ICANN84 | Assembleia Geral Anual – Encontro conjunto: GAC e ccNSO
Quarta-feira, 29 de outubro de 2025 – 10h30 às 12h IST

NICOLAS CABALLERO Sejam bem-Vindos mais uma vez. Vamos começar.

GULTEN TEPE Sejam bem-vindos à reunião do GAC, 29 de outubro, quarta-feira, 10h30, horário UTC. Por favor, levem em consideração que esta sessão está sendo gravada e se rege pelos padrões de comportamentos esperados pela ICANN, o código de conduta dos participantes da ICANN e as políticas anti-assédio da comunidade da ICANN.

Durante a sessão, as perguntas ou comentários apenas serão lidos em voz alta se estiverem apresentados de forma devida no chat, vão ter interpretação, vamos ter interpretação nos seis idiomas das Nações Unidas e português. Caso queiram utilizar a palavra, levantem a mão na sala de zoom e lembrem de dar os seus nomes para os registros e o idioma no qual vão falar, caso não seja inglês. Lembramos também que fale em um ritmo razoável para permitir uma interpretação correta. Passo a palavra agora ao presidente do GAC, Nicolás Caballero.

NICOLAS CABALLERO

Obrigado, Gulten. Sejam bem-vindos mais uma vez. Eu tenho a honra de apresentar meus colegas da ccNSO. A Presidente Alejandra, que está aqui na minha direita, Alejandra Reynoso. Vamos ter uma sessão muito interessante, muito interativa, no estilo do que fizemos, não sei, foi em Seattle.

Sim, a ideia é que exista uma participação ativa, que façam perguntas, interajam, não há nenhuma pergunta incorreta, enfim, vamos ter diferentes estações, postos para trabalhar. Antes de entrar em contexto e fazer essas apresentações sobre criptomoedas e um exemplo de fraude nos investimentos, que estará a cargo de Gabriel Andrews, do FBI, eu vou passar a palavra à Alejandra para que faça algumas considerações práticas para saber qual a dinâmica do trabalho de hoje. Por favor, Alejandra, seja bem-vinda mais uma vez.

ALEJANDRA REYNOSO

Obrigado, Nico. Sempre um prazer estar aqui na reunião com o GAC testando diferentes metodologias com vocês. Eu acho que isso é muito produtivo. Antes de entrar nos detalhes da atividade, eu acho que seria melhor escutar a apresentação de Gabriel. E quando ele finalize, eu vou contar um pouco tudo o que vamos fazer na seguinte parte. Obrigada pelo convite.

NICOLAS CABALLERO

Obrigado, Alejandro. Então, passo a palavra a Gabriel Andrews, do FBI. Por favor, Gabe.

GABRIEL ANDREWS

Obrigado, Nico. Obrigado, Alejandra. Vamos começar com o seguinte slide. Hoje estarei falando da categoria principal de crimes cibernéticos informados ao FBI nos últimos tempos, que tem a ver com a -- nos investimentos com criptomoedas. E também tem outro nome na mídia, talvez escutaram algum outro termo. E isso serve como informação para as nossas conversas.

Isso é uma coisa que surgiu na pandemia, houve várias consequências da pandemia. O que aconteceu é que existiam bandos de crime no sul asiático, que começaram no sudeste asiático, que trabalhavam com hotéis, com cassinos, e aplicavam métodos que explodiram, como a atividade para ganhar dinheiro.

Tinham trabalhadores que depois ficavam cativos, como escravos, e eram obrigados a fazer fraudes, pessoas ocidentais, contra pessoas ocidentais através de esquemas de fraude. E é muito importante conhecer que existem esses sistemas para o que vou contar depois. Vamos tratar alguns dos títulos que estavam nas manchetes, que estavam nos noticiários. Por exemplo, nas Nações Unidas preparou-se esse relatório para destacar esses esquemas de fraude, para que todo mundo soubesse o que acontecia nos últimos sete dias. Por exemplo, o exército de Mianmar conseguiu atacar um desses prédios onde se cometem essas atividades criminosas.

