SR. EDUARDO BARASAL MORALES: Bom dia, pessoal! Sejam aí todos bem-vindos a mais um Intra Rede aí que a gente faz sobre as principais questões na área de redes. Então, são debates, Mesas aí que a gente traz especialistas para conversar com vocês sobre essas questões que geram aí preocupação para os operadores de redes, administradores.

Bom, a nossa Mesa hoje vai discutir segurança de redes. E aí a gente teve convidados aí como do Cert.br, trouxemos aí o delegado que trabalhou na questão do Attack Mestre. Também temos ali pessoal de limpeza de tráfego. Então, aí vai ser uma discussão muito interessante sobre segurança de redes.

Mas antes da gente começar, eu queria dar alguns avisos. Primeiro deles, tá? Relacionado aos sorteios. Então, quem quiser participar dos sorteios dessa live, vão precisar se inscrever nos links que a gente vai colar agora no chat. Vão ser três sorteios. Primeiro deles vai ser da Eletronet, que vai ser ali 200 reais em voucher na Americanas.com. Então, o pessoal está colocando no chat para vocês. Quem quiser, no final da live, a gente vai fazer o sorteio da Eletronet. Teremos também o sorteio da 4Linux, que vai sortear aí um treinamento EAD à escolha do ganhador. Então, vamos colocar aí no chat também um outro formulário para quem quiser se inscrever aí no sorteio da 4Linux. E vamos ter também o sorteio da Netfinders Brasil, que também vai ser um curso EAD, só que é um curso de BGP multivendor. Então, para quem quiser pode se inscrever. São três sorteios e se inscreva em cada um deles, e, no final, a gente vai sortear os ganhadores.

Antes de começar, também queria fazer o agradecimento aos nossos patrocinadores, que é a Giovaneli Consultoria, Eletronet, Pró ISP, Netfinders Brasil, Juniper, Wztech, Editora Novatec, Icann, Cisco, Forte Telecom, 4Linux, VLSM, e apoio de mídia da revista RTI.

Então, agora, para explicar a Mesa, eu vou chamar o Antonio Moreiras, o gerente, para poder falar um pouquinho. Fique à vontade.

SR. ANTONIO MARCOS MOREIRAS: Gente, muito, muito bom dia para vocês! Sejam todos bem-vindos, bem-vindas a nossa live sobre segurança, que a gente espera que seja a melhor live de segurança do ano aqui. Com toda essa questão de pandemia, com toda essa... com todas essas milhares de lives que estão sendo feitas sobre assuntos técnicos, mas a gente realmente conseguiu convidados muito, muito legais, falando sobre muitos assuntos interessantes.

Ainda continuando sobre os avisos. A gente abriu inscrições para essa live com antecedência, para quê? Para quem precisa de um certificado de participação, precisa ou quer um certificado de participação. Então, muitos de vocês que estão aqui com a gente já fizeram a inscrição lá no site de cursos e eventos do NIC.br. Quem fez a inscrição vai receber um e-mail durante a live, para falar: Olha, estou aqui presente, né? Estou vivo e operante aqui, assistindo a live com vocês. E aí a gente vai gerar o certificado. Ah, mas, Moreiras, eu ainda não me inscrevi, o que eu faço? Bom, se inscreve agora. O pessoal vai colar o link aí no chat, ou entra lá em intrarede.nic.br, e tem lá o link de inscrição. Se inscreve. Do mesmo jeito, você vai receber e-mail de confirmação e você confirma que sim, está assistindo a live. E isso vai ficar até às 14 horas, né? Depois das 14 horas, não dá mais. A gente faz essa inscrição para quem está nos acompanhando ao vivo, faz o certificado para quem está nos acompanhando ao vivo, da melhor forma que a gente consegue. É claro que a gente não tem um controle 100% disso daí, mas a gente se esforça para fazer da melhor forma possível. Então, quem precisar de certificado, faz a inscrição lá no nosso site de cursos e

eventos, vai receber o e-mail, confirma isso e o sistema vai emitir um certificado depois, automaticamente, de participação na live.

E eu aproveito, como sempre, antes de falar da Mesa e passar a palavra para os painelistas, como sempre, eu peço para vocês darem o like aí no vídeo. Vocês já acompanharam, muitos de vocês já acompanharam com a gente, as lives anteriores, já conhecem a qualidade do evento e dos eventos que a gente promove. Então, nos deem esse voto de confiança. Por quê? Porque assim o YouTube, ele distribui, ele avisa o resto do pessoal que está inscrito no canal e que às vezes não ativou o aviso específico dessa live, ele avisa que a live está acontecendo. Então, quanto mais likes a gente tem, mais distribuição orgânica a gente tem no YouTube, para mais gente chega esse conteúdo, e a gente acha que é um conteúdo muito, muito importante, muito, muito legal, por isso que eu peço esse like para vocês. Depois, no final da live, se vocês não gostarem, aí você muda lá, tira o like, dá um dislike, faça o que quiser. Mas agora dá o voto de confiança para gente, coloca o like. Aproveita, já pega o link da live, com o like, e tudo mais, pega o link da live e cola lá naquele grupo de WhatsApp dos provedores, cola lá naquele grupo do Telegram de provedores, naquele grupo de Facebook, no pessoal aí do trabalho que pode se interessar pelo tema. Pode até colar lá no grupo da família, se tiver algum técnico, alguma coisa, está tudo bem. Certo? Traz o pessoal aqui que a Cristine, o Klaus, a Lucimara, o Kurt, está todo mundo ali se aquecendo para passar muito conhecimento para gente agora.

E eu agradeço, de antemão, aos painelistas, o delegado Alesandro, da polícia, que vai poder dar dicas para gente sobre como que o provedor pode interagir com as autoridades legais no caso de estar tendo um ataque, no caso de ter algum problema de segurança. Ele participou também da Operação Ataque Mestre, que prendeu um hacker que incomodava muitos provedores, que estava por atrás de muitos ataques DDoS. Ele vai poder falar um pouco disso para gente, acho que vai ser bem legal essa participação do delegado. A gente está muito feliz de ter ele aqui com a gente.

A gente tem o Kurt Urban, da UPX. Ele vai falar para a gente como faz limpeza de tráfego, como que funciona esse esquema de limpeza de tráfego. É bem interessante.

E temos pessoal aqui da casa, né? O pessoal do Cert.br. Temos a Cristine, o Klaus e a Lucimara, que vão dar um panorama para a gente sobre como que é a situação hoje dos ataques aqui no Brasil, o que o Cert.br enxerga, quais são os principais problemas. Vão falar também... O Klaus vai falar para a gente sobre flows. Muita gente usa flow aí para saber quanto de tráfego troca com o Google, quanto de tráfego troca com a Netflix, com o Facebook. Mas pouca gente sabe que dá para usar flow para monitorar segurança, e o Klaus vai mostrar para gente como que dá para fazer isso. Vai fazer mágica mostrando para a gente, isso, em dez minutos, mas ele vai mostrar, eu tenho certeza, de forma muito útil, que depois vocês vão conseguir ir atrás e implementar.

E a Lucimara vai falar sobre um assunto super, superimportante que são as CPEs. Se você escolher uma CPE mal escolhida, uma CPE que tem problemas de segurança, você pode ter muitos problemas na tua rede, você pode gerar ataques, você pode ser o cara que está gerando ataque DDoS para outros. Isso prejudica tua rede, prejudica a rede dos outros. E a Lucimara vai dar dicas importantíssimas sobre o que é uma CPE boa do ponto de vista de segurança, e como que a gente pode fazer uma compara de CPE que atenda aos requisitos mínimos de segurança.

Então, a gente espera muito para hoje. Um dos nossos painelistas que estava previsto, que era o Luciano, ele teve um problema particular. Ele não vai poder participar, mas a gente já conversou com o pessoal do Cert.br, com a Cristine, com o Klaus e com a própria Lucimara, e eles vão poder abordar também o tema,

que é Internet das Coisas, na apresentação deles. Então, a gente não vai sair perdendo em nada. Infelizmente, não vamos ter o Luciano para enriquecer o debate, para enriquecer a participação, mas o tema vai ser abordado na live da mesma forma. Felizmente, ele nos avisou a tempo para o pessoal preparar isso e vai ser bem legal.

Então, eu acho que, sem mais delongas, talvez pedindo um like de novo, né? Para vocês lembrarem. Mas, sem mais delongas, vamos passar a palavra para os painelistas. E a primeira painelista é a Cristine, que é do Cert.br, é gerente do Cert.br.

Então, Cristine, você é a responsável pelo Cert.br, você trata... O Cert trata incidentes de segurança na Internet a nível nacional. É a instituição que cuida disso para o Brasil inteiro. Você consegue nos passar, para começar a conversa, um panorama desses ataques aqui nas redes brasileiras? Quais são os principais ataques? A que tipo de problemas um administrador de rede, o pessoal que trabalha no provedor, precisa ficar atento? A palavra é sua, Cristine.

SRA. CRISTINE HOEPERS: Obrigada, Moreiras. Obrigada a todo mundo aí pelo convite, né? Dá para ver que está sendo um sucesso, vi que o pessoal está contribuindo com os likes aí.

E o que eu queria compartilhar, né? E vou começar a compartilhar. Eu tenho alguns slides aqui, que eu acho que como a gente vai falar de dados, é muito difícil falar de dados sem a gente ter algum número, alguma coisa. Para o pessoal que quiser, esses slides já estão lá na página do Cert.br, é só ir em Cert.br, no menu à esquerda tem uma área de palestras. Os meus slides estão lá, do Klaus, né? Como a gente tem bastante URL, bastante gráfico, acho que é legal o pessoal ter acesso a isso. E uma coisa que eu queria dizer já de antemão, assim, é que cada um tem uma visão sobre ataques na Internet, né? Então, eu vou dar uma visão do que são dados que a gente, no Cert.br, tem. E o que é essa visão.

Então, hoje, um dos nossos dados de incidentes, eles vêm da área de tratamento em incidentes, que é a área principalmente do nosso pessoal que cuida do e-mail cert@cert.br, que é o pessoal que recebe notificações e incidentes do mundo inteiro. Então você tem o mundo reclamando de ataques que saem do Brasil, tem o pessoal do Brasil reclamando de ataques que estão aí pelo mundo. E essa é uma das fontes do dado, mas a gente tem toda uma área de cuidado de análise de tendências, que ela tem dados de honeypots e de data feeds. E o que eu vou trazer aqui é um misto desses dados que a gente tem.

Então, para ter uma ideia do volume anual, né? Por exemplo, o ano passado a gente teve aí uns 870 mil incidentes, foi 4 milhões de e-mails, né? Os threat feeds, a gente tem os nossos próprios honeypots do Cert, a gente recebe dados relativos a todos os sistemas autônomos do Brasil, do Team Cymru, SpamHaus, ShadowServer, do Shodan. Então, a gente não consegue, óbvio, tratar cada único pacote que vem de cada dado, mas a gente tenta ao máximo tirar desses dados o que é mais importante, retestar, né? O Klaus depois pode até falar um pouco mais sobre como a gente tem usado isso nas notificações para os provedores. Notifica todo mundo. Então, tem muita gente que está aí na live, deve receber os e-mails do Cert notificando de problemas. E a gente tenta gerar estatísticas públicas, né? A gente não fica fazendo shamming ou tentando apontar o dedo, mas a gente tem uma noção de para onde estão indo as coisas e a gente compartilha alguns desses dados, tá?

Então, a gente lançou, uns 15 dias atrás, os dados do primeiro semestre desse ano. A gente geralmente lança só dados anuais, mas como esse está sendo um ano diferente, está todo mundo muito ansioso para saber se está aumentando incidente, se não está, e tem pandemia, e todo mundo falando disso, a gente lançou as estatísticas semestrais, né? E o que a gente notou é que continua a mesma tendência que era

2019, né? O que a gente mais teve são ataques de força bruta de credenciais, tá? Isso é o ataque número 1, e esse é o tipo de ataque que afeta a IoT, né? Então, a gente sabe que hoje tanto CPEs quanto Internet das Coisas, sim, eles estão cheios de vulnerabilidades, têm muito problema, falta atualização de firmware, né? A Lucimara depois vai poder comentar mais aí sobre esses desafios. Mas ainda, uma das coisas mais comuns exploradas pelas botnets, como Mirai e Bashlite, é credencial. Credencial fácil, credencial padrão que vem do fabricante e que está lá no manual. Então, esse é o ponto, só que não é só isso, né? O pessoal está testando muito outras portas, que a gente vai ver em detalhes, e Internet das Coisas é uma das coisas que a gente mais está recebendo, e aí é lembrar que é qualquer coisa que seja baseada, ou em Android, ou em Linux Embarcado. Então, é um misto de coisas que estão gerando ataques e que estão sendo infectadas, né? Então, e infectadas para quê? Para fazer DDoS, a maioria deles, UDP flood, para trocar DNS, vou falar um pouquinho. Isso aí continua, né? É um ataque que a gente tem no Brasil prevalente desde 2014. E mineração de criptomoeda, mas isso deu uma caída. A gente não tem recebido tanta notificação assim.

Então, se a gente for pensar, abrir um pouquinho esse número dos 300 e poucos mil incidentes notificados, né? Fraude? Sim, teve um pouco de aumento comparado com o primeiro semestre do ano passado, mas teve queda comparado com o segundo semestre, né? Então, a gente pode dizer que não foi tanta fraude assim, não aumentou fora dos padrões, né? Como era de se esperar, teve fraude envolvendo o tema de Covid. Mas não foi nada diferente do que a gente viu com fraude usando Copa do Mundo, usando Olimpíada, usando outras coisas, e falando de Black Friday, né? A gente sabe que isso vai acontecer e vai usar o tópico da hora, e vai tentar fazer isso daí. Só que é muito importante pensar que 96% são páginas falsas, e isso está muito relacionado com algo que a gente vai discutir aqui, nessa live de hoje, que é a invasão de CPEs para trocar a DNS. Então, assim, porque essa é hoje uma das maneiras que o pessoal tem direcionado as pessoas para página de fraude, né? Via essa invasão de DNS.

Outra coisa que é muito importante a gente ver, por exemplo, pega essa parte de varreduras. Praticamente tudo que está sendo notificado para nós nas top-portas aí, é força bruta de credencial, né? Então, não interessa se força a bruta de credencial de IoT, elementos de rede, roteadores, portas 22 e 23 aí, que a SSH e Telnet, é o que mais tem sido notificado. E-mail está muito prevalecente, tentar força bruta de e-mail. E aí são vários ataques, né? Lembrar que quase todo o serviço, você faz reset de senha via e-mail. Então, é muito importante tentar conseguir. Tem aquele monte de bases de senhas que vazaram, então o pessoal fica tentando fazer força bruta em N serviços também reaproveitando senhas. Lembrar que a gente continua tendo ataques de MikroTik, e não é mais só o winbox, tá? A gente também está tendo ataques em cima daquele protocolo de API de MikroTik, então é credencial e está muito prevalente, tanto Telnet com a porta de winbox quanto Telnet winbox e a porta da API.

E falando em negação de serviço, uma das coisas que a gente vê, assim, ele caiu com relação ao ano passado, mas é bom lembrar que ano passado a gente teve um recorde de notificações de negação de serviço para o Cert.br. E o que a gente recebe notificação? Que eu acho que isso é importante deixar claro para vocês. A maior parte das notificações que são mandadas para nós são pessoas sofrendo negação de serviço que está saindo das redes brasileiras. Então, não é necessariamente, o que a gente está vendo não são, vocês aqui, provedores e pequenos provedores, tal, reclamando para nós que estão sofrendo DDoS. É o mundo reclamando para nós que vocês estão gerando DDoS para eles. Então, isso é uma coisa que é muito importante a gente pensar, porque isso, ano passado, foi o recorde, os números ainda estão grandes, não são pequenos, né? E a gente teve uma pequena mudança. Em 2018/19, a maior parte das reclamações era de amplificação de tráfego. Isso ainda existe, mas esse primeiro semestre, a gente realmente focou... as reclamações estavam todas focadas em botnet de Internet das Coisas. E a gente

classifica como botnet de Internet das Coisas, mas isso envolve CPEs invadidos também, né? Então, é um misto de Mirai, de Bashlite e de outras botnets aí que infectam tanto CPEs quanto dispositivos IoT. Isso é que foi o grosso do que foi notificado para nós de negação de serviço.

