Estudo do Caso: O Ataque cracker à Vodafone Portugal

Salve jovem padawan, no artigo de hoje vamos falar sobre um ataque cracker que deixou quatro milhões de pessoas com limitação de acesso a rede de telefonia e internet em Portugal. Um caso grave devido à dimensão do ataque e o alvo, a empresa Vodafone, segundo diversos veículos da Comunicação social, as explicações vão desde ataques organizados por clãs, a inação da empresa, que pecou ao não garantir a segurança a seus clientes e não efetuar todas as diligências em atualização e segurança, alguns clientes postaram ferozmente nas redes sociais o descaso e negligencia a segurança de dados.

O que aconteceu na Vodafone Portugal?

Na noite de 07 de Fevereiro de 2022, houve um ataque massivo e orquestrado contra os serviços da Vodafone Portugal, que culminou com a queda do serviço total para um grupo de clientes, parcial e intermitente para milhões de clientes.

As autoridades portuguesas de cyber segurança estimam quem mais de quatro milhões de pessoas foram afetadas, número que poderá crescer até o final das investigações, para complicar ainda mais, o departamento de IT da Vodafone, até o momento não sabe o que ocorreu e está investigando o grau e profundidade do ataque.

Não garantindo se ocorreu vazamento de dados pessoais dos clientes e fornecedores, segundo os meios consultados os seguintes serviços foram afetados neste ataque: SMS, Telefonia Móvel, Telefonia Fixa, TV Stream, Cloud, Serviços de Fibra Ótica, Banda Larga ADSL, micro-ondas e off-line dos serviços 3G/4G/5G, em síntese praticamente todos os serviços foram afetados em maior e menor grau.

Nenhum grupo assumiu a autoria

Sempre de acordo com os meios de comunicação consultados até o momento nenhum grupo reivindicou a autoria, e segundo o comunicado dos órgãos oficiais, a linha de investigação seguida estuda a possibilidade de um ato de vingança, porém não são descartados crackers chineses e russos devidas as tensões pré-guerra na fronteira ucraniana, onde EUA, OTAN e CEE enfrentam-se diplomaticamente contra a Rússia.

O caso vem sendo acompanhado de perto pela equipe de Unidade de Combate ao Cibercrime (UNC3T) da Policia Judiciaria portuguesa, o equivalente à nossa Policia Federal, diversos de especialistas de segurança estão colaborando nesta cruzada, para descobrir o que aconteceu e por onde ocorreram.

Até o termina da escrita deste artigo, a policia diz que diferente de outros ataques ocorridos em Portugal por ransonware, até o momento nenhum resgate ou contato foi efetuado pelos cybercriminoos.

Espionagem Industrial

Jovem padawan não é filme de James Bond, mas outra linha de investigação sugere um ataque perpetrado por grupos econômicos, afinal acessar segredos comerciais, protótipos de produtos e mesmo código de fonte de aplicativos gera uma vantagem competitiva, que alguns grupos menos éticos podem-se beneficiar.

Lembre-se, novo trabalho é muito importante, um bom apps pode ser vendido por milhões de dólares, veja os inúmeros exemplos como Whatsapps, Instagram entre tantos.

Ataque ao Sistema Econômico e soberania nacional

Não se sabe ao certo, se foi dano colateral, ou alvo principal, porem durantes hora os ATM da rede Multibanco, ficaram inoperantes, devido a falha de comunicação na Vodafone, afetando a troca de informação entre a rede bancaria e atrasando os processamentos mainframe bath de todos os bancos portugueses, devido à falha de comunicações com alguns destes terminais e falha de envio dos arquivos com as operações dos clientes.

Para o púbico brasileiro ATM são as maquinas de autoatendimento bancário, administradas pela SIBS Sociedade Interbancário de Serviços, muito semelhante à nossa rede 24 horas, porem atendendo 100% da população portuguesa, pois todos os bancos do sistema financeiro são afiliados e participam.

Emergências medicas

O INEM teve que adotar os protocolos de contingencia, para garantir a prestação de serviços e o alerta em caso de emergências, devido à pane na Vodafone, apesar de momentos de tensão e incertezas, nada grave aconteceu até a altura do restabelecimento dos serviços.

