SR. ANTONIO MARCOS MOREIRAS: Tá.

ORADOR NÃO IDENTIFICADO: [ininteligível].

SR. ANTONIO MARCOS MOREIRAS: Vocês estão ouvindo aí, gente, agora?

ORADOR NÃO IDENTIFICADO: [ininteligível].

SR. ANTONIO MARCOS MOREIRAS: Ok. Bom dia. Eu estou ouvindo o meu retorno aqui.

ORADOR NÃO IDENTIFICADO: [ininteligível].

SR. ANTONIO MARCOS MOREIRAS: Acho que não. Um segundinho, gente, problemas técnicos. Talvez seja problema meu mesmo, problema meu mesmo. Gente, desculpa pelos probleminhas técnicos aí. Muito bom dia novamente! Eu sou Antonio Moreiras, do NIC.br. Estamos aqui no segundo dia da Semana de Capacitação On-line promovida pelo NIC.br. Começamos ontem com um conteúdo trazido pelo próprio NIC.br, pelo Thiago, pelo Eduardo, pela Erina, que falaram sobre RPKI. Um conteúdo de excelente qualidade, já está disponível aqui no Youtube o vídeo gravado de ontem, quem perdeu acompanhe porque é muito legal. E hoje a gente começa uma dinâmica diferente nessa semana, onde a gente traz parceiros de fora do NIC.br para trazer conteúdos para vocês de qualidade, conteúdos excepcionais. Hoje temos a participação da Cisco, com o Adalberto Lins, e da ScanSource, com a Josiane, que vão falar sobre segurança básica para provedores de internet. Vão falar de assuntos como Hijacking de BGP, Hijacking em DNS, como que funciona o comando controle, DDoS. E vão trazer, inclusive, dicas sobre como mitigar alguns desses problemas. Então, a gente está com altas expectativas aí sobre o conteúdo de hoje, a gente espera que ele seja, realmente, excepcional.

Então, desde já, eu peço para vocês darem um like no vídeo para o Youtube distribuir para todo mundo que está inscrito no canal do NIC.br, para ninguém perder esse conteúdo que vai ser excelente. Peço para vocês compartilharem o link do vídeo nos seus grupos de WhatsApp. Não precisa compartilhar no link da família não, tá? Mas no link lá do pessoal dos provedores, o pessoal do trabalho, etc., por favor, compartilhem o link, compartilhem no Facebook. A gente tem a transmissão no Facebook também, para que mais gente tenha acesso a esse conteúdo. Se alguém não puder assistir agora ao vivo, que está no horário de trabalho, acompanhe depois. O vídeo vai ficar gravado, logo depois da gente terminar a live o vídeo já fica disponível no Youtube.

É importante dizer que quem quiser um certificado, quem precisar de um certificado de participação desse minicurso, desse evento, tem que fazer a inscrição ainda hoje até às 14 horas. Então, a inscrição é só para quem está acompanhando aqui ao vivo o vídeo. O pessoal vai colocar o link de inscrição no chat do Youtube. Se alguém estiver acompanhando pela própria página do evento, tal, clica lá para acompanhar pelo Youtube, né? O pessoal vai colar também aí nos comentários do Facebook e principalmente no chat do Youtube. Então, acompanhem, veja o link lá, entre no nosso site de cursos e eventos, faça a inscrição, aproveita para se inscrever nas nossas listas de e-mail para receber avisos sobre eventos futuros desse tipo. Deem um ok lá para a gente poder mandar e-mails para vocês e avisá-los quando a gente tiver iniciativas desse tipo, cursos, eventos e outras iniciativas similares.

Eu vou pedir para o Pedro, aqui, que é o do pessoal técnico que está nos ajudando, que ele coloque agora um videozinho de 15 segundos, que é uma espécie de um teasing aqui, de uma amostra de um projeto

novo em que a gente está trabalhando com vídeos para comunidade não técnica, para a comunidade de usuários da internet, para os usuários leigos da internet, vídeos educativos.

Então, a gente quer, em breve, a gente vai lançar esse projeto, e eu quero só dar uma mostra do que a gente está fazendo. É um videozinho de 15 segundos, e eu já volto aqui falando, tá bom? [Pedro, você consegue colocar, por favor?].

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Bom, gente, espero que vocês tenham gostado, depois vocês dão o feedback para gente aí nos comentários do Youtube, no chat do Youtube.

A gente espera muito a participação de vocês no chat do Youtube, a gente vai estar acompanhando. Do mesmo jeito que foi ontem, a parte principal do curso, ela já foi gravada em vídeo. E a gente vai dar o play. Só que o Adalberto e a Josiane, eles estão aqui com a gente. Eles estão ao vivo aqui com a gente. Eles vão acompanhar o chat, vão acompanhar as questões, vão responder as questões que vocês forem fazendo no chat e vão anotando tudo, porque dali, quando acabar a parte que está gravada, o pessoal vai entrar ao vivo para bater um papo com vocês, para responder as perguntas que forem feitas no chat.

A gente fez dessa forma porque tem muita gente trabalhando com home office, né? O pessoal que está em home office, e sempre tem o risco, ah, de cair a internet. Então, para não ter nenhum problema com a live, não ter nenhum problema com o conteúdo principal a gente pediu para o Adalberto, para a Josiane: grava, por favor, o vídeo antes, a gente só dar o play lá na hora, mas vocês vão ficar lá interagindo. Dá até a chance de ficar interagindo com o pessoal no chat e respondendo as dúvidas ali no meio do vídeo. Se precisar interromper, o pessoal está aqui ao vivo, mas a ideia é que eles entrem logo em seguida para tirar as dúvidas de vocês.

O material está sendo colocado no site agora, os PowerPoints, subidas(F), o pessoal da equipe está trabalhando nisso. Em breve, ele vai estar lá disponível. Vocês vão conseguir fazer o download dos materiais pertinentes no site.

Vale dizer também que o curso de amanhã e o curso de depois de amanhã, ele tem uma parte prática que vocês podem acompanhar com uma máquina virtual. Então, vocês podem já olhar lá no site, fazer o download do material e se preparar para o curso de amanhã e para o curso de quinta-feira. Se quiserem acompanhar fazendo a experiência junto, aí na casa de vocês, no trabalho de vocês, vocês façam o download da máquina virtual e acompanhem. Se quiserem acompanhar só assistindo e vendo o pessoal, também não tem nenhum problema. Aí fica a critério de vocês.

Novamente, por favor, todo mundo dê o joinha aí no vídeo para o Youtube distribuir para o maior número de pessoas possível. E eu desejo a todos, hoje, um bom curso. Vamos todo mundo acompanhar o que o Adalberto e a Josiane têm para ensinar para a gente que eu acho que vai ser muito interessante.

Então, por favor, agora a palavra é de vocês, Adalberto e Josiane.

SRA. JOSIANE DE BARROS SILVA: Bom dia a todos. Espero que todos estejam bem em suas casas, seguros. Eu gostaria de agradecer a sua presença hoje aqui comigo nesse tutorial. Hoje a gente vai falar um pouquinho sobre Basic Security for regional ISP. Então, tenho bastante dicas e informações relevantes que se forem absorvidas da maneira correta vão fazer total diferença no dia a dia de vocês. Espero que vocês gostem do tutorial.

Falando um pouquinho sobre mim. Eu sou formada em Engenharia da Computação, possuo algumas certificações como CMNA, que é uma certificação para... determinada para pré-vendas com foco na solução da Meraki(F), que é da Cisco, faz parte da Cisco também. Possuo a certificação Cisco Fire Jumper para Elite. Fui a primeira mulher a conseguir esse título no Brasil. Tive que fazer, tive que criar um canal do Youtube, ajudar outras pessoas com conteúdo de segurança, com dúvidas técnicas, para poder conseguir esse título e, hoje, poder ministrar também esse treinamento para essa certificação que é o Cisco Fire Jumper.

Faço parte também da ONG Womcy, onde ela tem o intuito, a finalidade de captar essas mulheres que querem entrar na área de segurança, mas não têm uma oportunidade, não sabem como começar, onde partir, onde dar o pontapé inicial. A Womcy, ela faz todo esse processo de onboard de mentoria que pode ajudar essas mulheres que querem ingressar nessa carreira.

Sou consultora de projetos também na ScanSource para parte de segurança da informação. Atuo hoje com o Cisco, com soluções Cisco. Como eu já comentei, sou instrutora também do treinamento Cisco Fire Jumper e, nas horas livres, nas horas vagas eu gosto muito de estudar a parte de Red Team.

Então, basicamente, o que eu faço hoje dentro da ScanSource, eu trabalho com Blue Team, com soluções para defesa. Mas eu tenho um grande apreço a parte de Red Team. Então, eu acredito que trabalhar esses dois lados em conjunto, a gente chega no bem maior, que entrega uma solução e um valor muito agregado lá no final do conteúdo. A gente tem tanto essa parte de como o atacante, ele pensa, e como a defesa pensa também. Então, eu consigo saber os métodos, os comandos, os passos que esse atacante vai tomar e eu vou conseguir, do outro lado, da mesma forma, cercar para mitigar, para bloquear esse ataque.

E hoje, a agenda, a gente vai ter essas informações aqui. Começando pelos três pilares da segurança da informação. Essa parte vai ser mais teórica, mas vai ser mais breve. Erros comuns. Como que a gente se comporta, né? A gente às vezes não percebe, mas a gente tem algumas atitudes que podem trazer um certo grau de vulnerabilidade para nós, seja fisicamente, seja virtualmente. Então, eu deixei algumas dicas dentro de erros comuns. Eu vou falar também sobre o BGP Hijacking, a parte de DNS Hijacking ainda teórica e com o Cryptojacking eu já começo a fazer a parte teórica e eu tenho um... tenho ainda, vou apresentar para vocês, a parte prática do Cryptojacking, como que funciona a mineração em si, e a parte de mitigação dessa mineração. Vou falar também de Command & Control, tanto a parte teórica quanto a parte prática e como mitigar. E vou falar também a parte de Distributed Denial of Service, o que é. Quais são as diferenças de DoS para DDoS. Então, eu espero que vocês aproveitem e gostem bastante do material que eu preparei para vocês. Boa aula para vocês.

Agora que vocês já sabem como que vai ser o cronograma do nosso tutorial, então a gente vai começar por essa parte mais conceitual, mais básica, que são os três pilares da segurança da informação que é: confidencialidade, integridade e disponibilidade. Sem elas, sem esses três itens e alguns outros mais que a gente pode até citar a segurança não existe, a gente não consegue trabalhar sem esses três pilares. Então eu vou passar aqui o slide.

Começando pela confidencialidade. Então o que é? Quando a gente cita o nome confidencial, a gente quer dizer que é algo restrito, sigiloso, secreto e que não deve ser divulgado para pessoas que não tenham a devida autorização. Então, por que é tão importante a gente proteger essas informações confidenciais? Porque ela não se baseia apenas nas nossas informações como empresa, como ScanSource, como Cisco, como NIC.br. A gente tem que pensar que debaixo daquelas informações das empresas, atrás dessas informações das empresas, companhias, a gente tem nossos clientes, temos funcionários, temos

fornecedores que a gente divulga essas informações. Então, vamos imaginar que a gente tem um servidor lá na WS, ou até mesmo dando um exemplo mais simplório, mais simples que a gente tem no nosso dia a dia. Por exemplo, o seu usuário, ele precisa acessar o e-mail que fica no Gmail da vida ou no Outlook da vida, ou no Office 365, e ele tem esse acesso direto ao e-mail dele. Então, quem garante que é ele realmente que está tentando acessar aquele e-mail do Office 365, ou se não é uma outra pessoa se passando por ele para ter informações? Como, por exemplo, a gente vê muito acontecendo ataques de vazamento de dados onde empresas, como, por exemplo, na área de Healthcare, como hospitais, que os exames, os resultados dos exames desses pacientes foram divulgados. Já pensou se a pessoa tem uma doença que é um pouco mais grave ou até mesmo pode ser contagiosa, e todo mundo pode parar de conviver com ela ou olhar de uma maneira diferente porque teve aquela descoberta daquela informação que era confidencial, mas foi divulgada. E para vocês trabalhando com seus clientes, com informações como nome, CPF, RG, telefone, como vocês lidam com isso? Todos esses dados são informações pessoais e confidenciais das pessoas. Então, é muito importante que vocês utilizem algumas técnicas, ferramentas para ajudar na proteção.

Como criptografia de dados, então, onde você puder criptografar os dados, criptografa o máximo. Autenticação de múltiplo fator. Então, seja para seus equipamentos, seja para acesso aos e-mails, as suas aplicações que vocês precisam disponibilizar para seus colaboradores. O importante que tenha o duplo fator de autenticação para validar a real identidade e saber se realmente ele que está tentando acessar e não apenas basear com origem e destino e criar uma segurança com base nisso.

Gestão de acesso mobile, às vezes os seus funcionários, colaboradores, eles estão indo para rua fazer um atendimento, e as informações que eles utilizam é numa plataforma de colaboração de instant messenger que é muito comum, que vocês já devem até imaginar o nome, mas não é a ferramenta ideal para aquele tratamento daquelas informações como endereço dos seus clientes, por exemplo. Então, tem que ter um cuidado maior.

Outra coisa que eu coloquei aqui também, prevenção contra perda de dados, que é o DLP. Ter uma solução que proteja as informações confidenciais, como, por exemplo, documentos que contenha salário de funcionários para que eles não caiam em mãos erradas, ou seja aberto para outras pessoas, ou que eles sejam enviados por e-mail.

E eu acredito que seja mais essa parte de confidencialidade que eu queria deixar para vocês.

Agora, a parte de integridade. Integridade quer dizer que você enviou aquela mensagem, você mandou aquele e-mail e você quer que aquele e-mail chegue para aquela determinada pessoa da mesma forma que foi enviado, sem nenhuma alteração. Então, é para isso que serve a integridade, para garantir que esteja íntegro, que esteja correto essas informações que estão ali. E qual a importância? Então, da mesma forma que você enviou, você tem que receber. Então qual que é o problema que acontece com isso? De repente você enviou um e-mail, você, dono da empresa, gerente, diretor, envia o e-mail para o seu RH, ou para o seu financeiro pedindo para que seja depositado ou transferido para uma conta determinada, de determinado banco. Nesse caminho, o [ininteligível] pode detectar, pode capturar essa mensagem e simplesmente manipular essa informação e dizer que é para transferir para a conta dele. Então, você pode enviar esse e-mail, por exemplo, mas essa informação da conta vai para outra pessoa, e a pessoa do financeiro não vai conseguir identificar que realmente não é a conta, né? Só se ela fizer uma verificação mais profunda.

Então o que é importante para que não seja... para que vocês não sofram com essa falta de integridade? Eu deixei algumas soluções que vocês podem utilizar, que ajudam também a mitigar. Por exemplo, o antimalware, que ele te dá rastreabilidade. Então, se foi alterado algum registro, algum arquivo, ele foi duplicado na sua rede, ele está se movimentando lateralmente, tudo isso o antimalware, ele é capaz de detectar.

Solução de análise de comportamento. É um tipo de solução que, tanto antes quanto depois, é capaz de detectar ataques, ou até mesmo pós-exploração, que eu vou comentar para vocês numa aula prática que eu montei para vocês, um laboratório de Command & Control. Solução de análise de comportamento, ela se encaixa perfeitamente porque mesmo depois de você ter passado por todos os níveis de segurança essa solução de análise de comportamento, behavior analysis, ela consegue detectar comportamento anômalo e consegue mitigar, detectar ou fazer com que outra solução faça um bloqueio antes que se agrave mais, ou que vire algo pior.