E se a gente for olhar agora, dados que a gente tem de Honeypots e de Shodan, isso bate muito com o que está sendo reclamado para nós, tá? Essa tabela à esquerda, que ela disponível na verdade, até nessa página aqui dos Honeypots, nas nossas estatísticas, a gente tem as top 20 portas, né? Aqui cabia só as top 15. Vocês podem olhar que, assim, com... mas muito mais do que outras portas, é Telnet, né? Infelizmente, a gente continua tendo muito Telnet em elemento de rede, em CPE, em IoT. Aí a gente tentou cruzar isso um pouco. Isso aqui dos Honeypots, né? Voltando um pouco atrás, são varreduras. A gente está vendo os atacantes procurando por essas portas. Então a gente vê que mais procuradas, sim, são Telnet e SSH. E Telnet com uma vantagem muito grande. E aí a gente foi nos dados de Shodan, de IPv4 alocado ao Brasil, e realmente, a gente tem muito Telnet exposto na Internet, né? E não é só Telnet na porta 23. Não adianta só mudar a porta, os atacantes vêm também e vão achar essas outras portas. Então, a gente vê que tem Telnet nas mais variadas portas aí, e a gente tem os atacantes procurando. Mas se a gente for olhar as outras portas TCP, vocês podem olhar aqui, é muita coisa relacionada com força bruta. A gente tem RBP, a gente tem VNC, a gente tem aqui essas portas 5555, isso aqui é Android, tá? E tem também, isso aqui também é TR69 em alguns CPEs, você tem outras portas, você tem MikroTik sendo procurado aqui. Então assim, força bruta também é muito procurado.

Já as estatísticas de amplificação, né? Essa parte, esse gráfico à esquerda é o gráfico que está disponível quebradinho aqui nessa estatística de amplificadores, né? Sim, a gente melhorou muito, né? Todo trabalho que a gente está fazendo notificações, que o programa Por Uma Internet Mais Segura tem estimulado o pessoal a reduzir o número de amplificadores no Brasil. A gente teve uma melhora muito grande, mas teve uma melhora muito grande em quê? Em SNMP e em Ubiquiti, né? Que foram os dois que melhoraram, mas a gente continua com muitos amplificadores, né? E, sim, os atacantes continuam procurando. Nos nossos Honeypots, as varreduras campeãs são de CIP(F), que é credencial de ramais para fazer ligações de graça na Internet, mas daqui para baixo são protocolos de amplificação. Então, nessa página aqui de Honeypots vocês vão ver mais detalhes, o que é cada uma dessas portas aqui, mas isso aqui é amplificação. Então, assim, o pessoal está procurando, porque, sim, está disponível e isso é poder de fogo. E é um poder de fogo que está consumindo a banda de upload de vocês, porque cada vez que vocês têm um serviço desse de amplificação ou que vocês estão com IoT gerando ataques DDoS, uma botnet IoT, é a banda de vocês que está sendo consumida e vocês estão perdendo dinheiro, né? Enquanto esses ataques estão acontecendo.

E complementando um pouco, né? Eu comentei a parte de invasão de CPEs para alterar DNS, né? É lembrar que, sim, isso acontece, continua acontecendo. Eles redirecionam não só banco, serviço de pagamento, streaming, mobilidade, redes sociais, webmail, comércio eletrônico, é algo que tem credenciais, eles estão aproveitando para redirecionar. E a gente continua vendo esses DNSs maliciosos, então esse gráfico aqui é o número de servidores maliciosos sendo consultados pelos CPEs comprometidos. O Klaus vai retornar um pouquinho nisso aqui, quando ele estiver discutindo a parte de netflows, né? Como que daria para provedores tentarem detectar se você tem o CPE invadido ou não, né? E aí você vai ter que ir nesse CPE fazer gerência remota, ou trocar, ou instalar patchs ou trocar a senha, né? Mas é importante estar atento que isso está acontecendo e acontecendo bastante.

E apesar de a encomenda ter sido para eu falar um pouquinho sobre os ataques, né? Eu acho que, assim, não adianta também a gente ficar só falando do: meu Deus, o mundo está acabando. Mas o que a gente

tem que fazer para tratar desses ataques que são o top do que a gente tem? É o básico, né? É aplicar patchs, é manter sistemas atualizados, é manter na última versão, é ter múltiplos fatores de autenticação. E, pessoal, sim, o melhor seria ter um token hardware ubiquiti, mas lembrar que chaves criptográficas, pessoal, o seu roteador, invistam em ter acesso via SSH com chave criptográfica. Você pode ter SSH, chave criptográfica e um ubiquiti, dependendo do dispositivo que você tem, servidores. Quer dizer, qualquer tipo de segundo fator já ajuda, né? E recebam as nossas notificações, deem uma olhada como que estão os contatos de vocês no Whois, e o mundo está tentando avisar vocês que vocês têm problemas de segurança. Então, não descuidem, né? Tem algumas referências aqui também, lembrem que tem outras coisas, lembrem da importância de DNSSEC, lembrem da importância do RPKI, mudem para protocolos mais modernas, isso tudo é muito importante. E para quem baixar os slides aí, tem referências, muitas, sobre como implementar todas essas coisas aí.

E para também lembrar, a gente vai continuar entrando em contato, vocês vão continuar ouvindo falar disso, seja através do Programa Internet Mais Segura ou a gente notificando, mas eu acho que é importante vocês pensarem mesmo nessa parte de investir no básico, né? Tem que manter patchs, tem que cuidar, porque os incidentes estão aí, as botnets de IoT estão comprometendo os dispositivos, estão comprometendo os CPEs também. Os servidores de vocês estão com problemas. Quer dizer, tem que dar uma limpada na rede. Eu acho que isso é o mais importante aí para a gente pensar.

E era isso que eu tinha aqui na parte inicial. Obrigada aí, pessoal. Vou parar o meu compartilhamento e agradeço aí o espaço para falar.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Cris. Realmente foi muito interessante tudo que você falou.

Agora eu vou chamar o Klaus para fazer uma apresentação, né? Klaus, após aí a fala da Cristine sobre os incidentes de segurança aqui no Brasil, eu gostaria que você apresentasse um pouco sobre flows, né? Até porque, muito administrador de rede não sabe que análise de flows pode identificar ataques, né? Pode ajudar a resolvê-los. Às vezes o pessoal só associa flows a gerenciamento de rede. Por isso eu queria que você explicasse um pouquinho, de maneira simples, para o nosso público, como eles podem trabalhar com flows. Então, fique à vontade.

SR. KLAUS STEDING-JESSEN: Eduardo. Não, você está coberto de razão. A ideia é... Deixa eu só compartilhar minha tela aqui, só um instantinho.

Antes de mais nada, eu queria só agradecer a participação de todos. Eu vi que a gente está quase com mil pessoas aqui na nossa sessão, então acho que é muito, né? O agradecimento primeiro para quem está nos assistindo, um bom dia a todos. E para os nossos painelistas também.

Então, seguindo nessa linha que o Eduardo falou, realmente, os objetivos hoje, que eu queria passar para vocês, é basicamente, assim, que todo mundo saísse muito claro, tá? Que provavelmente você já tenha habilidade de gerar netflows na sua rede, tá? Em seus elementos de rede. Isso pode ser, hoje em dia tem switch que faz isso, roteador, tem firewall, tem appliance que faz isso, tá? Com custo zero, tá? Muitas vezes a pessoa nem se dá conta disso, né? Dá para implementar um coletor, e os comandos que a gente vai ver aqui são todos em cima de software livre, tá? Então também dá para fazer isso com custo zero, tá? E, como o Eduardo comentou, sim, muitas redes falam: sim, sim, a gente tem netflow, mas a gente só usa para engenharia de tráfego, tá? Ok. Excelente, uma poderosa ferramenta para isso. Mas o que a gente queria convencer todos aqui é que, sim, além disso, tem vários usos interessantes de netflow para

detecção de botnets, tudo aquilo que a Cristine estava comentando de IoT disparando ataque de negação de serviço, ataque saindo da sua rede. A gente vai ver alguns exemplos simples, onde você consegue, de maneira trivial, achar esse tipo de anomalia na sua rede, né? Então, como eu comentei, nesses nossos exemplos, a gente está usando software livre, nesse caso, nfdump, e para captura de tráfego, nfcapd ou sfcapd.

Então, só uma revisão muito simples, né, pessoal? Quando a gente está falando de netflow, nós estamos falando do que exatamente, tá? Então, assim, netflow foi um protocolo que começou com a Cisco lá atrás, tá? Já teve várias versões aí, hoje em dia, é um padrão Ietf, né? Ipfix. Todo vendor, hoje em dia, implementa isso de alguma maneira ou outra, tá? E qual que é a ideia? Imaginem o netflow como um protocolo de sumarização de tráfego. Então, você tem elemento de rede, né? Imagina aquele nosso exemplo ali, um roteador ali no meio. Ele está vendo todos os pacotes que estão transitando por ele, mas não, a gente não vai logar pacote a pacote, tá? A ideia do flow todo é que ele vai gerar um registro dessa comunicação, né? Então, basicamente pensem nele como um registro, que é uma tupla de dados, onde basicamente esse elemento de rede vai dizer para nós, no final de um tempo, dizendo: Olha, eu vi uma comunicação entre o... entre, nesse nosso exemplo ali, nesse cliente, acessando um destino, então, eu tenho um IP de origem, um IP de destino. Porta origem, porta destino. Nesse nosso exemplo é uma seção http, uma seção de porta 80, ali, de servidor web. Qual foi o protocolo, tá? Isso aqui é bem simples, pessoal. Dependendo da versão que você tem, você vai ter muito mais coisa aí, tá? Você vai poder ter AS de origem, AS de destino. Você vai poder ter flags TCP que foram observadas no caso de TCP. Mas a gente pensar numa ideia de metadados, tá? Ah, essa comunicação durou X segundos, tá? E isso, esse elemento de rede seu vai exportar isso para um servidor da sua rede que é um coletor de flows, tá? Naquele nosso exemplo no slide anterior, isso seria nfcapd ou sfcapd, que capturaria isso e gravaria em disco, tá? Uma vez gravado em disco, você então consegue fazer consultas em cima disso, tá?

Uma dúvida muito comum, pessoal, é assim, é por isso que a gente, muitas vezes, insiste em falar, chamar isso em netflow, tá? A gente vê isso muito nos nossos cursos, né? O pessoal, às vezes, você acha, você fala em flow apenas, e existe uma certa confusão. O cara: Ah, é, isso, eu tenho flow na minha rede. Quando, na verdade, ele estava se referindo a um espelhamento de porta de switch e captura de pcap, captura de pacote a pacote. Não é isso que nós estamos falando aqui, tá? Até porque isso não escala em grandes redes. Imagina você fazer isso aí, você tem uma interface 100 giga e você está capturando pacote a pacote, e jogando num disco, né? E tem questões de privacidade envolvida também, né? Você não vai estar querendo... ressaltando aqui que netflow não está olhando para payload de pacotes. A gente não sabe o que transitou ali, entre aquele cliente e servidor, mas o que eu quero convencer vocês aqui que só sabendo que existiu essa comunicação pode ser extremamente útil, tá?

Então, vamos avançar aqui, pessoal. Exemplos, tá? Como que poderia ser um exemplo de um netflow aí de uma rede. Então, por exemplo, nesse caso, eu escolhi um dia específico e fiz uma consulta, eu quero ver tudo que é protocolo DP, com destino à porta 53. Então, a gente está vendo tráfego aí DNS, né? E limitei os destinos. Me mostra todo mundo que falou, então, com esses dois IPs aí do Google, tá? 8844, 8888. E aí, ele vai basicamente me falar todas as... um resumo, né? Quer dizer, toda a comunicação que aconteceu desses clientes aí com esse servidor, tá? Vai te dar um sumário no final, com total de pacotes, banda, tá? Pacotes por segundo, etc., tá? Então, esse aqui é um exemplo só para a gente ilustrar um pouco o que a gente está falando aqui.

Tá, mas e aí? O que isso me ajuda do ponto de vista de segurança, né? Então, assim, só fazendo um link com o que a Cris falou de servidores de DNS maliciosos, que é um negócio que a gente está vendo

continuamente, né? Como que funciona esse ataque? Você tem CPEs dos seus clientes sendo comprometidos, o atacante vai lá e muda a configuração de DNS desse CPE. Então, agora esse CPE não consulta mais o seu recursivo, ou o do Google, ou qualquer outro legítimo, mas consulta um DNS do atacante. E, como vocês podem esperar, esse DNS do atacante, ele responde de maneira maliciosa para alguns domínios, né? Então, como que a gente poderia fazer isso aí? Imagina que você tem esses flows, isso faz parte já da sua arquitetura, a sua rede já captura esses flows normalmente, e você poderia fazer isso até de maneira automatizada, você pode ter um chrome num servidor seu, que todo dia ou toda hora, enfim, faz uma consulta querendo saber o que exatamente? Ah, me mostra todo mundo aí que é protocolo UDP que tenha destino na porta 53, que venha de uma rede específica minha, clientes, por exemplo, um segmento meu de... que tenha CPEs, e que não seja para DNSs que eu considero legítimas. Ou seja, o meu próprio recursivo DNS ou outros, aí, Google. Você coloca o que você quiser nessa lista. Basicamente, então, eu estou vendo o quê? Tráfego DNS para servidores recursivos que não são aqueles que eu considero legítimos, tá? O que... E aí? Esse resultado pode me mostrar potencialmente o quê? Tá? Você vai começar a ver tráfego com destino para DNSs que não naquela sua lista legítima. Ah, mas isso é necessariamente malicioso? Pode ser que não, pode ser que você vai ter que incrementar a sua lista com outro servidor DNS legítimo. Mas é importante ter isso no radar. Quer dizer, por que esse cliente meu está fazendo uma consulta para um DNS estranho, com uma latência grande? Tem essa questão também, tá? Então, assim, em vez de consultar o meu recursivo com 1 milissegundo de latência, o cara está indo para um negócio com 300 milissegundos, né? E potencialmente sendo fraudado, porque essas respostas que ele está obtendo aí são maliciosas. Então, é um comando, pessoal. Você poderia automatizar e ganhar um relatório de: Opa, tem alguma coisa estranha aqui na minha rede, tá? E aí, mas o que eu faria com esse dado? Ah, eu me convenci que, realmente, é um CPE que está comprometido, né? Então, isso... até fazendo um link depois para a parte da Lucimara. Isso aí a gente entra numa discussão de como é que a gente eleva a barra aí para ter CPEs que permitam atualização de firmware, trocar senha padrão, né? Mas vai entrar em algum esquema nesse... uma discussão nesse tipo aí, né? Correção de [ininteligível], etc., tá?

Falando de IoT, que o Moreiras também tinha comentado, né? Hoje em dia, a gente tem visto muito, ainda está vendo muito Mirai, bashlite, etc., né? Quer dizer, como é que funciona isso? Esses malwares saem varrendo a Internet, exploram várias anormalidades, mas Telnet também, força bruta também é uma delas, infectam o equipamento, baixam um binário embarcado, né? Um binário do próprio malware, se conectam num comando de controle e aguardam por comandos, e aí os comandos são invariavelmente ataque à rede X, ataque a Y. Então, você vai ter um bot na sua rede, quer dizer, uma máquina sua ou de cliente infectada, espalhando ataques aí contra terceiros, tá? Hoje em dia, tem várias fontes, pessoal, hoje em dia tem várias fontes públicas, onde a gente pode ter acesso a esse tipo de dado. Quer dizer, que dado? IPs de comando e controle de IoT. Ali tem um exemplo, aquele ali que a gente listou, né? E como é que eu poderia fazer isso nos meus flows, né? Posso basicamente olhar, me mostra todo mundo que é TCP e que tenha como destino um desses IPs aí que eu salvei no arquivo txt, tá? E aí todo dia você pode manter esse arquivo atualizado, tá? Putz, tenho clientes meus que acessaram... esse destino, tá? Quer dizer, provavelmente é um IoT aí... pode ser um CPE invadido, tá? E, de novo, a gente cai naquelas questões de mitigação. Você está vendo comunicação de comando e controle, tá? Tem um outro exemplo ali embaixo também, outros IPs maliciosos que pode usar, o pessoal do urlhaus também é bem interessante, tá?