Foi utilizada a r**ede SIRESP e recorrendo aos sistemas redundantes para atenderem as chamadas da população.**

Entenda sobre segurança

Atualmente todos os serviços estão centralizados em poucos Data Centers e a principal porta de entrada são ataques de Engenharia Social, vencida a primeira barreira de segurança e uma vez dentro da empresa, os cybercriminosos começam um levantamento das brechas de segurança, utilizando de inúmeros scripts próprios ou de terceiros obtidos na Dark Web e nos fóruns de hackers, na terceira fase utilizam-se de worms dormentes para infectar diversos servidores para liberar o maior número de acessos e por fim começam o DeadEnd, derrubando o máximo de serviços possíveis.

A parte mais perigosa é que durante o processo de infestação, começa o processo de cópia de informação e transmissão para outros servidores, onde serão processados, minerados e posteriormente vendidos na Deep Web, onde criminosos comuns podem utilizar as informações para chantagem e outros fins menos próprios.

Não se sabe o que ocorreu internamente na Vodafone e o quanto de informação foi vazado, a princípio os especialistas de segurança alertam, que existe uma possibilidade de invasão dos celulares de clientes, controle de Smarts TV e IOTs, visando principalmente capturar áudios e imagem através das câmeras, copiando dados financeiros e de cartão de credito.

O que é Engenharia Social?

É um ataque hacker altamente especializado contra alvos na Peopleware, pessoas altamente convincentes iniciam contatos por whatsapp, e-mail ou telefone contra os alvos previamente escolhidos e através de muita lábia, conseguem convencer a vítima a ceder tokens, user-ids e passwords de acesso.

Muitas vezes a vítima não se apercebe do ocorrido tamanha convicção e segurança passada pelo cyber criminoso, outras vezes os dados são capturados por programas sniffers, que monitoram seguimentos de rede, como exemplo cito Echelon, PRTG entre outros.

Atualmente existe uma outra categoria de programas espiões, utilizando brechas de segurança em celulares e permitindo a monitorização completa, como exemplo cito o Pegasus da empresa israelita NSO Group.

O alvo após longo escrutínio dos hackers, acaba perdendo momentaneamente o acesso aos sistemas, enquanto os hackers entram e apagam o acesso, em casos extremo, ocorreram casos em que a pessoas foi raptada e mantida em cativeiro durante o tempo do ataque.

O que é ataque Worm?

Primeiramente padawan, vamos falar sobre Worm, em informática é um malware, um pequeno software cujo o objetivo principalmente é crescer e multiplicar-se, infectando o máximo possível de computadores em uma rede.

O grande perigo do Worm e que altamente mutável, gerando clones de si com mutações para dificultar a identificação por softwares antivírus, são softwares autônomos, isto é, uma vez iniciado o processo de multiplicação e invasão, não necessita de iteração humano, explorando brechas de segurança e escondendo-se em diretórios seguros.

Ocorrido a primeira fase do ataque worm, com os computadores comprometidos, inicia-se a segunda fase que consiste em instalar bots, ou seja, uma gama de serviços maléficos, que os hackers utilizaram para fins maléficos, desde ataques de negação de serviço, a roubo de dados e no pior deles destruição de hardwares, softwares e base de dados.

O que é Bots?

São os programas que funcionam sem necessidade de comandos humanos, em sua sub-classe Malware, são utilizados em conjunto com o worms, para neutralizarem defesas das redes infectadas, possibilitando aos hackers controlarem inúmeros periféricos e acessarem base de dados. São também conhecidos como botnets, devido a sua afinidade e dependência de redes para espalharem-se e operarem.

O que é ransonware

Esta é a modalidade mais FDP de ataque cybernetico, no passado acontecia contra pessoas, as vezes por gozação, obrigando a vitima a postar fotos humorísticas/humilhantes, ir até um lugar publico com uma vestimenta ou cartaz, porem com o passar dos anos evoluir para a velha tradicional chantagem, onde grupos solicitam a transferência de crypto-moedas ou transferências via paypall ou western union.

O computador algumas vezes fica totalmente bloqueado, após o ataque, mas na maior parte das vezes, após o furto das informações e acesso a documentos, o hacker apenas informa a vitima através de um pop-up solicitando o pagamento.

Em caso mais cruéis incluem até um relógio com contagem regressiva até o momento final, causando mais danos psicológicos e danos morais a vitima.

O que é Malware?

Caro padawan como deve ter visto nos parágrafos anteriores o Malware é uma categoria de Software projetada para usos criminosos e maleficos, sendo que exploram vulnerabilidades conhecidas e mesmo desconhecidas de software, vide ZeroDay. Muitos casos os hackers estudam Sistemas Operacionais a fundo, para encontrar bugs, utilizando-se de engenharia reversa e descompilaçao para acessarem códigos fontes.