Solução de Anti-Spam que vocês podem aplicar para poder proteger e manter a integridade dessas informações que estão sendo trafegadas.

E sobre disponibilidade, por último, não menos importante, o que é disponibilidade? É o que garante que os dados dos sistemas poderão ser acessados e disponíveis por indivíduos no momento em que eles desejarem acessar essa informação. Então, se meu usuário, ele tentar acessar esse serviço tem que estar disponível. Então, por exemplo, meu usuário quer tentar acessar a internet e, por algum motivo, ela não está disponível, eu vou ter dor de cabeça, né? A minha reputação pode ficar ruim, até mesmo pode acontecer esse problema de ataques à disponibilidade pode ser também por concorrência entre service providers. Você pode mitigar isso com algumas ferramentas que eu deixei aqui como anti DDoS, algumas soluções de Proxy, antivírus, mas, basicamente, o que vai te ajudar é pensar. Um exemplo que me veio na cabeça agora: se uma empresa, ela tem uma única abordagem, ela não tem redundância, ela não tem backup, se um dia acontece uma indisponibilidade e acabou a luz ou morreu o servidor, como que ela vai ter acesso àquelas informações? E as informações não são só daquela empresa, são de fornecedores, de clientes. Como que fica? A empresa, no exemplo que eu estou dando, tem 20 anos de idade. Mas aconteceu um desastre, e todos esses dados foram perdidos, e a empresa não tem nenhum registro e tem que começar tudo do zero. Então, é importante também ressaltar que o backup faz parte do nosso dia a dia. Redundância de link, redundância de equipamento também deve ser levada em conta. Os Patches, muita gente tem... demora muito tempo para poder fazer essa atualização de Patch, então, lançou um Patch novo que resolve tal problema do sistema operacional X. Então, você demora um mês para poder verificar se aquele Patch é válido, se não tem nenhum problema. Então, isso tem que ser automatizado, tem que ser mais rápido. Esses Patches, eles têm que ser testados em ambientes separados, homologados e colocados em produção para que esse tempo não gere uma abertura maior para poder os atacantes explorarem a sua rede, por exemplo. Então fica a dica.

E agora, o próximo slide que eu vou falar agora é de erros comuns. Essa parte de erros comuns é aquela parte de quem nunca fez ou quem nunca viu alguém fazendo. Isso é mais para trazer um alerta para vocês mesmo.

Começando pelo cara/crachá. Então, nesse momento muitas pessoas devem estar se perguntando: ah, por que a Josi está falando sobre isso? Sobre crachá. Mas muitas vezes passa despercebido, já vi pessoas da corporação também fazendo o mesmo, como a Mariana Godoy fez. Ela chegou a compartilhar a foto do crachá dela com o QR Code e as informações como foto e nome dela inocentemente. Então, eu vejo muito

acontecendo isso. Por exemplo, você vai pegar um transporte público, um ônibus ou metrô e você se depara com pessoas com crachá, indo para casa com o crachá pendurado, às vezes tem o número do CPF e o nome completo, às vezes tem a foto. Pensando, assim, muitas pessoas vão falar assim: ah, mas o que tem? O que pode trazer de prejuízo, de problema? Já vi pessoas também em restaurantes guardando lugar com crachá, deixando o crachá lá em cima da mesa, em shopping também. Que tipo de problema a gente pode ter? Eu já vi, eu já acompanhei muitos Pentests físicos onde eles testam a segurança física da corporação. Então, eles tentam passar por seguranças ou até mesmo clonando o crachá. Já vi muitos levando para gráfica. E a gráfica, sem nenhuma preocupação, faz um... clona esse crachá e entrega para pessoa, a pessoa vai lá e faz o teste, tenta entrar na empresa. E se ela for pega, ela disfarça, finge que não aconteceu nada, que ela entrou no lugar errado, na empresa errada. Existem pessoas que fazem isso. Então, se você não chegou a ver, não teve essa experiência, eu conheço pessoas que fazem esse tipo de Pentest. Às vezes a pessoa... Tem pessoas que fazem esse teste, mas tem pessoas que têm uma malícia. Então, a gente não sabe qual intenção das outras pessoas, então, sempre importante alertar nossos usuários, os funcionários sobre isso.

Confiar no usuário VPN. Nesse tema de home office, né? Muitas pessoas indo trabalhar de casa, a TI teve que fazer um trabalho gigantesco para que todo mundo fosse comportado e pudesse acessar seus recursos através da VPN e da sua casa, do jeito mais confortável e mais seguro possível. Mas nem sempre os seus usuários, eles estão na VPN. Nem sempre eles estão. Geralmente eles precisam acessar uma aplicação, acessa essa aplicação, depois que terminar de acessar essa aplicação ele não precisa mais de nada para navegar. Ele consegue acessar o e-mail dele diretamente, o Office 365 dele diretamente, então, ele não vai utilizar. E toda essa segurança aplicada dentro desse túnel da VPN não vai valer de nada, então, ele vai estar saindo localmente pela internet, onde ele não tem nenhuma regra de segurança, nenhuma política de segurança para protegê-lo. E como que fica essa situação? E quando a gente voltar desse home office, desse isolamento, essa máquina dele, aonde ele começa a navegar, todo dia ele navega por redes sociais, conteúdo que, às vezes, ele pode clicar e ele não percebe que está acessando uma página que é maliciosa. E esse computador, ele vai voltar, esse computador corporativo, ele vai voltar, esse notebook, volta para corporação, depois da pandemia, e como que vai ficar isso quando colocar isso no ambiente, na rede? Você tem alguma solução para validar se esse equipamento, essa Compliance, ele está atualizado? Se ele não possui nenhuma aplicação que não deveria estar instalada lá ilegalmente? Como que você consegue validar isso? Então, para que vocês pensem um pouco sobre essa questão. A gente está vivendo um momento histórico, totalmente diferente do que a gente já tinha vivido, mas a gente tem que pensar as coisas estão acontecendo agora e vão ficar pior depois quando a gente voltar. Então, se já foi um reboliço todo para TI correr atrás dessa mudança para home office, vai ser pior na hora da volta, quando todos esses computadores, a maioria, certeza que vai ter alguma coisa, alguma infecção, voltar para rede e começar a gerar problema para o ambiente corporativo, para rede corporativa onde estão os servidores, enfim.

A DMZ, Demilitarized Zone, ou zona desmilitarizada. Então, aqui do lado direito eu deixei um desenho aqui para vocês, uma imagem onde a DMZ, ela faz com que os seus usuários, você tem um servidor Web, você tem um servidor de e-mail, um servidor de arquivo, se os seus usuários estão na outside, esse seu público, esses seus clientes que precisam acessar essas informações, consumir essas informações, eles não tenham acesso a sua rede inside. Então, a DMZ serve para isolar a sua rede interna da sua rede outside, sua rede externa para criar uma certa confiança, para que mesmo que essa pessoa consiga ter acesso, ela não consegue pular, fazer esse intermédio para sua rede inside e comprometer onde você tem os seus servidores, os seus dispositivos instalados. Então, você consegue criar um grau de isolamento e confiança

com a DMZ. Então, é uma coisa muito importante que muitas pessoas ainda não têm, não fazem isso, não praticam e isso é algo básico que a gente prega para os nossos clientes. Então, com o firewall você consegue resolver isso sem nenhum problema.

Não sei se vocês já ouviram falar do Shodan, que é o Google dos hackers. Então, você consegue encontrar em todo o globo, todo o mundo, informações sobre os roteadores que têm o seu default password. Então, se ele está como nessa imagem admin admin(F) você consegue pegar essas informações, ter acesso a esses dispositivos e modificar as configurações dele. Esse tipo de atitude de não alterar o password default facilita e muito os hackers a conseguir invadir esses equipamentos. Então, outra coisa que é importante, antes de eu repassar para outras informações, utilizar duplo fator de autenticação desses equipamentos para validar a real identidade desse usuário que está tentando acessar. É sempre importante, além de trocar o password, dispositivos IoT. Como que vocês controlam esses dispositivos. No Shodan você tem informação sobre geolocalização desses dispositivos, você consegue filtrar por essas portas. Câmeras de vigilância, web cam. Então, eu já... não vou abrir no caso para vocês, eu vou abrir aqui uma demo do Shodan, mas se vocês pesquisarem, vocês vão encontrar câmeras com password default, isso dentro de casa, dentro de corporações, e você consegue ver as pessoas trabalhando lá tranquilamente sem imaginar que tenha alguém lá vigiando elas. Então, é muito importante, se vocês puderem e tiverem um tempo, dar uma olhadinha no Shodan, e filtrar, e ver como que é, realmente, a gente está exposto, dessa forma. Se a gente não tomar umas medidas básicas, a gente fica exposto, tanto por seus dispositivos de redes, enfim.

E outro exemplo que eu deixei aqui que é de servidor Web. Então, aqui no... vou circular aqui para vocês. Na primeira parte eu tenho o servidor Web que está aqui no Kali, final 125, e estou acessando a página normal. Mas eu resolvi dar um /Admin para ver o que acontecia. E eu tenho acesso, e esse servidor Web, ele me cospe na tela a informação de um diretório e informações do sistema também, como IP e porta.

Aqui na segundo foto mais detalhes dessas pastas, desses diretórios, desses arquivos. E se eu tento acessar um desses arquivos, ele me mostra que o que tem dentro desses arquivos. Então, aqui, o que foi mostrado na tela que eu tinha colocado, bem-vindo ao meu tutorial de SecureGirlNinja! Como que eu faço para tirar essa informação? Eu não quero que meus diretórios fiquem expostos, eu não quero mostrar isso para o mundo. Então, basicamente você entrando aqui nesse endereço /etc/apache2/apache.conf você consegue no diretório raiz, que é o /var/www onde tem options indexes followSymLinks você tira essa opção de Index, tirando essa opção de Index, o lado direito aqui, as informações do diretório já não ficam mais disponíveis, isso eu estou falando para vocês, é uma configuração básica que muitas pessoas não fazem no servidor Web. E aqui do lado ele me retorna um erro, Forbidden, mas ele me dá algumas informações do sistema operacional, IP e porta.

E a gente vai ver aqui no outro slide. Então, a versão do serviço que está rodando, ele cuspiu aqui na tela para mim, mas eu não quero que continue aparecendo essas informações. Então, aqui no security.conf das configurações do servidor Web existe uma opção chamada ServerTokens(F) OS, onde você pode setar de full a prod, sendo full é totalmente as informações, completamente você vai disponibilizar nessas requisições, nessas manipulações. Ou você pode colocar opção de prod, que é o mínimo possível de informações. Então, é recomendável que você altere, ao invés de OS para prod para que ele não apareça essas informações de sistema operacional. E ele saiu aqui esse output só apenas com a parte server, o IP e porta. Então, ainda tem informações que estão aparecendo, que estão sendo cuspidas aqui no meu navegador.

Então, eu quero tirar essas informações, o que eu faço? Existe uma outra opção chamada server signature(F) onde está habilitado, então você pode dar o server signature off, e basicamente você já vai conseguir restringir o acesso às informações, o seu servidor, ele não vai dedurar quem ele é, que sistema operacional ele é, que versão ele tem. Então, são coisas simples que podem ajudar vocês também no dia a dia a se policiarem quanto a isso.

E quando a gente olha para essa capa a gente já tem uma ideia de como que vai ficar essa parte de BGP Hijacking, o que significa. A gente tem fluxo normal e de repente a gente tem um desvio desse fluxo, desse tráfego indevidamente.

Então, separando aqui o que é Hijacking, então, a tradução dele é sequestrar, ou o ato de assumir o controle, ou usar algo que não lhe pertence para sua própria vantagem. BGP, que é o Border Gateway Protocol, utilizado para direcionar tráfego pela internet, permitindo que as redes troquem informações de acessibilidade para facilitar o acesso a outras redes.

E fazendo a junção dos dois a gente tem o sequestro BGP, que é aquisição ilegítima de grupos de endereços IP. Então, eu alego que esse endereço IP pertence a mim e acabo corrompendo as tabelas de roteamento da internet mantidas pelo protocolo Border Gateway Protocol, que é o BGP. Fazendo a analogia, a gente tem o BGP como um serviço postal da internet. Então, quando a gente coloca uma carta em uma caixa de correio, o serviço postal, ele processa essa correspondência, escolhe uma rota rápida e eficiente para entregar a carta ao destinatário. Aí, da mesma forma, quando alguém envia os dados pela internet, o BGP, ele fica responsável por examinar todos esses caminhos disponíveis em que os dados vão percorrer e escolhe qual que é a melhor rota e o que geralmente significa alternar entre Sistemas Autônomos.

Então, aqui nos Sistemas Autônomos a gente tem a internet como a rede das redes, que é dividida por centenas de milhares de redes menores, então, conhecidas como Autonomous Systems ou AS. Aí cada rede dessa ela tem essencialmente um grande conjunto de roteadores executados por uma única organização. E essas organizações, esses Sistemas Autônomos, eles pertencem aos ISPs e outras organizações que possuem alta tecnologia, ou empresa de tecnologia, universidades, instituições científicas. E cada Sistema Autônomo que desejar trocar informações pela internet de roteamento tem que ter um SN, que é Autonomous System Number ou Sistema Autônomo Registrado, que é número de Sistema Autônomo.

Então, os ASs são como agências postais individuais e cada cidade pode ter centenas de caixas de correio, mas o correio nessas caixas deve passar pela agência postal local antes de ser roteada para o destino. Então, os roteadores internos em uma AS são como caixas de correio, encaminham as suas próprias transmissões de saída para os ASs que, então, usa o roteador BGP para levar essas transmissões até os seus destinos.

Aqui foi um caso que aconteceu, até tem o link aqui, a fonte da ZDNet, aonde a Rostelecom, ela, talvez proposital ou por acidente, ela fez um pequeno... ela cometeu um errinho aqui. Então, seguindo a pesquisa aqui da ZD, o último grande sequestro da Rostelecom, que aconteceu em 2017, a empresa, ela sequestrou rotas de BGP dessas empresas aqui que eu coloquei para vocês, das maiores entidades financeiras, como Visa, Mastercard, HSBC e outras mais. Então, todo esse tráfego que ia diretamente para essas empresas foi direcionado para Rostelecom. Talvez seja intencional ou não, mas aconteceu dessa forma. E muitas pessoas podem pensar assim: ah, mas por quê? O que tem a ver? Mas só um redirecionamento. E essas informações? Instituições financeiras, compliance, a gente começa a pensar: quais as informações

sensíveis estão passando por ali? E se eu decriptografar aquele tráfego, o que eu consigo encontrar ali? Então, a brincadeira começa por aí.

E para tentar manter essa ordem foi criado alguns projetos como o ROV, RPKI e o Manrs também, que é... Opa. Passou aqui. Normas mutualmente acordadas para segurança na base de roteamento. Então, temos algumas empresas que estão se ajudando, colaborando para tentar manter a ordem nessa grande internet, essa rede das redes. E aqui feito uma análise com o endereço da Rostelecom, eu consegui identificar que aqui tem um médio risco. As alterações de records dessa Rostelecom, lá em 2017, na época que aconteceu esse problema, e o tráfego dela é muito incomum. A gente tem uns picos de requisições. Então, a gente pode começar a pensar que talvez seja intencional esse redirecionamento. De vez em quando, ela anuncia que ela tem aqueles prefixos que não são dela, que não pertencem a ela, ela anuncia aquilo lá, todo o tráfego daquelas empresas passa a vir para ela, para a Rostelecom e tem picos de tráfego de requisições. Então, talvez faça sentido ter sido intencionalmente.