Também o Space X interrompeu o serviço de starlink para esses acampamentos onde se fazem essas fraudes. E o meu próprio

Departamento de Justiça dos Estados Unidos apreendeu 15 bilhões em moedas de bitcoins de um dos esquemas de fraudes que correspondia ao matador de porcos, como se chamava no grupo Prince.

Isso não só envolve o FBI, mas também o Departamento de Justiça dos Estados Unidos. E a forma em que funciona é assim. Há uma atividade de phishing que começa no início da fraude, mas não se faz através de correio eletrônico. Mas o que vamos encontrar, geralmente, é uma mensagem nas redes sociais ou nos aplicativos de texto que parece uma mensagem acidental enviada por alguém e começa uma conversa.

Podem perguntar se estão interessados em uma relação de amizade ou romântica, ou talvez uma relação de negócios. Começa de forma muito sutil, mas esse elemento de trabalho escravo permite que aqueles que cometam phishing levem tempo para criar essa afinidade com aquele que recebe essas mensagens. Então, quando transformam a conversa numa possibilidade de investir, numa chance de criptomoeda interessante ou nova, já houve toda uma construção de etapa de confiança ou afinidade. Isso é diferente ao phishing tradicional, onde talvez existia um correio muito bem armado.

Nesses casos, é um processo lento de phishing, que leva dias, ou inclusive semanas, e apenas pode acontecer porque essas pessoas estão sendo cativas e obrigadas a fazer parte do trabalho escravo e dessa forma permanecem. E o elemento também dos domínios,

porque vocês podem perguntar, se não há um correio, qual é o elemento, o componente dos correios que está envolvido? Quando se estabelece essa armadilha e eles falam, "ah, eu tive esse retorno do investimento, eu quero compartilhar essa chance com você".

O que vão dar para vocês através dessas mensagens de chat é essa informação das bolsas nas quais se comercializa as criptomoedas. Esses criminosos registram em grande volume. Então, quando falamos das registrações massivas, justamente este é um dos exemplos. Às vezes podem registrar centos ou milhares ou centenas de domínios que correspondem a estas bolsas de criptomoedas.

E, quando preparo essa estrutura, isso eu peguei de outra apresentação, mas para explicar o que vai acontecer aqui na esquerda, nesses retângulos que aparecem na tela, que estão púrpura, rosa e amarelo, começa reunindo esses domínios semelhantes pelos quais podem passar, que duram três meses. Podem passar ao seguinte, depois desse tempo.

E como tem tantos domínios que escolher, podem fazer esse pulo, mas utilizam uma técnica chamada, em inglês, CNAME forwarding, onde mudam as configurações dos nomes nesses domínios, então, levam ao seguinte domínio, esse nome, e depois para outro e outro, até poder chegar ao website de criptomoedas, finalmente. Isso permite que um nome de domínio semelhante apareça no navegador, mas passa por diferentes etapas antes de chegar à resolução.

Não espero que todos conheçam os nomes canônicos, mas alguns nomes devem ser conhecidos por vocês e operam no ccTLD. Tem que saber essa tática. Então, se encontram, vão poder reconhecer como é a manobra. Quando os investigadores querem investigar essa situação, percebem que é difícil explorar a infraestrutura justamente por essa tática.

Então, utilizam por dois motivos, porque dificulta a investigação, as autoridades e, por sua vez, podem passar por esses domínios registrados em grande volume, mantendo uma certa proteção na infraestrutura que está por trás de todo este esquema. Então, para dar um pouco de contexto para a atividade que vamos fazer hoje, o que queria era apresentar esse sistema de fraudes para que estejam familiarizados, mas também pedir aos colegas da ccNSO que digam se já viram nos seus espaços de trabalho dentro do gTLD .info, .top, .net se foi utilizado esse tipo de fraudes.

Mas não posso falar com certeza se há muita visibilidade disso, e talvez também pode estar acontecendo no espaço dos ccTLDs, há diferentes organizações que estão utilizando este sistema. Então, a pergunta seria, vocês reconhecem esses relatórios que têm a ver com registrações massivas de websites de criptomoedas, ou talvez tenham esse reenvio de CNAME.

