras, por assim dizer. Embora nem sempre haja um ataque mais sofisticado, mas a IA generativa aumenta a escala e o alcance. Aqui está escrito, os cyber-criminosos vão progressivamente integrar as técnicas de IA e esses criminosos já usam técnicas nos seus planos.

Nem tudo são más notícias. Exceto pelas imagens, você vê aqui os rostos estão deformados, então nós dizemos para o (inint) [00:29:49] o que é gerado, embora o aprendizado por máquina pode aumentar a escala e a frequência dos ataques, o IA pode detectar os e-mails de phishing. Os e-mails de phishing gerados por IA são diferentes dos e-mails comuns que você geraria e são diferentes dos phishing manual.

E o processamento da linguagem natural ajuda as ferramentas de IA generativa a entender processos e fabricar textos que parecem ser autênticos e humanos. Embora essa tecnologia existente, podemos usar a IA para detectar a IA, saber o que está acontecendo. Então, atacar

vetores e estratégias que usam IA para abuso. Acho que todos já sabem disso, a desinformação política não é necessário, mas usar humanos praticamente. E abuso orientado para o lucro e escalonamento e acelerar as empresas criminosas.

O cibercrime está relacionado com dinheiro, que é gerado para os criminosos. Então, eles utilizam estratégias para garantir o lucro. Então, a IA para detectar isso está se desenvolvendo rapidamente. Então, nós achamos que isso é uma continuação do mesmo cenário de ameaças que haviam. Os atores que decidem utilizar a tecnologia para obter vantagens, o lucro e a tarefa é garantir que estejamos a par do que está acontecendo e empregar medidas que possam mitigar ou mesmo combater essas práticas ou ameaças.

Eu falei sobre IA e o DNS. Eu não vou falar muito sobre blockchain e DNS, já falamos disso em outros fóruns. Dentro da ICANN há um relatório publicado SSAC123. E também organizamos um painel na oficina do SSAC 2024, em Washington, em setembro. Esse relatório está disponível e esse painel incluiu especialistas no espaço de blockchain.

Incluiu então o diretor de tecnologia da ICANN e há uma excelente colaboração entre o SSAC e o OCTO da ICANN para termos essa coordenação em termos de pesquisa. Então, para garantir, não duplicar o trabalho.

Aqui do meu ponto de vista, é o slide mais importante e que mais interessaria o GAC. Nós vemos que ao longo do tempo os que elaboram

política, precisam de capacitação, precisam ser informados sobre os principais temas por pessoas que sabem do que estão falando, mas que falem de forma acessível, entendível e não só ficar falando jargões e nós temos a oportunidade de fazer isso.

Nós também elaboramos relatórios que geralmente têm dezenas de páginas. E o que nós estamos tentando fazer é resumos de 500 palavras, mais ou menos, uma ou duas páginas. Nos ajudaria muito se vocês nos dissessem, vocês que elaboram políticas, quais são os temas mais importantes para vocês. Temos 126 artigos escritos. Nós queremos saber o que seria útil para vocês e queremos trabalhar junto com vocês para poder fornecer artigos informativos para vocês e seus públicos.

Por exemplo, vocês trabalham no governo, vocês podem ter reuniões importantes sobre resiliência, instabilidade e muitas vezes você vai nessa reunião, você tem colegas, outros funcionários que não sabem, não estão informados sobre os fatos reais e fazem recomendações sobre o que eles não conhecem de fato. Então nós precisamos encontrar como combinar uma solução de política com a viabilidade técnica. O que é importante é que as políticas são sejam elaboradas com base em fatos, em dados reais. E nós gostaríamos muito de abrir esse canal com o GAC oferecendo o escopo completo, tanto em termos de profundidade como de escopo, além dos documentos que nós já fornecemos.

NIGEL HICKSON: Muito obrigado por essa visão geral. Nós, como elaboradores de políticas, nós devemos muito às recomendações recebidas da

comunidade técnica de outras partes da ICANN. Eu lembro bem há alguns anos, quando estávamos discutindo abuso de DNS, em termos da nova rodada de gTLDs e outros temas, que o relatório do SSAC, eu não me lembro do número, dava detalhes sobre isso e isso influenciou muito as nossas recomendações.

Eu acho que nós temos muito espaço para trabalharmos juntos e também a refletir sobre o interesse em blockchain e em particular em abuso de DNS. Então agradeço muitíssimo por nos informar sobre esses problemas. Chegou a hora de perguntas ou comentários. Temos aqui o representante dos Países Baixos.