Começando a seção de DNS Hijacking. Talvez alguns conheçam, outros não. Então, DNS Hijacking, todo mundo conhece o que significa DNS? Que se refere a Domain Name System. A sua tradução: sistemas de nome de domínio, o que, na prática, é como se fosse numa lista telefônica, quando a gente precisa ligar para alguém, geralmente a gente sabe o nome da pessoa que a gente quer ligar, mas a gente nunca lembra o número dela. Então, funciona dessa forma, para o DNS também. A gente vai tentar navegar, vai acessar um Google.com.um, um Cisco.com. A gente digita Cisco.com. e é endereçado, encaminhado para o endereço correto daquela página, daquele domínio. Então, assim que funciona a partir do DNS. E Hijacking em si é o sequestro, então, o sequestro desse sistema de nome de domínio.

Isso que eu acabei de falar para você, isso para o usuário é imperceptível, agora nos bastidores a gente tem uma hierarquia com essas informações de quais são os processos que levam até chegar a esse domínio que a gente deseja acessar. Então, a gente tem Root Name Server, ou servidor raiz, que opera na zona raiz. Ele pode responder diretamente para consultas de registros que estão armazenados ou até mesmo que estão em Cache. E se estiver em Cache, ele já tem aquele endereço de destino do domínio e ele já te repassa isso. Ou se ele não encontra essa informação no Cache, ele encaminha essa solicitação para o servidor de Top Level Domain, que é o TLD, que está aqui mais abaixo. E para quem não sabe, o Top Level Domain é aquele mais à direita, aonde a gente tem o .com no final do acesso de cada domínio, o Cisco.com. ou ScanSource.com.br. Tudo isso muda conforme o Top Level Domain.

Então, a gente tem dois tipos, tem o country code, que é baseado na localização dos países, então a gente tem o .br, o.pt que eu dei como exemplo, que é Brasil e Portugal. E o genérico Top Level Domain onde eu dei uns exemplos de .com, que são organizações comerciais, sem restrições, e o .edu que é para estabelecimentos de educação superior.

E mais baixo a gente tem o servidor autoritativo. Esse servidor autoritativo, ele que possui os registros originais. Ele que está mais próximo desse domínio que eu quero acessar. Então, ele que conhece esse domínio, por exemplo, o Cisco.com, ele conhece muito bem.

E o DNS Recursivo, a gente pode utilizar tanto do ISP, que vem, chega na nossa casa, a gente pode utilizar o DNS recursivo, que já vem default, ou nós podemos utilizar também outras soluções, tanto Umbrella, Cloudflare. Então, do Umbrella, no caso que eu estou dando o exemplo aqui que eu dei o IP 208.67.222.222, e também o IP secundário aqui que eu dei. Você pode redirecionar esse DNS externo para fazer o processo de DNS Recursivo. Então, o que ele faz, basicamente, é seguir todo esse caminho, passar pelo servidor raiz, depois passar pelo Top Level Domain até encontrar o servidor autoritativo que tem o

conhecimento e autoridade sobre o domínio que eu quero acessar. Então esse é o papel do recursivo, ele faz todo esse trajeto também.

E aqui nessa imagem, acredito que fique até um pouco mais simples para poder enxergar como que funciona. Então, essa máquina está tentando acessar o Cisco.com, aqui na informação 1. Ele vai passar pelo servidor, pelo DNS Recursivo, o DNS Recursivo vai procurar lá no servidor raiz, no root, qual que é esse com ponto, né? Esse ponto no final é implícito, mas existe ele aqui. E esse DNS autoritativo, raiz, ele vai responder com o endereço do DNS autoritativo Top Level Domain. Então, ele respondeu com o endereço do Top Level Domain. Então, o recursivo, ele vai procurar lá no autoritativo Top Level Domain se existe o www.cisco.com. E esse TLD.com responde com o endereço aonde existe um autoritativo que tem e que conhece esse Cisco.com, que ele chega aqui até esse endereço e retorna qual o IP de destino desse domínio para que o DNS Recursivo retorne e isso vá essa informação para o nosso navegador, e a gente consiga acessar esse site.

Qual a importância do DNS, né? Então, sem DNS a gente não vive, vamos dizer assim. Então, DNS Recursivo, ele é muito importante, se ele for interrompido por algum motivo, a gente pode ficar sem conexão aos nossos sites, ao menos que você tenha na sua mente quais são os endereços de cada página que você precisa acessar e digitá-la, incluí-la lá nos seus host files. Então, se você tem essa informação, que eu acho difícil, você pode também acessar sem o DNS Recursivo, mas é praticamente impossível.

E se você tiver um DNS Recursivo, mas ele estiver funcionando desacelerado, né? Pode ser que tenha algum problema acontecendo. Às vezes você está utilizando um recursivo gratuito ou, às vezes pode ter uma indisponibilidade, então, pode ocorrer essas falhas também com o seu DNS Recursivo. Então, é muito importante, porque você não vai conseguir fazer resolução e não vai conseguir fazer essa requisição e completar e chegar até o seu destino, que é o seu domínio.

Aqui eu separei alguns tipos de ataques de DNS Hijacking. E aqui estão os quatro principais. Então, onde a gente tem o local DNS Hijacking, onde você... essa sua máquina, esse seu usuário é infectado com malware, um Trojan, onde esse atacante, ele altera as configurações regionais do seu DNS e redireciona para um site malicioso. Então, toda vez que você tentar acessar o google.com vai ser direcionado para um site malicioso.

Temos também o router DNS Hijack. Então, lembra aquele default password que está setado no seu roteador, que você vai alterar depois desse tutorial. Então, esse mesmo, esse default password, os atacantes, eles utilizam para poder alterar as configurações de DNS e fazer o redirecionamento para um site malicioso também. Então, ele pode fazer com que todos esses usuários conectados acessem essa informação fake.

Rouge DNS Hijack, então, esse servidor DNS, ele é invadido, e todos os registros DNS, eles vão ser alterados e ser direcionados para um tráfego totalmente malicioso. Também existe essa possibilidade.

E a última que é o é o Main in The Middle DNS Hijack, então, o atacante, ele intervém a comunicação entre o usuário e o servidor DNS e exibe um endereço de IP falso que redireciona o usuário para um site malicioso.

Então, nós temos esse cardápio de opções de ataque que podem ocorrer. E algumas motivações, a gente já imagina que é por dinheiro, né? Então, a gente tem opções do Pharming, um tipo de ataque que é Pharming, onde você é direcionado para sites que contém propagandas e anúncios. Ela não tem nenhuma função concreta, nenhum valor, mas é só para gerar receita mesmo para esse atacante.

E o Phishing, que além de te direcionar para um site malicioso, ainda consegue também pegar o gancho de conseguir roubar algumas credenciais, informações confidenciais, então, é mais um detalhe que a gente pode ficar atento.

E o que deixei para vocês? Um acontecimento, já faz um tempinho. Então, quando a blockchain.info teve esse DNS Hijacking, né? Teve o sequestro de nome de domínio. Então, na verdade, foi até divulgado no Twitter, isso foi em 2016, aqui em cima foi uma publicação que aconteceu, foi informado que foi feita essa alteração crítica. E dentro da nossa plataforma do Umbrella, pesquisando pelo brockchain.info, no investigate, ele me dava as informações, como elas estavam antes de ser alteradas. Por exemplo, aqui no dia 12... Opa, espera aí, 7/12/2016. Espera aí, 12/7, desculpa, está ao contrário aqui para mim. Última vez visto, né? Ele foi visto no... em 2016 também, mas só que ele não tinha dois endereços IPs associados a ele. E vocês podem reparar que o tempo de vida dele é muito maior do que os endereços que já estavam lá. Aqui mais embaixo tem mais detalhes, acho que é a mesma informação. Mas aqui à direita mostra a chamada, né? As informações que foram alteradas do servidor de nomes, dizendo que toda a requisição que for enviada para blockchain.info fosse direcionada para esses endereços novos, que seriam dos atacantes. Deixa eu mudar aqui. E fazendo uma busca aqui, uma investigação, mesmo isso tendo acontecido já faz um tempo, você consegue puxar essas informações de alteração, tanto do MX quanto NS records que foram alterados, conforme se vocês compararem o último slide que vai ficar disponível para vocês, que se trata das mesmas informações, das mesmas informações que foram alteradas em 2016. E aqui do lado direito você tem mais informações sobre o whois. Qual foi a data que foi criado, qual foi o update, quando que vai expirar. E que esses servidores de domínio estavam associados com outros domínios que eram maliciosos e também uma mostra de arquivos maliciosos que tem relacionado a esse domínio.

Então, para não ficar muito extenso, direto o treinamento, vou dar uma pausa agora para gente fazer um... para ir no banheiro, tomar uma água, um café, de 15 minutinhos. Aí daqui a pouquinho a gente retorna com o conteúdo do tutorial. Então, eu aguardo vocês até daqui 15 minutos.

[intervalo]

SR. ANTONIO MARCOS MOREIRAS: Olá, gente. Então, a gente está fazendo agora a pausa aí proposta pela Josiane, podem aproveitar para tomar água e ir ao banheiro. E eu vou aproveitar aqui para o pessoal que ficou aqui acompanhando, esperando esses 15 minutinhos, só para lembrar a vocês que o material já está online, já está no site, tem os slides lá. Quem quiser fazer o download pode fazer o download para acompanhar o restante da apresentação.

O que o pessoal pergunta direto aí no chat: o vídeo vai ficar disponível? Sim. O vídeo fica disponível aqui no Youtube. Posso incorporar ele e colocar ele no meu site? No site do provedor? No meu grupo? Sim. É um vídeo do Youtube. Você pode incorporar ele no seu site, pode colocar ele para tocar na sua aula, se você for professor, etc. Você pode usar esse vídeo como você usa qualquer vídeo do Youtube aí, isso é permitido, tá bom?

O que mais? Eu gostei muito da comparação que a Josiane fez do BGP com o correio, né? Com o serviço de correio. Eu nunca tinha ouvido falar essa comparação, achei de uma didática, assim, excepcional. Bem como as explicações de todas as ameaças de segurança que a gente ouviu até agora, né? É muito legal.

Então, a gente vai esperar mais alguns minutinhos aí para todo mundo dar tempo de tomar uma aguinha, de fazer essa pausa, de ir ao banheiro, de descansar um pouquinho. E a gente, daqui a pouquinho, a gente

já volta com a continuação do vídeo da Josiane. Tá bom? Vocês podem ir aí continuar interagindo no chat do Youtube. A gente está anotando todas as perguntas, a gente está colocando aqui para os palestrantes, eles estão acompanhando. E daqui a pouquinho a Josiane e o Adalberto também vão entrar ao vivo para responder às dúvidas de vocês. E daqui a pouquinho a gente continua com a apresentação. Tá bom?

Ah, gente! Estão me lembrando aqui, o pessoal dos bastidores aqui, estão me lembrando de lembrar vocês para que façam a inscrição. Quem quiser o certificado tem que fazer a inscrição hoje até às 14 horas. A gente não estende esse tempo, a gente não tem como abrir exceções, porque a gente não tem como a gente medir quem está aqui de fato ou participando do evento ao vivo e quem não está. Então, a forma que a gente tem de fazer isso aproximada é divulgando esse link de inscrição aqui durante o evento e limitando o tempo de inscrição, né? Então, está aberta a inscrição até às 14 horas. Quem fizer a inscrição lá no site de curso e eventos para esse evento tem o certificado online. Quem não fizer a inscrição, a gente, infelizmente, não tem outra forma da gente emitir esse certificado. Então, quem precisar do certificado, não se esqueça. Veja o link que está sendo colocado aí no chat do Youtube. Se alguém estiver acompanhando pelo site do evento em si, pelo site semanacap.bcp.nic.br, clica para assistir direto pelo Youtube, clica no próprio vídeo do Youtube que fica incorporado, ele tem o linkzinho "assistir no Youtube". Entra direto na página do Youtube que lá tem o chat, aí você consegue interagir pelo chat, fazer perguntas pelo chat, a experiência de interação fica muito mais rica se você assistir direto na página do Youtube, né? É a forma... o site do evento é só uma forma, um atalho para você conseguir chegar no vídeo de uma forma mais simples. Tá bom?

Eu vou sair aqui da imagem. A gente vai voltar a ver a imagem do vídeo agora ainda com a pausa do café. E daqui a pouquinho a Josiane retorna com a segunda parte da explicação, e chegamos, e continuamos. Tá bom?

Gigabit internet, [ininteligível]. Não chegou no fim da apresentação, não. A apresentação não acabou ainda, a apresentação vai continuar. A gente só fez uma pausa para o pessoal tomar uma água, ir no banheiro, descansar um pouquinho, eu estou aqui enrolando, dando alguns avisos enquanto isso, né? Mas são avisos que já foram dados no início da live. A gente já vai retornar com a explicação da Josiane, com Adalberto e, depois, com eles ao vivo tirando as dúvidas de vocês, tá bom?

Lembro a todo mundo que está assistindo aí que é importante para gente que vocês deem o like no vídeo, porque a distribuição orgânica do Youtube, a distribuição gratuita que o Youtube faz dos vídeos para o pessoal que está inscrito no canal, para o pessoal interessado no tema, ela depende desses likes. Se o vídeo tem bastante like, o Youtube faz aparecer para pessoas, se o vídeo não tem bastante like, o Youtube não faz aparecer. Por isso que eu fico insistindo, que eu sei que é um pouco chato, eu e todo mundo que faz conteúdo no Youtube fica insistindo para derem o like. Mas o pessoal que acompanhou ontem já viu como foi a qualidade do evento. O pessoal que acompanhou até agora já viu a excelente didática da Josiane. E eu acho que o vídeo merece um like, merece ser distribuído para mais gente. Então, se vocês concordarem comigo, por favor, deem esse like. E daqui a pouquinho a Josiane retorna, tá bom?

SRA. JOSIANE DE BARROS SILVA: Voltando.

Falando de Cryptojacking. Todo mundo sabe o que é um Bitcoin ou já ouviu falar do que é um Bitcoin. É uma moeda muito cobiçada. Todo mundo quer ter uma fraçãozinha dela, mas o que difere da nossa moeda real, enfim? O Bitcoin, Monero, Bitcoin, seria uma criptomoeda, uma moeda virtual que a gente pode gerar através de criptografia. Então, tudo que a gente possui dessa fração de Bitcoin não chega a ser a moeda em si, a moeda inteira. A gente possui uma parte desse montante que todo mundo tem. E a forma como é

feita a transação dessa encriptação e da remuneração, entre aspas, desse processamento utilizado para poder validar essas transações, essa recompensa que você ganha com a fração dessas moedas, dessas criptomoedas, é de uma forma diferente. Então, a gente pensa que como a gente vai fazer uma transação no banco, a transação é centralizada nas instituições financeiras. Com essas moedas, essas criptomoedas é diferente, é totalmente descentralizada, né? A gente tem Blockchain e tem um... é totalmente dependente, todo mundo valida todas as transações. Então, eu valido a transação do Joãozinho, o Joãozinho valida a transação da Maria e da minha transação, todo mundo vai validando as transações. E a forma... fica mais difícil de quebrar, de hackear, de ter uma violação nesse método decentralizado.