Para as conversas que vamos manter nas possíveis políticas que poderiam ser formuladas com a ICANN no espaço dos ccTLDs, talvez poderíamos considerar algum tipo de verificação dos domínios associados. Ou seja, se temos um relatório sobre um

domínio, talvez teríamos que ver o que aconteceu com os outros domínios que foram registrados ao mesmo tempo para ver se também fazem parte da fraude ou estabelecer diferentes controles através das APIs para poder ver o que acontece com essas registrações massivas.

Eu acho que, dessa forma, poderíamos talvez ter essa informação para a formulação de políticas. Então, eu acho que, segundo o meu cronômetro, já passaram oito minutos. Então, agradeço pela atenção e há muita resposta que está sendo tratada e de dar a essa fraude. E, com prazer, vou participar da conversa.

NICOLAS CABALLERO Obrigado, Gabe. Foi muito interessante. Aqui temos as perguntas. Isso é muito importante para os operadores de ccTLDs. Estão recebendo de forma de uso indevido ou de abuso sobre esse tema? Estão vendo registrações massivas mais o reenvio dos CNAMES, dos nomes canônicos? Essa seria a primeira pergunta. Mas agora vou passar a palavra à Alejandra, quem vai apresentar os detalhes e as características da atividade que vamos fazer nos próximos 75 minutos. Passo a palavra a Alejandra.

ALEJANDRA REYNOSO Obrigado, Nico e Gabriel, pela apresentação. Sei que tinha um tempo limitado, então vamos levar em conta as perguntas que fez e responder depois. Na próxima atividade, como fizemos antes, vamos ter mais interação. Será uma experiência onde, de fato, estarão de pé e vamos falar do uso indevido do DNS com diferentes

assuntos, com pessoas do GAC e alguns colegas da ccNSO. Por exemplo, na primeira estação, temos o uso de inteligência artificial na detecção e prevenção do uso indevido ou do abuso.

Na segunda estação, temos os desafios das registrações massivas, justamente o que mencionou o Gabe. Na seção 3, está a investigação do abuso com as carteiras de nomes de domínios. Na estação 4, estão os marcos nacionais para a prevenção de fraudes. E na estação 5, estão os acordos de notificadores de confiança.

Então, o que pedimos é que, tomando a devolução da última vez, vocês pediram que fizéssemos mais rodadas, mas para isso necessitaríamos mais tempo. Então, agora vamos ter três rodadas e em cada uma pode escolher qual o ponto que querem escolher. Passado o tempo, tem que mudar a outra estação e assim temos cinco estações.

Dessa forma, vamos ter três opções para interagir nessas estações, mas também vamos incluir depois um resumo de cada estação para que todos tenham a chance de ter toda a informação se foi que não conseguiram passar por todas as estações. Aqui estão os nomes dessas estações, vamos manter na tela para que vocês possam ir se deslocando. Como controlamos o tempo aqui? Vamos colocar um cronômetro aqui. Muito bem. Então, Nico.

NICOLAS CABALLERO Obrigado, Alejandra. Antes de começar com o trabalho nas estações, se deslocando por elas eu quero voltar a pergunta de Gabe. Gostaria de ter alguma resposta daqueles que estão

conectados por Zoom ou daqueles que estão aqui também a essas perguntas.

Deixe-me dar um tempinho de 3, 5 minutos antes de começar com o trabalho das estações, por favor. Com todo o campeonato de lutadores de boxe que vai acontecer. Alguma devolução, alguma resposta sobre, especialmente dos operadores ou dos ccTLDs, com respeito à questão do reenvio de CNAME, desses nomes canônicos? Não esperamos que todos sejam especialistas nesses -- ou na realidade do DNS, ou reenvios de CNAME. Alejandra?