Outra coisa muito útil, pessoal, aquela história de top talkers, né? Detecção de grandes geradoras de tráfego. Por que eu estou interessado nisso, né? Bom, uma vez que eu quero receber um comando para atacar um terceiro, certamente esse cara vai gerar bastante tráfego, né? Outra opção é: você tem um amplificador daqueles que a gente aqui do Cert notifica toda semana, milhares de AS brasileiros, né? Você

tem um DNS recursivo aberto, um SSDP, por aí vai, tá? Que está sendo abusado por terceiros para amplificar tráfego. Como que você poderia pegar isso daí? Essa linha de nfdump, basicamente você está fazendo o quê? Eu estou ordenando os flows por bytes, tá? Estou dizendo assim: Olha, só me interessa flows com mais de 10 gigabytes, que trafegaram mais de 10 gigabytes, aí você, obviamente, adapta para sua realidade. Eu só quero ver os top 10, tá? E basicamente eu estou selecionando... Tem que ser um bloco da sua rede, né? Eu quero ver que seja originado na sua rede e que não tenha como destino essa sua rede. Ou seja, eu quero tráfego... não quero tráfego interno. Eu quero o tráfego saindo da minha rede, tá? "Ah, mas eu tenho um servidor meu aqui que eu sei que gera muito tráfego, tal". Ok. Você pode excluí-lo naquela lista ali, você pode ter um arquivo seu que você mantém de servers que, sim, são caras que geram bastante tráfego, e aí todo o resto você quer ver, tá?

Então, um exemplo aqui, pessoal. Um exemplo real, tá? Esse foi uma rede que usou esses métodos aqui justamente para detectar esse tipo de coisa. E a primeira linha que salta aos olhos, opa! Tem um IP na minha rede que, sozinho, gerou 1.4 terabyte de tráfego, tá? Então, se você olhar naquela penúltima coluna ali, à direita, ele, sozinho, consome 200 megabytes por segundo, tá? Certamente um candidato para você dar uma olhada e ver do tipo: Tá, e aí? Esse cara é legítimo? Não é? Quer dizer, ele, sozinho, gerou 1.9 megaflows, tá? Quer dizer, um único host da sua rede foi responsável por 16% de todos os flows de todo esse período, né? Entãoé um cara que, como a Cris comentou na apresentação dela, está degradando... está usando recursos valiosos seus, vais gerar incomodação depois, porque isso está atacando alguém e depois alguém vai reclamar que esse negócio está saindo da sua rede. Quer dizer, é algo que você, de maneira preventiva, poderia olhar e, como eu falei, com [ininteligível] que são... não precisa ser feito na unha, tá? Você pode fazer isso de maneira automatizada, tá? Então essa que é a ideia.

Então, acabando aqui, pessoal, referências. Encorajo vocês a olharem aquele último link, tá? Uma apresentação excelente do pessoal CSIRT da Unicamp, tá? Mostrando na prática como eles estão usando flows para resolução de incidentes, tá? Tem palestra deles também. Está disponível no YouTube. E tem o restante aí, o RFC, que define IPFIX e nos diferentes fabricantes, tá? Juniper, MikroTik, Cisco, etc., tem documentação específica, tá?

Então, basicamente essa era a parte. Isso aqui a Cristine comentou. Eu acho que é muito importante a gente focar nesses três tópicos, tá? E, depois, na apresentação, quem quiser dar uma olhadinha outros protocolos, pessoal, que a gente recomenda fortemente estão disponíveis aí, tá? Com isso, eu agradeço, pessoal, e retorno, então, para o Eduardo e para o Moreiras. E agradeço aí.

SR. ANTONIO MARCOS MOREIRAS: Klaus, muito obrigado pela apresentação. Foi muito interessante. E o Klaus, e todos os painelistas, eles continuam aqui com a gente, eles retornam depois.

Pessoal, a gente está vendo bastante gente interagir no chat, colocar as perguntas, e é para fazer isso mesmo. O pessoal da nossa equipe está anotando as perguntas, e, depois dessa rodada inicial, quando todos os painelistas fizerem essa apresentação de dez, 12, 15 minutinhos aí, a gente vai trazer essas perguntas do chat e começar uma rodada de debates aqui, de respostas, né? Se a pergunta for direcionada, a gente manda para a pessoa específica. Se for uma pergunta genérica, a gente chama todo mundo para responder. Então, por favor, interajam.

E eu vi muita gente importante e interessante e que a gente está muito feliz de que está assistindo a live aqui com a gente, por exemplo. Por exemplo, o nosso diretor presidente, o Demi Getschko, que foi o cara que fez a primeira conexão de Internet aqui do Brasil. Está com a gente na live. A Profa. Liane Tarouco, também é uma pessoa importantíssima na história da Internet brasileira. Eu vi ela colocando comentários

aí no chat. Eu estou muito, muito feliz de ter a participação dela. O [ininteligível] está por ali. A Emily Varela, que está sempre envolvida em questões aí de governança da Internet. O Prof. Adriano Cancian, grande especialista em segurança. É uma honra muito grande ter tanta gente legal e todos vocês que estão aí nos assistindo, né? É muito interessante essa participação.

E falando do pessoal que está fazendo essas perguntas no chat, interagindo no chat, a gente tem visto muitas interações legais do pessoal que assistiu a live. Por exemplo, a gente tem visto muita gente postar no LinkedIn os certificados de participação, tanto da live quanto dos nossos EAD IPv6, de outros eventos que a gente faz, o pessoal tem colocado no LinkedIn. A gente vai lá e comenta. E a gente fica muito, muito feliz, porque mostra o quanto pessoal tem gostado e aproveitado desses eventos.

Inclusive teve uma colocação no LinkedIn, foi do Prof. Henry Alves Godoy, se não me engano, eu vi também algum comentário dele hoje aqui no chat no YouTube. Ele é professor de redes da Fatec, e ele nos contou que ele passou para a turma dele de redes a tarefa de assistir essa live, valendo nota, porque ele achou que ia ser uma verdadeira aula de segurança, e eu acho que ele tinha razão, está sendo uma verdadeira aula de segurança.

E se tiver outros professores aí assistindo a live, eu queria até pedir para vocês falarem: Ó, sou professor de tal faculdade. Sou professor de tal faculdade. Coloca aí no chat. É, os alunos do professor estão aí. Se tem algum aluno aí, a Francis já colocou ali: Aluna do professor Kelton(F) aqui. Se tiver também algum aluno que o professor pediu para assistir a live, comenta aí com a gente. É bem interessante para gente saber isso.

E eu vou chamar agora o Kurt, Kurt Urban, da UPX. Um dos ataques que mais preocupam a operação de uma rede é o ataque de negação de serviço. E o que é possível ser feito quando se recebe um ataque desses, né? Muito se comenta por aí de limpeza de tráfego, mas o que é realmente essa limpeza de tráfego? Como que isso funciona? A gente sabe que a UPX trabalha com isso, e você é um especialista nisso. Então, Kurt, por favor, tome a palavra, e se possível, nos explique essa questão.

SR. KURT URBAN: Primeiro agradecer aí, né? O convite aí para participar desse evento, tal.

Então, na parte do negação de serviço, primeiro é identificar o que está sendo impactado mesmo. Se é uma aplicação, se é por causa de um problema nessa aplicação que não foi bem feita aí. Um pequeno acesso nela voltado a tirar ela do ar consegue tirar ela, né? Aí, o tratamento seria na própria aplicação, né? Eu vou focar mais seria na aplicação, no caso, DDoS, né? Que é o que está pegando mais com pessoal aí, né?

Então, o que pode ser feito, né? A pergunta que vocês fizeram. É proteger, primeiro, identificar o que é o alvo desse ataque, né? Então, a explicação do Klaus foi excelente, porque é a forma mais fácil de a pessoa, mais rapidamente, tentar identificar o que está sofrendo, né? Com... Na rede dela, né? Depois de identificado o que é, qual é o alvo daquele ataque, e que for o caso, o tipo de ataque, seria fazer uma proteção antes do alvo, se possível, para deixar o alvo, vamos supor, vivo, né? E aquele tráfego malicioso não chegar nele, tá? E como fazer essa proteção? Essa proteção pode ser feita colocando equipamentos dentro da própria casa do cliente, né? Da própria rede dele, que vai... O cliente vai fazer o tráfego passar por esses equipamentos, tudo, tirar fora o tráfego malicioso, antes de chegar no alvo. Ou ele poderia contratar serviços de proteção em nuvem, que, na hora que detectasse o ataque, esse tráfego seria desviado para esse serviço, ele faria a filtragem inicial, a filtragem do ataque e entregaria o tráfego já

filtrado para a rede do destino, tá? Cada caso tem sua vantagem, né? E também existe a possibilidade da forma mista, a pessoa ter ferramentas internas e utilizar também nuvens de mitigação para ajudar, né?

No caso de tratamento dentro de casa, né? O que... O pessoal tem que ter equipamentos, roteadores e máquinas para poder filtrar esse pacote, né? Qual que é a vantagem disso? Como está tudo dentro da casa dele, ele consegue customizar bem mais a filtragem, né? Mas isso tem certas desvantagens. Por quê? Quando o ataque chega nesses equipamentos, toda a infraestrutura desse... da rede desse alvo tem conseguido suportar esse ataque. Se for um ataque DDoS gigantesco, né? Ele teria que conseguir suportar esse ataque. Se não... Se ele saturar os links dele até o equipamento de filtragem dele, o ataque foi bem sucedido, né? Ele foi... Não adianta ele conseguir proteger o equipamento final se a rede dele já está saturada, né?

Quando utiliza mitigação em nuvem, as nuvens, geralmente, têm a capacidade gigantesca para suportar o ataque, ela faria essa filtragem e mandaria já o tráfego limpo, né? Então, fica mais barato, por quê? Com o equipamento dentro de casa, você tem que pensar que certos equipamentos você tem, além de adquirir o equipamento, você tem a licença do equipamento, e esse equipamento, ele tem um volume, né? Então, dependendo do tipo de ataque, você tem que colocar vários equipamentos em paralelo para poder ajudar a suportar o ataque. No caso da nuvem, a nuvem tem essa função. Então, acaba saindo mais barato, porque a pessoa não precisa investir tanto na rede dela para suportar os ataques. E existe o caso misto, que ela pode ter equipamentos dentro de casa. Ela vai filtrando os ataques pequenos, e bem configurado, né? E deixa, quando o ataque ultrapassar o limite de mitigação dos equipamentos dele, ele encaminha os anúncios para a rede, para a nuvem de mitigação e o tráfego passaria primeiro pela nuvem, antes de chegar na rede dele. Então, a nuvem pegaria o volume grande do ataque, que pode ser em volumetria de pacotes ou volumetria de dado, de banda mesmo, filtraria, entregaria uma taxa menor, que poderia ser refiltrado, no caso da rede do cliente, no caso misto, né? E entregue para aplicação da forma correta, né? Esse seria, então, o que poderia ser feito, tá?

Agora, outra pergunta que foi feita aí seria sobre a limpeza de tráfego, como que funciona, né? Para limpar o tráfego, lógico, você vai colocar um equipamento, né? Vai passar o tráfego... os pacotes todos por equipamento, que vai analisar todo... os padrões daquele tráfego. E, de acordo com o que já foi pré-configurado, ele vê se aquele tráfego... Aquilo é normal? Aquele alvo, né? Vamos pegar um exemplo: você tem o servidor web que tem um tipo de acesso, geralmente porta 80, http, tal, que é o normal dele numa volumetria X. Tudo bem, tem picos, tal. Mas de repente, começar a chegar pacotes SSTP nele, isso não é uma coisa normal, né? Então, o sistema poderia... detecta esse tipo de coisa, ou um ataque até http, mas numa volumetria muito maior do que normal, vindo de redes que normalmente não acessam, né? Isso é indicativo de um ataque. Então, começa a ser feito de acordo com parâmetros já pré-configurados, começa a ser feita a filtragem, deixar passar o tráfego por um... de um caminho, de outro não, né?

No caso de usar a mitigação em nuvem, muita coisa que acontece também é utilização da engenharia de redes. Porque como essas redes de mitigação, elas têm muita conectividade, muitas vezes, o ataque, quando chega um ataque, é detectado que ele tem uma tendência a vir por um certo local. Então, o filtro, ele atua mais numa origem específica e na outra... e onde não está passando o ataque não gera essa interferência, essa filtragem, que qualquer equipamento que colocar a mais no meio do caminho, gera um aumento de latência, né? Então, com essa engenharia de rede, você consegue colocar o filtro numa origem específica. E na outra origem que não está tendo ataque deixar o tráfego passar mais direto, impactando menos no alvo do ataque, né? Os efeitos colaterais de aumento de latência são bem menores, né?

Agora, como que funciona também para a gente detectar, né? Como é essa parte de detecção do ataque? O cliente, ele pode deixar o tráfego passando o tempo todo pelos equipamentos de mitigação e aí, nesse caso, gera um aumento de latência. Outra forma é utilizando os flows ou duplicação de pacotes, de alguma forma. Ele analisar o tráfego que está chegando, e, de acordo com padrões já pré-configurados no sistema, quando é detectado uma anomalia no tipo do tráfego, esse tráfego... esse alvo que foi detectado, que está com esse tráfego anômalo, esse tráfego vai ser desviado para os equipamentos que fazem a inspeção do pacote, né? E essa inspeção é feita por vários protocolos diferentes, várias formas diferentes e geralmente utilizam de inteligência artificial para poder ir aprendendo e aplicando os filtros nas bordas. Então, um exemplo, esse que falaram. Uma CPE que está sendo... foi comprometida e está sendo usada como fonte de ataque. Aquele IP específico daquela hora que, lógico, esse IP pode mudar, naquela hora, aquele IP está gerando muito tráfego, vou dar um exemplo, SSTP, e o sistema detectou isso. Então, na hora que é detectado que aquela fonte gerou... está gerando esse tráfego anormal, esse ataque, por FlowSpec, normalmente, é aplicado filtros nos equipamentos de borda, e, durante um tempo, aquele IP fica de quarentena, aquele IP de origem fica de quarentena. Então, aquele tráfego não chega mais nos equipamentos de mitigação e, por consequência, não chega mais no destino do alvo. E aí a análise dos pacotes, que são coisas mais complexas, gasta mais CPU. Quando o padrão de ataque é detectado, uma origem é detectada, ela é isolada, e aí os equipamentos ficam com CPUs livres para poder continuar analisando os pacotes e o sistema vai se realimentando, né?

Então, existe o sistema que o tráfego pode passar o tempo todo, e o sistema que quando é detectado que tem o ataque, joga para a caixa, acabou o ataque, ele volta o tráfego direto, sem ficar analisando... Sem ficar analisando, não, a análise é feita o tempo todo. Mas sem ficar abrindo pacote por pacote para ver se realmente tem... aquilo é pacote lícito ou ilícito, né?

No caso de um ataque em nuvem, existe também uma possibilidade com alguns clientes, que a nuvem, ela pode... O cliente anuncia, na hora que ele quer, para a nuvem de mitigação, e a nuvem fica analisando de acordo com os parâmetros que o cliente pré-configurou já no sistema, se aquele tráfego é normal para aquele destino. Se não for normal, a nuvem de mitigação desvia para os equipamentos dela que fariam mitigação para aquele tipo de ataque. Então, equipamentos que tratam um ataque tipo TCP, é um tipo de equipamento. Um equipamento tipo UDP, ataque UDP, vai para outro tipo de equipamento otimizado para aquele tipo de ataque, né? E faz a filtragem e entrega. Existem clientes, que eles já têm esse sistema de flow interno e tudo e eles pedem para a nuvem deixar já: Olha, fica com todo o filtro ligado. Se eu anunciar para você, já entra com a mitigação total. Não precisa reanalisar os pacotes. Aí cada cliente tem a sua forma de contratar o serviço, né?

É basicamente assim que é feito a limpeza, né? É feita a análise dos dados, [ininteligível] dentro de equipamentos, cada equipamento tem seus algoritmos de filtragem, e passa para o cliente o tráfego limpo. Tem mais alguma pergunta?

SR. EDUARDO BARASAL MORALES: Oi, Kurt. Calma, as perguntas a gente vai deixar para o final.

SR. KURT URBAN: Ah, tá joia.

SR. EDUARDO BARASAL MORALES: Muito obrigado pela apresentação que você fez. Realmente, foi bem interessante. Até porque você já puxou gancho dos flows que o Klaus comentou.

SR. KURT URBAN: Pois é!

SR. EDUARDO BARASAL MORALES: E já falou do CPE, que vai ser a nossa próxima apresentação com a Lucimara.

Mas antes da gente chamar a Lucimara, eu queria dar uns avisos. A gente está gerando o certificado da live. Então, pessoal, vai ser colado agora no link lá, no chat, que é para você ganhar o certificado. Então, precisa se inscrever e depois precisa ficar atento no e-mail, porque vai ser enviado um link de confirmação de que você está assistindo. E esse e-mail, às vezes, está indo para caixa de spam. Então, dá uma olhada na sua caixa de spam para ver se você recebeu esse e-mail, para poder clicar no link e ganhar o certificado ali, no final da live.