Então, como que funciona? A gente olha para o Blockchain separado por blocos mesmo, então, até dá uma analogia aqui como o livro razão público, ou o livro contábil, que faz o registro de cada transação de moeda virtual. Então, a cada dez minutos esse novo bloco, ele é criado e carimbado com as informações e um novo registro é criado por esses mineradores que ficam validando essas transações de bloco. E o que tem a ver, né? Mas por quê? O que tem a ver essa mineração? O que me impacta? É que eu deixei um link como referência para vocês dos países que são, que consideram legal ou ilegal, ou é neutro com relação a Bitcoin, à mineração, enfim, mas é nesse ponto que eu queria chegar com vocês. Todo esse processo de mineração é feito de duas formas, ou você instala um Malware nessa máquina desse usuário e conta com a sorte que nenhum dos antivírus, nem dos antimalware vai detectar. E esse software, ele fica minerando ali por tempos, por tempos. E o minerador, ele vai ganhando nas suas custas, ele vai utilizando o seu processamento, o seu poder computacional, processamento, energia, porque você trabalha no limite, consome mais energia. Os componentes, a vida útil do seu hardware, ele vai se desgastando, vai se limitando. Dessa forma, a gente tem o primeiro método, que é antigo e tradicional que vocês utilizam, que as pessoas utilizam o Malware para poder fazer essa mineração.

Outra forma que a gente tem é na parte de script rodando no Web Browser. Então, a gente não tem mais a necessidade de instalar, enviar por e-mail um documento que tenha um arquivo lá que vai instalar na máquina do usuário, ou até mesmo um pen drive que está infectado para colocar, plugar na máquina do usuário, ou deixar lá no chão, para que quando ele passe, ele tenha curiosidade, plugue na máquina dele e comece a minerar. Você não tem mais essa necessidade. Você tem opção de Cryptojacking, onde você cria uma conta, onde você pega aquela conta, aquele [ininteligível] de conta sua e cria um script em JavaScript e direciona todo tipo de mineração do seu Browser. Então, se o usuário, ele tentou acessar o google.com, e o google.com existe um script de mineração que está embutido lá na página, quando o usuário acessar vai ficar minerando. Enquanto ele estiver naquela página vai minerar, vai minerar, até o momento que ele sai daquela página e para de minerar. Então, aquele script, ele direciona, toda a mineração vai para a conta daquele invasor ou daquele atacante que está fazendo essa mineração, enfim.

Quais são os sintomas que a gente tem quando tem um Cryptojacking, quando está acontecendo o Cryptojacking? Para que a gente consiga identificar. Então, a gente consegue identificar através de lentidão, se você abriu o seu gerenciador de tarefas, se você vai ver que CPU está no limite, está quase 100% ou está 100%. A performance dele fica afetada até para abrir um navegador, abrir uma página, você não consegue, não consegue fazer processos básicos que você faria normalmente. Em laptops e celulares também isso é muito pior, porque você tem celular, componentes menores e que não são tão eficazes, são menos eficientes e que vão durar menos tempo ainda, né? Então, se você tem uma bateria que dura um pouco, dura bem menos do que normalmente, então você vai degradando cada vez mais o hardware, consumo elétrico, tudo isso vai desgastando e reduzindo a vida útil do seu dispositivo.

Outra coisa, deixa eu até ver aqui. Muitas pessoas falam assim: ah, mas Cryptojacking? O que, além disso, mas isso daí é o computador da empresa. E aí, lhufas, né? Mas a gente tem que pensar da forma, assim, que o nosso maior bem que a gente tem são os nossos dados. Minha mãe falava muito que nosso maior bem era o nosso nome, antigamente. Agora são nossos dados. Então, se esse minerador, ele instalou, ele embutiu no seu navegador, ou ele te entregou através de um e-mail um executável para poder minerar na sua máquina, ele pode muito bem abrir portas e brechas para outros criminosos fazerem ataques como Ransomware, Malware, como anticontrol(F), outros tipos de ataques que eles podem embutir em conjunto com a mineração. Então, é algo mais prejudicial do que a gente pensa. Então não adianta só olhar para o nosso umbigo e falar: não, essa máquina é só da empresa. Mas a gente tem que pensar como um todo. Então, começou a detectar, viu que está muito lento, procura analisar se é algum processo que está rodando, se é o seu navegador que está aberto e está consumindo essa performance toda. Então, já é um alerta para vocês.

Depois de falar um pouco sobre como que funciona Cryptojacking teoricamente, agora a gente vai para parte prática. Montei um laboratório para vocês. Deixa eu fechar minha apresentação. Aqui na minha máquina um Kali Linux, e tem uma outra máquina aqui que é Windows, deixa eu mostrar para vocês, que também está aberta, mas eu vou ficar aqui no Kali. Aqui no Kali eu tenho duas redes. Uma sem a solução que é Umbrella, que não é capaz de detectar Cryptojacking, e a outra rede que é Umbrella, que aí eu já vou para parte de mitigação.

Então, antes de começar, eu já estou aqui sem Umbrella, eu vou fazer um teste para ver se não está sendo detectado. Eu rodo esse teste aqui do Umbrella, e ele dá essa informação de Oops. Se estivesse funcionando, a solução ia estar verdinho essa tela. Então, o que eu vou precisar para fazer a demonstração? Eu vou utilizar uma página do Blogger que eu criei com o nome de securegirlninja. Criei uma página onde eu posso pré-visualizá-la. Repare que não tem nenhum conteúdo e nenhuma informação e descrição acima dessa página aqui do Youtube que eu coloquei como exemplo. Então eu vou fechar aqui essa página. Depois eu vou retornar para vocês o que mudou.

Outra ferramenta que eu vou utilizar vai ser o CoinIMP. Deixa só atualizar essa aqui. Deixa eu desligar a rede, habilitar novamente e dar um refresh. Pronto, voltou ao normal. Ok. Para que eu preciso do CoinIMP? CoinIMP, ele me possibilita, ele me dá a opção de criar códigos. Ele já me dá um código pronto, um script que eu posso embutir nessa página do Blogger ou num site que eu tenha fake, isso pensando no modo do lado do atacante, você tem essa possibilidade. Então, aqui ele te dá duas opções de moeda virtual, no caso, o Monero não está mais disponível, eu só vou ter mintame.com para fazer o teste. Aqui ele me dá algumas médias de hashes que foram calculados, isso foi em alguns outros testes que eu fiz antes da demonstração, aqui embaixo eu tenho a opção de get the code, onde ele vai mostrar qual o script que eu preciso colar na minha página. Posso fazer uma mineração local, então, daqui mesmo dessa máquina Kali, se eu der o start mine, aqui embaixo, posso alterar parâmetros, por exemplo, eu posso trabalhar com uma thread, ou duas ou mais. E quanto que eu vou utilizar de CPU? Então, no caso eu posso utilizar 70, 50, então eu posso ir diversificando para que não seja tão detectável essa mineração. Posso adicionar sites também. Aqui se eu adicionar um novo site, ele vai me gerar um código. Eu posso clicar aqui, adicionar um site para vocês entenderem. Teste 1, save e adicionar. Ele adicionou. Eu posso editá-lo, removê-lo ou visualizá-lo. E aqui ele me mostra, ele me dá um parâmetro que eu posso diminuir o uso de CPU para poder minerar, então eu posso utilizar 60, 70, 40, no mínimo 10. Posso adicionar algumas informações. Então, eu quero mostrar uma notificação que esse site, ele possui algum tipo de mineração. Ou eu posso tirar esse alerta de notificação que está sendo minerado enquanto a pessoa está acessando aquele site. Posso bloquear o conteúdo, até que a pessoa aceite, permita a mineração. Então, ela não vai

ter o acesso ao conteúdo que está no meu Blogger, por exemplo, enquanto ela não aceitar essa mineração. E é só você dar um copy aqui, ele copia automaticamente, e você consegue colar isso na página. No meu caso, eu vou aqui em cima em get the code. Então, mesmas opções, eu quero utilizar 30% para não chamar muita atenção e eu quero adicionar uma notificação para que esse usuário saiba que eu estou minerando. Então, se vocês perceberem aqui no comando, ele vai mostrar no topo da página que este site está minerando, ele tem o script, no caso o JavaScript minerando para o coinimp.com. Mas aqui embaixo eu posso alterar algumas informações, eu posso mudar a mensagem que aparecerá no topo desse navegador, dessa página. Posso aumentar, mudar a posição dessa mensagem, dessa notificação. O tamanho dela, eu posso aumentar e também diminuir. Mudar a fonte. Vou mudar para vermelho e preto, para destacar. E ela vai ficar dessa forma aqui que vai aparecer. Ele te dá um exemplo da pré-visualização. E, feito isso, eu vou até adicionar um block. Então, eu vou deixar sem block aqui, eu vou fazer primeiro com uma notificação. Então aqui está 30%, dou um copy, vou a página do Blogger em layout, em Add a Gadget, você vai ter a opção HTML e JavaScript. Você pode colocar qualquer nome que você bem entender, o meu eu vou colocar Cryptojacking, vou dar um paste, e aquele comando que eu copiei basicamente vai estar aqui coladinho, eu dou um save, ele salvou aqui. Agora, se for em page de novo e der um pré-visualização, agora, todo o usuário, toda pessoa que for tentar acessar minha página do Blogger, para esse caso de teste de Cryptojacking, vai aparecer a informação que o site está minerando através de um script em JavaScript. Então, se a pessoa acessar essa página, sem ela saber, vai estar minerando, vai estar utilizando poder computacional, dependendo do nível de utilização de CPU, vai estar exigindo mais energia a ser consumida. Então, a gente consegue fazer dessa forma, do modo stealth, e se eu voltar aqui, eu vou abrir a minha máquina aqui do Windows, eu vou passar para ela, aí já estou aqui no CoinIMP. Vou dar um refresh só para ver se está funcionando tudo certinho. Rodo o teste também do Umbrella para ver se não está detectando nada. Então, está liberado. Aqui na máquina do Windows eu quero que vocês reparem e acompanhem como está o consumo de CPU antes de eu rodar uma mineração local. Então, está variando de 62, 58. Deixa eu fechar algumas coisas aqui. Acho que tem algumas pastas abertas. Command prompt, posso fechar, e eu vou deixar só o desk manager Firefox que eu estou utilizando. Então, perceba que fica na casa de 25, no máximo.

Então vou voltar aqui no CoinIMP, no campo local miner, percebam que aqui está zerado e [ininteligível] então eu posso considerar aqui uma thread, mas eu quero deixar em 50% de utilização o CPU. Então eu vou começar a minerar. E eu vou acompanhando aqui, e vocês podem reparar que vai aumentando o consumo da CPU aqui, no meu processamento. Então se eu quiser aumentar, eu posso ir aumentando cada vez mais. Deixei em 90%. Pronto. Então agora eu vou fazer o seguinte nas minhas máquinas, tanto Kali quanto o Windows, eu deixei algum tipo de mineração. No caso, deixei uma página do CoinIMP, deixa até eu voltar aqui no Kali e mostrar para vocês. Então eu vou deixar aberta aqui a página com essa notificação e eu vou mudar para o meu Wi-Fi que tem a solução para poder mitigar. Então eu vou mudar aqui as duas placas de Wi-Fi da minha máquina também. Alterei da minha máquina, só aguardar aqui desconectar e conectar de novo. Vou no Windows, desconectar e conectar de novo. Uma breve resolução de problemas de laboratório. Vou alterar aqui a configuração do meu Windows. Vou voltar aqui para o meu Kali Linux, enquanto isso e faço um teste se está funcionando o Umbrella. E ele já está ativo. Agora eu vou dar um refresh nessa página. Perceba que o anúncio de mineração sumiu. Vou dar um refresh na página do CoinIMP. Agora eu vou aceitar o risco. Ele nem deixa eu prosseguir, deixa eu tentar carregar de novo para ver se ele vai deixar. Ele já bloqueia o acesso a página do CoinIMP. Agora eu vou voltar aqui na minha máquina do Windows, que eu acho que já resolveu o problema. Pronto, resolvido problema aqui na Internet que deu, então eu vou dar um refresh e não foi. Eu vou tentar acessar a página do CoinIMP de novo, e ele não deixou. Não fiz o teste anteriormente, mas já está funcionando o Umbrella, clica em

advanced. Aceitar riscos e, mesmo assim, ele não deixa prosseguir e acessar mais o site. Então eu vou abrir uma nova página. Digitar aqui só CoinIMP.com, e ele não deixa mais eu acessar a página no CoinIMP. Então eu vou dar uma olhada agora como que ficou lá no Kali, onde eu tenho acesso ao Umbrella. Então eu vou logar aqui rapidinho. Logo aqui na página inicial, deixa ver se está na conta certa. Agora na página inicial, carregando novamente na parte de cryptomining tenho sete requisições bloqueadas nas últimas 24 horas. Então se eu clicar em view trend ele vai me direcionar para todas as requisições de cryptomining. Então a última requisição que eu tive aqui foi às meia-noite agora do dia 4 de agosto. Então, se eu clicar aqui, ele vai me transferir para o report active source onde posso filtrar por bloqueados. A minha identidade que está cadastrada como network device no Wi-Fi daqui de casa. E eu posso... deixa eu filtrar aqui, network device cryptomining bloqueadas. E aqui a última requisição que eu tenho para o CoinIMP. Se eu puxar aqui mais para o nada(F), ele vai me dar mais detalhes do IP de conexão. Esse 124 aqui é a minha máquina do Windows tentando acessar esse IP externo, que foi bloqueado pelo motivo da categoria de cryptomining. Então ele me dá aqui o horário e a data que aconteceu essa requisição. Então três pontinhos aqui, eu posso filtrar mais detalhes. Filtrar por esse endereço de destino, esse domínio CoinIMP.com, ver se mais alguém tentou acessá-lo. Posso filtrar também pela identidade, que sou eu aqui tentando acessar, pelo IP de destino, pelo IP de origem, e eu posso clicar aqui em view domain in investigate. Se eu clicar em view domain in investigate, ele vai puxar todo o histórico desse domínio. Então você já vê automaticamente que ele pode ter um baixo risco, mas ele tem categoria de segurança que é com relação a cryptomining. E o tráfego de requisições DNS desse domínio é bem atípico. Então bem parecido com o que vocês vão ver em um outro exemplo na minha apresentação onde você tem uns picos, né? Os spike rank(F). Então em determinado período de tempo ele teve alguns picos, e você pode notar que teve algumas alterações de MX, históricos de segurança, ó, categoria de segurança, se eu clicar aqui, ele me dá um ícone aqui de um Malware. Se eu clicar nele, ele me aparece que foi no dia 27 de março de 2018, foi adicionado um Malware. E se eu for filtrando na linha do tempo, ele vai me mostrando quando ele foi removido, quando ele foi adicionado. Mais aqui para baixo eu tenho todas as informações dos endereços dos nameservers, outros tipos de DNS, informações sobre whois, o nome de registro, quando foi criado, quando foi atualizado e quando vai expirar. Informações de criação como e-mail address, tipo de e-mail, os nameservers e se eles estão associados a alguns outros domínios que são maliciosos ou não. Se eu quiser saber um pouco mais, eu posso clicar aqui, ele me mostra qual domínio exatamente é malicioso que está relacionado a esses nameservers. Se eu der um show para mais detalhes, eu tenho mais informações de contatos dessa criação de registro, até mesmo o número de telefone. E as requisições em torno do globo, então a maioria dessas requisições estão nos Estados Unidos. No Brasil, deixa ver se tem alguma porcentagem, a gente tem um pouco mais de 1% de requisições vindas do Brasil, e todas essas aqui embaixo são amostras de Malwares, de Trojans.