O que são falhas Zero Day?

Zero-day ou 0day, em desenvolvimento de softwares, são bugs descobertos por hackers, mas que o fabricante/desenvolvedor do software desconhece, por isso a expressão zero dias referindo o tempo que a softhouse sabe da existência do problema.

Normalmente são publicados artigos sobre falhas Zero Day em comunidades hackers e/ou acadêmicas, neste momento é iniciada a corrida, de um lado equipes Jedi tentando minimizar o dano, bloqueando a brecha, a empresa desenvolvedora criando atualizações de segurança para proteger a base de clientes e usuários e por outro lado Crackers atualizando worms e bots para explorarem maliciosamente esta falha.

O perigo vive na Cloud e está à espreita

Vivemos tempos estranhos e perigosos, ao migramos para nuvens, muitos Data Centers acumulam informações pessoais e vitais, a segurança destes dados é vital, por isso muito cuidado com o trabalho remoto, pois perdemos o contato com as pessoas da empresa e somos vítimas fáceis a cyber-ataques.

Nos como membros ativos da comunidade DEVs, devemos ter cuidados adicionais quando codificamos, evitando deixar bugs que serão explorados por hackers, ter atenção especial ao utilizar softwares open-source, garantir a segurança de nossos equipamentos através de senhas fortes e robustas.

Evite utilizar-se softwares piratas ou crackeados, muito cuidado com mensagens estranhas, solicitando acesso e fornecimento de senhas a terceiros. Atente se seu equipamento tem antivírus e todas as atualizações de segurança foram exploradas.

Não forneça seu user-id, senha e token de acesso a terceiros, o uso é pessoal e intransferível, você poderá perder seu emprego e ainda ser processado criminalmente. Não sendo alarmista, mas todo cuidado é pouco.

Momento MegaJaba

O tiozão é mainframe raiz, são mais de 3 décadas dedicado aos sistemas centrais baseados em Z/OS da IBM e garanto o super xerife RACF é a prova de invasão, sendo que ataques contra mainframes é muito difícil e raro, devido à complexidade da tecnologia e as barreiras de acesso aos serviços.

O que devemos aprender com isso? A segurança é fator indispensável para toda e qualquer empresa, o software deve ser robusto, o hardware a prova de penetração e os profissionais de segurança devem ser altamente treinados e qualificados.

Não adiante colocar empresas terceirizadas que contratam funcionários com salários irrisórios e expostos a longas jornadas de trabalho para garantirem o funcionamento de atividades críticas do negócio, muitas vezes os cybercriminosos subornam funcionários para obterem acesso e conhecimento do workflow de trabalho, executivos demitidos e com grande conhecimento são outros procurados para ações deste tipo.

O investimento é necessário, treinar, capacitar e remunerar bem profissionais de IT é primordial, afinal danos de imagens e a repercussão negativa na imprensa internacional e fator decisivo para o sucesso ou fracasso de uma empresa.

Conclusão,

Foi um texto longo, mas necessário jovem padawan, tu es novo na jornada, as vezes por inocência pode prejudicar-se e causar danos a empresa, perdoe o tiozão por excesso de zelo, mas segurança é primordial e com a nova LGPD, tudo virou questão de vida e morte.

Empresas podem sucumbirem devido as elevadas multas, processos criminais por negligência e responsabilidade civil, dados pessoais vazados podem destruir a imagem e reputação das vítimas, imagine os hackers tendo acesso a sua vida pessoal, vida financeira, pastas de vídeos e imagens, conhecimentos de hábitos e costumes. É vital nos programadores unidos protegermos nossos códigos através de testes e adoção de boas praticas em programação.

Como citei muitos jornais, desta vez, deixei ao final os links, lembrando que na internet tudo é tão dinâmico e fugaz, que as matérias podem não estar mais disponíveis em datas futuras.

Saiba mais sobre o ataque a Vodafone

<https://zap.aeiou.pt/ataque-a-vodafone-espiar-camara-micro-461958>

<https://www.cisoadvisor.com.br/vodafone-portugal-sofre-ataque-servicos-sairam-do-ar/>

<https://www.dn.pt/sociedade/vodafone-e-a-mais-recente-vitima-em-6-anos-onde-saude-tambem-e-alvo-14570078.html>

<https://ionline.sapo.pt/artigo/761772/ataque-a-vodafone-espionagem-industrial-e-uma-das-pistas-?seccao=Portugal_i>