ALISA HEAVER: Agradeço pela apresentação, o trabalho do SSAC. Eu não tenho muita certeza se há uma pessoa de contato no GAC com o SSAC e também o contrário.

RAM MOHAN: Acho que não temos alguém com essa função formal. Seria muito bom, e é claro, e se vocês quiserem podemos designar alguém, mas a única coisa que fazemos no SSAC é que se qualquer pessoa, inclusive essas pessoas de contato que entrem, que possam participar, mas que tenha especialmente expertise também seria muito útil. O Gabe, que está aqui sentado é membro do SSAC, e em alguns casos, o Gabe pode ter acesso para fazer uma transferência de informação informal.

NIGEL HICKSON: Obrigado pela pergunta. A resposta para a pergunta é que não temos essa pessoa de contato. É algo que poderíamos considerar porque é algo importante, porque somos um comitê consultivo transparente e a

sua informação está bem publicada, mas seria útil ter alguém trabalhando nessa função. Bom, eu com óculos, sem óculos, não sei, não consigo ver. Mas o representante da Austrália, Ian.

IAN SHELDON: Sim, só mencionar que há bastantes pedidos para intervir aqui no Zoom. Eu sou Ian Sheldon da Austrália. Obrigado por essa apresentação que é muito útil. Há muito conhecimento exaustivo representado aqui e os membros do GAC temos muitos trabalhos, muitas tarefas no GAC, e também fora da ICANN. Então para solicitar a sua assistência, quão grande seria essa assistência com assuntos vinculados ao DNS ou fora desse fórum?

RAM MOHAN: Boa pergunta. Bom, a nossa ajuda está aplicada aqui na ICANN, mas se vocês precisarem de ajuda dos nossos membros, podem recorrer a ela fora da ICANN.

NIGEL HICKSON: Obrigado. Agora Estados Unidos e depois passamos as mãos levantadas aqui no Zoom.

LEONARD HAUSE: Fala o representante do Departamento dos Estados Unidos. E quando vocês falaram da combinação da IA regenerativa e abuso do DNS. Vocês falaram ou fizeram algumas boas práticas, alguns desses registros, para que possamos chegar à raiz dos problemas para saber onde esses problemas começam? Isto é, algo que possamos ver e identificar como parte da IA generativa. Eu não sei se há boas práticas nos seus relatórios e muito obrigado por seu trabalho.

RAM MOHAN: Eu não sei como responder essa pergunta, mas sim, posso pedir alguns especialistas no SSAC que respondam isso e depois posso transmitir essa resposta. Mas no espaço da ICANN parte da consideração que se é verdade que embora seja certo que com a IA generativa, depois de umas horas podemos agregar um nome de domínio a resolução, também podemos ter muitas mensagens alusivas saindo, mas também podemos no espaço da ICANN para mitigar isso rapidamente. Por exemplo, se esse abuso acontece num período de uma hora, então seria possível então mitigar isso em minutos depois de ser detectado, é essa pergunta que eu queria fazer.

NIGEL HICKSON: Obrigado pela pergunta e também a resposta. Fala Gemma, da União Europeia.

GEMMA CAROLILLO: Obrigado, Nigel. Como vocês estão perguntando sobre possíveis assuntos de interesse, estava pensando que aqui no GAC quando falamos do uso indevido do DNS, entre outros temas, falamos sobre o uso de ferramentas preditivas. E na União Europeia temos experiência nesse assunto, mas seria muito bom se já pudéssemos ter material ou um espaço para continuar trabalhando e analisar o potencial das ferramentas preditivas para evitar abusos do DNS antes de passarmos para a mitigação, depois no (inint) [00:45:24]. Não sei se entendi a questão da IA generativa. Realmente não estamos aumentando todo um espectro de possíveis ameaças, mas uma quantidade enorme de ataques que poderíamos ter, mas não significa que sejam ameaças que são mais sofisticadas.

RAM MOHAN: Obrigado pela pergunta. Sim, é verdade. A escala nas ameaças é o que aumentou drasticamente e não especificamente o espectro delas. Quem quer aqui, algum membro quer responder ao colega.

GABRIEL ANDREWS: Sim, eu posso dar uma perspectiva breve do ponto de vista das forças da lei, os grupos criminosos estão utilizando a IA para fazer suas atividades mais eficientes, (inint) [00:46:41] não criminosos são os velhos truques, só que agora estão utilizando novas ferramentas. Essa mensagem que podemos transmitir a partir da visibilidade que nós temos atualmente.

RAM MOHAN: Deveriam reformular essa primeira pergunta para que os outros membros prestem atenção e possam responder.