Aqui ele te dá um score de 0 a 100, sendo 100 o nível mais crítico. Então você pode acompanhar que aqui bastante amostras de arquivos foram detectadas, próxima ao score 100, que é o limite máximo de criticidade. Ele me dá qual o resultado do antivírus, mais informações e posso também fazer uma investigação com esse hash, onde ele me dá mais informações sobre o artefato, que tipo de nível de confidencialidade que ele utiliza, se ele é severo, qual pontuação que ele leva, e eu posso fazer investigação profunda aqui também.

Só voltando aqui em policies. Basicamente a configuração que está citada aqui no meu Wi-Fi é para regra de DNS policies. E basicamente é muito simples, eu estou dando match nessa regra(F) Casa São Paulo, em segurança, configurações de segurança e dou edit. E a única coisa que fiz foi habilitar essa opção aqui de bloqueio de cryptomining. Automaticamente quando eu estou no Wi-Fi, na rede que eu tenho essa

solução, ele bloqueia automaticamente. Então essa foi a demo de Cryptojacking ou cryptomining, como vocês desejarem chamar. Eu espero que vocês tenham gostado. E agora vamos seguir com o restante do conteúdo.

Vamos dar início ao Command & Control, ou C2, ou Callback, como vocês já devem ter ouvido. Começar pelo Cyber Kill Chain, não sei se conhecem, mas são as sete etapas de Cyber Kill Chain, que aumentam visibilidade, e enriquece, aumenta a nossa compreensão sobre as formas, as táticas, as técnicas, os procedimentos que um adversário pode utilizar contra a nossa defesa, a nossa equipe de [ininteligível]. Então o primeiro ponto: reconnaissance. A parte de reconhecimento, onde o atacante, o invasor, ele seleciona o alvo, pesquisa, tenta identificar a vulnerabilidade de rede de destino. Weaponization, que seria o armamento, você se armar, onde o adversário, ele cria uma arma de Malware, de acesso remoto, com vírus ou warm(F), e ele consegue adaptar a uma ou mais vulnerabilidades. Passo 3, delivery, que é a entrega. O invasor, ele consegue transmitir a arma para o alvo, por exemplo, através de anexos de e-mail, sites ou unidades de USB. E a quarta etapa é exploitation, que é a parte de exploração, onde o código do programa da arma de Malware é acionado e ele executa ações na rede de destino para explorar vulnerabilidade. Passo 5: instalação. Essa arma de Malware que a gente criou, ele instala o ponto de acesso, por exemplo, um backdoor, e utiliza, e mantém esse backdoor para ser utilizado pelo invasor. Agora passo 3, que é o Command & Control, enfim... Passo 6, isso mesmo, Command & Control, onde o Malware, ele permite que invasor tenha acesso persistente, manual ao teclado, a rede de destino, então ele consegue implantar esse agente. Então mesmo que o usuário tente reiniciar a máquina, ele consegue restaurar esse agente. Esse agente permanece ali, e ele consegue fazer... ele consegue tomar, finalizar as ações e os objetivos, que é o último passo, onde o atacante, ele executa ações para atingir seus objetivos, como exfiltrações de dados, ou até mesmo destruição de dados, ou criptografia para resgate, para pedir algum resgate em troca de dinheiro.

E nós temos também o Mitre. Também é uma estrutura de kill chain, conhecido como Mitre Att&Ck. Ela é uma estrutura com modelos de táticas, técnicas e procedimentos usados por alguns atores, de alguns invasores, ou adversários, como vocês preferirem chamar, e que é um recurso muito útil, tanto para o time de Blue Team quanto de Red Team. Então a gente pode [ininteligível] comportamento durante comprometimento e representar os cenários do mundo real e ajudar os nossos clientes a determinar a eficácia dessas contramedidas que a gente tem listada no slide, tanto para o quadro ATT&CK, que tem quatro matrizes, que eu vou falar mais para frente, que é Enterprise, Mobile e ICS, que é no próximo slide. Então fica dividido assim. Tem o pré-ATT&CK, é onde se faz toda parte de reconhecimento, armamento, e o ATT&CK, a gente tem alguns módulos, como, por exemplo, o Enterprise, Mobile e ICS. Então Enterprise sendo Windows, Mac OS, Linux e Cloud, Mobile, Android e IOS, e ICS, que é Sistema de Controle Industrial.

Como que funciona aqui as etapas do comando e controle? Então tem toda a parte de coleta de informações do alvo, fazer todo o mapeamento do comprometimento da rede interna, escalar privilégios. Então se você não tem um privilégio de super admin, você só tem de system. Você consegue ir escalando os privilégios. Captura de credenciais, tanto em texto em claro, ou o hash dessas credenciais. A manutenção desse acesso, como eu comentei para vocês. Vocês conseguem fazer uma persistência no backdoor, que, mesmo que reinicie a máquina vocês conseguem manter acesso à comunicação com o Command & Control, não perde o agente. Pivoteamento. Movimento lateral. Comprometer outros serviços e sistemas. E um ponto que a gente quer chegar, que é estabelecer um canal de comando e controle. E, por fim, as ações como exfiltração de dados.

Algumas características do Command & Control, uma comunicação assíncrona. Então o meu servidor mandou o comando para o agente, que é a vítima, não é de imediato. Acontece você depois de... você pode programar quantos segundos esse seu agente pode dar uma resposta. A linguagem de programação utilizada no framework, que a gente vai ver também na parte prática. Canal de comunicação, quais são os protocolos. O Beacon, que vocês vão ver mais para frente, que é o default delay na plataforma, na ferramenta que a gente vai utilizar. E o default delay é a quantidade de vezes que o agente vai perguntar para o servidor se ele tem algo a fazer. O Jitter é a variação do Beacon, que é o default delay. Então o Jitter, ele vai ter uma porcentagem de variação para menos ou para mais que você pode definir.

Agentes. Quais são os sistemas operacionais que são suportados. Os agentes podem ter ou não um kill date, tipo uma data de validade. Suporte na comunidade ativa. Interface de utilização, mais utilizada linha de comando, mas também tem a GUI.

A ferramenta que a gente vai utilizar para a nossa parte prática vai ser o Empire, que é uma ferramenta de pós-exploração, um PowerShell puro. Então a gente tem capacidade de executar alguns agentes sem precisar rodar mesmo o PowerShell.exe. E tem outras funcionalidades, alguns componentes que a gente vai ver mais para frente. Mas tem uma aqui que eu quero comentar para vocês, que quando a gente ouvir sobre servidor de controle a gente fala em listener, e no caso aqui é escrito em Python3, e nossos agentes, que são as vítimas, estão escritos em PowerShell.

E nós temos o assincronismo de comando e de resposta enviada pelo servidor e agente. Um desenhinho aqui como que vai ficar no final. Então tem de um lado o atacante, que é o listener, que ele utiliza módulos para poder criar essas conexões e mandar comandos para esse agente, que é o stager ou o launcher, como vocês podem ver que é o alvo do lado direito.

Pois bem. Vamos dar início à nossa parte prática do tutorial de Command & Control. Eu queria só fazer um resumo antes de começar a falar, que quando eu estiver falando sobre listener eu estou falando sobre o servidor, o atacante em si, e quando eu estou falando de stager, ou agente em si, eu estou falando desse agente, da vítima, que está instalada na máquina da vítima. No caso, o listener é o meu Kali Linux, e o agente, ou loucher, vai ser o meu Windows 10, que vai ser a vítima. Então esse laboratório que eu preparei para vocês eu estou utilizando a ferramenta Empire. Nesse caso, a gente vai ter uma simulação de um atacante dentro da rede. Então se você não fez o investimento devido com segurança, ou até mesmo investiu com firewall, e esse atacante, ele conseguiu ter acesso a sua rede, ele começa a comandar, a ter controle sobre as suas máquinas, o perímetro já passou. Então você já tem um ponto de falha, um ponto de brecha que só algumas ferramentas são capazes de detectar. Então, por exemplo, aquela ferramenta que eu mostrei para vocês na última demonstração, que é Umbrella, que atua na camada de DNS. Então assim que tiver uma requisição, clicou no link malicioso, que vai instalar o Malware ou um software que vai controlar, esse agente ser instalado na máquina, você já consegue bloquear ali mesmo. Mas se em algum momento, algum ponto da segurança da sua rede falhou, e esse atacante conseguiu se implantar na sua rede, essa vai ser simulação que eu estou fazendo agora. Mas no final eu vou dar simulação do exemplo mais comum que acontece.

Então deixa aqui a página inicial do Empire. Eu só vou... vocês podem observar que não tem nenhum listener, nenhum servidor e nenhum agente instalado. Então a gente vai instalar juntos. Então userlistener. Eu vou utilizar o mais comum, http, dou um info, e ele vai me mostrar quais são os valores que eu preciso preencher no atacner(F). Isso pensando a visão do atacante. Então eu vou precisar setar qual o nome do listener. Qual é o endereço, ele já pegou que é o meu, é o final 125, que é o meu Kali. Qual a porta que eu

vou utilizar. O [ininteligível], que é responsável por essa troca de chave entre servidor e o agente. Default delay são os... a gente começa a falar de Beacon. Então o agente, ele vai ficar perguntando em um em um segundo para o servidor se ele tem alguma coisa a fazer ou não. O Default Jitter, ele é uma porcentagem que você pode utilizar, tanto de 0.0 até 1.0, que condiz a 100% de variação. Então em cima do default delay, então a cada um segundo esse agente vai me perguntar se tem alguma coisa para fazer. Esse DefaultJitter, ele vai, por exemplo, 20% ele vai variar a mais ou a menos para que seja mais difícil de detectar, seja mais stealth. Default Profile vai ser alguns comandos, as comunicações que ele vai fazer, como admin, get.PHP, para tentar disfarçar esse processo. Eu acredito que só.

Vamos começar setando um nome aqui para o meu listener, que vai ser o servidor. Vou deixar como listener1. Eu vou setar o valor da porta, que vai ser 80. O default delay eu não vou alterar, porque já está um segundo, já está ideal, então assim que fizer alguma alteração. Eu posso até setar como dois segundos porque vai ter um teste final que vai sair uma música e eu quero que vocês acompanhem e dê tempo de ver. Então default delay, eu vou deixar dois segundos. Jitter eu posso colocar, por exemplo, 10%. Então 10%. Opa. E o [ininteligível], eu vou setar o [ininteligível], que é a chave de comunicação desse meu agente com o servidor. Então se você não souber qual que é a senha, então você pode colocar a senha secreta e ele vai cuspir na tela qual o hash MD5 dessa senha. Então eu copio e dou um set staging de novo, e colo o hash MD5. Dou um enter e um execute. Ele vai gerar esse listener. Ele foi criado, já foi startado com sucesso.

Então eu vou para página principal, digito main. Já percebam que aqui já foi criado um listener. Então eu tenho um servidor para gerar esses comandos, essa comunicação. Agora eu vou criar o agente. Então user stager. Opa. Eu vou utilizar o multi launcher, então multi launcher. Vou digitar info, ele vai me dar as informações que eu preciso setar na coluna de required. Tudo que é true eu preciso informar qual que é o nome do meu listener, desse servidor que vou buscar. Qual a linguagem que eu vou utilizar, se é PowerShell, se é Python. Vai ser codificado em base64, e safe check(F) não preciso alterar. Então a única coisa que eu setaria, que já está setado, mas eu vou fazer para que vocês entendam, set Listener Listener 1. E agora eu dou um comando de generate. Ele vai me gerar esse código gigante aqui em base64, que eu copio e eu vou agora para a minha máquina Windows. Então eu vou para o Windows aqui, abri o PowerShell, lado direito vou colar esse comando, dou um enter. Volto para minha máquina do Kali. E esse agente, ele foi criado, então o nome dele é QNEYM5R7, com IP final 124. Então ele já está pronto para que eu possa brincar, mandar alguns comandos para ele.

Então página principal, em agents, ele vai mostrar aqui o agente. Então eu não vou alterar o nome do agente. Então eu vou pegar, eu tenho essas opções de comandos que eu posso utilizar. Então eu posso dar um kill, um kill date. Eu não falei de kill date para vocês, mas é como se fosse um prazo de validade desse agente. Ele pode ter, eu não quis colocar. Eu posso dar o Interact, que é o que a gente vai fazer. Então eu vou dar um interact. O meu agente. Digito usemodule. E no usemodule ele vai me dar um monte de comandos que posso tentar coletar dados, imputar dados nessa minha vítima. Então eu vou pegar aqui um [ininteligível]. Deixa eu só pegar aqui qual que é [ininteligível]. Você copia qual que é o módulo que você quer utilizar para fazer essa coleta de informações, vai lá embaixo em usemodule, cola esse módulo. Eu já tenho acesso a ele. Digito info. Ele vai me mostrar que tipo de informações são requeridas para poder rodar esse comando, esse modo. Então preciso de acesso de admin? Não, é mentira. OpsecSafe? Isso vai gerar algum alerta para o meu usuário final, lá para [ininteligível] minha vítima? Ele é totalmente safe. Então se estiver true, aqui não vai gerar nenhum alarme, nenhum alerta na máquina. E o que eu preciso para rodar esse comando? Preciso que tenha um agente ativo. Então eu já tenho esse agente, que é o KNE(F) que eu falei para vocês. Então eu simplesmente posso dar um execute. E ele começou a executar.

Ele vai começar a me mostrar mais informações da máquina Windows, que ela está com username suporte. Últimas mudanças, grupo de AD, regras de firewall vai aparecer aqui também. Então eu vou deixar ele carregando aqui do lado.

Dar um main(F) para atualizar e acessar agents aqui de novo, interact. Opa. Interact, meu agente. Deixa eu ver se já carregou aqui o comando. Carregou. Então vocês podem perceber que é bastante informações que esse comando, esse módulo que eu utilizei, ele me traz. Então regras de firewall, se é permitido, qual porta que é permitido, bastante informações que na mão de um atacante é ouro. Vale ouro. Ele tem o seu ambiente na mão dele. Todas essas informações aqui ele tem acesso. Então eu vou cancelar aqui. Vou dar um back em usemodule. Existe um comando que eu vou mostrar aqui para vocês, só para ver a interação que você pode mandar input, eu posso mandar, daqui do meu Kali Linux, eu posso mandar aqui no Windows 10, que ele faça logoff, que ele restart, ou até mesmo que peça um... ele bloqueia a tela. Eu posso mandar vários inputs e posso coletar dados também. Então eu vou mandar um imputo de troll, então vai aparecer no PowerShell como se fosse um cara dançando e tocando uma música de fundo. Então eu espero que vocês escutem essa música. Então colei aqui, como eu pego aqui mais informações sobre esse módulo, preciso de acesso de admin é falso. E OpsecSafe agora não é mais true, é falso. O que isso quer dizer? Que vai me gerar alarme na ponta da minha máquina da vítima. Então na hora que eu rodar esse script a pessoa vai detectar que tem algo de errado. Então ele vai me perguntar aqui se eu desejo continuar na hora que eu der um execute. Então esse módulo não é OpsecSafe. Você quer rodar mesmo assim? Eu vou rodar. Deixa eu só preparar aqui a minha máquina do Windows. Certinho. Eu vou dar um enter. E alterno para o Windows.