Bom, vamos continuar aí as nossas apresentações. Eu vou chamar agora a Lucimara, né? Lucimara, existem muitos incidentes de segurança relacionados a roteadores domiciliares, né? Ou CPEs, como a gente já viu nas apresentações anteriores. Dizem que o motivo disso é devido a poucas medidas básicas de segurança implementadas no CPE, do próprio fabricante. Por isso eu gostaria de saber a sua opinião sobre o assunto, se existe algo que os fabricantes possam seguir como referência, ou então algum guia que alguém possa utilizar na hora de comprar um dispositivo, né? Um CPE. Então, fica à vontade.

SRA. LUCIMARA DESIDERÁ: Bom dia, pessoal! Só colocar aqui meus slides para... no share. Eu queria agradecer o convite e queria agradecer também às mais de mil pessoas que estão aí nos assistindo. Muito obrigada pela audiência.

Eduardo, está... entrou aí o meu share?

SR. EDUARDO BARASAL MORALES: Ainda não, estamos esperando.

SRA. LUCIMARA DESIDERÁ: Ainda não? Espera aí.

SR. EDUARDO BARASAL MORALES: Agora foi.

SRA. LUCIMARA DESIDERÁ: Agora foi? Então tá. Deixa só... stop aqui...

Muito bem. Então, vamos lá. Bom, bom dia a todos! E a pergunta foi a história dos CPEs e como comprar isso adequadamente. Eu vou, na verdade, começar contando um pouquinho de história sobre a BCOP de requisitos mínimos de segurança para aquisição de CPE. E eu vou começar contando um pouco do contexto da época que a gente começou a desenvolver essa especificação. Aliás, eu vou, na verdade, contar primeiro o que é uma BCOP, né? BCOP é uma Best Current Operational Practice, ou uma melhor prática operacional corrente, né? É um documento que basicamente, traz algum guia, uma tentativa de resolver um problema operacional no contexto dos operadores de rede. Então, o nome BCOP surgiu nesse contexto de operadores de rede.

Eu vou, então, falar um pouquinho da época que motivou a gente a desenvolver esse documento, essa boa prática. Em 2016, no final do ano de 2016, quando a gente estava começando a ideia de um grupo de antiabuso aqui na América Latina, foi quando surgiu, explodiu a Mirai. A Mirai, aquela botnet famosa, né? De dispositivos IoT usada para gerar ataques de negação de serviço. Então, esse gráfico mostra um retrato da época, né? Lá nos idos do dia 20 de setembro de 2016, quando teve um ataque gigante ao site [ininteligível] foi quando a Mirai veio a público. Até então, a gente sabia que existiam botnets de IoT, mas a Mirai foi a que trouxe um patamar diferente aí para história, né? Porque, afinal de contas, até então os ataques de negação de serviço chegavam lá aos seus 40, 50 gigabits por segundo. E aí a Mirai trouxe isso

para um outro patamar, que é para 600, né? Um terabit por segundo, e aí a coisa começou a ficar bastante complicada. Porque mitigar ataques deste patamar é muito difícil, né?

Mas aí a gente... Vou contando aqui um pouquinho da história, né? Dia 20 de setembro foi quando a gente tomou conhecimento efetivo do poder de fogo dessa botnet. Aí lá no dia 30 de setembro, aliás, quatro anos atrás, no dia de hoje, o código fonte da Mirai veio a público, né? Ele foi divulgado na Internet. E aí começou-se então a desenvolver uma série de variantes desse malware, dessa botnet para infectar outros tipos de dispositivos. Foi aí, então, que no dia 27 de novembro de 2016 teve o ataque famoso a Deutsche Telekom, né? Na verdade, foi um ataque genérico a dispositivos que tinha uma determinada vulnerabilidade no protocolo de gerenciamento de rede, lá do TR-069. E aí, isso infectou aproximadamente 1 milhão de dispositivos na Deutsche Telekom e infectou também outros dispositivos no mundo. Então, aqui no gráfico você vê essa linha azul, foram dispositivos infectados aqui na América Latina, dados dos nossos honeypots, né? E aí a Deutsche Telekom ficou fora do ar, por quê? Porque essa variante em particular, para os dispositivos CPEs deles, ela tinha um problema que ela derrubava. A tentativa dela de sair se propagando era tão intensa, que ela acabava derrubando o próprio CPE, né? Aliás, aqui, só para também deixar claro, CPE, a gente fala muito da sigla, sigla CPE, acho que muita gente está acostumada, mas só para deixar claro. CPE é o quê? É aquele dispositivozinho que a gente usa, que o operador usa para conectar o assinante à rede do provedor, né? Então são aí os modems, os routers, Wi-Fi, né? Esses são os dispositivos que a gente está falando.

E por que a Deutsche Telekom conseguiu se recuperar desse ataque, né? É um exemplo bastante interessante, porque a Deutsche Telekom tinha gerenciamento de rede pesado de seus dispositivos. Então, ela conseguiu, junto ao fornecedor dela, gerar um novo firmware, uma correção para o problema do firmware dela, né? No protocolo que estava com a vulnerabilidade, e ela conseguiu distribuir isso na rede dela. Em dois dias, ela estava operando novamente sem problemas, né? Então, isso é o quê? Isso é uma lição para gente.

O que eu tiro dessa história aqui que eu comecei a contar? Bom, IoT tem um problema sério de segurança, né? A Mirai, ela explorava um problema que é normal, é comum a todos os CPEs e à grande maioria dos CPEs e à grande maioria dos IoTs, que é, ela tinha... ela usava senhas fracas, né? Senhas que não eram... estavam hardcoded, né? Gravadas no código fonte do dispositivo, eram facilmente descobertas, era um conjunto de aproximadamente 60 senhas. Bastava o atacante tentar um Telnet na porta 23 usando aquela senha e ele ganhava acesso ao dispositivo, né? Então, o que a gente viu quando a Mirai veio à tona, né? Que segurança é negligenciada, né? Ela é negligenciada até nos próprios dispositivos de segurança, porque a Mirai, ela começou com câmeras de vídeo, câmeras web, gravadores de vídeo, né? E, com isso, os próprios dispositivos de segurança estavam inseguros. E que a gente vê também que... como falta pensar em segurança desde o projeto. O pessoal acha que a segurança é problema da equipe de segurança. E não é verdade, porque, por mais que exista uma equipe de segurança que tente tratar os problemas, tem coisas que a gente não consegue resolver. Não adianta que você não vai conseguir resolver um problema de uma senha gravada no código que dá acesso irrestrito ao seu dispositivo e você não consegue desativar, né?

Então, a gente vê aí que grande parte dos fabricantes ainda repete velhos erros, né? Então, o problema de autenticação falha ou inexistente é um deles. A gente vê muito senha padrão comum para todos os dispositivos, senhas gravadas em código, contas ocultas backdoor, a ideia... Ou ele criou esse backdoor para fazer um teste enquanto estava em desenvolvimento ainda do código, o firmware do dispositivo, ou então porque realmente, ah, ele quer... precisa... que ele quer dar manutenção naquele código

posteriormente, naquele device posteriormente, aí ele cria um backdoor que o fabricante não conta para ninguém. Ele não conta para ninguém, mas o lado negro da força descobre fácil, e aí eles vão usar isso contra a gente. Protocolos obsoletos, sem criptografia, né? O Telnet, a gente achava que tinha morrido há muito tempo e ele continua vivo aí nos atormentando. Serviços desnecessários ativados por padrão, então, a gente vê muito SNMP, SSDP, [ininteligível] essas coisas que não têm por que estar ativas e eles estão lá gerando... podendo ser abusados para gerar amplificação de negação de serviços, né?

Outro grande problema que a gente vê nos fabricantes de IoT e de dispositivos CPE é que a grande maioria deles não tem claro ainda... não possui um ciclo de vida de gerenciamento de updates e de suporte para esses dispositivos, ou não tem um mecanismo correto de bug report. Então, a gente teve um problema o ano passado com um fabricante bastante... é um fabricante do exterior, mas que é muito utilizado aqui no Brasil. E como eles não tinham um mecanismo, um processo de fazer bug report, eles recebiam os bug reports dentro da própria lista de discussão do fabricante, com todo mundo envolvido. Aí um certo pesquisador descobriu um problema na rede... no dispositivo, tentou notificá-los, e eles negavam na lista: "Não, isso não é problema. Isso é problema do protocolo". Não, não é problema do protocolo. O protocolo não estabelece certos limites, mas na implementação você tem que limitar, porque recursos da implementação não são irrestritos. Eu sei que chegou num ponto de discussão lá no chat que o próprio fabricante revelou como que se explorava o bug. Ou seja, ele fez full disclosure do problema, de como atacar, sem antes criar uma solução para aquele problema, né?

Então, existe uma falta de maturidade grande ainda, da indústria em pensar como resolver esses bugs de segurança, porque eles vão existir sempre. A gente está falando de uma indústria de hardware, né? Dispositivos IoT, CPEs e tudo mais. Mas, na verdade, o que rola dentro desse hardware é software, né? O firmware é um software, que é desenvolvido por pessoas e vai ter bug, vai ter que ser corrigido. Então, a indústria precisa pensar em mecanismos corretos de fazer bug report, de fazer distribuição de updates. Não é simplesmente deploy and forget, né? Instala e esquece. Isso poderia ser que acontecesse no passado, quando a gente tinha os dispositivos totalmente isolados no cantinho deles. Mas a partir do momento que você joga um dispositivo numa rede como a Internet, ele está aberto a ser atacado por todo mundo que está na rede, né? Então, não dá para achar, não dá para ser mais inocente, e achar que: Ah, eu não preciso criar mecanismos de segurança de autenticação, porque o meu device está isoladinho. Meu device não está mais isoladinho e ele precisa de atualizações.

E outra coisa que falta também na indústria são políticas claras de como isso é tratado, né? A gente vê da época... na indústria de software, isso evoluiu, né? Então, evoluiu já, a gente vê fabricantes que passaram a dizer: Olha, eu vou dar suporte nos meus produtos por X anos, né? Com X anos eu paro de dar atualizações genéricas, mas eu continuo dando atualizações de segurança. Então, isso precisa ficar claro também para os dispositivos, né? Qual é a política de atualização de segurança que você vai ter naqueles devices.

E aí, por que a gente tem que se preocupar com segurança de CPE, né? Aí falando para os ISPs. Que a gente vê que existe muito esse pacto operacional de negócio para esses operadores, para esses provedores de acesso. Então, assim, a partir do momento, que um malware como o Mirai ataca a sua rede e toma conta do seu dispositivo, você está [ininteligível] a sua rede comprometida, alguém está abusando dos seus recursos, o seu recurso está sendo utilizado por um terceiro para o benefício dele. Então, ele vai estar gerando dinheiro com ataque de negação de serviço, que eles vendem isso como serviço, né? E quem está pagando o recurso é você. Está pagando com o seu device e pagando com o seu uplink, né? Eu me lembro que na época que a gente estava discutindo documento na fase inicial, a gente... Eu, conversando com pessoas, com provedores e consultores da área, eles me diziam o seguinte: "Lucimara, eu instalo um

dispositivo na rede, não dá 15 minutos, ele não é mais meu, né? Alguém já tomou conta dele e está usando ele para alguma outra coisa". Então, esse é um problema que é o seu recurso que está sendo usado de forma indevida.

Aí você tem o que quando o seu dispositivo da sua rede está sendo usado de maneira inadequada, né? Você tem degradação. Você tem indisponibilidade do seu próprio serviço, e aí o teu cliente vai ficar insatisfeito e vai querer procurar um outro, né? Ou então vai te dar um outro problema que é o suporte técnico, né? Ele vai começar a te ligar: Olha, a minha rede está lenta, a minha conexão à Internet está ruim. E aí você vai ter que ter o trabalho de ficar falando com ele no telefone, você vai ter que ter pessoas para dar suporte técnico, em alguns casos, você vai ser obrigado a deslocar um técnico para a casa do usuário para trocar o equipamento dele, né? Eu me lembro de um dos casos que também que nos contaram, que era assim, quando a Mirai, a variante para CPE ganhou aí o mundo, e foi afetado também provedores aqui no Brasil, eles falaram: "Lucimara, a gente teve que montar uma loja e pedir para os nossos clientes virem trocar os CPEs deles na nossa loja, porque a gente não tinha como mandar um técnico na casa de cada uma das pessoas para trocar os dispositivos". Então, isso é dinheiro também que se perde, né? Recurso que você vai ter que desperdiçar para tratar problema que pode melhorar, né?

Aí tem também o problema de reputação, reputação sua com seus clientes e sua com os seus parceiros, né? Porque se dentro da tua rede o teu CPE está gerando tráfego espúrio para atacar a rede de outra pessoa, e você faz, por exemplo, um peering com alguém, o seu tráfego espúrio vai passar pelo peering. Aí o teu parceiro vai começar a ficar bravo com você: poxa, você está consumindo o meu uplink, você está consumindo a minha banda com tráfego espúrio. Além do que também você pode começar a cair em listas negras, né? Os blacklists XP. E aí os seus IPs vão começar a ficar comprometidos, e você vai perder capacidade de utilizar seus recursos de IPs.

E aí, como diz o velho ditado também: "É melhor prevenir do que remediar". Mitigar DDoS é muito custoso, é muito pesado você ter que tratar lá no final, quando tem aquela avalanche de pacotes e de tráfego, como o Kurt nos explicou. Precisa de equipamento específico, precisa de pessoas especializadas para tratar aquele tráfego. E aí, se você conseguir limpar a tua rede e evitar que o tráfego malicioso saia dela, você vai estar evitando que o tráfego chegue no destino. Então, tratar o tráfego, evitar que ele saia da rede, é mais... é melhor do que você simplesmente deixar para tratar uma negação de serviço lá no final.

E aí, o que, então, a gente tem que pedir para os fabricantes, para a indústria, para nos trazerem, para melhorar a nossa vida? Bom, tem que pedir que segurança deve ser por projeto e por padrão. By design, by default. Ela não pode ser opcional, ela não pode ser uma coisa "ah, lá na frente a gente resolve o que vai acontecer". Não, ela tem que ser pensada desde o início do projeto, do desenvolvimento desse projeto. Tem que ser pensada com boas práticas de desenvolvimento de software seguro, né? Aí eu aproveito para falar aos nossos professores e alunos que estão aí assistindo a nossa live, né? Por favor, pensem no contexto aí das aulas de vocês, desenvolvimento seguro de software, né? E é preciso também que a gente tenha configurações padrão de fábrica seguras, né? As configurações, elas precisam ser restritivas ao invés de permissivas. Não pode vir com serviços abertos que você não usa, e principalmente ativar o antisspoofing por padrão. Como eu falei, a antisspoofing, que é você filtrar tráfego que não é legítimo da tua rede, tráfego que tem um IP de origem falsificado. Quanto mais próximo da origem do tráfego você implementar esse tipo de medida de filtragem, melhor é. Quanto mais dentro do core da rede, mais complicada e mais complexa é você fazer esse tipo de filtragem. Então, o CPE é o local ideal para você ativar esse tipo de filtragem, é matar o problema na origem, não deixar nem que ele se propague, né?

Outra coisa que a gente precisa e que é muito importante a gente ter, lembrando o caso da Deutsche Telekom, mecanismos de update de gerenciamento remoto, né? Tem que ser possível fazer esse tipo de coisa e tem que ser seguro, porque senão você acaba gerando um problema ainda maior que é o teu canal de update, o teu canal de administração virar um mecanismo também de ataque, né? E é preciso pensar que tem que planejar para fazer update em larga escala. Então, você vê, Deutsche Telekom tinha quase 1 milhão de dispositivos, e você tem fabricantes que têm dispositivos espalhados pelo mundo todo. Então, é preciso pensar que o produto atende em larga escala e o update precisa ser feito em larga escala, né? E, idealmente, a gente pedir que os fornecedores tenham aí um grupo de resposta a incidentes de segurança em produtos, o que a gente chama de Psirt, né? Isso tem muito relacionado com a maturidade desses fabricantes, né?