GEMMA CAROLILLO: Muito obrigada. Vou reformular a pergunta. Entre diferentes assuntos, nos pediram que passássemos aqui para obtermos informação do SSAC no GAC, muitas vezes discutimos sobre os abusos ao DNS e muitas vezes nos referimos ao uso de ferramentas preditivas para evitar abusos do DNS antes de chegar à fase da mitigação.

RAM MOHAN: Alguém que quer responder?

BENEDICT ADDIS: Sim. Algumas questões sobre o abuso do DNS que se prestam ao uso de ferramentas preditivas como botnets e malwares que utilizam algoritmos muito preditivos de malware com semanas inclusive antes de que aconteçam e com uma certa exatidão, podemos diagnosticá-los com uma certa exatidão, mas eu teria seria muito cauteloso com as

ferramentas da IA e algumas coisas que vão poder servir como prognósticos, mas nem todas.

STEVE CROCKER: Para poder operar processos preditivos é necessário agir com diligência para ter acesso aos registros e dados de registro. Estamos agora num período que é bastante complexo, em que está na confidencialidade, privacidade para proteger os usuários de formas de assédio, etc. Mas ao mesmo tempo, às vezes é impossível ter acesso aos dados para fins legítimos, especificamente para fazer análises preditivas ou correlações entre os domínios.

Portanto, pode ser um pouco enganoso e não é fácil responder essa pergunta de como podemos oferecer acesso a esses dados para que possam se fazer análise preditiva de que precisa, ao mesmo tempo, proteger a privacidade. Aqui há então uma inter-relação entre essas duas ideias.

NIGEL HICKSON: Obrigado pela pergunta, pelas respostas. Essa pergunta gerou respostas excelentes. E Santosh agora da Índia.

T. SANTOSH: Obrigado Nigel. Obrigado Ram Mohan pela apresentação tão detalhada sobre o abuso do DNS. Vamos começar falando dos aspectos básicos agora e a IA pode ajudar com a exatidão do WHOIS, porque essa é a questão básica e porque podemos ter um sistema então implementado em que a ferramenta nos diga bom, isso aqui na mesa não está exatamente no WHOIS, portanto não podemos delegar esse domínio.

RAM MOHAN: Sim, obrigado. A pergunta específica é o que podemos (inint) [00:50:57] os algoritmos a uma base de dados, compará-los com o mundo real para chegar a uma conclusão. Mas, como o Steve falou, uma grande parte desses dados não estão disponíveis, não estão tão protegidos e hoje não está acessível os conjuntos de dados que poderiam oferecer informação para essas ferramentas não estão disponíveis, e embora a tecnologia esteja disponível.

BARRY LEIBA: Eu gostaria de mencionar também que não são os dados que devemos verificar, os que não estão disponíveis, mas também aqueles que precisamos para alimentar a máquina.

GREG AARON: Os dados de contato para o domínio não estão disponíveis para muitos de nós, para empresas de segurança, órgãos da lei, por exemplo, mas sim há outras partes que têm esses dados. Como registradores (inint) [00:52:14] e registradores agora que fazem controles da exatidão através de diferentes métodos como .nl nos Países Baixos ponto .uk e basicamente agora os registradores são aquelas partes que podem fazer as verificações, a exatidão e impedir um potencial cyberdelito.

Também temos os dados do WHOIS, dados de compra para algumas ferramentas financeiras utilizados para projetar nomes de domínio, endereços IP de fontes, entre outras coisas. Portanto, temos um uso potencial do IA, mas que não estão nessas partes.

NIGEL HICKSON: Muito obrigado. Temos mais duas ou três perguntas no chat, então vamos para as perguntas, temos seis minutos, portanto vai ser difícil, mas devemos resumir. Marco.

MARCO HOGEWONING: Eu vou ser breve. Vou repetir o que os meus colegas falaram. Agradeço a vocês pela ajuda. Vocês perguntam o que é importante para nós e nós respondemos que tudo é importante. E acho que nos ajuda a entender o impacto das tecnologias emergentes sobre a estabilidade do DNS, também a internet em geral.

E gostaria, enquanto as prioridades, o SSAC também está considerando o diálogo global vinculado com o pacto digital mundial. E se há algum trabalho que possamos fazer para ajudar a todos, é uma oportunidade para que o SSAC contribua para essas conferências globais atuais e isso tem a ver também com a segurança e a estabilidade que você mencionou.