Eu digitei um Q(F) aqui para sair, então tudo bem. Fechou aqui certinho. E eu consigo ver tanto aquele início da conexão, vou até mostrar aqui para vocês, bem aqui atrás. Ele gera, não sei se vai estar mais aqui, mas acho que dá para pegar outro PID(F) dele. Deixa dar um enter. O ID do processo da tarefa que criou foi o número 2. Então tudo isso você consegue ir pesquisando aqui dentro da máquina Windows. [ininteligível]. Então você pode pesquisar pelo PID(F), se você tiver. Nesse caso aqui, eu tinha que ter mostrado na hora que criou o agente. Na hora que cria aquele agente, que você cola aquele script no PowerShell, ele gera um PID que você pode pesquisar nesse process(F) hacker para identificar o processo por ali também.

Voltando aqui para o Kali. Pois bem, então essa forma que eu expliquei para vocês é como funciona a visão do hacker, tentando manipular essas vítimas, essas máquinas que estão infectadas com agentes nas suas máquinas. E tem outra forma que você também pode receber o e-mail, até simulei aqui um e-mail de boleto vencido dizendo que "não foi identificado o pagamento", para que evitar ser enviado para o Serasa, ele dá opção de atualizar o boleto e pagar em qualquer instituição. Na hora que eu clico, ele me direciona para uma máquina maliciosa. Então se eu não tenho uma proteção a nível da que tenho aqui em casa, que é na camada de DNS, que ela atua na requisição, então ela já fez o bloqueio assim que eu fiz requisição, que eu cliquei nesse link, ele já bloqueou o meu acesso.

Então eu vou acessar aqui para mostrar para vocês como que fica nos relatórios, e como que eu faço para configurar, para bloquear Command & Control. Então, enquanto abre aqui, só para falar para vocês que vale a pena investir em ferramentas que protejam o seu perímetro, todos os trechos, todas as zonas da sua rede. Mas é importante que vocês tenham também uma solução que proteja quando esse ataque acontecer, quando essa invasão acontecer, que você tenha ferramentas para detectar. O que se chama a pós-exploração. Então o indivíduo, ele conseguiu se apossar do seu ambiente, da sua rede, da sua

máquina, do seu ativo, enfim, e você consegue detectá-lo mesmo assim, mesmo depois de ter passado por todos seus perímetros e suas zonas de segurança.

Então aqui, logo na página inicial do Umbrella, ele aparece como Command & Control, três requisições, eu posso clicar em view trend, mas eu vou clicar em reporting. Pronto, carregou. Em reporting, Activity Search, clico em block, apply. E a requisição do endereço para atualizar o boleto que eu recebi com destino para essa URL, a minha identidade é essa mesma aqui, o IP é do Kali Linux com destino a esse IP que aparece aqui. Então eu vou arrastar mais para o lado, e foi bloqueada essa requisição porque é um Command & Control. E o horário e a data de hoje, 3 de agosto, à 0h29min. Então se eu for aqui em policies, DNS policies, mostrar para vocês como é simples fazer o bloqueio. Na regra que eu estou passando, que estou dando o match, que é Casa SP, dou um edit. E se eu clicar aqui em edit de novo, consigo bloquear apenas clicando... dando um check box, eu consigo bloquear contra Malware, domínios novos que foram visto, Command & Control, chamadas Callbacks, ou C2, Phishing Attacks, DNS dinâmico, domínios prejudiciais, até mesmo tentativa de exfiltração de dados através do DNS [ininteligível], VPN e cryptomining, que faz parte da última aula prática que eu passei para vocês sobre cryptomining. Tudo isso só dando check box aqui, marcando e desmarcando, eu consigo proteger instantaneamente. Espero que vocês tenham gostado. Até a próxima.

Dando início ao módulo de DDoS. Então a gente vai entender um pouquinho quais são as diferenças do DoS para o DDoS. Então basicamente no DoS, que é o Denial of Service, ou negação de serviço, a gente tem uma técnica utilizada pelo atacante para poder deixar esse... tirar esse serviço de operação. Então a gente pode utilizar um computador, um roteador ou uma rede. Como que funciona no ataque DoS? Então você tem no exemplo: eu, Josiane, estou fazendo um ataque direcionado para deixar esse serviço fora. E só a Josiane fazendo essa operação para poder tirar esse serviço do ar. Com o DDoS, que é o Distributed Denial of Service, que é negação de serviço distribuído, a gente tem uma técnica utilizada diferente, que ela é feita de uma forma coordenada e distribuída. Então a gente, ao invés de ter só a Josiane fazendo aquele tipo de operação, aquele ataque, eu tenho um conjunto de computadores botnets trabalhando para poder tirar esse serviço do ar.

Então o nosso objetivo aqui, o objetivo desse ataque é esgotar totalmente, ou exaurir os recursos, as aplicações e serviços da rede, fazendo com que esse tráfego e esse usuário que estejam utilizando esse tipo de serviço, que seja legítimo, não consiga acessar esse serviço. Então a gente tem principais alvos, como, por exemplo, servidores de jogos, bancos, governo, partidos políticos, entre outros. E todos nós estamos sujeitos a sofrer esse tipo de ataque. Então pode ser um ataque direcionado a um, um exemplo, você tem o seu vizinho da frente, ele tem costume de colocar música alta no final de semana, e você sabe que ele utiliza um roteador para poder acessar a Internet e colocar aquele tipo de música. Então você decide enviar, inundar de pacotes TCP aquele roteador até uma hora que não consiga mais suportar, e o roteador acaba crashando, e ele acaba travando, e ele, para poder retornar ao serviço, a operação desse roteador, a pessoa vai ter que desligar e ligar de novo. Então esse é um ataque DoS. O DDoS você tem mais de uma pessoa atuando para poder complementar, completar com sucesso esse ataque.

Então tem uma observação que eu deixei aqui na apresentação que muitas pessoas confundem com invasão. Então Denial of Service ou Distributed Denial of Service, ele atinge, principalmente, ele fere principalmente aquele pilar que eu mostrei para vocês no começo da apresentação lá no início, que é a disponibilidade, então ele fere a disponibilidade.

E alguns tipos de motivação, a gente tem um hacktivismo. Então a junção de um hacker com ativismo, hack com ativismo. Uma forma de protesto para promover suas ideologias, enfim.

A Lei de Talião, "olho por olho, dente por dente". Então se você sofreu um ataque de DoS, DDoS, e você descobre por... às vezes, você acabou descobrindo que determinada empresa fez aquilo, utilizou tal recurso e você quer utilizar da mesma arma para poder dar o troco na mesma moeda. Então existe essa possibilidade também.

Script Kidies, talvez vocês não tenham ouvido falar, mas é o termo dado às pessoas inexperientes que praticam atividades semelhantes às de hackers. Então essas pessoas, elas ficam rodando comandos, comandos, comandos sem saber o que fazem e acabam, ou acontecendo algumas tragédias, de por um acidente alguns desses scripts que elas rodarem acabar realmente tirando do ar, ou alguma coisa sai do padrão, sai dos trilhos e dá errado.

Concorrência desleal. Às vezes um novo service provider abriu perto de vocês, enfim, um exemplo, e por ele não ser tão próximo e não manter os preços abaixo do acordado, ou no mesmo patamar acordado pelos ISPs da região, então ele se torna um alvo, uma concorrência desleal onde os services providers antigos tomam essa decisão de fazer um ataque DDoS para o service provider novo para que ele tenha indisponibilidade de seus serviços ofertados.

E alguns impactos, como, por exemplo, serviços e recursos legítimos que ficam indisponíveis, como comentei. Perda de credibilidade do seu cliente, o que seu cliente vai pensar da entrega, do valor dos seus serviços, sendo que você, num determinado momento, durante esse ataque à disponibilidade, você não tem uma abordagem, uma largura de banda maior para poder suportar esse tipo de ataque. E backup, se você não tem nenhum backup, ou você pode ter problemas para restaurar esse backup durante um ataque desses, então isso vai ocasionar em aumento dos custos. Então, às vezes, a gente se depara com uma situação que é muito comum no Brasil, muito comum o brasileiro, a gente bota a mão no bolso depois que já aconteceu alguma coisa. Aquela velha história, não adianta chorar pelo leite derramado. Então o brasileiro é bem assim, ele tem que apanhar para poder tomar uma ação.

Tipos de ataque. A gente tem três tipos de ataques aqui, que é o primeiro que é volumétrico, o segundo que é na camada de aplicação, e o terceiro que é exaustão de recursos de hardware. Então uma observação que eu deixei aqui que podem ser usados isoladamente, ou até mesmo em conjunto, em conjunto é bem mais efetivo. O ataque DDoS volumétrico, ele tem como função, como intuito, exaurir a banda disponível. Então ele envia para esse alvo um grande volume de tráfego, e eles utilizam meios, e esses meios são botnets, máquinas com bastante banda, ou até mesmo pouca banda. Então essa negação distribuída(F) de serviço com o uso de amplificação é um tipo de ataque volumétrico que explora características e protocolos da Internet. Então a gente tem um exemplo aí, que é o DRDoS, Distributed Reflective Denial of Service como exemplo disso, que utiliza táticas de IP forjados, spoofados(F) para que os pacotes amplificados sejam direcionados para o alvo do ataque.

E, na camada de aplicação, mais difícil de serem detectados, porque podem ser confundidos com alguns problemas de implementação dessa aplicação, diferente do volumétrico, não precisam de muitas máquinas, nem de muito tráfego para ser utilizado e exploram as características de aplicação, ou Layer set. Então tem alguns exemplos de táticas que são utilizadas através do HTTP Flood, VoIP (SIP Invite Flood), Slow Read DDoS. O HTTP Flood, ele é um tipo de ataque de negação de serviço distribuído no qual o invasor, ele manipula essas solicitações indesejadas de http gate(F) e post para atacar esse servidor ou aplicativo da Web.

E exaustão de recursos de hardware. Então a gente tem os ataques de exaustão de recursos de hardware, que tem como o intuito consumir o máximo da capacidade dos equipamentos e também esgotar esses recursos desses equipamentos. Ao fazer esse direcionamento aos roteadores a gente pode tentar consumir esses recursos como CPU, memória, capacidade de encaminhamento de pacotes por segundo, e em firewall, e na verdade IPS, Intrusion Prevention System, a gente pode tentar consumir também a capacidade da tabela de estado de conexões.

Então a gente tem exemplos que eu deixei para vocês, como fragmentação, TCP Syn Flood. E um ataque de inundação TCP Syn Flood ocorre quando o invasor inunda o sistema com solicitações Syn a fim de sobrecarregar o destino e torná-lo incapaz de responder às novas solicitações, e as de conexão, ou tráfego legítimo.

E algumas formas de detecção, então sempre validar os fluxos de saída e entrada de tráfego. Através dos flows é muito importante, vocês conseguem detectar esse tipo de comportamento. Existem soluções dedicadas para proteção, para mitigação de DDoS, onde você pode aumentar uma largura de banda de mitigação. Então até mesmo da Cisco a gente tem alguns dispositivos que trabalham em conjunto com outros fabricantes que são totalmente integráveis. Essas mudanças de comportamento são detectadas por soluções que analisam esse fluxo, esse netflow, esse flow, e consegue detectar um padrão, e quando tiver uma anormalidade ele consegue detectar. E você consegue mitigar ou jogar fora esse fluxo ruim e deixar somente o legítimo.

Callbacks. Existem também algumas plataformas que eu já mostrei para vocês nas outras demonstrações que também você consegue bloquear essas Callbacks ou Command & Controls também.

Intrusion Deteccion/Protection. Aqui também. IDS/IPS, a gente tem, você pode aplicar uma camada a mais, seja a partir de detecção e proteção, com firewalls de próxima geração, antivírus, antimalware. Tudo isso vai poder ajudar ainda mais a deixar o seu ambiente mais seguro.

E deixo por último a utilização de honeypots, que tem o intuito e a função de simular falhas de segurança. Então é basicamente uma armadilha. Então o atacante, ele acha que está possuindo acesso à sua rede, que ele está conseguindo te atacar. Mas, na verdade, é um ambiente de teste, onde você vai testar e vai conhecer quais são os comandos que esse atacante está jogando, quais são as ferramentas que ele está utilizando no seu ambiente, e tudo isso é apartado do seu ambiente real, do ambiente corporativo e de produção. Então fica mais fácil mitigar antes que ele chegue na sua rede principal.

E é isso. Eu gostaria de deixar aberto para perguntas. Gostaria de agradecer muito a NIC.br, a Cisco e a ScanSource pela oportunidade de poder estar conversando com vocês passando essa mensagem, eu espero que vocês tenham gostado do conteúdo, e é isso.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Josi. Realmente tudo que você falou foi muito interessante para os provedores.

Antes da gente ir para a parte de perguntas, pessoal, que a Josi vai estar aqui ao vivo com a gente respondendo as dúvidas que vocês vão colocando lá no chat do YouTube. Então, está com alguma dúvida? Escreve lá que a gente já vai chamar a Josi para responder. Eu queria dar alguns avisos. Primeiro deles é com relação ao certificado. Até às 2 horas da tarde você pode se inscrever para ganhar o certificado dessa live. Então basta ali acessar o link que a gente está colocando agora no chat do YouTube, se inscreve que você ganha o certificado dessa live.

A outra coisa que eu gostaria de ressaltar é sobre o formulário de avaliação. Esse é um formulário simples, tá? São duas perguntinhas. Uma é uma nota para live. A outra é o que a gente pode melhorar. Novamente, a gente pede para vocês escreverem porque a gente tem uma semana inteira, cheia de conteúdos, e o que a gente pode ir fazendo ao longo dos outros dias ou para outros eventos futuros, né? Se vocês gostarem bastante da Semana de Capacitação On-line a gente pode pensar em fazer outros e outras vezes. Então eu estou pedindo para o pessoal do NIC colocar ali o formulário de avaliação, colocar o QR Code para vocês irem preenchendo e eu já vou chamar Josi para responder.

Antes da Josi falar, eu queria também chamar o Adalberto, afinal, Adalberto, a gente falou que ia ser um dos palestrantes, mas até agora não apareceu. Ele está escondido dentro do Zoom, do Zoom, na verdade, da nossa transmissão, e a gente gostaria de ouvir um pouquinho o Adalberto falando. Adalberto, pode comentar um pouquinho?

SR. ADALBERTO LINS: Claro, pessoal. Bom dia a todos, de novo. Primeira coisa que eu quero fazer é agradecer ao pessoal do NIC pela parceria e pela paciência com a Cisco nos últimos três anos de parceria que nós fizemos, aí durante os fóruns regionais e etc. Antonio Moreiras, Eduardo Morales, Erina, Tiago Jun, e todo pessoal de back office que está ajudando nessa transmissão. E parabenizar principalmente porque, pessoal, só quem acompanhou de perto o começo da idealização desse evento no ano passado. Obrigado pelo convite em dezembro, que foi feito para Cisco e para ScanSource para esse evento. Mas só quem acompanhou de perto sabe o quanto que o NIC trabalhou e o quanto que foi discutido para essa remodelação e adequação à pandemia, e mudança de formato. Pessoal, foi realmente algo, assim, homérico e digno de muitos aplausos para o pessoal do NIC. E ficou excelente.

Do lado da ScanSource, agradecer à Leni pelo apoio [ininteligível]. Josiane, hoje foi teu dia, foi show! Realmente o pódio hoje foi todo teu, está totalmente de parabéns. Mas é importante ressaltar que esse treinamento foi feito com base no material Cisco, mas tem muito conteúdo didático e tutorial independente de plataforma. Esse foi o objetivo inicial desse tutorial, e foi feito com louvor. Teve até uma certa discussão ali no chat. É claro que a ferramenta de teste fez parte do tutorial e é o que a gente tem de mais fácil. Por que foi escolhido Umbrella? Porque ele é muito fácil de demonstrar e muito fácil de manusear. Acho que essa é a primeira coisa e mais importante nesse caso. Teve bastante discussão ali de onde ele é aplicável ou não. Eu não quero tratar isso aqui, não é o nosso interesse. O importante aqui foi realmente a parte do tutorial e mostrar para vocês que tem ferramentas e não é só ferramentas Cisco, tem várias ferramentas no mercado. É claro que o conteúdo de academia Cisco, Net Academy, segurança e tudo mais é bastante grande.

