Estudo do Caso: Ataque Fatal a Americanas Ponto Com

Fevereiro quente: O que aconteceu nas Americanas.Com

Salve jovem padawan, hoje o dia dos 5 patinhos, vamos nos debruçar em mais um ataque mediático em uma grande empresa da internet os Analistas de CyberSegurança não estão tendo paz, depois dos ataques ao Ministério da Saúde, o colapso da Vodafone Portugal, ataques a Claro e outras empresas, desta vez o ataque foi abortado antes das consequências nefastas.

Como dizia um colega de projetos passados, nós trabalhamos 8 horas por dia, com salários achatados, pressão e risco de terceirização para proteger a empresa contra hordas de bárbaros, trolls nos portões, exploits em tuneis, phishing pelas janelas, XSS em carros bombas, protegemos com suor e lagrimas e quando fazemos bem nosso trabalho, ninguém se lembra que existimos, ou que foi solicitada a licença dos softwares xyz top plus.

Mas basta que ocorra um ataque de um hacker solitário ou squad, que o mundo cai sobre nossas cabeças, lembrem-se sempre o malfeitor trabalhara 24 horas por dia, 7 dias na semana e os 365 dias do ano, explorando uma a uma, as inúmeras técnicas apreendidas na Deep Web.

Quando encontra, publica no submundo apregoando a façanha, pedindo apupos e avisando outros grupos numa collab do mal e começam a explora-la em busca de vantagens, o protocolo a ser seguido é: enviam worms, cavalos de troias, instalam keylogers, esmiúçam e preparam o caminho criando a estrada dos tijolos amarelos, deixando softwares em stand-by, esperando o dia D e com isso será o final do mundo, os zombies invadiram, milhares de bots avançaram e a Rainha será raptada.

O Caso Americana.Com

O maior conglomerado de lojas virtuais do Brasil, vendendo uma vasta gama de produtos e sendo o portal para o comercio de pequenos vendedores, fornecendo sua infraestrutura logística.

Uma anomalia foi detectada no dia 17 de Fevereiro, sendo o Twitter o local onde apareceram as primeiras informática, primeiro discreto, posteriormente o pássaro azul veio abaixo, o povo começou a postar, foram milhares de twittes com perguntas, trollaçoes, indignações e medo.

A equipe técnica foi acionada e começaram o processo de investigação, não sabemos o que foi encontrado, mas garanto o que foi encontrado aterrorizou tanto a cúpula da empresa, que a medida seguinte todos os sites foram derrubados, preventivamente para auditoria, deixando os websites do portal off-line e até o momento que escrevo este artigo, continuam down, para pensar é difícil apurar as perdas, mas somente os danos de imagem derrubaram as ações da empresa em 8%, prejuízo aos acionistas e investidores ao Bovespa .

Lembrando que o portal Americanas engloba os conhecidos sites de e-commerce Submarino, ShopTime e SouBarato,além de dezenas de outras lojinhas virtuais. Negociam todos os segmentos e atinge as classes sociais de “A” a “E” e vendendo a nível global.

O que aconteceu?

Como reportado ocorreu problemas de negação de serviço, as primeiras queixas eram que o site estava off-line, no decorrer do dia, mais e mais pessoas indagavam nas redes sociais o problema.

O que é negação de serviço?

É um tipo de ataque usando bots e zombies com o objetivo de inundar um servidor Web com solicitações e com isso derrubar o serviço, deixando o site off-line, conhecido tecnicamente como DDoS (negação distribuída de serviço).

Normalmente é um ataque de infantaria cracker, cujo o principal objetivo e mascarar o real ataque, pois aproveitando-se da brecha e queda em cadeia dos servidores, os invasores podem ser dirigir ao pote de mel.

Existem inúmeras maneiras de efetuar o ataque, mas o mais comum é a Engenharia Social, enganando algum empregado ou cliente, que instala inadvertidamente um malware ou fornece uma senha de administrador ao cracker.

Etapa seguinte é alugar uma rede de botnets ou criar a própria, deixando a equipe de segurança ocupada em apagar o incêndio, inclusive alguns infiltrados podem até estar nesta equipe de contingência.

Qual o objetivo dos ataques?

Existem duas principais vantagens visadas por atacantes: PRESTIGIO e o bom e velho lucro financeiro. Nos primórdios da Internet, todo jovem aspirava ser um grande nome no mundo da informática, o Robin Hood dos oprimidos, o Arsene Lupin dos ataques cyberneticos, ganhar os 5 minutos de fama e ter seu nome nas manchetes dos jornais.