Então, isso é o que... esses são tópicos que a gente tratou bastante na BCOP, né? Na boa prática. A BCOP, ela é o quê? Um documento de requisitos mínimos. A gente não aborda tudo lá, 100% dos problemas. A gente tentou pegar aqueles problemas que são mais iminentes, mais visíveis e mais básicos e que estão acontecendo em larga escala e geram bastante problema. Então, tem lá... é uma listinha, inclusive, um checklist mesmo, que vocês podem usar para fazer a compra do dispositivo. Esse trabalho foi desenvolvido dentro do LAC-Aawg, que é o grupo da América Latina e Caribe... Latin American and Caribbean Anti-Abuse Working Group. Surgiu numa parceria com a NOG(F), né? Que é um grupo já bastante estabelecido há muito tempo nos Estados Unidos e propagou pelo mundo. Ela traz aí a indústria para... de diversas áreas para combater abusos, em rede, em mensagens, em mobile. E surgiu uma parceria e a gente criou, né? Nasceu assim o LAC-Aawg. E esse documento foi desenvolvido numa parceria, né? Um trabalho conjunto do Lacnog aqui na América Latina, com a NOG(F) lá nos Estados Unidos. E aí o documento nasceu originalmente em inglês para atingir o mercado como um todo global. Está traduzido já, para japonês, para coreano e para português. Vocês têm os links aí. O pessoal acho que também deve ter colocado links lá na live. Desculpa, no YouTube.

E, enfim, explorem o documento, deem uma olhada. A ideia é que se sigam esses requisitos para conseguir fazer uma compra adequada de equipamento. Porque uma vez que você tenha equipamentos adequados na sua rede, você vai sofrer menos com problemas de gerenciamento, com problemas de tráfego espúrio dentro da tua rede. E uma vez que a gente tem equipamentos adequados, fica mais simples, você evita problemas futuros. A ideia é tentar evitar problemas.

Enfim, é isso que eu tinha para dizer. Estou aberta a perguntas e vou passar para nosso moderador aí, obrigada, Eduardo, obrigada, Moreiras.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Lucimara. Muito interessante a apresentação. Documento aí muito importante.

Bom, agora, eu acho que chegou a hora que muita gente estava esperando, né? Que é a hora que o delegado Alesandro vai falar. E sem desmerecer os demais participantes, né? Porque... mas o pessoal, os demais participantes são da casa, estão falando de temas técnicos, e o delegado é o nosso convidado de honra aqui nessa live. Acho que tem muita gente curiosa para saber como é que foi essa operação, tal. Eu acho que é a hora de vocês que estão assistindo a live aí reforçarem o convite no grupo do WhatsApp, no grupo do Telegram: Ó, pessoal, o delegado vai falar agora. Vai contar daquela operação lá que prenderam aqueles hackers. Onde, na verdade, quem foram os guerreiros aí foi o pessoal da polícia, né? Não foi quem foi preso que foi o guerreiro. O guerreiro foi o delegado Alesandro e todo o pessoal que fez essa operação e concluiu essa operação com sucesso.

Mas, antes de passar a palavra para o delegado, eu quero reforçar que os materiais de quem preparou slides, do Klaus, da Cris, da Lucimara, estão na página do evento. Vocês podem entrar lá na agenda. "Ah, não está. Acabei de entrar". Dá um refresh. Está lá, sim. Os materiais estão lá.

Pessoal está meio preocupado também em relação aos sorteios, a gente confirmou com o pessoal do 4Linux, eles estão recebendo os dados, está tudo certinho, o pessoal da Eletronet também, o pessoal da NetfindersBrasil também, e quem vai fazer o sorteio somos nós, agora no final da live. Então, fiquem despreocupados. Tem sorteio de verdade, tem prêmio de verdade, e o sorteio é feito ainda durante a live aqui. O Eduardo é quem vai fazer o sorteio no finalzinho.

E, antes, última coisa antes de passar a palavra para o delegado: estamos com mais de mil pessoas assistindo essa live, o que é muito legal. Agradeço muito, muito a audiência de vocês. Mas temos só 700 likes, né, gente? Vamos dar uma reforçada aí. Vamos dar aquele joinha no vídeo para que o YouTube distribua esse conteúdo para muito mais gente. Vocês não estão gostando do conteúdo? Fala a verdade. Conteúdo está muito bom. Então, dá o like para o YouTube distribuir isso para mais gente, para o conteúdo chegar em mais gente. Tá bom?

Então, agora, delegado Alesandro. Primeiramente, a gente quer parabenizar a você e toda a ação da polícia pela Operação Attack Mestre. Os criminosos que eram envolvidos nisso estavam dando prejuízo há muito tempo para muitos provedores de Internet, consequentemente, para os usuários finais também, que ficavam sem o serviço. E a gente está bastante curioso para saber um pouquinho sobre a operação, sobre seus resultados. Além disso, é importante ter em mente que muitas vezes o pessoal dos provedores, quando está sob ataque, não sabe o que fazer. Os outros painelistas aqui já falaram do que o pessoal tem que fazer do ponto de vista técnico, né? Como ele mitiga o ataque, como ele detecta o ataque, como ele consegue limpar o tráfego, como ele consegue comparar equipamentos que evitam que esses ataques aconteçam de forma geral. Mas em relação aos criminosos, o que dá para fazer? O provedor abre um Boletim de Ocorrência? Tem uma delegacia específica? Ele tem que levar alguma evidência? Um e-mail, log? Isso vale? Ele precisa de um advogado para fazer o processo andar? Como que funciona isso tudo?

Então, passo a palavra para o senhor, já agradecendo novamente a sua presença aqui na live.

SR. ALESANDRO GONÇALVES BARRETO: Bom dia, Moreiras, bom dia, Eduardo. Parabéns a todos aí pela organização do evento. Muito obrigado a todos que estão assistindo. Realmente, um alcance grande. O nível dos palestrantes aí que falaram anteriormente aumenta mais o brilhantíssimo do evento. E venho aqui apenas colaborar um pouco com o evento.

Bom, eu sou delegado da Polícia Civil do Piauí. Atualmente me encontro no Laboratório de Operações Cibernéticas do Ministério da Justiça e Segurança Pública. O que nós fazemos aqui? A gente dá suporte aos outros estados, principalmente na... chamo isso de uma arte, na arte de buscar a evidência no ciberespaço quando se deparar diante de crimes cometidos. E a gente dá apoio aqui a diversos cenários. Posso falar de Operações Luz na Infância, ela teve seis fases já, com participação de oito países. Tivemos uma recente, que foi a Operação Data Broker. Os criminosos, eles se utilizavam de dados de consumidores que eram ofertados ilegalmente na Internet, criavam perfis fakes e terminavam por aplicar um golpe milionário. A busca e apreensão que foi realizada dentro do presídio do Goiás pela Polícia Civil do Goiás resultou em R$ 500 mil. Então, estou mostrando que o cibercrime é bastante lucrativo, e a polícia precisa tomar alguns encaminhamentos.

E o que a gente tem visto é que as Polícias Judiciárias, nos últimos anos, elas têm evoluído bastante nesse cenário. Vai no Google e coloca: Operação Internet. Vai ver uma gama de operações que foram realizadas até então. E nesse contexto se destaca a Operação Attack Mestre. Ela... nós, aqui do ministério, apenas demos o apoio, conseguimos integrar operação com a Polícia Civil do Tocantins e a Polícia Civil do Goiás. E os criminosos, dois particularmente, estão presos, tá? Um foi preso no interior de São Paulo, desde então se encontra preso. O outro, o guerreiro, que não tinha nada de guerreiro, ele foi preso ontem novamente. Então se encontra preso por prisão preventiva. E esses criminosos estavam causando problema com diversos provedores no país, certo? Então, utilizavam celulares habilitados em SIM card internacional, exigiam o pagamento em criptomoeda e, até então, algo impossível e não realizado pelas Polícias Judiciárias. Então, a Operação Attack Mestre, ela se destaca por esse pioneirismo, de mostrar que é possível fazer, é possível buscar autoria e materialidade, independente do crime praticado. Então, asseguro a vocês: não vai acabar, mas pelo menos vai amenizar um pouco, tá? A gente conseguiu mitigar um pouco o problema e chamar a atenção para o problema, [ininteligível] está vendo.

O que eu vi nas palestras anteriores, eu sou um forte defensor, prevenção. Acho que prevenção é o grande remédio para tudo isso. Ainda há a cultura que segurança, investir... que segurança é gasto. E não. Segurança é investimento, tá? Quando você faz investimento em segurança, você consegue mitigar uma boa parte desse problema. E como até a palestrante anterior falou, se você vai fazer depois, os gastos são enormes. Mas vamos trazer aqui para questão da Operação Attack Mestre. Ela mostrou que o problema ocorreu, só que nós temos inquéritos tramitando no Goiás e no Tocantins. Eu tenho certeza absoluta que todos os estados foram vitimados. Precisa que as vítimas procurem a delegacia de polícia. Há uma crença que: "Ah, eu tenho que procurar a Polícia Federal?". A Polícia Federal, ela tem uma expertise já na área, mas ela tem um nicho de crimes que ela vai investigar, certo? No caso desses crimes, eles são de atribuição das Polícias Judiciárias estaduais. Então, procure a delegacia, registre a ocorrência. Só que o Boletim de Ocorrência por si só não traz tanto efeito, há a necessidade de instaurar um inquérito policial, tá?

Então, como que o inquérito, ele é instaurado? Tem diversas maneiras, por portaria, por representação. Se a sua empresa tem um advogado, faz uma representação criminal e encaminha para o delegado de polícia contando o que houve: "Ó, a minha empresa foi vítima de ataque há tanto tempo, nós registramos a ocorrência, o número do boletim é esse". A pessoa que atacou, ela usava o codinome, vamos lá, guerreiro. Esse indivíduo foi preso pela Polícia Civil de Tocantins e do Goiás, lá se encontra inquérito tramitando, solicite empréstimo... prova emprestada. Para quê? Para que ele também seja indiciado para o que ele cometeu contra você, tá? Então, quanto mais processos ele responde, quanto mais inquéritos vão responder que vão resultar em processo, mais difícil vai ficar situação deles. Então, vão sair condenações, e se causaram um prejuízo terrível a vocês, precisam responder criminalmente.

O que é um detalhe também, a gente precisa reforçar: quando o provedor for vítima de ataque, quais dados são interessantes para a polícia? Primeiro, exigiu pagamento? Quando? Como que é esse pagamento? Depósito em conta bancária? A carteira de criptomoedas, certo? Qual foi o número que manteve contato, tá? Qual foi o número que manteve contato? Como que foi o contato? Houve algum contato por e-mail? Houve algum contato via rede social? Essas informações são de extrema relevância. E um outro aspecto também, assim, cuidado com print de tela, tá? Captura de tela, ela não serve muito não. Se tem alguma situação que você consegue ver no... que está na... foi publicada, por exemplo, numa rede social, ou em alguma página, use ferramentas, como, por exemplo, HTTrack, para fazer o salvamento desse conteúdo. É importante que haja salvamento de logs, etc. Então, quando você tem essas informações, elas são relevantes. De dia e hora que ocorreu o fato, quem tomou conhecimento do fato. Volto a repetir, as contas bancárias, e lembrem-se de preservar o conteúdo, tá?

Um outro questionamento que vocês podem fazer: mas qual a delegacia que eu procuro? Se na sua cidade tiver uma delegacia de repressão a crimes cibernéticos, eu recomendo que procure, por quê? Porque é um tipo... é um crime informático próprio, tá? Então, exige especialização dos policiais que vão investigar o fato. "Alesandro, mas eu moro no interior de tal estado". Procure a delegacia mais próxima da sua residência. A polícia vai olhar: ó, nunca investiguei isso. Delegado, tramitou um inquérito na delegacia de Palmas. Mantenha contato lá que ele vai passar todas as informações e... como que posso falar? Vai ter as condições necessárias para haver o indiciamento e iniciar uma persecução criminal contra esse indivíduo.

Mais um detalhe, é importante, eu preciso enfatizar isso novamente: investimento em segurança da informação, tá? Sempre quando a gente atua aqui em diversos cenários, a gente sempre reforça o caráter da prevenção. Em várias ações que atuamos aqui contra abuso, exploração sexual infanto-juvenil, nós sempre reforçamos o quanto é importante o trabalho preventivo. Trago esse cenário também para os provedores. Tem que haver esse investimento, tem que haver prevenção. Se você previne, se você está atento, muitos ataques vão ser mitigados e você vai garantir a continuidade do negócio. Não vai ter interrupção e fica tudo mais fácil de lidar.

E, por fim, é importante essa aproximação com as Polícias Judiciárias. As Polícias Judiciárias estão avançando, tá? Attack Mestre, volto a repetir, o pioneirismo. Como falou Moreiras: de fato, essa operação teve vários guerreiros, tá? Mas são guerreiros da Polícia Judiciária, que abdicaram de dias, de noites e de finais de semana para indicar quem cometeu esses... quem praticou esses fatos. Então, estou à disposição para eventuais questionamentos.

SR. EDUARDO BARASAL MORALES: Bom, muito obrigado, delegado. Realmente, foi muito boa toda a sua explicação e foi bem clara, falando das ferramentas ali de que as pessoas podem utilizar para guardar informações e, depois, apresentar num inquérito jurídico, para apresentar para a polícia.

Bom. Agora a gente terminou a parte ali das apresentações iniciais, a gente vai para a parte de perguntas. Só que antes da parte de perguntas, pessoal, eu gostaria ali de reforçar algumas coisas. Uma delas é o formulário de avaliação. Então, agora a gente vai colocar um QR Code aí na tela, vai colocar o link no chat para vocês preencherem o formulário de avaliação. Formulário de avaliação é bem simples, são duas perguntinhas, para você dar ali uma notinha de 0 a 10 do que você está achando da live até agora e a outra para escrever algum comentário. Então, se você quiser falar que gostou da live, que a gente deve fazer mais lives, ou então alguma coisa que você não gostou, o que a gente pode melhorar, a gente aceita sugestões. Então, a gente pede encarecidamente para que vocês coloquem a sua opinião no nosso formulário de avaliação, tá? Então, está aparecendo aí o QR Code, preencham ele, ele é bem simples ali, duas perguntinhas.

Em paralelo, eu vou pedir aqui para a equipe de comunicação já colocar também os links, novamente, dos sorteios. Então, se você quiser participar do sorteio, serão feitos sorteios durante essa live, no final a gente vai sortear. Vai ser uma da Eletronet, que são 200 reais em voucher da Americanas.com, uma da NetfindersBrasil, que vai ser um curso de BGP EAD para você poder assistir e um curso da 4Linux à escolha do ganhador. Então, são esses três sorteios, são três links diferentes. Não adianta se inscrever em um e achar que vai ganhar no outro, não é, são empresas diferentes. Eles vão passar para a gente fazer o sorteio no final da live, tá?

Então, esses são os avisos relacionados ao sorteio. Tem também o aviso do certificado, que muita gente está colocando no chat. Então, a live, ela dá certificado. Você precisa se inscrever no link que o pessoal está colocando aí no chat e, depois, confirmar no link enviado por e-mail. Então, dá uma olhada ali na caixa de

spam, se não está ali na sua lixeira, em alguma caixa... lembra até o e-mail que você cadastrou. Porque às vezes você cadastrou o e-mail que você usa diferente do corriqueiramente. Preste atenção nisso para poder clicar no link certo. Então, aí você vai conseguir o certificado.

Outra pergunta que o pessoal tem feito muito aí no chat, que a gente tem visto, é se essa live vai estar gravada. Vai, vai estar gravada, vocês podem assistir depois. Então, vai estar aí o link, depois o pessoal vai escrever no chat. Então, não precisa... se você perdeu alguma parte, você pode assistir depois, tá? Sem nenhum problema.

Mas, terminado aí os avisos, eu vou colocar agora a pergunta para a Cris, que veio aí do Renan Menezes e do Marlon Boeck(F): "Como fazer para relatar os Scams que estamos sofrendo?". E também: "Como reportar sites de phishing se passando por e-commerce famosos?". Então, gostaria que você pudesse comentar um pouquinho, Cris.

SRA. CRISTINE HOEPERS: Perfeito, Eduardo. Eu vou, até considerando o tema, vou fazer um hijacking de tela aqui um pouquinho, porque eu acho que vai ser mais fácil eu responder comentando aqui.

Notificação de incidentes, eu acho que tudo depende do tipo de incidente, né? E como tinha... como comentaram dois, tanto Scam quanto o outro, a gente tem um documento que foi escrito por nós aqui do Cert, que está lá no site do BCP, NIC.br, que é o portal de boas práticas, você vai aqui em boas práticas, "notificação de incidentes". Por que eu puxei isso aqui? Porque eu acho que é interessante pensar que depende para quem você vai notificar o que é incidente que você está notificando. Então, essa parte do a quem notificar, uma das coisas que a gente fala assim: Ah, pode ser o Scam de rede, pode ser um phishing. E aí o phishing depende, né? Depende. Ele é um phishing que está hospedado num site que foi comprometido ou ele é um phishing que o atacante está contratando um serviço e está colocando no ar? Quando ele põe no serviço, às vezes, ele cria domínio, ele não cria? Então, tudo vai depender o que você está fazendo.