ALEJANDRA REYNOSO Eu gostaria de abordar a pergunta para a ccNSO. Se considerariam elaborar uma política para isso. Mas a ccNSO tem um mandato muito limitado para elaboração de políticas e a IANA, que trata dessa questão. Então, como, por exemplo, a retirada do ccTLD, a transferência. Então, nós não temos políticas para para o ccTLD como realizar o seu trabalho. mas temos um comitê permanente de abuso do DNS que tem um repositório de melhores práticas para ser compartilhado, mostrando como os ccTLDs tratam isso. Então, eu espero que essa atividade possa ampliar essa conversa.

NICOLAS CABALLERO Então, a segunda pergunta, sobre as experiências dos operadores de ccTLDs, tenham ou não, e que possam contribuir com informações. Bom, não há mãos levantadas. Então, muito bem.

Muito obrigado, Gabriel. Agradeço muito, foi muito importante e isso é relevante para todos os representantes do GAC.

ALEJANDRA REYNOSO Nós vamos, então, reunir respostas às perguntas do Gabriel. Então, eu os convido a se levantarem e escolherem uma das estações e teremos 18 minutos e o tempo então começa agora.

Olá a todos. Acabou o tempo. Por favor, vão terminando as conversas e que mudem de estação. Vamos começar então um novo cronômetro daqui um minuto.

Por favor, vamos começar a segunda rodada. Mudem de estação. Passem, se desloquem de uma estação para a outra e iniciemos o cronômetro.

Quero advertir que faltam apenas dois minutinhos.

Acabou o tempo. Agora temos a terceira rodada. Podem mudar de estação. Vamos começar o cronômetro em um minuto.

Muito bem. Espero que tenham entrado na terceira estação. Vamos começar o cronômetro agora.

Esse é o aviso de dois minutos.

Acabamos o tempo. Peço que retornem aos seus assentos. Estamos prontos para os resumos. Muito obrigada.

Retomem seus assentos para recomeçar a atividade.

Bem. Estamos prontos. Vamos começar com a estação número 1 com o uso da Inteligência Artificial na detecção e prevenção de abuso.

NICOLAS CABALLERO

Na estação 1 quanto o uso de inteligência artificial. Em primeiro lugar nós explicamos, eu e o Christian, no .nl, explicamos o que é aprendizado de máquina, IA, a diferença entre ChatGPT, como detectar tendências e tráfegos. Não necessariamente relacionadas a LLMs ou IA generativa e as medidas que os Países Baixos estão utilizando para combater o abuso do DNS.

Excelentes perguntas, não só sobre a tecnologia em si, mas a implementação, o que acontece sob o capuz, por assim dizer. Eu espero que os participantes tenham gostado. Gostaria de agradecer ao Chris e à equipe dos Países Baixos. Então, esse é o meu breve resumo da estação 1.

ALEJANDRA REYNOSO

Agora, passando para a estação 2, desafio dos registros de domínio em massa.

PETER KOCH

Não tivemos uma definição de registro, mas discutimos por que isso é um desafio. Mas, por outro lado, não é tão importante. Também discutimos os registros automatizados e diferenciando a

comunicação entre o registro e o registrador. Então, ver onde deve ser verificado.

MARTINA BARBERO

Foi muito interessante, com boas perguntas. Nós discutimos como abordar problemas relacionados ao registro em massa. A atenção entra em identificação com a capacidade de entender a intenção dos registros em massa. Alguns usos podem ser legítimos, então como se faz, como ocorre esse atrito e como desincentivar.

Também mencionamos a diferença em identificar organizações e indivíduos. Isso demanda diferentes práticas e abordagens. Também falamos de diferentes práticas no espaço de ccTLDs. Muitos registros avaliam comportamentos considerados suspeitos depois dos registros em massa e como tratar esses casos antes do registro em si.

Falamos dos perigos disso, como mencionado pelo Gabriel da FBI, e qual seria a reação e o tempo necessário para tratar disso muito rapidamente. Eu espero que isso tenha ajudado.

ALEJANDRA REYNOSO

A investigação de abuso nos portfólios de domínios. Susan Chalmers e Crystal Peterson.