Pessoal, eu quero passar a palavra agora para a Josi. Josi, parabéns.

[aplausos]

SR. ADALBERTO LINS: Foi bastante importante e amei o conteúdo, amei a maneira como foi adaptada e como você passou para esse público, o trabalho que você e o [ininteligível] fizeram para transmitir a ideia, para adequar a ideia para esse público nosso de provedor. Foi muito bom, parabéns.

SR. EDUARDO BARASAL MORALES: Adalberto, antes de chamar a Josi, teve um comentário do pessoal voltado para a Cisco, se pode dar voucher da Umbrella.

[risos]

SR. ADALBERTO LINS: É, do voucher a gente pode verificar, eu até comentei no nosso chat interno que isso é uma ideia bastante interessante. Mas, pessoal, no site onde tem [ininteligível] produto na Cisco Umbrella, você pode, primeiro, ter a versão free para usuário doméstico, que é um pouco mais limitado. E se você quiser dar uma experimentada nas ferramentas todas, tem uma versão de trial, então o voucher/trial, a diferença é basicamente é o tempo que você consegue ficar degustando ali e testando a brincadeira. Mas já está anotado já, e a gente vai ver isso internamente.

Uma outra coisa importante. As operadoras estão colocando essa solução, inclusive aqui no Brasil, e essa solução de Umbrella, de DNS faz parte do Switch de segurança da Cisco, e está incluso em vários equipamentos, como, por exemplo, SD one, solução corporativa de SVA, SV One ou de UTM fornecido para pequenas ou grandes empresas também de UTM, tem o Umbrella lá dentro, apesar dele ser um produto separado, ele está embarcado em várias soluções da Cisco e pode ser conjugado com outras soluções não Cisco também. Então é só um spoiler, desculpa, sei que não é nosso objetivo hoje. Mas já que o pessoal comentou de licença, eu vi que teve bastante calor ali no chat sobre isso. Se vocês quiserem, depois, podem entrar em contato comigo no LinkedIn ou pelo e-mail direto, adalberto@cisco.com, ou pela própria Josi, que a gente pode tentar ajudar aqui vocês o máximo possível.

SR. EDUARDO BARASAL MORALES: Obrigado, Adalberto. Pessoal está me avisando aqui que vai colocar o QR Code de novo no formulário de avaliação, pessoal. Por favor, preencham esse QR Code, preencham o formulário. A gente tinha colocado anteriormente, mas o link não estava certo, agora o link vai estar. Por favor, nos ajudem dando um feedback do que vocês acharam da nossa transmissão.

Enquanto isso, eu vou preparando a Josi. Muito obrigado novamente ali por tudo que você fez ali nesse tutorial, realmente foi muito bom. E eu já vou começar falando das perguntas que o pessoal mandou. Então teve uma pergunta: "Você ainda tem esse canal no YouTube que você citou com os vídeos de segurança?". Então pode falar um pouquinho do [ininteligível] mandou.

SRA. JOSIANE DE BARROS SILVA: Oi, pessoal. Bom dia para vocês. Vocês estão firmes e fortes aí esperando pelas perguntas, pelas respostas agora dessas perguntas. Respondendo agora o Binari(F). Tenho ainda o YouTube, só que ele está meio que desatualizado. Tenho que atualizar ele, mas recentemente eu vou atualizar, prometo para vocês. Deixa até mudar para cá, eu mandei no chat para vocês do YouTube um link dele, se vocês quiserem me seguir, quiserem se registrar também podem, fiquem à vontade. Não é nenhuma obrigação. E mais para frente eu vou postar mais conteúdo dentro desse canal.

Mas a respeito ao conteúdo que eu estava ajudando outras pessoas durante a certificação que eu comentei que é o Fire Jumper Elite, especificamente é dentro de uma plataforma da Cisco, Cisco Community, onde várias pessoas têm dúvida de, tanto da parte [ininteligível] Switch, Wi-Fi, colaboração, Data Center, segurança, enfim, todo mundo tem dúvida, então você pode ajudar e colaborar para tirar essas dúvidas. Então eu ajudei muito para poder passar nesse exame final dessa certificação, você precisava estar ativa nessa comunidade e responder todas essas perguntas.

SR. EDUARDO BARASAL MORALES: Muito bom. Vamos para próxima pergunta, do Júlio César: "No caso, quando há um sequestro no AS todos os domínios dele têm suas informações roubadas?".

SRA. JOSIANE DE BARROS SILVA: Quando é informado esse número, tudo é direcionado, no caso, para esse atacante, ele vai direcionar esse fluxo, esse tráfego para esse atacante, e ele pode... O que ele pode fazer? Ele pode fazer o decryption desse tráfego [ininteligível]. No caso que eu dei foi umas empresas no ramo financeiro. Então se você tem cartões de crédito, processamento de cartão de crédito, se você envia

esse tráfego tudo para esse atacante, o que acontece? Ele pode fazer um decryption desse tráfego e começar a pegar esses dados dentro desse tráfego. Tem esse risco, mas você pode alarmar isso para as autoridades, enfim, entre aspas, e conseguir reverter essa situação. Mas esse é o risco que você corre tendo esse fluxo, esse tráfego sendo direcionado.

SR. EDUARDO BARASAL MORALES: Bom, tem uma outra pergunta aqui da Vanessa Melo. Ela está acho que comentando da parte da Umbrella, se essa tela da Cisco que você estava mostrando, ela é aberta ou era produto pago. Se você puder comentar um pouquinho.

SRA. JOSIANE DE BARROS SILVA: Legal, Vanessa. Como funciona? Até o Adalberto, ele já adiantou que as ferramentas que eu utilizei, algumas são Cisco, na verdade, dando um spoiler, são todas, as três que eu tenho aqui são Cisco. Mas não necessariamente você precisa ter um equipamento Cisco, a gente está fazendo o treinamento mais voltado para service provider. Mas se você é um usuário final e pretende aumentar mais a segurança dentro do seu ambiente pode utilizar também. Tem versão do Umbrella totalmente gratuita, que é Umbrella home. Até [interrupção no áudio] também o licenciamento que é mais voltado para organização como um todo e também para service provider, isso eu não vou entrar em detalhes, porque não cabe aqui dentro do nosso treinamento. Mas se vocês tiverem interesse, eu posso explicar mais a fundo para vocês. Mas essa tela que eu mostrei para vocês é do Umbrella corporativo. Então tem uma licença, sim.

SR. EDUARDO BARASAL MORALES: É, deu uma travadinha, Josi. Você quer complementar um pouquinho?

SRA. JOSIANE DE BARROS SILVA: Ah, então, desculpa. Deixa eu falar de novo. Então se você tem... a gente está voltando o treinamento para service provider. Existe o treinamento focado para service provider do Umbrella. Mas não necessariamente você, usuário final, quer proteger o seu acesso à Internet da sua casa, por exemplo, da sua residência, e você quer proteger com Umbrella, você tem uma versão gratuita, que ela é mais básica, possui alguns recursos de customização, de controle de conteúdo através do DNS. Mas também existe esse que eu mostrei na apresentação que é o corporativo, que possui uma assinatura, uma licença. Esse que eu mostrei, ele é pago.

SR. EDUARDO BARASAL MORALES: Ah, muito bom. Obrigado.

Vamos lá para a próxima pergunta. Teve do Eric Rainer(F): "Já se nota a preocupação da proteção a dados de usuários especificamente motivado pela LGPD?". Pode comentar?

SRA. JOSIANE DE BARROS SILVA: Claro. A gente está nesse impasse da LGPD. Muitas pessoas falam: "Ah, mas se eu for seguir o que está falando só vai começar a entrar em vigor em maio". Mas se isso muda em um passar de tempo, em piscar de olhos, daqui dois meses vai entrar em vigor, como você consegue ter esse ambiente preparado? Você já aplicou as configurações mínimas? Porque quando vier a valer essa lei você vai ter que enviar relatórios de que você, por exemplo, se tiver incidente, você vai ter que ter uma ferramenta para enviar esse relatório para informar como que foi. Até que ponto você conseguiu proteger esse ambiente, porque as autoridades, elas vão cobrar isso. Existem também peritos, não sei se vocês ficaram sabendo. Existem peritos que incidentes ou até mesmo uma periodicidade, eles podem checar se existe mesmo esses controles de segurança aplicadas à privacidade dos dados. Então até mesmo o seu usuário, o seu usuário final, ou até mesmo o seu fornecedor, eles descobrem que tem um vazamento de dados. Você está preparado? Nem falando de segurança ainda, você está preparado para receber, por exemplo, uma... o seu call center, o pessoal do atendimento, o seu SAC, ele está preparado para receber essas ligações dos seus usuários? As pessoas que têm os dados pessoais vazados, para poder fazer esse

atendimento e solucionar o problema deles? Então não é questão somente de segurança, tem que pensar na infraestrutura como um todo para estar preparado para Lei Geral de Proteção de Dados. E se você não correu atrás, corra, porque a qualquer momento eles podem... Está um vai e vem dessa lei. Uma hora fala que vai entrar nesse ano, outra fala que vai entrar no ano que vem. Então a gente está muito à mercê deles. Então é importante que vocês não deixem para fazer isso fazer essa... meu Deus, fugiu a palavra. Fugiu a palavra, enfim, em cima da hora. Então é bom que vocês corram, já vão adiantando esse processo de adequação LGPD antes mesmo de ela entrar em vigor.

SR. EDUARDO BARASAL MORALES: Legal.

Vamos para a próxima, do Nilson Bandeira: "Não existe uma forma de inibirmos essas buscas com programas maliciosos para buscar as portas abertas sobre os IPs válidos?". E ele até comenta que aconteceu com roteadores TP-Link recentemente.

SRA. JOSIANE DE BARROS SILVA: Legal. Essa foi a pergunta do Nilson, né? Perfeito. Então, existe, sim, outras formas. Não quer dizer que essa demonstração que eu fiz para vocês que tudo é uma bala de prata, uma única caixa, uma única coisa vai resolver todos os problemas de segurança. Não vai. Então esse é um dos procedimentos, uma das ferramentas que utilizei para poder mitigar. Existem outras ferramentas, como, por exemplo, firewall, que ele faz aquele papel também de DMZ que eu comentei no início e ele pode fazer o controle também por portas abertas sobre IPs válidos, como o Nilson comentou. Então existem outras ferramentas que se complementam e ajudam a deixar mais forte essa camada de segurança do ambiente, do service provider, enfim, do usuário final que vocês estejam falando, ele ajuda a melhorar. Então em conjunto é muito melhor que apenas uma solução na camada de DNS, por exemplo, você pode ir agregando mais a sua rede, tá?

SR. EDUARDO BARASAL MORALES: Interessante. Tem agora alguns outros comentários, não é nem muito uma pergunta, tem uma do Marcelo Gondim, ele fala: "Esse é o grande problema de muitas CPEs desatualizadas, dessetadas com usuário e senha, padrão de fábrica de diversos fabricantes". Falando de CPEs virem coisas demarcadas, e a pessoa que compra, o provedor que compra nunca muda a senha, deixa sempre aquela senha padrão. Nesse caso dos CPEs o que a gente vê muito dos ataques é que tem ali os DNSs trocados, com objetivo de fazer um Hijacking. Queria, se você pudesse comentar esse comentário do Marcelo.

SRA. JOSIANE DE BARROS SILVA: Sim, não sei nem se posso comentar o nome de fabricante, porque, na verdade, eu estou aqui acompanhando o Adalberto, que é da Cisco. Mas [ininteligível] já acompanhei ataques desse nível, de DNS Hijacking, direcionamento. Eles conseguem, através dessa senha default alterar registros de DNS e direcioná-los para um DNS malicioso, do servidor do atacante. Então existe isso também. E importante, além da gente trocar essa senha, o seu login do acesso do roteador, do seu Switch, enfim, se vocês colocarem o duplo fator de autenticação. Porque mesmo que os seus usuários, vai, eles consigam acesso a sua senha, mas se você tiver duplo fator de autenticação, só realmente quem deve acessar vai conseguir acessar esse equipamento. Então é mais uma forma de garantir que realmente ele que está acessando.

SR. EDUARDO BARASAL MORALES: Ah, legal.

Vamos lá. Teve também ali um comentário do Gigabit Internet. Ele perguntou ali se vai ter um tutorial de instalação de algum servidor DNS. Eu já vou puxar o gancho que é para amanhã. A gente vai ter ali o pessoal da Icann explicando sobre servidor DNS Recursivo, sobre Hyperlocal. Então guarda ali para

amanhã. Tem até o material de pré-instalação. Então, se você quiser seguir o tutorado, fazer os comandos em conjunto, você precisa baixar a máquina virtual antes. Então entra lá no nosso site e já baixa a máquina virtual.

Mas vamos lá para uma outra pergunta, do Edson, do Cefet do Paraná. Sobre Cryptojacking, que ele ficou interessado: "Hoje existem celulares, tablets mais potentes que muitos desktops e notebooks. Esses hackers estão aumentando a área de atuação? Eles estão focando para todos os devices? Ou é só alguns em específico pensando no Cryptojacking?".

SRA. JOSIANE DE BARROS SILVA: Isso todos são afetados. Então se você acessa do seu desktop, do seu laptop, do seu dispositivo mobile, todo mundo pode sofrer, sim, com Cryptojacking. Não é específico para um tipo de hardware e um tipo de software, todo mundo pode sofrer com isso.

SR. EDUARDO BARASAL MORALES: É, afinal, o atacante, ele está interessado em ganhar dinheiro, não está interessado em saber qual é o dispositivo que você está usando, então ele está focando em vários.

Bom, outra pergunta aqui do Diego Sánchez: "Josiane, você está usando algum outro recurso da Umbrella? Fora configurar o DNS do Umbrella na sua máquina?".

SRA. JOSIANE DE BARROS SILVA: Como que funciona aqui? Então eu fiz o direcionamento do meu roteador, meu DNS externo para o DNS do Umbrella, e estou passando pelas políticas de DNS e categorização do Umbrella. E eu tenho outras soluções também que eu comentei aqui no chat. Que eu tenho o behavior analysis e também um TM. A princípio são tudo Cisco, só abrindo aqui, como eu trabalho especificamente com segurança e tenho alguns equipamentos de teste Cisco, então eu utilizei eles para poder fazer a demonstração. Não porque eu estou puxando sardinha para isso. Mas só para parte de teste do Kali Linux e do Windows eu utilizei somente o Umbrella.

SR. EDUARDO BARASAL MORALES: Legal, agora está vindo um monte de perguntas no chat, tentando acompanhar, mas está difícil. Mas tem até alguns que a gente pode até comentar da parte do NIC, do NIC.br. O Murilo Sérgio Rodrigues, ele pergunta: "Qual o curso de segurança da Cisco mais voltado para ISPs?" Só falar um pouquinho, eu já passo para você, Josiane, que você é expert nesse assunto. Mas na questão de segurança, a gente tem alguns cursinhos do Netacad, que a gente fez parceria com a Cisco, que está disponibilizado no nosso site dos cursos e eventos. Então, se você, por acaso, quer fazer esses cursinhos mais introdutórios pode se inscrever pelos cursos e eventos e fazer cursinhos do Netacad da Cisco. Mas assim, eles são introdutórios, tem cursos muito mais importantes sobre segurança, e eu gostaria que você comentasse um pouquinho sobre esse assunto.