A parte da Scam, acho que a parte importante de relatar é para o dono do IP ou para o dono do AS. E por quê? Porque provavelmente aquele é um ativo de rede, ele é um servidor, ele é alguma coisa que está invadida e que está gerando ataques, e você vai estar não só reduzindo esses ataques, mas ajudando aquela rede a se recuperar. A gente sempre recomenda copiar cert@cert.br, porque a gente vai tendo uma noção do que está acontecendo, a gente pode, às vezes, saber um contato melhor. A gente pode ajudar essa notificação, né?

A parte de phishing, a gente também sempre recomenda: não adianta muito você... quando é um domínio que foi criado para fazer o phishing. Imagina que o cara registrou Americaanas.com. Não adianta você reportar para Americaanas.com. Você vai ter que reportar para onde estava hospedado. Então, você vai ter que achar qual era o AS, onde estava hospedado, mandar o link certinho, né? Porque tem muita gente que às vezes fala: Ah, tem um phishing no seu site. Imagina você reportando isso para uma empresa de hosting, algum provedor. Mas tem aonde? E a gente tem umas modificações que às vezes são assim, elas são incompletas, né? Se você está reportando um Scam, tem que mandar o log, tem que ter um time stamp, quem está do outro lado precisa saber exatamente o que eu estou notificando.

Então, esse aqui, ele tem dicas de como buscar os contatos, o whois, como achar o CSIRT, como fazer para achar isso aí. E, para quem quiser também mais detalhes, a gente tem aqui modelos de notificação. Você pode baixar. A gente tem em zip, em português e em inglês. Então, se vocês quiserem reclamar para alguém de outro país que está fazendo isso, ou reclamar de phishing que está hospedado em outro país, a

gente tem os textos aqui. Então, por exemplo, se você for olhar, que é o que a gente fala aqui, que é ataques à rede em geral, que em geral é para Scam, força bruta, tal. A gente tem um arquivinho em português, já com o texto aqui, e a gente tem o texto também em inglês, para facilitar a notificação. A mesma coisa acontece para phishing e para ataques de DDoS com botnet.

Qual é a ideia dessas notificações? É a gente ajudar a limpar rede, né? Nenhuma dessas notificações aqui, ela vai ser direcionada, do ponto de vista ou legal, ou do ponto de vista de prender alguém, ou alguma coisa assim. Elas são realmente para ajudar as redes que estão comprometidas e que não sabem que estão comprometidas, para que esses administradores possam aplicar suas políticas, identificar máquinas com problema, botnets, né? Então, nesse documento a gente reuniu vários tipos, né? Como a gente comentou, você tem aqui modelos para download, são arquivos zip, todos templates em português e inglês, para cada um deles, para poder integrar ferramentas que vocês tiverem, tá? E quem tiver dúvidas e quiser entrar em contato com a gente lá no Cert, a gente pode tentar ajudar vocês também.

Então, espero que isso ajude a parte técnica, como que a gente faz para notificar, e sempre copiem a gente lá. Mas vou lá mandem na cópia mesmo. Não mandem dois e-mails. Porque é importante o cert@cert.br estar na cópia. O to do e-mail lá, o para é a rede, o contato de whois, e o CC a gente, porque aí a gente sabe quem foi notificado e a gente pode ajudar a achar contatos melhores, a gente pode ter noção de ataques novos que estão aparecendo, a gente pode contatar uma rede que está começando a gerar muito ataque e perguntar se ela precisa de ajuda, né? Então, assim, essas são coisas aí importantes. Era o meu comentário sobre isso.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Cris. Realmente, acho que esses templates ajudam bastante, até porque a gente tem muita gente com dificuldade em língua, né? Inglês. E deixa tudo já bem definidinho, fica bem fácil para a pessoa notificar.

Delegado, você gostaria de complementar essa pergunta? Acho que o CERT.br não tem uma ação de polícia, né? Então, eles dão as notificações, dão uma ajuda e todo esse auxílio, auxílio técnico, mas não é uma polícia. Você pode complementar?

SR. ALESANDRO GONÇALVES BARRETO: Ok, Eduardo. Acho que a Cristine foi bem específica já. A importância da notificação. Eu só vou puxar um pouquinho mais o que pode ser complementado também. Algumas redes sociais, e as mais utilizadas, Facebook, Instagram, Twitter, etc., eles têm também canais para reportar irregularidades, certo? A gente tem visto muito, em vários golpes, o criminoso hospeda uma página falsa e vai publicar ela no Facebook, por exemplo. Então, as plataformas, elas têm os canais para que alguém que foi prejudicado, ou que possa ser vítima, ou foi vítima, possa utilizar esse canal para também denunciar e remover a página lá dentro. A gente tem visto, bota, hospeda um phishing e vai lá no Facebook, uma boa engenharia social, cria uma página parecida com a instituição financeira, para trazer as vítimas e direcionar para a página dele. Então, utiliza também esses canais, que eles são importantes para deixar a rede mais limpa. Então a denúncia, a notificação é muito importante.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, delegado.

E eu gostaria de fazer agora uma pergunta direcionada para o Klaus sobre flows. Uma mistura, na verdade, de perguntas que vieram aí no chat. Klaus, qual é o melhor momento para se implantar o Netflow? É quando o provedor já está sob ataque ou isso dá para ser feito em momento diferente? Funciona tanto com IPv4 como com IPv6? Tem alguma preferência? Algum protocolo que funciona melhor? E a gente

pode usar os findings dos flows para gerar regras automáticas e fazer mitigação do ataque de alguma forma? Como funciona isso? Por favor.

SR. KLAUS STEDING-JESSEN: Moreiras, são ótimas perguntas, tá? Começando, então, pela primeira. Essa questão de qual é o melhor momento, tá? Melhor momento é agora, pessoal, tá? Assim, não deixe isso para o momento do ataque. Isso é que nem log de servidor. "Ah, estou sendo hackeado, deixa eu agora habilitar o log". Tarde demais, né? Então, isso cai naquela categoria de lição de casa, você já tem que ter isso. Você tem que já ter uma rede instrumentada, para que no momento da necessidade aí você tenha esse recurso, tá? Até porque, pessoal, algumas coisas, dependendo do equipamento que você tem e do tráfego, você vai requerer um certo find turning(F), tá? Assim, o que eu quero dizer com isso? Vários protocolos de Netflow você vai ter que configurar sampling. Eu não vou conseguir fazer um para um, porque eu tenho um limite que a caixa suporta. Então, tem várias coisas que vão demandar uma certa experimentação para a sua rede, tá? Uma vez que isso entra em regime, isso aí funciona tranquilo, você vai esquecer que tem Netflow, até que um dia você vai precisar. Então, isso já tem que estar rodando, vamos dizer, de maneira tranquila, e não no momento do ataque. No momento do ataque é o pior momento possível. Você está sob estresse, né? Sua rede está sob estresse, tentando resolver o negócio, você vai colocar mais uma variável na sua rede, que é uma configuração nova de equipamentos, tá? Essa não é hora de fazer isso aí.

Falando sobre IPv4 e IPv6, sim, os Netflows mais modernos têm suporte para os dois, a não ser que você tenha um Cisco velho com Netflow V5, que só tinha suporte para V4. Mas, digo assim, equipamentos relativamente mais novos têm suporte para os dois, sem problema nenhum, tá? Muitas vezes a escolha, obviamente, vai depender do que você tem de equipamento, tá? Então, assim, por isso que a gente botou os links no final lá: como é a documentação para Juniper, Cisco, MikroTik, lembrando que hoje em dia tem firewalls, por exemplo, e appliances que também geram. Então, a recomendação é: dá uma olhada no manual do seu fabricante e dá uma olhada, mas se for relativamente recente, sim, vai ter suporte para IPv4 e IPv6.

Respondendo a última pergunta, Moreiras, então, a questão de se dá para fazer regras automatizadas e tomar ações automatizadas. Sem dúvida, dá. Mas acho que aí entra aquela história, como tudo na vida, a gente tem que pensar que tem prós e tem contras, né? Sim, tomar uma ação automatizada é rápido, certamente, mais rápido do que um humano ir lá e começar a fazer regras e aplicar filtros, ou aplicar no routing para isso ou para aquilo. Então, sim, tem esse benefício que você reage rapidamente. A desvantagem é que tem um grande potencial de dar um tiro no próprio pé. Então, assim, se isso realmente não for malicioso, e dependendo do que é essa sua contramedida, você pode, vamos dizer, a ação pode ser pior do que o ataque, né? "Ah, automaticamente faço no routing de metade dos meus clientes". Então, você basicamente efetivou o ataque, esses caras não falam mais com a Internet. "Ah, eu bloqueio tal coisa". Então, a minha recomendação seria, sim, tem um grande potencial para automatizar coisas, né? Mas eu gastaria um tempo, pega uma pessoa para entender bem esses padrões de ataque antes de automatizar coisas, tá? Acho que isso seria o melhor dos dois mundos aí.

Então, basicamente seria isso daí, Moreiras, para essas minhas perguntas.

SR. EDUARDO BARASAL MORALES: Obrigado, Klaus. Realmente foi esclarecedor.

Bom, vamos seguir aí com as perguntas. Eu tenho uma pergunta agora do Fábio Aquino e do Silvio Rangel, que elas são muito parecidas, e eu vou fazer para o Kurt. Os serviços de limpeza ou o filtro na nuvem não geram uma maior latência na minha rede, considerando que eu não tenho problemas, no caso? Porque se

eu tiver problemas com ataques DDoS, é lógico que vai ter ali a limpeza e vai gerar uma latência. Então, tipo, passar todo o tráfego enquanto eu não estou recebendo ataque e a limpeza de tráfego não gera lentidão nos roteadores, nos dispositivos meio? Então, essas são dúvidas do Fábio Aquino e do Silvio Rangel. Então, Kurt, fique à vontade.

SR. KURT URBAN: Beleza. É, a mitigação em nuvem vai depender muito do provedor que vai fazer essa mitigação. Comparar um sistema de mitigação hospedado todo no exterior, na hora que tiver um ataque e o cliente jogar todo o tráfego para a nuvem, todo o tráfego vai ter de ir para o exterior. Então, mesmo que o cliente esteja... o acesso à rede desse cliente seja feito do Brasil, ele seria roteado pelo exterior. Então, lógico que a latência ia aumentar. Qualquer equipamento que estiver no meio do caminho vai gerar um aumento na latência mesmo. Mas, então, colocar nuvem de mitigação com a presença nacional já reduz bastante a latência por não precisar mandar tráfego para o exterior, né? Outra coisa é que geralmente as nuvens de mitigação, elas têm vários uplinks, vários pontos de conectividade. E a inteligência da mitigação, se ela consegue detectar que, vamos supor, um ataque para um cliente específico está vindo muito da Ásia, da Europa, alguma coisa assim, ele consegue colocar aquele link específico, aquele uplink passando pela mitigação, mas num tráfego, um exemplo, vindo do IX não, que não geraria esse ataque. Então, o tráfego que vem pelo IX não sofreria com esse desvio para os equipamentos de mitigação e não geraria esse aumento de latência considerável. Lógico que o tráfego que está vindo da rede, que está gerando esse ataque, né? Como vai ter de passar pelas ferramentas e também vai depender muito do tipo de ataque. Tem ataques que são bem mais complexos, né? E aí geraria uma análise bem maior dos pacotes, gera, lógico que tem um aumento de latência, né? Mas é uma coisa que a gente não pode garantir que sempre vai gerar um aumento considerável. Vai depender muito do tipo de ataque.

Agora, sobre impactar os equipamentos de rede. Quando usa o sistema de mitigação em nuvem, o tráfego já chega bem mais limpo para a rede de destino, né? Então, equipamentos que sofrem muito com problema de processamento de pacotes por segundo não vão receber aquela volumetria de pacotes. Então, eles não vão sofrer tanto com esse ataque, né? No caso da mitigação em nuvem. E no caso dos provedores de mitigação, eles têm os equipamentos todos divididos e redundantes, tal, para poder suportar essa volumetria inicial. Então, a parte de sobrecarregar os equipamentos de rede não tem tanto problema, não.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Kurt.

Eu gostaria de direcionar agora a próxima pergunta para a Lucimara. Na verdade, são duas perguntas aqui em uma que eu vou fazer. Tem uma dúvida, que é a seguinte: como que a gente monitora um CPE que já está na nossa rede em busca de redirecionamento de DNS? Como que a gente sabe se uma CPE está sendo usada por uma botnet, ou está sendo usada para algum tipo de ataque? As CPEs disponibilizam algum tipo de recurso para isso?

E um outro ponto, eu gostaria que você comentasse um pouquinho mais, Lucimara, sobre como, na prática, o provedor faz para ter uma CPE que se adéque a todas aquelas especificações sobre as quais você falou? Ele compra e testa? Ele confia em algum selo? Ele tenta fazer uma compra coletiva dentro de uma associação e daí exige aquilo? E se for um fabricante lá do outro lado do mundo, dá para exigir? Como que você... que conselho você dá para pessoal do provedor para ele conseguir colocar em prática isso? Por favor.

SRA. LUCIMARA DESIDERÁ: Obrigada, gente, obrigada pela pergunta. Eu vou, na verdade, mencionar o próprio Klaus aqui na primeira parte da resposta, né? Monitorar se o meu CPE está sendo redirecionado,

acho que o Klaus deu um exemplo especificamente sobre isso, né? De que como flows podem ser utilizados para justamente você identificar se na tua rede você tem um CPE que está usando um DNS fora daqueles DNS considerados bons para serem consultados, né? O seu próprio ou algum DNS público comum. Então, flows é uma forma bastante boa, recomendada para você conseguir identificar se o teu CPE está sendo abusado aí para fazer redirecionamento de DNS.

Em relação a compras de equipamento, eu diria que fazer a compra por uma associação, ela tem mais vantagens, né? Então, você consegue gerar um poder de compra maior, uma barganha melhor em relação ao seu fornecedor. Então, você tem um volume maior de gente comprando, e aí fica mais claro que a demanda por aquele produto, por aquela segurança, por aquele produto de melhor qualidade, ela vem de mais gente e não de apenas um único provedor, né? Então, eu diria que se as associações se unissem e dissessem "a gente vai comprar em conjunto usando esse conjunto de requisitos", você está favorecendo o mercado como um todo, por trazer produtos de mais qualidade, e o próprio... cada um dos provedores, que vão conseguir barganhar melhor aquele produto.

E em relação a acervo, né? A gente... a ideia da BCOP não é gerar um selo de segurança, não é gerar um produto certificado, né? A gente não gosta dessa ideia, porque como o mundo dos problemas de segurança, ele é extremamente dinâmico, quando a gente pensa em falar "ah, tal dispositivo está atendendo, é seguro", você corre o risco de gerar uma imagem enganosa, né? Como você tem que aplicar... a dinâmica de surgirem novas ameaças e novos problemas é muito grande, então, não dá para a gente dizer: Ah, tal equipamento é seguro. Acho que a ideia não é essa. A ideia é você ter... pensar em maturidade para que o teu fornecedor consiga gerar rapidamente atualizações a esse produto. Se você pensa em certificar, se você amarra muito, e aí você não consegue gerar rapidamente, com a velocidade necessária os patchs e atualizações que você precisaria para manter aquele dispositivo realmente seguro ao longo tempo. Espero que eu tenha respondido à pergunta.

SR. EDUARDO BARASAL MORALES: Respondeu, sim, Lucimara. Muito obrigado.

Bom, vamos seguir aí com as perguntas. Tem agora uma pergunta do Hudson Alves Amaral: "Poderiam comentar sobre ataques a servidores SIP?" Então, Klaus, você poderia comentar?

SR. KLAUS STEDING-JESSEN: Posso, posso comentar, sim. Bom, ataques a servidores SIP, pessoal, o que... quando a gente está falando disso, basicamente é o que, né? Isso a gente já observa, por exemplo, na [ininteligível], há muitos anos, tá? Imagina que você levanta um servidor SIP na sua organização, uma Asterisk da vida. O que está constantemente acontecendo são varreduras, então, na Internet para achar esse servidor SIP, o atacante acha, tá? Estamos falando de 50, 60 UDP, né? Porta 50, 60 UDP. Ele acha lá o seu... um ramal seu, e vai fazer o quê? Força bruta, né? E aí, fazendo aquele link com que a Cris comentou lá no começo, né? Do... um dos grandes problemas que a gente vê até hoje é se basear em senha apenas, tá? Então, o cara vai lá, tem software que faz isso de maneira automatizada, scanners específicos de SIP, ele vai lá, vai tentar fazer força bruta da senha do ramal. Uma vez descobrindo isso, ele vai usar o seu ramal, a sua empresa para fazer chamadas, tá? Então, assim, no final do mês você vai ganhar uma conta de chamadas internacionais, que alguém na Internet afora aí fez usando esse seu ramal SIP, tá? Falei de Asterisk, mas pode ser qualquer coisa.