SUSAN CHALMERS

Fala Susan Chalmers, dos Estados Unidos, NTIA, que é autoridade de políticas do ccTLD dos Estados Unidos .US. Eu vou falar de

alguns pontos gerais. Então, a nossa estação falou em termos nos próximos PDP para verificação de domínios. Então, quando o relatório de abuso é recebido, o .US é a fonte de autoridade de informações de registro nas zonas dos Estados Unidos. Isso é muito único.

O TLD dos Estados Unidos proíbe o uso de serviços de privacidade e proxy como política, o que nos dá uma situação específica para mitigar abuso a partir das contribuições recebidas. Crystal, eu passo a palavra para você.

CRYSTAL PETERSON Na nossa revisão que fizemos durante as três sessões. Vimos como nós, como registros, detectamos domínios associados e portfólios de domínio, inclusive a política aplicada a criptomoedas. Os Estados Unidos é único porque em suas políticas de não usar serviços de proxy e privacidade. E nós, do ponto de vista do registro, nos ajuda a apoiar a mitigação de abusos da comunidade utilizando dados de contrato dos registros. A sessão foi excelente porque revisamos como nós definimos o que é um domínio associado e o que podemos fazer em termos de mitigação.

ALEJANDRA REYNOSO Passando para a estação número 4, Bruce Tonkin e Ian Sheldon.

IAN SHELDON Na estação 4, tivemos uma excelente discussão sobre marcos nacionais antigolpes. O Bruce falou de etapas necessárias para

detectar golpes e a sua prevenção em detecção. Na Austrália, temos um centro antigolpes que foi estabelecido para tratar desse desafio e é um local onde a população pode vir e relatar golpes.

Trabalham junto com o operador do .AU. Tem ações bastante rápidas quando há um golpe. A questão quantos golpes são um problema de cibersegurança e quantos são um problema de proteção do consumidor. Na Austrália, esse centro anti-golpes está dentro da comissão de concorrência e consumidor. Então, a cibersegurança faz parte desse departamento de proteção dos consumidores, do governo.

Tivemos excelentes discussões sobre qual é a exigência de nexus. Temos problemas de credenciais roubadas, mesmo que a exigência de nexu. Podemos identificar outros problemas de roubo de credenciais e usados em golpes.

ALEJANDRA REYNOSO Na última estação, acordos de notificador confiável.

JAKE VINCET Eu vou ser breve. No .UK, nós temos esse notificador confiável e as camadas, riscos e os benefícios de termos esses acordos de notificador. Então, alguns não são tão populares e aceitos, e há um problema de jurisdição, como verificar se são precisos, exatos.

ALEJANDRA REYNOSO

Agradeço a todos. E, ao concluir aqui, eu peço que respondam à pesquisa no Mentimeter. Se não houver informações, se não acharam que as informações não foram suficientes nesses resumos que fizemos, nós vamos enviar. Com isso eu passo a palavra ao Nico.

NICOLAS CABALLERO

Agradeço Alejandra, a ccNSO, foi uma sessão fantástica. Eu adoro. Essa é a que eu mais gosto. Claro, com todo o respeito a outras partes constituintes, eu gostaria de fazer outras sessões como essas, com as outras partes constituintes. É muito participativo, podemos cooperar mais. É muito importante que vocês respondam. Usem 45 segundos do seu tempo para responder a pesquisa do Mentimeter, porque nos ajuda a decidir, por exemplo, se o tempo para cada rodada é adequado, deve ser mais longo, mais curto, ou temos mais tempo para as conclusões. Muito obrigada.

É o final da nossa sessão. Desculpem os 4 minutos de atraso. Teremos almoço agora e terão 15 minutos a mais porque teremos uma reunião da liderança do GAC. Vocês devem voltar... Desculpem, são 30 minutos, então voltem às 15 para as 2. Alguém é contra? Bem, muito obrigada. Essa sessão está encerrada. Agradeço a todos e peço uma salva de palmas para a ccNSO.

[FIM DA TRANSCRIÇÃO]