Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

Transcript dos slides apresentados em palestra no evento Summit - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes, 2º painel, realizado na sede da Febraban em São Paulo, na data de 17 de abril de 2017.

Slide-1: Summit - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

Bom dia a todos!
Sou Washington Almeida, Engenheiro Eletrônico e Perito Forense Digital.
Primeiramente agradeço à organização do evento pelo convite, representado pela Infi, para participar desse painel.
Meus parabéns aos companheiros de mesa pelas apresentações.
É um prazer estar aqui e compor uma mesa com profissionais tão bem preparados.
Vamos seguir então com essa última parte de apresentação do painel.

Slide-2: Ausência de transparência na coleta de dados online

Um primeiro impacto para os usuários quando da ausência de transparência na coleta de dados online é o que percebemos ao acessar uma página de uma empresa em um país que possui uma legislação de privacidade como os Estados Unidos, e outro país que não possui uma legislação, como no caso do Brasil.
Note que na página da Microsoft, nos Estados Unidos, o usuário recebe uma informação que ao usar o site o usuário concorda com o uso de cookies para o analítics, conteúdo personalizado e ads.
Na página da mesma empresa no Brasil, não há nenhuma notificação quanto ao uso desses recursos, e o usuário não recebe nenhuma informação do que possa ocorrer com seus dados enquanto estiver navegando naquele site.

Slide-3: Implicações práticas para o usuário

E essa falta de transparência traz implicações práticas para o dia a dia do usuário no uso da internet.
Essa é a tela do litghbean, que é uma extensão para o navegador Firefox, e esse recurso está disponível para os usuários. Instalar uma extensão para o navegador significa adicionar recursos extras para ele, ou seja, agregar funcionalidades que ele não possuia originalmente.
A funcionalidade extra que o Lightbean agrega, que não está presente nas versões originais dos navegadores, é justamente mostrar tudo que ocorre quando de nossa navegação nos sites da internet.
Então, no exemplo, eu acessei um site e sem que eu soubesse, o site me conectou a outros seis sites, que são parceiros dessa empresa que eu acessei.
Desses seis sites de parceiros, quatro deles, os que estão em conexão com as linhas azuis, vem coletar informações dos cookies gravados no meu computador, sem a minha permissão.
Os cookies são arquivos criados pelos websites que você visita, e usados pra lembrar suas preferencias, históricos, entre outras informações.
Mas o usuário não consegue perceber isso, e eu só consigo visualizar o que ocorre com minha navegação porque estou utilizando uma ferramenta como essa do Lightbean.

Slide-4: Serviços para o ambiente da nuvem

Eu poderia afirmar com quase absoluta certeza que todos nós dentro desse auditório faz uso de ao

Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

menos um desses recursos da nuvem.
E a prática do armazenamento em nuvem se dá tanto para soluções corporativas como também para o usuário final. Tanto um quanto outro consomem serviços da nuvem.

Slide-5: Ameaças cibernéticas para serviços da nuvem

Mas mesmo os mais sofisticados serviços de nuvem vivem em constantes ameaças.
Essa notícia circulou nos principais canais de comunicação do mundo dando conta de uma ameaça sofrida pela Apple, em que um grupo hacker chamado “Turkish Crime Family” teria infectado a nuvem sob domínio da Apple com um ransomware, e eles já teriam acesso às contas dos usuários.
Os criminosos estão se tornando muito audaciosos e ao mesmo tempo muito sofisticados.
A data limite para pagamento do ransomware era 7 de abril, e felizmente a Apple não cedeu às ameaças e também nenhuma ocorrência foi observada por conta dessa ameaça.