Tantos criadores de vírus deleitavam-se vendo os estragos de suas criaturas, dando entrevistas, fazendo deface em WebSites, atacando com mensagens as inúmeras causas sociais, eram os pichadores virtuais, fonte de dor de cabeça aos administradores de website, que necessitavam ter backups a mão, para repor a página inicial, foram pouquíssimos portais que escaparam ilesos.

Ganhos financeiros

Rapidamente alguns grupos viram vantagens econômicas e financeiras em atacar sites, algumas vezes como mercenários contratados por concorrentes, outras vezes por governos estrangeiros e atualmente por membro das diversas Máfias do mundo.

Com o aumento da segurança nos serviços financeiros digitais com uso extensivo de token, os cybers criminosos olham para outras vítimas: pagamentos eletrônicos, venda de dados pessoais, roubo de código fonte e sequestro de bens.

É cada vez mais comum, a invasão, furto e pedido de resgate e devolução de senhas, inúmeras grandes empresas foram vítimas deste tipo de crime, porem para evitar mancha na reputação e perda de confiança no mercado, silenciam-se e pagamos valores aos cybercriminosos.

Um dos mais bizarros e o DNS Hijacking onde invasores modificam servidores DNS, desviando o trafego do site, nos casos mais elaborados, fazem desvio para um caminho alternativo, onde filtram os pacotes que desejam e ao final reencaminham a solicitação ao site destino, difíceis de serem identificadas e muitas vezes passando despercebidos dos admins.

Casos de phishing são mais simples de elaborar e limitados a vítimas incautas causando dando individuais, mas muitas vezes catastróficos para os envolvidos, causando perdas financeiras, cancelamento de cartão de credito e outros problemas.

Dever ético dos Desenvolvedores e programadores

A nossa categoria profissional tem conhecimento técnico acima da média, podendo descobrir furos facilmente, temos uma obrigação ética e moral com os nossos stakeholders de protege-los contra os ataques crackers, mesmo assim falhamos, pois infelizmente em alguns pontos estamos atados.

Os prazos apertados, alta complexidade das soluções, constantes atualizações/deploys/release, alta rotação das equipes, equipes terceirizadas, quarteirizadas e quinteirizadas que dificultam muito a segurança do código, baixos salários facilitam a cooptação de elementos vulneráveis dentro do time, a busca pelo lucro torna as empresas e gestores vulneráveis, afinal como proteger a Empresa, quando o assédio do inimigo é generoso?

Enormes backdoors, politicas de logins arcaicas, falta de auditoria e acompanhamento de logs e monitoração constante dos serviços, diariamente surgem novos malwares ou updates dos antigos. Exploits construídos sobre medidas e publicação de tutoriais e vídeo-aulas na Dark Web, visando formar novos lammers que sonham em se tornar Black Hats.

O que é um Black Hat?

Na Dark Web são os senhores absolutos do conhecimento, especialistas piratas, corsários, ronins que exploram vulnerabilidades buscando obter vantagens financeiras, são elementos lendários e invisíveis, não gostando de publicidade.

Montam squads formando lammers e crackers fornecendo o know-how, apontando o Norte e facilitando os trabalhos, a origem do nome refere-se a identidade visual dos antigos filmes de faraoeste, onde cowboys combatiam na fronteira do oeste americano, facilmente identificáveis os mocinhos usavam chapéus brancos e os vilões chapéus negros.

A título de curiosidade no mundo hacker existem 3 tipos mais conhecidos e importantes, o White Hat, hackers do bem, os Black Hats já citados e os Greys Hats que estão no meio do caminho, comentando boas ações e as vezes cometendo pequenos crimes.

A torre dos Magos

Existe na Dark Web inúmeras guildas de necromantes virtuais, mestres em cybercrimes os mais habilidosos dos Black Hat, que criam novos capítulos no Necronomicon Hacker, deixando a sociedade virtual indefesa contra os vírus e malwares, com centenas de worms, malwares,0Day Exploits e cavalos de troia.

Visando proteger a Web, existe uma Torre de Cristal, um farol em meio as trevas onde o conhecimento do BEM e compartilhado e distribuídos, magos e mestres Jedi monitoram e ajudam na criação de soluções. Estou me referindo a OWASP, ou Open Web Application Security Project), ou Projeto Aberto de Segurança em Aplicações Web.

Além da OWASP, existem inúmeros paladinos que lutam contra os malwares, inspirado no primeiro e polemico deles John MCafee, que trilhou o bom combate, abrindo o caminho para inúmeras outras torres de defesa contra o cyberataque.

Numa guerra sem trégua onde os usuários comuns são peões neste jogo, com inúmeros ativistas, corsários e renegados pelo caminho, tornando a jornada mais empolgante.

Depois do Viajandao

Voltemos ao caso Americanas, até o momento os administradores não se pronunciaram a respeito do ocorrido, ministério público, Procon e outros órgãos reguladores estão atentos e aguardando.