Outra coisa um pouco mais recente que a gente tem visto. Bom, então, a gente escreveu o Listner, que simulava esse Asterisk já há muitos anos. Para quem tiver curiosidade, pessoal, inclusive o Ceron(F), que estava aqui, eu vi ele no chat ainda há pouco, ele é um dos autores, tá? A gente escreveu um artigo a seis mãos, então, o Ceron(F), a Cristine e eu, que a gente publicou lá naquela Login, da [ininteligível]. Se você

der um Google por SIP e Login vocês vão encontrar esse artigo, inclusive com dicas, no final, de como eu mitigo um pouco esses ataques, mas é basicamente força bruta, limitar a exposição desse dispositivo para a Internet e aumento de monitoração, tá?

Mais recentemente, a gente viu um outro ataque em cima desse tipo de servidor, que é explorando aquela porta AMI, a Asterisk Management Interface, que o default é a porta 50/38 DCP, mesma ideia, só que em vez do cara chegar via 50/60, ele chega na porta de gerência, vamos dizer, do seu Asterisk, e pior ainda, faz força bruta e ele consegue fazer muito mais estrago para ações de ramais, mudar configuração do seu equipamento, etc.

Então, acho que qual seria recomendação? Isso que a gente falou: cuidar com tudo que depender de senha apenas, tá? Quer dizer, o que for possível mover para um esquema de múltiplos fatores de autenticação. Aumento da monitoração. Evitar aquele cenário, pessoal, que a gente vê muito. "Ah, mas o estagiário botou uma máquina de teste na sexta-feira à tarde e aí na segunda ele vai terminar de configurar", né? Você sabe o que vai acontecer na segunda-feira, né? Essa máquina aí já passou o final de semana inteiro comprometida. Então, ter sempre esse mindset, pessoal, do tipo: colocou uma máquina nova na rede, ela já tem que entrar correta, tá? "Ah, mas ainda-- ainda preciso fazer uns ajustes". Pense numa rede, talvez, de [ininteligível], algo que você conecta nela primeiro, termina de fazer o que o você tem que fazer e aí coloca na Internet. Então, acho que isso vale para servidor SIP e vale para qualquer serviço que você tiver configurando. Então, espero ter respondido aí, Eduardo.

SR. ANTONIO MARCOS MOREIRAS: Respondeu, sim, Klaus. Muito obrigado, hein?

Pessoal, a participação de vocês está sensacional no chat. A gente está com 989 likes. Olha, faltam 11 likes para chegar em mil. Vamos chegar nos mil likes aí antes de fechar a live. Ainda tem meia hora para fechar a live. Tem um tempinho. Vocês podem dar esse 11 likes até lá. Pessoal ficou aqui alvoroçado. Já tinha mandado um abraço para a Profa. Liane. Mas agora há pouco no chat interno o pessoal: "A Profa. Liane está assistindo o chat! Está assistindo a live! Alguma coisa de certo a gente deve estar fazendo aqui, né?". Muito legal. Então, novamente, um abraço. Um abraço para o Omar Kaminski. Fazia tempo que não o via nos eventos do NIC.br. Um abraço.

E a próxima pergunta é uma pergunta do Prof. Robson, do Instituto Federal de São Paulo, ali de Guarulhos. É uma pergunta para o delegado Alesandro e para a Cristine: "Qual é a forma correta dos professores de segurança da informação abordar esse assunto? Como que se pode mostrar esses ataques para os alunos e o que é melhor falar para eles? Como se ensina a se proteger desses problemas?" Cristine, Alesandro, o que vocês podem falar para gente? Passo a palavra primeiro para a Cristine.

SRA. CRISTINE HOEPERS: Ok, Moreiras. Eu acho que, assim, hoje em dia tem muitas maneiras da gente fazer. A única coisa que eu diria, assim, o mais importante é o que não fazer, né? Não gerar ataques na Internet, não baixar ferramentas e sair usando, né? Eu acho que é pensar que, assim uma das coisas mais importantes, e que poderia ser a primeira coisa, é tentar ver o que está acontecendo no próprio tráfego da rede, poderia colocar o laboratório, colocar um Honeypot. A gente tem até um documento na nossa página, lá na área de documentos do Cert, falando prós e contras de Honeypots. Mas a gente, por exemplo, aprende muito sobre ataques, muito do que a gente vê como as botnets se propagam, como os ataques de SIP funcionam. Quer dizer, tudo isso a gente faz via Honeypots, você só precisa necessariamente gerar ataques para ver como eles funcionam. Hoje é muito também fácil montar laboratórios. Procurem, hoje tem muitos lugares que têm capture the flags, dessa área de como fazer forense, como você procurar por rastros de invasão em computadores. Então, assim, tem muitas maneiras

de você fazer isso, porque é meio que um mito de que: "Ah, eu preciso aprender a atacar para aprender a proteger". Não, você precisa aprender a ver como são esses ataques. Quer dizer, a gente vê muita gente, assim, entender como isso se manifesta na rede, aprender TCP IP, ver como que eu conseguiria pegar o tráfego e entender que está acontecendo esse ataque na minha organização, né? Para quem é da área de software, acho que você conseguir baixar um bom software ou ter um Honeypot um pouco mais ativo, vendo como que são esses exploits, acompanhar listas de discussão. Acho que tem bastante coisa que dá para fazer, mas sempre pensar que tem que ser uma coisa ética e você não pode fazer parte do problema, né? Então, você jamais vai poder fazer isso de frente para a Internet, né? Hoje, por exemplo, uma das grandes dificuldades quando você tem uma Honeynet, que é ter um monte de Honeypots que são máquinas de verdade comprometidas, você tem que fazer um firewall para proteger a Internet do seu laboratório. Então, lembrar disso também. Não é porque você tem um laboratório na universidade que: "Ah, está de frente para a Internet. Botei uma DSL que se infectou e está gerando ataque". Quer dizer, não é assim. Fazer com responsabilidade e proteger a Internet desses ataques aí.

Esse acho que era o meu comentário inicial.

SR. ALESANDRO GONÇALVES BARRETO: Ok, só complementando aqui o que a Cristine falou, é muito importante a situação de laboratório trabalhar de forma ética, certo? A capacitação, ela tem que primar por isso. O que a gente tem visto nos últimos anos, e assim, isso está crescendo no Brasil. Possivelmente, a gente já até consiga nos próximos meses montar uma estrutura semelhante ao [ininteligível], nos Estados Unidos, que é um centro onde se agrega academia, iniciativa privada e poder público num só lugar, onde se fortalece bem a capacitação, se fortalece bem o compartilhamento de boas práticas e tem sido uma maneira bem-sucedida de enfrentamento à criminalidade cibernética. Eu sempre onde ando as pessoas me questionam: qual o melhor software para enfrentamentos? Eu digo um: a capacitação. Então, profissionais bem preparados, bem capacitados, entendendo como as coisas funcionam, porque não pode tomar providência quando o problema ocorre. A gente tem que antecipar cenários. Quem antecipa cenários, então, quando se monta laboratórios, se entende como está funcionando, se entende como que aqueles ataques estão ocorrendo, fica mais fácil. Então, professor, invista nesse cenário e coloque os alunos para trabalhar nessa estrutura, e eu acho que é um caminho a ser bem sucedido.

Só queria voltar um pouquinho na questão da Attack Mestre. O que é importante também, pessoal? Que a gente tem visto muito aí grupos de WhatsApp como canal técnico para compartilhamento de incidentes. Não é esse o caminho. O WhatsApp, ele não tem memória, tá? As empresas que são atacadas, elas têm que compartilhar incidentes e boas práticas em canais adequados. Então, quando você fortalece isso, é melhor até: ah, tem alguém que foi atacado em Porto Alegre, mas esse problema já ocorreu no Rio Grande do Sul, já ocorreu em São Paulo. Quando é esse compartilhamento, fica mais fácil.

SR. EDUARDO BARASAL MORALES: Perfeito, delegado. Muito bom.

Bom, a próxima pergunta eu vou fazer para o Kurt. Kurt, quando que um provedor deve contratar uma limpeza de tráfego? No momento do ataque? Ou antes disso? Tem alguma diferença? E já complemento a pergunta: como que vocês identificam um ataque?

SR. KURT URBAN: Isso é interessante. Pode ser contratado a qualquer momento, durante o ataque ou antes dele. O ideal, lógico, é antes dele. Por quê? Agora eu vou pegar a segunda parte da pergunta, que vai explicar a primeira. Quando a gente configura o sistema para... de mitigação, a gente pega parâmetros da rede do cliente. Identifica os IPs, para que são usados os IPs, para poder configurar os sensores, para identificar se aquilo é um ataque ou aquilo é um tráfego normal, né? Eu vou dar um exemplo: o IP que é

usado no concentrador NAT, ele tem um perfil de tráfego totalmente diferente do IP usado no servidor web. Então, os sensores têm que ser configurados para cada caso. Se o cliente já entra sob ataque, a gente não tem o parâmetro "o que é o normal daquela rede". Então, vão entrar parâmetros já do sistema, default do sistema, mas que não está totalmente otimizado para aquele cliente. Isso pode gerar falso positivo. Ou seja, julgar tráfego para as caixas de mitigação para ser analisado que não seria de ataque, gerariam... gerando latência, né? Ou pode ser o contrário. Deixar passar uma parte de ataque para o alvo porque o tráfego não foi detectado como um tráfego anormal, né? Então o ideal é configurar antes a rede, já colocar todos os parâmetros, fazer teste nela, porque quando chegar um ataque, a detecção vai ser muito mais rápida, porque cada elemento está bem identificado e consegue detectar antes e ser bem mais eficaz, né?

Então, mas a qualquer momento pode ser contratado, né? Só que a contratação durante o ataque pode gerar um inconveniente no instante inicial do serviço. Outro motivo também é que a gente precisa é anunciar aquele cliente nos nossos upstreams, tem que liberar filtros para propagar rotas. E isso tudo depende de um tempo, né? Então, se entrar sob ataque, a gente depende também de filtros dos terceiros serem aplicados para poder acatarem as rotas desse cliente que estaria entrando. Acho que foi isso.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Kurt. Gostaria de fazer a próxima pergunta para a Lucimara. Lucimara, a gente sabe que tem muitos produtos que são produtos antigos, mas que ainda estão no mercado, CPEs, por exemplo, que são produtos de 2013, são projetos antigos, mas que continuam sendo vendidos. E tem problemas sérios de segurança, às vezes, no nosso trabalho de disseminação do IPv6 também a gente encontra com problemas sérios de adequação a protocolos, né? E o que o provedor pode fazer? Ou o que a gente pode fazer, de forma geral, não só provedores, mas o que seria a solução para isso?

SRA. LUCIMARA DESIDERÁ: Bom, obrigada pela pergunta.

Assim, o que já está no passado, no backlog aí, já existe de 2013, acho que infelizmente a gente não tem muito o que fazer. É pensar daqui para frente, e a gente realmente começar a cobrar isso do mercado. Então, esse é um dos pontos que está lá na BCOP, que é exigir a política clara e dizer por quanto tempo a empresa vai oferecer esse suporte e essas atualizações de segurança, para que você [interrupção no áudio].

SR. EDUARDO BARASAL MORALES: Pessoal, a gente teve aí um pequeno probleminha com a Lucimara. A gente já retoma com ela para responder essa pergunta, tá?

Bom, enquanto isso, eu vou fazer... eu vou passar para a Cris, que gostaria de fazer um comentário.

SRA. CRISTINE HOEPERS: Beleza, Eduardo. É um comentário, não sei se a Lucimara também ia abordar isso, mas é um comentário sobre essa questão de CPEs, né? E o que fazer com essa questão. Acho que é o que ela fala. Quer dizer, o que já está no passado aí, quer dizer, não tem muito como mudar e tem algumas iniciativas, e tem gente que pensa: Ah, vamos certificar. Tem outro que acha que tem que fazer isso, aquilo. Mas uma coisa que a gente tem que lembrar sempre, e isso a gente tem a ver com outras colocações que eu vi o pessoal respondendo no chat, até quando eu falei em educação, software seguro e tal, que é lembrar que não dá para a gente certificar software. Então, não tem como certificar que a minha rede interna está segura. Não tem como gerar um software certificador de que eu tenho segurança interna na organização. Eu não tenho como certificar nem que um software qualquer está com todas as questões de segurança.

Então, o comentário só que eu iria fazer e que tinha muito a ver com outras áreas, e o pessoal falando: ah, era interessante a gente certificar de que tem um software legal, que o aluno vai fazer o software seguro. E não tem como a gente certificar coisas, softwares, não tem como eu provar que um software não tem problema de segurança, não tem como eu provar que uma determinada rede não tem problema, porque softwares são complexos, eles são código, eles vão evoluir com o tempo e não tem muito como você fazer isso. Por isso a importância de tudo o que Lucimara falou na apresentação dela, que é você ter um cenário em que você cobre que o fabricante vai ter que ter patch, mas não que você diga que você vai ter que ter o certificado. Eu só fiz esse comentário porque eu vi muitos comentários no chat falando em: "Ah, certificar que a rede interna, ter uma certificação que o APP está ok. Como eu certifico que a minha rede está com um software ok?". Não certifica, porque isso é impossível de fazer. Então, por isso que a gente tem que lutar por ter patchs, porque os problemas vão aparecer e você tem que instalar o patch e você vai ter que correr atrás, porque a Internet é mais complexa.

Então, acho que é pensar, a gente não cair nessa falsa ideia de que daria para eu ter alguém fazendo um selo de segurança, né? Era o comentário que eu ia fazer. Mas eu tenho certeza que a Lucimara, agora que voltou, eu vi que ela agora está de volta aí, ela vai complementar essa parte aí.

SR. ANTONIO MARCOS MOREIRAS: A gente conseguiu retomar o contato com a Lucimara. E eu vou só relembrá-la da questão aqui, por causa da correria. Mas a questão era a seguinte: a gente tem as CPEs que às vezes estão abandonadas, né? Estão abandonadas no mercado. São projetos antigos, projetos, sei lá, de 2013, 2012, mas que ainda estão sendo vendidas. Então, o que fazer para resolver essa situação?

SRA. LUCIMARA DESIDERÁ: Pessoal. Desculpa. Só retomando, então, o que eu tinha falado inicialmente. A gente começar a cobrar no que a gente for comprar agora que o fabricante traga essa política e deixe claro por quanto tempo ele vai oferecer essas atualizações. A gente precisa gerar essa demanda do mercado e elevar a barra, porque senão a gente vai continuar tendo esse problema de que o fabricante vai lá, entrega, e aí ele tira de linha e fala: "Não vou mais fornecer patch". Então, é cobrar que ele tenha uma política clara de suporte e de atualizações, né?

E, assim, queria só trazer uma coisa que aconteceu há um tempo atrás. Acho, assim, que a gente não pode ficar esperando regulamentação, né? Mas existe uma consulta pública da Anatel, e eles incluíram nessa consulta pública uma... que é obrigatório, para os dispositivos do tipo CPE serem adequados a essa BCOP que a gente comentou aqui, que a gente falou aqui. Então, eu diria... e nessa consulta pública, eles falam lá em estabelecer um certo prazo para que seja provido atualizações de segurança para os CPEs. Então, diria aí para vocês ficarem de olho em algumas coisas que podem acontecer um pouco pela frente, mas não esperem que isso seja a bala de prata. Acho que a gente precisa começar agora a gerar demanda mesmo e exigir do mercado, subir a barra, tá? Obrigada.

SR. ANTONIO MARCOS MOREIRAS: Obrigado, Lucimara.

Gente, a gente está chegando pertinho já do horário final programado da live. Eu lembro que a gente tem os sorteios. Então, ainda dá tempo. Se vocês querem participar dos sorteios, peço até para o pessoal aí de apoio da comunicação colar novamente os links no chat. Dá tempo de se inscrever. A gente vai abrir agora uma rodada para os palestrantes fazerem seus comentários finais, falarem um pouquinho do que quiserem, do que acharem relevante. Não dá tempo mais da gente pegar mais as perguntas. A gente sabe que tem muitas perguntas ainda no chat, na medida do possível, depois, a gente vai passar essas perguntas para o pessoal para, quem sabe, tratar isso num outro evento, de outra forma.