Slide-6: Relatório de ameaças cibernéticas na nuvem

A empresa Netskope, especializada em serviços de nuvem, emitiu um relatório sobre as ocorrências de ameaças em 2016 no ambiente de nuvem.
Eu chamo atenção a dois apectos nesse relatório. Mais de 80 por cento das ameaças tiveram severidade alta, o que significa uma alto potencial de infecção para o ambiente da nuvem.
O outro aspecto é o surgimento dos chamados droopers, que recebem esse nome em virtude de seu método de infecção acontecer em pequenas porções, como na tradução “a conta gotas”.
Essa classe de malware está em seus estágios iniciais de desenvolvimento e eles serão as grandes ameaças que os sistemas PDVs (Pontos De Vendas) deverão enfrentar nos próximos anos, como veremos mais adiante.
A grande maioria dessas ameaças são os malwares, que vem do inglês “Malicious Software, que tem como principal característica a execução de alguma ação nociva quando em contato com o ambiente infectado.

Slide-7: Relatório de ameaças cibernéticas na nuvem (cont.)

Tres pontos também me chamaram a atenção nesse relatório.
Mais de 40 por cento dos serviços não permite aos administradores desses serviços reforçarem o controle de senhas. E acaba ficando na percepção dos usuários utilizar as senhas que ele bem entender, sendo elas fortes ou fracas.
Mais de 50 por cento dos serviços de nuvem não especificam nos termos de serviço que o cliente é o dono dos dados.
Apesar de parecer óbvio, a ausência dessa especificação pode gerar extensos debates jurídicos, principalmente quando da ocorrência de vazamento de dados de uma empresa.
E por fim, mais de 80 por cento dos serviços da nuvem não faz uso de criptografia para os dados armazenados.
Implica que se um dado vazar, e ele não estiver criptografado, o dado poderá ser acessado e lido sem a menos dificuldade.

Slide-8: Ameaças cibernéticas da rede TOR

Nos slides que seguem, vamos comentar das ameaças que emergem da rede TOR, e eu queria antes explicar, basicamente, o mecanismo de funcionamento da rede TOR para dar uma melhor compreensão da motivação que os indivíduos mal intencionados tem em hospedar seu conteúdo

Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

nesse ambiente.
Basicamente a rede TOR foi criada para prover o anonimato, que é uma forma de se evitar que os sites vasculhem conteúdos nos computadores dos usuários, entre outras motivações.
Para contextualizar, no exemplo desse slide, temos o computador que recebe seu endereço IP do provedor de conexão, aquele provedor que você paga mensalmente para ter o serviço de acesso à internet.
Esse computador pode acessar a rede TOR tanto pelo navegator TOR, como através de um cliente de conexão à rede TOR.
Esse computador faz uma solicitação de acesso à rede TOR e nesse processo é criado um túnel criptografado desde o computador até o que é chamado de Exit node, que é a saída da rede TOR para alcançar o destino solicitado pelo usuário.
A forma de esconder o IP original do computador, provendo o anonimato, acontece da seguinte forma:
1. O Guard node é o roteador que conhece o endereço IP do computador que solicitou o acesso.
2. Ele então submete a solicitação para um outro roteador chamado de relay node, porque ele fará a retransmissão dessa solicitação, porém, nesse processo o Guard node subtrai a informação do IP do computador, ficando ele com a referencia codificada desse solicitante.
3. O relay node faz a retransmissão da solicitação do Guard node para o Exit node, que levará a solicitação até o site de destino.
Na prática, quando o site tenta identificar o IP do computador pra injetar os ads, ler os cookies, etc., ele terá como informação o IP do Exit node, que é um IP falso, então ele não consegue atuar de forma invasiva nesse computador.
Somente com sofisticadas técnicas, recursos que demandam muita pesquisa e elevado nível de proficiencia técnica de profissionais muito experientes é que se consegue identificar o IP real de uma máquina dentro da rede TOR.
Em virtude disso, diz-se que é praticamente impossível a identificação de uma máquina operando na rede TOR, o que é um problema para os escritórios de advocacia e para a justiça que precisam justamente do endereço IP na produção de prova dos atos ilícitos praticados nesse ambiente.