RAM MOHAN: Alguns aspectos de segurança e estabilidade da internet e a governança são assuntos aos quais prestamos atenção permanente, queremos nos envolver nesses assuntos e não temos uma estrutura com a qual possamos enviar um coordenador de links, mas temos membros que participam ativamente nos seus trabalhos cotidianos e que nos informam. E parte disso é o que nos levou à criação da equipe de trabalho sobre código aberto. Um dos membros no grupo reconheceu que o foco colocado em nível governamental e que poderia ser útil.

BARRY LEIBA: Há três formas em que o SSAC pode e decide trabalhar. Temos a diretoria que nos pede algo, a comunidade também pede talvez que nos foquemos em um aspecto X que é importante para a comunidade. Essa é também uma possibilidade.

NIGEL HICKSON: Temos mais algumas perguntas. Desculpem. Não entendi bem a ordem aqui das perguntas. Não, é a vez do Wang Lang.

WANG LANG: Muito obrigado pela fantástica apresentação. Você mencionou o blockchain, o DNS também e sabemos que a ICANN aceitou trabalhar com os registradores nesse assunto. O que vocês acham sobre o futuro do DNS?

RAM MOHAN: O SSAC não preparou um relatório específico sobre o blockchain, mas sim sobre a evolução do DNS, as novas tecnologias. O que eu acho que a tecnologia está evoluindo, devemos abraçar esses espaços em lugar de falar em termos de proteção dos nossos. Mas o que é importante é ter outros espaços de nomes querem integrar seu espaço de nomes e do DNS, o que deveria ser feito de forma responsável com estabilidade e segurança. Esse é o centro disso. E o que nós consideramos quanto a esse assunto. Há outras questões que poderiam existir, em que produzimos um relatório sobre o blockchain, mas há muitos assuntos que ainda não foram cobertos, ainda não chegamos lá.

NIGEL HICKSON: É a vez do Owen Fletcher.

OWEN FLETCHER: Essa ação foi fantástica. A IA e os abusos do DNS são exemplos perfeitos de um assunto em que os conhecimentos e a expertise do SSCAC podem ajudar o GAC para tentar criar uma posição, passar evidências e estarmos informados.

Seria fantástico ter mais esse tipo de interações, incluindo as sessões de capacitação com o SSAC e eu falei isso no comentário no chat. E esta apresentação descreve um tipo de abuso que não é específico para o DNS, embora muitas dessas coisas podem ser utilizadas pelos criminosos que cometem abusos do DNS. Vocês consideram, segundo a definição de abuso da ICANN, vocês consideram que a velocidade de criação de domínios falsos vai se acelerar ou que levaria a um aumento na quantidade de casos de abusos? É algo que deveríamos prever para os próximos meses ou anos.

RAM MOHAN: Lógico, com a tecnologia e a tecnologia vai permitir que a complexidade e a escala sejam simples e, portanto, sim, poderíamos então lidar com isso, há dinheiro aqui para receber por tudo isso. E ontem o Jeff falou que a labor de um bom phishing é de 25.000 dólares, esse custa 200.000 dólares e inclusive 1.000 dólares a rede de nome de domínios, esse não é um fator dissuasivo, não. E, portanto, se seguirmos essa cadeia de lógica, veremos que cada vez mais há esse tipo de abusos é o que eu acho pessoalmente.

MERIKE KAEO: Pessoalmente, eu estou encarregada da segurança no dia a dia. Eu não confio em nada, nem filtros. Eu quero ver as campanhas que são feitas. E o que é interessante é que é a inteligência artificial que gera isso. Há

tipos de phishing que cada vez são mais (inint) [01:00:49] e acho que eles olham o que a gente publica no Facebook, no LinkedIn e estão focados especificamente em autoridades específicas. Eles têm a inteligência para que pareça mais crível. E isso é algo importante. Quanto mais rapidamente pudermos agir e dissuadir, melhor. Isso é muito importante.

NIGEL HICKSON: Acho que devemos encerrar aqui, acabou o tempo. Mas essa foi uma reunião muito produtiva. É incrível o trabalho que vocês estão fazendo e há muito interesse nesse trabalho que vocês estão fazendo. E sempre é um orgulho para mim falar que muitos de vocês contribuíram não apenas ao trabalho da ICANN, mas também da comunidade técnica.

Muito obrigado e obrigado pelo oferecimento de continuar trabalhando em diferentes assuntos. Encerramos aqui a sessão. E aos colegas que estão aqui no fundo da sala, que horas é que começamos a sessão de amanhã, por favor?

JULIA CHARVOLEN: Vamos começar 13:15, horário Local. É sobre assuntos vinculados aos registros.

RAM MOHAN: Nós agradecemos o convite. Esperamos que não seja a última vez que nos convidam, muito obrigado.

[FIM DA TRANSCRIÇÃO]