Agradeço muito, muito a participação de vocês todos. Não estou mandando ninguém embora ainda. Eu quero vocês até o finalzinho, entendeu? Mas já vou agradecendo a participação, que foi muito legal, todas as perguntas foram muito legais.

E começo essa rodada com a Cristine. Cristine, você pode fazer suas considerações finais?

SRA. CRISTINE HOEPERS: Posso sim, Moreiras. E eu acho que eu queria voltar num comentário que eu fiz na minha apresentação, que, assim, pessoal, invistam no básico. A gente tem... os ataques vão ficando complexos, sim, vocês vão precisar ter várias tecnologias, vocês vão precisar pensar em tudo o que a gente falou aqui, em ataques evoluídos, tal. Mas lembrar que às vezes você põe tudo a perder porque você esqueceu de instalar o patch, porque você tinha uma senha fraca no seu roteador, e a gente já viu casos, assim, de provedor que era exatamente isso: era o roteador que tinha uma senha fraca. Alguém invadiu aquele roteador, começou a sequestrar tráfego, fazer coisa, quer dizer, você pode ter o seu negócio... botar a perder o seu negócio por falta de algumas coisas básicas, né? Então, invistam no básico também. Não esqueçam disso. É muito fácil às vezes você se distrair com novas tecnologias e esquecer que está faltando alguma coisa muito básica aí nessa área de segurança. Queria só dar essa mensagem aí.

SR. EDUARDO BARASAL MORALES: Muito obrigado, viu, Cris?

Agora eu vou chamar o Klaus para dar a última palavrinha.

SR. KLAUS STEDING-JESSEN: Obrigado, Eduardo. Bom, agradecer, então, todas as pessoas aí, mais de mil, que nos assistiram. Então, vai o agradecimento aí.

De mensagem final, pessoal, eu acho que, assim, eu queria reforçar um pouco isso que a Cris falou, tá? A gente focar no elefante na sala. Antes de sair implementando coisas mirabolantes, lembrar que uma grande parte dos comprometimentos que a gente vê no dia a dia são basicamente por unidades antigas, tá? "Ah, o cara invadiu meu servidor WordPress", aí você vai ver, é um CVE de três anos atrás. Meu elemento de rede tinha um firmware de cinco anos de idade, tá? Então, pensar nisso. Pensar que qualquer lugar da sua rede onde você dependa de autenticação apenas com senha vale a pena aí fazer uma lista e tentar melhorar isso daí. Pode ser um negócio simples, tá? Um servidor que você acesse via SSHA, você começa a fazer isso com chave, tá? Não só senha. Você começa a fazer isso com [ininteligível], tá? Hoje em dia, se você tem [ininteligível] gerencia recursos aqui no Registro.br, por exemplo, ativa o token, hoje está fácil de fazer isso aí. Você pode usar um Google Autenticator. Você pode usar um UBQ(F) direto do browser. Então, isso é extremamente importante.

E fiquem de olho nas notificações que a gente manda, que o mundo está mandando, alertando vocês de problemas. O que a gente ouve todo dia, o pessoal: "Ah, mas isso aí cai numa conta que ninguém lê. Muito difícil, cai no consultor". Então, assim, tem... a gente se esforça muito aqui no Cert para mandar logs claros e com instruções claras do que fazer, tá? Mas não adianta nada se isso cair no [ininteligível]. E depois disso, bom, vai a minha recomendação, olhem com carinho essa questão de Netflow, façam como lição de casa. Não adianta ligar isso na hora do problema, tá? E tenho certeza que vocês... é mais uma ferramenta muito útil para ser usada do ponto de vista de aumento aí da segurança de vocês.

Essas seriam minhas palavras finais. E agradeço novamente todo mundo, pessoal.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Klaus. Realmente, o que você falou aí de olhar esses e-mails é uma coisa que a gente alerta até nos cursos. É realmente importante.

Bom, vou passar agora para o Kurt fazer as considerações finais. Fique à vontade.

SR. KURT URBAN: Queria agradecer de novo a participação. O que posso falar, assim, na parte de proteção de DDoS é, principalmente, conhecer a rede. Se o cliente consegue a rede dele, ele até consegue alimentar as ferramentas de mitigação de forma mais assertiva. E muito cliente, na hora que entra para... a gente pede: ah, passa documentos para preencher, para poder a gente começar a configurar a proteção. A gente não conhece a rede dele, os equipamentos, e isso é uma forma interessante até achar serviços que estão abertos, que o pessoal falou, serviços que vêm abertos por default(F) em alguns equipamentos, né? Equipamento que não precisa ter acesso SSH de fora. Por que deixar liberado isso, né? Então, o conhecer a rede é importante para a própria rede e, no caso de um ataque DDoS, ajudar a ferramenta de mitigação ser mais assertiva. Era isso aí que eu tinha [ininteligível] falar.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Kurt. Lucimara, você pode agora tomar a palavra e fazer suas considerações?

SRA. LUCIMARA DESIDERÁ: Gente, obrigada de novo pela oportunidade de estar aqui, trazer essa mensagem. Então, assim, eu... pedir a vocês que leiam o documento, que busquem mais informações. Se tiver dúvidas, por favor, fiquem à vontade para entrar em contato com o grupo lá do LAC-AAWG e a comunidade. E lembrem que a ideia é começar a levantar a barra de segurança junto ao mercado, junto aos fabricantes. Não significa que você vai ter que fazer tudo 100% do dia para a noite, não é isso. Não estamos... não é falar em: vou substituir o meu parque em 100%. Não é isso. Ninguém está pensando que isso vai virar a chave da noite para o dia, né? Então, é começar, é dar os primeiros passos, né?

E é isso. A gente trabalhando junto, porque, infelizmente, combater DDoS e combater esses ataques na Internet é um esforço que é coletivo, ninguém vai resolver o problema sozinho. Então, a gente precisa começar a fazer, e não é virar uma chave, não é do dia para noite que a coisa se resolve, mas a gente precisa começar a dar o primeiro passo. É isso, obrigada.

SR. ANTONIO MARCOS MOREIRAS: Delegado Alesandro Barreto, por favor, as suas considerações finais.

SR. ALESANDRO GONÇALVES BARRETO: Bom, primeiro que queria parabenizá-los pelo evento, de altíssimo nível, bem prestigiado, mais de mil curtidas, ainda dá mais tempo, né, Moreiras? De curtir mais ainda. Dar o like lá na página.

E algumas lições ficam para a gente. O que precisa fazer para mitigar esse cenário? Investimento em segurança, educação, capacitação a todo instante, compartilhamento de boas práticas. E um cenário que eu acho fundamental é a conscientização. Não adianta você comparar algo que custe uma verdadeira fortuna, enquanto vai ter alguém que trabalha na tua empresa que está clicando tudo, que está deixando informações expostas, informações pessoalmente identificáveis expostas em redes sociais. Então, se você consegue juntar esses aspectos, como Luci falou anteriormente, isso não é do dia para noite, mas precisa começar. Não agora. Precisa começar já ontem. Então, quem se antecipa vai ter vantagens nesse cenário.

Então, por fim, agradeço demais por ter participado. E bem feliz de estar ajudando nesse enfrentamento da criminalidade cibernética. Não é fácil. Cada dia a gente tem que estar se superando, a cada dia a gente tem que estar ultrapassando barreiras, mas as Polícias Judiciárias, elas estão conseguindo evoluir e estão também conseguindo ajudar o país nessa mitigação desses ataques.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado.

Daqui a pouquinho a gente vai fazer o sorteio, lembrando, a gente tem o sorteio hoje da Eletronet, de um voucher de R$ 200 na Americanas, um sorteio de um curso da 4Linux e um sorteio de um curso da NetfindersBrasil. O Eduardo está se preparando aqui para fazer esse sorteio. E, enquanto isso, eu tenho alguns avisos ainda a dar a vocês. Então, fiquem por aí. Não vão embora, não.

Primeiro, eu quero lembrar a todos que a gente tem o formulário de avaliação. Pessoal já colou o link há algum tempo aí, eu vou pedir para o pessoal de apoio que cole de novo link do formulário de avaliação. É bastante importante vocês colocarem lá, darem a nota, são duas questões só. É muito, muito rápido. Você não vai levar nem cinco minutos para preencher isso daí, aliás, cinco minutos não. Acho que você não vai levar nem cinco segundos. Você vai dar uma nota para o evento e você vai colocar um ponto negativo lá. Um ponto em que a gente precisa melhorar, se quiser. Se quiser só dar a nota, só dá a nota. Se você conseguir identificar o pior ponto, a pior coisa que a gente fez para a gente conseguir melhorar para o próximo, vai ajudar muito a gente a fazer esses eventos serem cada vez melhores, certo? Então, por favor, preencham. É bastante importante para a gente.

Quem precisar de certificado de participação tem até às 2h da tarde para conseguir fazer a inscrição, receber o e-mail, confirmar o e-mail, e daí a gente consegue emitir o certificado de participação, tá?

Quero agradecer novamente aos nossos patrocinadores, que nos ajudaram a viabilizar esse evento, outros eventos, outras iniciativas de formação que a gente faz aqui no NIC.br. O Giovaneli, a Eletronet, Pró ISP, Netfinders Brasil, a Juniper e a WZTech, a Editora Novatec, a Icann, a Cisco, a Forte Telecom e a 4Linux.

Na última live, no mês passado, eu... Aliás, desculpa. Não foi na última live. Foi num evento que a gente fez chamado de Semana de Capacitação, eu mostrei para vocês, como um teasing de um projeto novo, alguns vídeos. São vídeos de 15 segundos que a gente tem preparado sobre boas práticas de uso da Internet, sobre como a pessoa pode usar, como um cidadão, como um usuário da Internet leigo em tecnologia pode usar a Internet corretamente. Quais são os direitos da pessoa na Internet, quais são os deveres da pessoa na Internet, como a pessoa... como a Internet funciona. São videozinhos sempre curtinhos, sempre de 15 segundos, que não têm fala, que é só o vídeo. Pode ter uma musiquinha de fundo. Eu vou pedir agora para o pessoal aqui do apoio técnico para colocar novamente um desses vídeos, para quem não viu durante esse último evento ter uma ideia do que eu estou falando. É um projeto que ainda vai ser lançado, é disso que eu quero falar com vocês. E vamos assistir ao vídeo primeiro. [Por favor.]

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: [interrupção no áudio]. Opa, estava sem áudio aqui. São vídeos curtinhos, são vídeos que dá para você inserir na sua rede social, mandar o link via WhatsApp, via Telegram, vai ter uma versão, um gif animado, vai ter versões em diversos formatos e tamanhos. E a gente conta, para esse projeto, com o apoio do pessoal dos provedores, do pessoal da academia, dos professores e de outras entidades aí para ajudar a gente disseminar essa informação. E o lançamento desse projeto vai ser no dia 21 do próximo mês, numa live. A gente vai fazer isso numa quarta-feira, igual essa live aqui, uma quarta-feira, dia 21 de outubro. Então, anotem na agenda aí para vocês participarem, para vocês nos prestigiarem nessa live e entenderem como que vai ser esse projeto, que tipos de vídeos exatamente a gente vai lançar. Não vou nem falar o nome agora. É para deixar na curiosidade mesmo. Não vou nem falar o nome da iniciativa, mas no dia 21 vocês vão saber, vocês vão saber como que vai ser. E acho que vai ser legal. Vai ser legal para a gente e vai ser legal para vocês também, porque tem, às vezes, alguns conceitos que ajudam o seu usuário final a entender como que a rede funciona. Ajuda, às vezes, entender que o problema não é sempre do provedor. Por exemplo, quando a gente explica para o usuário como que

funciona o Wi-Fi na casa dele, ou que tipo de... que o Wi-Fi da casa dele tem uma determinada capacidade e que isso pode causar lentidões em vídeos se muita gente usar ao mesmo tempo. Quando a gente explica, assim, conceitos de uso da Internet para o usuário, isso pode ajudar o provedor a atender reclamações que aparecem lá no call center, ou até evitar essas reclamações, quando o usuário consegue entender um pouquinho melhor como utilizar a Internet de uma forma correta e plena. Então, conto desde já com a presença de vocês nesse evento do dia 21 de outubro.

E eu quero lembrar que essa série de lives também não acabou ainda. Temos duas lives, uma em novembro e uma em dezembro, programadas. Então, temos uma live sobre PTTs, focando tudo que aconteceu durante a pandemia, e temos uma live com uma análise da Internet toda em 2020. Então vão ser lives também interessantíssimas. Vamos nos esforçar para que sejam tão boas quanto todas as outras, quiçá melhores.

Quero também avisar do BCOP, do curso BCOP, em formato EAD, que estamos com as inscrições... as inscrições vão ser abertas no dia 4 do mês que vem. O curso BCOP vai ser do dia 9 ao dia 13 de novembro. E quero lembrar também... O curso BCOP, para quem não sabe, é um curso de boas práticas operacionais. A gente fala muito de BGP, de como se conectar corretamente aos PTTs, de como configurar os filtros do PTT... no BGP. De como a gente implanta RPKI, como implanta IPv6, de como a gente faz uma série de configurações do ponto de vista de operação, do ponto de vista de segurança, que são fundamentais para o provedor funcionar corretamente.

Quero lembrar também do Camada 8. Camada 8 é o nosso podcast. Procurem nas principais plataformas de podcast por Camada 8, vocês vão nos achar lá. O último podcast foi uma entrevista interessantíssima com o pessoal da Akamai, falando como que funciona uma CDN, como você faz a distribuição de conteúdo. Temos aí o próximo aí programado, que é sobre as plataformas de games, que também está muito interessante. Vai ser lançado ainda. Vocês podem esperar aí, na segunda semana, sempre na segunda quarta-feira do mês nós lançamos um episódio novo. Então, fiquem atentos ao Camada 8, já tem episódios sobre IPv6, tem episódios sobre PTT, sobre PGP, sobre a pandemia. Tem vários episódios muito, muito legais, muito interessantes no nosso podcast.

Os materiais da live, dessa live aqui estão online já, estão no site da live, no intrarede.nic.br, é só ir lá na agenda. Está tudo lá. "Ah, não está". Dá um reload na página que está sim, certo?

E eu acho que é isso. Como estão os preparativos para o sorteio, Eduardo? Já está tudo no jeito? Os ganhadores já estão escolhidos? Não, os ganhadores não podem estar escolhidos ainda, certo? Então, eu vou passar a palavra para o Eduardo, ele vai dar sequência aos sorteios da live de hoje.

SR. EDUARDO BARASAL MORALES: Tudo bem, Moreiras. Bom, vamos aí fazer o sorteio.

Então, eu vou fazer os três sorteios, vai ser o sorteio da Eletronet, o sorteio da NetfindersBrasil e o sorteio da Eletronet, da NetfindersBrasil e o da 4Linux. Então, vamos começar aí com o da Eletronet. Então aí o primeiro ganhador é o Vinícius Nunes de Bona. Esse daí ganhou os R$ 200 no voucher da Americanas. Depois o pessoal vai entrar em contato com você pelo seu cadastro lá, que foi o seu e-mail, e você vai ganhar o voucher de R$ 200 da Americanas.

Vamos agora para o 4Linux. O 4Linux foi o Luiz Yuri de Azevedo. Então, o Luiz Yuri ganhou um curso EAD à sua escolha. Então, o pessoal vai entrar em contato com você, e você vai ganhar ali o curso que você desejar na 4Linux.

E agora a NetfindersBrasil, que vai sortear um curso de BGP, né? Multi-homing lá, que quem ganhou foi o Jesiel. Lá no cadastro deve ter lá o seu e-mail, tudo. Eles vão entrar em contato com você, Jesiel.

Então, esses foram os três sorteios que a gente tinha para fazer para vocês. Então, depois aí, quem ganhou vai receber o aviso. E acompanhe aí os outros eventos que a gente faz, que muitos deles vão ter sorteio também, então, vocês vão poder participar.

Bom, faltou falar algumas coisas, Moreiras. Você pediu like aí no YouTube, mas não pede like para o nosso Camada 8, né? As outras plataformas também têm avaliação. Então, quem quiser assistir lá, ouvir o Camada8, depois ali dá um like lá para a gente, para a gente poder propagar e continuar fazendo novos episódios. Também faltou falar os patrocinadores. Vou agradecer aqui a Giovaneli consultoria e treinamentos, a Eletronet, Pró ISP, NetfindersBrasil, Juniper, WZTECH, Editora Novatec, Icann, Cisco, Forte Telecom, 4Linux, VLSM e o apoio de mídia da revista RTI.

Então, muito obrigado a todos por terem participado. Muito obrigado aos painelistas que participaram, e a gente se vê no próximo Intra Rede. Então, até mais.