Slide-9: Crescimento das ameaças cibernéticas

E as ameaças cibernéticas crescem de forma vertiginosa por conta de milhares de sites que operam na rede TOR, comercializando produtos especializados para os mais variados tipos de fraudes.
Somente nesse site há mais de 40.000 produtos voltados para fraudes, sendo que mais de 24.000 produtos tem como alvo o setor bancário.
Mais de 5.000 prudutos voltados para fraudes com cartões.
Quase 1.800 tipos de dumps.
Os dumps são coletores de transações que ocorrem com cartões de crédito e débito. Recebe o nome de dump porque ele faz uma cópia dos dados durante uma transação, e os envia para algum servidor hospadado também na rede TOR.

Slide-10: Serviços especializados em fraudes - MaaS

Aqui um exemplo de um produto comercializado nesse ambiente: Google Adsense Fraud 2017.
O Google Adsense é um programa de publicidade onde as pessoas pagam o Google para colocar anúncios, e o Google então paga sites para hospedar os anúncios. A pessoa que adere ao programa é paga quando as pessoas clicam nos anúncios que estão em seu site ou blog.

Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

Sites comprometidos são invadidos para modificar o código original pelo código malicioso.
Operacionalmente, ambos funcionam de forma equivalente, sendo que quando o usuário cliclar em um Adsense como esse, ele vai ser direcionado para a publicidade e ao mesmo tempo um código malicioso começa ser transferido para o computador do usuário, onde se iniciará todo um sofisticado processo de infecção.
É o que chamo de Malware as a Service, pois hoje há duas classes de atividades criminosas nesse mundo underground. Os criminosos que desenvolvem suites gráficas completas voltadas para fraude, e os vendem para uma outra classe de criminosos, que não possuem esse intelectual para desenvolvimento. E essa segunda classe de criminosos que disseminam essas ameaças na internet.

Slide-11: Ataque ao setor bancário em 22-10-2016

Essa notícia tomou as páginas dos principais canais de comunicação nas últimas semanas, dando conta de um ataque hacker com sucesso a um banco brasileiro, e toda infraestrutura falsa do banco estava hospedada na nuvem da Google.
Ao todo 36 domínios do banco, incluindo recursos da rede interna como o sistema de e-mail, entre outros, foram comprometidos.
E os hackers ficaram por cinco horas capturando todas as transações que ocorreram durante esse período de tempo.
O erro do banco foi terceirizar sua infraestrutura de DNS.

Slide-12: Ataque ao setor bancário em 22-10-2016 (cont.)

E porque os hackers se interessam tanto em comprometer os serviços de DNS?
DNS vem do inglês Domain Name System, um serviço criado para facilitar o processo de uso da internet.
O serviço consiste, basicamente, em converter um nome para um endereço IP. Funciona assim: quando você se conecta ao site www.banco123.com.br o serviço de DNS converte esse nome para um endereço IP do banco, porque é mais fácil gravarmos nomes do que gravarmos endereços IPs.
Suponhamos que, hipoteticamente, o endereço IP desse banco seja 200.20.20.20.
Então imaginem o cenário. Um hacker consegue comprometer o serviço de DNS desse banco e redireciona o nome www.banco123.com.br para o endereço IP onde ele tem controle do ambiente.
Foi exatamente isso o que aconteceu com o banco. Depois de redirecionar seus domínios, os hackers tinham o acesso ao seu ambiente e até os certificados digitais eles fizeram parecer como se fossem verdadeiros.

Slide-13: Ameaças cibernéticas para o setor bancário

No final de Fevereiro a Visa emitiu um alerta mundial a respeito de um malware que foi identificado com o nome Flokibot, projetados para comprometer especificamente os sistemas integrados dos Point of Sales brasileiros, porque no Brasil se faz uso do cartão com chip, e o processo de gravação dos dados, quando da transação financeira, são diferentes dos cartões que não utilizam chips.
Esse malware está nos estágios iniciais de evolução e promete ser uma das mais perigosas ameaças que o setor deve enfrentar nos próximos anos.
Vamos tentar mostrar suas características em mais detalhes.

Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

Slide-14: Droppers – Anatonia do ataque

Primeiramente, como esses malware alcançam os Pontos de Vendas?
Exemplos como o do AdSense Fraud é uma forma de injeção desse tipo de malware.
Baixar programas não licenciados da internet é outro bom exemplo.
Em segurança da informação, um payload refere-se à parte de um vírus de computador que executa uma ação nociva.
No exemplo, uma pequena parte do vírus está sendo injetado na memória do computador, de forma criptografada, o que torna muito difícil a deteção por programas anti vírus.
Uma vez que o código é totalmente transferido e carregado na memória do computador, o programa é descriptografado e auto-executado, sinalizando as principais syscalls de controle do ambiente Windows para iniciar o processo de controle e infecção do computador.
Quando todo o processo é finalizado, esse robo apenas espera pelas informações sensíveis para capturar os dados de transações e enviar para algum servidor hospedado na rede TOR.

Slide-15: Resolução de incidentes - Detecção

Na resolução de incidentes existem excelentes pipelines de tratamentos desenvolvidos pela Microsoft, pela Price, além de outras empresas.
Nós trouxemos aqui um pouco do que ocorre na prática, para não ficar apenas no empírico.
Então, na fase de detecção é comum verificar o files do Linux, ou o Explorer do Windows, fazerem chamadas de rede, coisa que não deve ocorrer, pois eles apenas indexam pastas e arquivos.
Essa anomalia normalmente é seguida de uma sobrecarga no tráfego de rede, que se bem monitorada é rapidamente percebido por um administrador de redes.
Outro componente é o computador comunicando com servidores hospedados na deep & dark web, através dos serviços como o TOR, IIS, anoNET, FreeNet, entre outras.

Slide-16: Resolução de incidentes - Análise

Uma vez detectado o incidente, ele é seguido de uma análise mais minuciosa onde se procura obter as informações dos recursos envolvidos no ato ilícito.
No exemplo, todos os recursos estão operando dentro da rede TOR. E através do que chamamos de um ataque de enumeração, foi possível identificar o IPV6 da máquina de origem.

Slide-17: Resolução de incidentes - Discovery

A partir dos recursos que nos interessa enumerar, passamos para o processo de descoberta de cada um dos recursos analisados.

Slide-18: Relatório

Por fim é emitido um relatório onde é detalhado todas as informações referentes aos recursos analisados, e o que é importante para a justiça é dar a localização do endereço IP onde ocorre o ilícito.
Por que no final é o IP que estamos buscando para localizar as atividades criminosas que ocorrem na internet.

Summit Febraban - Armazenamento de dados na nuvem: análise técnica e resolução de incidentes

Slide-19: Serviços de nuvem para o setor bancário

Quando um banco buscar por um serviço de nuvem, o que é importante considerar?
Uma primeira pergunta seria: Que tipo de dado será hospedado na nuvem? Dados publicos? Dados internos do banco? Dados dos clientes? Dados de fornecedores? Dados de parceiros?
Essas respostas podem mapear para qual tipo de nuvem a empresa deve contratar: Um serviço de nuvem público? Privado? Ou híbrida, que agrega características tanto da nuvem pública como privada?
Em relação a segurança da informação, as políticas do fornecedor do serviço de nuvem são aderentes às políticas de segurança da empresa?
O desequilíbrio nessa aderência pode trazer problemas futuros para a contratante.
O serviço do fornecedor faz uso de criptografia para os dados armazenados?
Esse ponto é substancialmente importante principalmente levando em consideração análise de riscos envolvendo vazamento de dados.
Qual o nível de serviço esperado?
Esse itens estão resumidos aqui, mas a lista de itens a ser verificados é bem extensa, e quanto mais detalhado, melhor será a aderencia do serviço às expectativas da empresas de quem as contratam.

Slide-20: Fechamento e agradecimentos

Bem pessoal, era isso que eu queria compartilhar com vocês, o tema na verdade é bem extenso, mas acredito que os pontos apresentados são de relevância para nossa comunidade, principalmente para o setor bancário em relação às ameaças que foram apresentadas.
Essa apresentação está disponível em meu site, juntamente com um transcript simplificado do que foi apresentado aqui no dia de hoje.
Muito obrigado! Até a próxima.