A grande problemática é que foi atingida uma empresa cotada em Bolsa de Valores, acendendo os alertas para fraudes de Bolsitas, a CVM e Bovespa estão estudando as transações para ver se ocorreram fraudes de day-traders e outros grupos.

A Febraban está acompanhando o caso, para ver se ocorreu algum risco financeiro ou bancário devidos a suposto vazamento de dados e exposição dos clientes. Informações cadastrais podem favorecer ataques de phishing direcionados no Black CRM.

Perder 8% dos valores das ações afetou acionistas, Fundos Investimentos Imobiliários, Corretoras e investidores internacionais, com certeza irá gerar repercussões de longo prazo, apertando ainda mais a fiscalização e controlo dos diversos órgãos.

Ocaso do Show do Thiaguinho

O ataque deste final de semana, tem tudo haver com ransomware, pois no momento de maior impacto promocional, grande investimento do Grupo Americanas empublicidade no BBB da Rede Globo, patrocionando um show musical com Thiaguinho.

Esperava-se um boom de acesso, compras onlines impulsionadas pela publicidade nas redes sociais, o Big Brother é um alavancador sem igual, mas devido a essa ação inexplicável, foi tudo perdido.

Os suspeitos do ataque a Americana

Depois que a PF desbaratou os membros do CyberTeam, os seus sucessores foram o grupo Lapsus, que criou um grupo no telegrama e ficou famoso nos inúmeros ataques a sites do governo, estando muito ativos nos últimos meses e provocando o caos.

O poder do Backup

Não existe bala de prata, mas a salvação da pátria é o BACKUP. Tenha backups atualizados, tenha rotinas de cópia de segurança, treine suas equipes a usar o GITHUB e proteja sua instalação.

Treine aspectos de segurança

Toda empresa tem que criar programas de segurança, cursos de reciclagem e atualização constante, todos devem passar em testes e trabalharem sob uma ótica mais defensiva, os bárbaros estão no portão.

Os perigos da Sabotagem

Atenção padawans, usar bibliotecas de terceiros copiadas em site open-source é um perigo, afinal em meio há milhares de linhas de código, podem estar escondidos trechos ou mesmo blocos completos de códigos maliciosos.

A falta de auditoria de software, controle de objetos e uso indiscriminados de soluções prontas podem abrir brechas e deixar a instalação insegura, salários baixos e alta rotatividade de funcionários são outros problemas a segurança do projeto.

Ransomware

Em outros casos, o fruto do trabalho foi colocado em leiloes no Porto Royale da Dark Web, a Vodafone o cracker queria 2500 dólares para vender o login de um Admin, no pouco claro caso da JBS custou 11 milhões de dólares, no Ministério da Saúde queriam 50.000 reais.

A cada dia surge novos casos e mesmo as pessoas físicas não estão a salvo, pois nos meios de comunicação foram publicados inúmeros casos de pessoas chantageadas por roubos de fotos e perde de acesso a redes sociais.

Agentes da Lei

Pense nos inúmeros agentes da lei que indiretamente fiscalizam o software: Febraban, CVM, Bolsa de Valores, Ministério Público, Procon, Policia Federal e Policia Técnica. Muitos olhos no vigiar e punir. Cuidado com o código produzido, olho vivo e atenção, um teste mal feito, um programa descuidado, aquele deploy desorganizado, poderá render pena de prisão e o envolvido ser cadastrado na ABIN e outro órgão de vigilância.

Com perdas na casa dos 4 bilhões de reais, muitas cabeças irão rolar e processos judicias serão instaurados e a elite dos caçadores de cyber criminosos entrara em ação, este ataque afetou muita gente e com certeza pessoas que perderam tanto dinheiro assim buscarão um payback.

Conclusão,

Caro padawan acredito que esta história não terminou, teremos mais capítulos assustadoramente reais, até o momento as equipes técnicas estão investigando e apurando os estragos, provavelmente o resultado final não chegara ao grande público.

O Risco de Imagem e a credibilidade sistemas são frágeis e podem provocar debandadas afetando todos os integrantes do mercado virtual, lojas online que durante anos tentaram convencer os clientes sobre a segurança e forçar o uso de e-commerce em detrimento do comercio físico.

Lembre-se sempre no que o Tiozão diz, somos responsáveis sobre aquilo que cativamos, digo produzimos, somos criadores, um trabalho intelectual de alta responsabilidade, veja no caso do TSB Bank, da Vodafone e agora da Americanas o problema social gerado não é possível de quantificar e apurar facilmente, mas saiba dinheiro foi perdido, negócios deixaram de ser feito, pessoas demitidas e imagens danificadas.