SRA. JOSIANE DE BARROS SILVA: Eu acho que o Adalberto pode me ajudar também com relação à essa questão de certificação, alguns cursos. Porque a gente tem algumas plataformas que são restritas a parceiros. Não sei se tem algum curso, alguma certificação específica que pode ser utilizada para service provider. Se você puder comentar, Adalberto.

SR. ADALBERTO LINS: Tem sim, pessoal. Dentro do próprio Net Academy tem bastante conteúdo específico para service provider. E a gente está evoluindo também junto com o próprio NIC, e o NIC já é uma Net Academy específica para alguns assuntos da comunidade de service provider, e a gente está aumentando esse leque cada vez mais. O que o Eduardo comentou é bem pertinente, mas são cursos mais básicos e mais genéricos no momento, mas também interessantes para service provider iniciante e tudo mais. Agora, dentro do próprio Net Academy existem módulos mais avançados, até de coisas muito específicas de ISP, como, por exemplo, MPLS, VPLS, BGP para operadora. Então realmente o conteúdo dos

treinamentos são bastante completos, né? Estão disponíveis, sim. Vai ser uma questão de olhar e conversar com a Net Academy do coração de vocês mais próxima e verificar a disponibilidade dos cursos. Normalmente as Net Academys disponibilizam o treinamento sob demanda, além de terem as turmas abertas. Ou muito provavelmente a gente deve ter isso daí com mais facilidade nas Net Academy direto, mas temos disponível, sim.

SR. EDUARDO BARASAL MORALES: Ah, muito legal isso. Quem sabe a gente não consegue abrir esses outros cursos na parceria com a Cisco e a gente consiga distribuir mais informações de segurança, já que tem muita gente interessada.

Bom, tenho uma outra pergunta vindo do Leonardo [ininteligível] Lopes: "A implementação do RPKI ajuda na maioria desses ataques?". Bom, só comentar que a gente fez ali um tutorial ontem sobre RPKI, comentando dos ataques e falando um pouco da validação. Então não dá para solucionar todos os problemas de segurança com uma solução, tá? O RPKI, ele atua em uma parte, como tem outras soluções que atuam em outras partes.

Eu vou deixar a Josi responder, porque ela que é expert, ela até citou o RPKI no dia de hoje. Mas, assim, recomendo você assistir também o tutorial de ontem, lá a gente foca também são os ataques e explica como que você pode se proteger. Josi, por favor, comenta um pouquinho.

SRA. JOSIANE DE BARROS SILVA: Olha, essa pergunta eu deixaria para responder no privado, porque vai dar uma novela. Se você puder anotar quem foi que solicitou essa pergunta, a gente pode conversar depois também. Acho que vai dar... ter bastante tempo para conversar.

SR. EDUARDO BARASAL MORALES: É.

SR. ADALBERTO LINS: Pessoal, complementando, tem vários assuntos que dão pano para manga. E aproveitando o gancho agora da Josiane, tanto RPKI, como a parte de [ininteligível] service, monitoramento e detecção de ataque com Netflow, tem muito assunto. Tem realmente muito assunto. Acho que foge um pouco do escopo do que a gente está conversando aqui hoje. Mas estamos à disposição de vocês para os desdobramentos desse tutorial e ajudar vocês o máximo possível.

SR. EDUARDO BARASAL MORALES: Aquilo lá, inclusive o nosso tutorial ontem teve três horas e foi só sobre RPKI, não dá para gente falar tudo de RPKI nesse momento. Mas, assim, ele ajuda em alguns ataques, principalmente ali no roubo de prefixo, que é o que a gente cita mais no nosso tutorial, no vazamento de rotas. Mas eu recomendo que assista o dia anterior. E como eles falaram, eles também vão deixar aí o contato. Então se vocês quiserem tirar ali alguma dúvida, depois podem mandar mensagem para eles ali. Como eles disseram, eles vão mandar um monte de informação, espero que mandem nosso tutorial em conjunto.

Mas voltando ali. Eu acho que essa é uma pergunta mais até para o Adalberto, que veio aqui do Gilson Banini: "Existe alguma restrição de usar cliente do Umbrella em máquinas virtuais como Microsoft Azure, AWS, Google?". Então o pessoal está perguntando também muito de compatibilidade. Não sei se você quer comentar, Adalberto?

SR. ADALBERTO LINS: Bom, isso pode ser tanto eu quanto a Josi. O Umbrella, você tem diversas maneiras de você implementar. De novo, não é nosso objetivo aqui falar de produto só porque veio a pergunta. Mas, a princípio, para você utilizar o Umbrella, você apontou o DNS e acabou. Então se você tiver uma máquina dentro de uma Cloud, se você tiver alguma coisa do tipo, uma das maneiras de simplesmente começar a

usar o Umbrella é apontar o DNS. Aí as chamadas de DNS feitas por aquela máquina e pelos aplicativos e clients que estão dentro daquela máquina vão utilizar Umbrella. Mas existem outras formas de fazer isso. Você pode fazer isso com servidor de DNS Proxy dentro da empresa, para você poder ter o contato de endereços privados. Você pode fazer isso através de outros produtos, por exemplo, o próprio firewall da Cisco, dentro da Cloud usando o serviço de Umbrella. Então tem bastante formas de implementar isso. Depende de qual que é o nível de proteção que você quer e depende de quanto que você está colocando as soluções de segurança para trabalhar em conjunto.

Josi, pode ficar à vontade para complementar qualquer coisa que você quiser também.

SRA. JOSIANE DE BARROS SILVA: Perfeito. E a solução, não querendo falar só de solução Cisco aqui, ela é entregue na nuvem. Você faz o direcionamento DNS, mas o gerenciamento diretamente na nuvem da Cisco. Obrigada, Adalberto.

SR. EDUARDO BARASAL MORALES: Legal. Vamos para a última pergunta, porque, afinal, sei que, pessoal, vocês mandaram muita coisa agora no chat lá, a gente não vai conseguir ler, porque a gente já está terminando nosso tutorial, mas a Josi e o Adalberto vão deixar contatos e depois vocês podem mandar mensagens para eles.

Então, é do Wanderson Tales: "Josiane, no seu ponto de vista, por que muitos fabricantes não implementam em seus produtos mecanismos de segurança, visto que todos têm esse conhecimento e impacto?". Ele está falando assim: por que as coisas de segurança não vêm por default? Se você puder comentar um pouquinho. Sobre a sua opinião, né?

Acho que a Josi deu uma travada ali, a gente acabou perdendo ela. Quer comentar, Adalberto?

SR. ADALBERTO LINS: Sim, posso comentar. Enquanto ela não volta. Principalmente porque segurança implica em você derrubar serviço. Isso daí é um tema muito complexo, muito complicado. Então se você habilitar todos os sistemas de segurança que você tem disponíveis no equipamento, o equipamento simplesmente não vai passar tráfego nenhum, ele não vai saber que tráfego precisa passar e que tráfego não precisa passar. Então isso é uma coisa que precisa tomar cuidado.

Tem um exemplo bem interessante de uma operadora europeia que a gente discutiu bastante. O Eduardo vai até lembrar do que a gente comentou isso no passado também, que eles viraram para os assinantes deles e simplesmente habilitaram o Umbrella para todos os assinantes como SVA. E começaram a cobrar lá € 1 a mais na conta de cada assinante, para poder proteger aquele assinante, independente do assinante querer. Na Europa, no país onde foi feito isso é possível fazer esse tipo de configuração, esse tipo de oferta. O pessoal ligava para cancelar, e na hora de ligar para cancelar o atendente estava preparado para explicar para eles o benefício de segurança e tudo mais, e 99% não cancelou e manteve o serviço.

Isso no Brasil seria simplesmente inviável de implementar. A nossa regulamentação dos provedores diz que todo tráfego de cliente não pode ser tocado. Forma análoga a isso está dentro dos roteadores. Tudo é uma questão de compromisso. Se eu habilito uma coisa que é importantíssima em todo roteador, que é o control [ininteligível] protection, eu estou consumindo recurso na máquina e eu estou fazendo com que a máquina fique mais lenta. Então para alguns clientes velocidade é importante, para outros clientes segurança é importante. Para o mesmo cliente pode ser que em uma interface seja importante segurança e em outra interface seja importante a velocidade. Então não tem muito jeito o que fazer isso.

Você tem os recursos do equipamento, o ideal é que a gente pudesse ter um profile e para esse tipo de cliente eu habilito esse default e para outro tipo de cliente eu habilito outros defaults. O que todo fabricante faz, inclusive a Cisco, é olhar a média dos clientes, o que faz sentido estar como default para maioria dos clientes, e a gente envia o equipamento para o provedor de uma maneira pré-configurada, que a gente acha mais sentido e mais genérico possível. Lembrando que o cliente pode ser usuário doméstico, pode ser um provedor, pode ser uma empresa corporativa, pode ser um small business, uma grande empresa, então realmente os setting default precisam ficar de forma mais genérica.

SR. EDUARDO BARASAL MORALES: Quer complementar, Josi, um pouquinho? Dar uma última fala?

SRA. JOSIANE DE BARROS SILVA: Deu uma caída aqui, eu voltei. Ainda está na mesma pergunta?

SR. EDUARDO BARASAL MORALES: Sim.

SRA. JOSIANE DE BARROS SILVA: Tá ok. Então, na minha opinião, não posso falar muito como fornecedora. Mas gerado, criadas essas caixas com todas funcionalidades, faz pipoca, faz arroz, faz tudo ao mesmo tempo, entrega isso para o cliente. E, depois que é entregue isso, essa inteligência que eles costumavam vender, mil e uma utilidades é entregue, mas só que essas atualizações, essas informações não são recorrentes. Então existem bugs que não são fixados. Então tem que tomar muito cuidado com empresas que saem vendendo mil e uma utilidades, Bombril da vida, vamos dizer. Porque ás vezes você precisa de uma solução que seja mais focada e específica, por exemplo, uma solução de firewall separada de uma solução de antimalware, você separar as coisas. Porque às vezes você tem tudo junto, a empresa te vende e não entrega a inteligência que ela falou que tinha, ou até mesmo te cobra depois uma inteligência. Vai, você vai me paga mais R$ 100 para ter essa inteligência atualizada. Então é bom vocês verificarem o antecedente, ver se a empresa é mesmo [ininteligível] com vocês, se realmente existe uma atualização dessas informações e que ela não vai te cobrar depois por isso, já venha, já esteja embutido no pacote.

SR. EDUARDO BARASAL MORALES: Obrigado, Josi.

Bom, a gente está chegando agora nos finalmentes. Eu queria só agradecer a sua participação, Josi. Agradecer a participação do Adalberto, realmente foi esclarecedor esse tutorial. Muita gente aprendeu. O público foi muito bom. E agora eu vou chamar o Moreiras para terminar a nossa live.

SR. ANTONIO MARCOS MOREIRAS: Bom, gente, realmente reitero os agradecimentos que o Eduardo já fez ao Adalberto, da Cisco, a Josi, da ScanSource. Gostei muito do tutorial. Espero que vocês que estão acompanhando pelo YouTube e Facebook também tenham gostado. Imagino que sim, porque tem bastante gente acompanhando até agora, teve bastante perguntas, bastante participação pelo chat, e a gente conseguiu felizmente colocar bastante perguntas para Josi responder e foi muito legal.

Eu lembro que essa semana continua. Amanhã a gente tem um minicurso sobre DNS promovido pelo pessoal da Icann. Daniel Fink está aí também acompanhando a live agora, fazendo comentários no chat do YouTube e ele vai estar amanhã falando sobre DNS, sobre DNSSEC, sobre Hyperlocal, sobre como fazer DNS Recursivo com Unbound, com bound(F), e vai ser muito interessante. O tutorial de amanhã, o minicurso de amanhã tem uma parte prática. Quem quiser acompanhar fazendo a parte prática em conjunto, acessa a página da Semana de Capacitação, semanacap.nic.br., e tem lá as instruções para você fazer o experimento prático junto com o instrutor amanhã durante o minicurso. Quem não quiser, tudo bem, só assiste.

Lembro também que a gente tem a live do Intra Rede sobre o assunto de segurança, sobre ataques nos provedores dia 30 de setembro. Então, desde já anotem na agenda. O pessoal falou muito, teve muitas dúvidas, na verdade, perguntando sobre materiais relacionados à segurança. Eu gostaria de lembrar a todos que a gente tem muito material disponível no NIC.br. Tem, por exemplo, uma página de documentos no site do Cert.br. Vale a pena entrar no site Cert.br, e dar uma navegada geral no site, porque tem muito, muito material interessante e tem material voltado para todos os públicos lá, inclusive pessoal de provedores. E a gente tem um site chamado [ininteligível] seg, que tem recomendações específicas lá para os provedores sobre como melhorar a segurança, em vários aspectos, fala de [ininteligível] e fala de diversos aspectos de segurança. Então eu gostaria de reiterar essa recomendação de vocês olharem esses materiais, olharem esses sites que a gente tem.

Gostaria também de pedir mais uma vez para que vocês preencham o formulário de avaliação dessa live. Isso é bastante importante para a gente. O formulário de avaliação é muito simples, muito simples, são só duas questões. Vocês não vão levar nem cinco minutos para preencher. A gente pede para vocês darem uma nota para a live e, para você, se quiser, colocar um comentário sobre como a gente pode melhorar. Então diz para a gente lá qual foi a pior coisa que a gente fez aqui na live, e a gente vai tentar melhorar para próxima, quem sabe para amanhã, quem sabe para de quinta, se a gente... se não for um ponto que a gente consiga melhorar tão rápido, a gente vai tentar melhorar para as lives futuras, assim que for possível.

É muito importante para a gente essa participação de vocês. Eu sei que vocês já deram like no vídeo, já ficaram quase três horas aqui participando com a gente. Isso é um sinal que muito provavelmente vocês gostaram, mas para a gente é importante saber no que a gente precisa melhorar. Então, por favor, preencham isso daí.

De novo, agradeço a todos. Muito obrigado, Adalberto, muito obrigado, Josi.

Ah, lembrando aqui. O pessoal da organização está me lembrando que as inscrições para quem quer receber o certificado só vão até às 14 horas. Então se alguém precisa de certificado de participação desse evento online, desse minicurso online, preencha no link que vai aparecer no chat do YouTube, preencha a inscrição lá no site de cursos e eventos NIC.br. Aproveita lá para assinar as nossas listas de e-mail, para permitir que a gente mande para vocês avisos sobre eventos similares, sobre cursos similares que a gente vai fazer no futuro.

Então eu agradeço novamente aos instrutores aqui desse tutorial, desse minicurso, a toda a equipe de organização, que inclui o Eduardo, toda a minha equipe que participou disso, o pessoal da comunicação. A Carina está aqui com a gente. Muita gente da comunicação ajudou a gente na organização dessa live, na divulgação dessa live, [ininteligível]. O Pedro do suporte técnico, que está aqui operando todos os equipamentos, transmissão, coloca vídeo, acerta as coisas. Então muito obrigado a todos. Sem vocês, a live não seria possível. E sem vocês que estão assistindo também não seria possível. Muito obrigado pela audiência de vocês, pela atenção de vocês. E a gente se encontra amanhã às 9h da manhã aqui nesse mesmo canal do YouTube para falar sobre DNS. Muito obrigado, a gente encerra a live aqui por hoje.