FIESP: Painel 2 – Palestra Ransomware

Transcript dos slides apresentados no evento promovido pela FIESP : Proteção X Sequestro de Dados Pessoais - A importância da conscientização sobre proteção de dados pessoais; Ransomware – nova modalidades sequestro de dados; precauções e pontos de atenção para empresas, 2º painel, realizado na sede da FIESP em São Paulo, na data de 21 de Junho de 2017.

Slide-1: Ransomware – nova modalidades sequestro de dados

Bom dia a todos!
Primeiramente agradeço à organização do evento pelo convite, representado pela Diretoria de Segurança da FIESP, para participar desse painel. É um prazer ter a oportunidade de estar aqui no berço da Industria e compartilhar um pouco de nossa experiência.
Meus parabéns à mediadora desse painel, Dra. Florence, que muito contribuiu na confecção dessa minha apresentação, e também aos companheiros de mesa Dr. Caio e Dr. Paulo por suas apresentações.
Como estamos tendo a honra de estar aqui na casa da Industria, minha apresentação traz, fundamentalmente, nossas preocupações com o ransomware nas redes industriais.
Vamos iniciar a primeira parte da apresentação desse painel com uma pequena demonstação da ação de um ataque de ransomware pelo vetor de ataque mais comum que são os e-mails.

Slide-2: Ransomware em ação

Note que o usuário está trabalhando e consegue abrir suas planilhas, verificar o conteúdo, sem grandes problemas até então.
Mas o usuário recebe um e-mail com um anexo, e inadvertidamente ele abre esse e-mail.
Sem perceber uma série de ações estão sendo executadas a partir do momento que ele abriu o anexo de e-mail e então o usuário é surpreendido com as mensagens características da infecção por ransomware.
E o usuário tenta abrir seus arquivos, mas os arquivos foram todos encriptados e não são mais reconhecidos no ambiente operacional do usuário. Na verdade esses arquivos não poderão mais serem abertos, a exceção que o usuário tenha backup desses arquivos.

Slide-3: Sobre os tipos de vírus

Bem, nós vamos falar do ransomware e pra contextualizar eu listei algumas classes de pragas digitais, que sempre aparecem nos contextos envolvendo o tema de vírus de computador.
Malware é um termo que vem do inglês **Mal**icious Soft**ware**, e consiste em um programa que tem como principal característica a execução de uma ação no dispositivo infectado.
Spyware, assim como o Malware, vem do inglês **Spy** Soft**ware**, e essa categoria de malware têm como objetivo monitorar as atividades de um sistema.
Os bots, que vem do inglês Ro**bots**, são programas capazes de se propagar valendo-se de falhas nos programas, permititindo comunicação com o invasor.
Os Cavalo de Tróia, termo que também veio do inglês **Trojan Horse**, são programas projetados para serem recebidos como “presentes”, porém, além de executar as funções para as quais foram programados, executam outras sem o conhecimento do usuário.
Worm é outro tipo de malware capaz de se propagar autônoma por meio de redes, enviando cópias de si para outros computadores, também se valendo de falhas em programas.
Os Keyloggers, são programas que capturam e armazenam as teclas digitadas no computador infectado. E a lista é grande, mas penso que esses são os mais comentados.

FIESP: Painel 2 – Palestra Ransomware

Slide-4: O que é o Ransomware

O ransomware é um malware que tem por objetivo bloquear o acesso à arquivos e sistemas, encriptando os dados da vítima e solicitando resgate dos dados mediante um pagamento, cuja moeda de negociação é normalmente a moeda digital denominada Bitcoin.
Quando falamos em encriptar os arquivos, é importante compreender que um arquivo é quebrado em milhares de partes em um dispositivo, como disco rígido de um computador, e ordenados de uma forma sequencial. Encriptar é semelhante a embaralhar essa sequência lógica por uma formulação matemática, que chamamos de algoritmo, de forma não ser mais possível o reconhecimento desses arquivos pelos aplicativos.
E existem duas classes de ransomware: o Locker, que apenas bloqueia o acesso ao dispositivo, ação mais comum nos ataques em smartphones, e o Crypto que, como o nome sugere, encripta os dados que encontrar nos drives lógicos.

Slide-5: Você pode ser infectado por ransomware quando:

E podemos sofrer a infecção por ransomware quando acessar um website comprometido, abrir anexos de e-mails phishing, conectar dispositivos USB e HD's extarnos infectados, fazer instalação de apk's suspeitos, deixar e instalar os patches de segurança dos sistemas, lembrando que o WannaCry infectou as máquinas que não tinham o patch MS17-010 instalados, malwares que vem embutidos em programas suspeitos, e outras vulnerabilidades, como antivírus desatualizados.

Slide-6: Ransomware: Anatomia do ataque

Eu divido o processo de infecção por ransomware em seis estágios. E é importante dividir em fases porque podemos identificar algumas ações isoladas a cada estágio analisado.
O primeiro estágio é o da distribuição, via os vetores que elencamos no slide anterior
O segundo estágio é o da infecção, quando o malware alcança o dispositivo e inicia os processos de sinalizar as principais syscalls do ambiente operacional do dispositivo pra controlar o sistema operacional e completar as atividades de infecção.
O terceiro estágio é onde o ransomware se comunica com os servidores remotos para gerar as chaves de criptografia e obter a chave pública, necessária para criptografar os dados.
No quarto estágio o ransomware varre o ambiente para localizar todos os arquivos do ambiente.
O quinto estágio é onde ocorre o processo da criptografia dos arquivos, e nesse estágio o ransomware exclui os pontos de restauração, e no caso do Windows exclui também o conteúdo do Volume Shadow Copy.
E o sexto e último estágio é onde ocorre o crime de extorsão, com o pedido de resgate dos dados, normalmente em bitcoin.

Slide-7: Ransomware: evolução

Esse slide ilustra a evolução dos tipos de ransomware que foram desenvolvidos ao longo dos anos. Note que nos dois últimos anos de 2015 e 2016 o crescimento é bastante preocupante, e da para se ter uma idéia do que ainda está por vir. O aparecimentos de diferentes tipos nesses números implica em refletir se os ataques por ransomware estão tendo retorno para os criminosos a ponto de se propagar com esse expectro de crescimento.

FIESP: Painel 2 – Palestra Ransomware

Slide-8: Penetração do WannaCry em 12/05/2017

E como consequência do crescimento desse espectro, o mundo assistiu uma das maiores atividades de ataque cibeernético de todos os tempos com o WannaCry, no dia 12 do mês passado.

Slide-9: Redes Industriais - ICS

Bem, hoje estamos aqui no berço da Indústria, e eu quero chamo a atenção para os riscos de infecção por ransomware as redes industriais. ICS vem do inglês, Industrial Control System.

Slide-10: Controle das Redes Industriais - Sistemas SCADA

As redes industriais são controladas pelos sistemas SCADA. SCADA vem do inglês Supervisory Control And Data Aquisition, e o ambiente das redes industriais diferem das redes corporativas porque elas operam em regime de missão crítica, um ambiente onde, nos dias atuais, não cabe mais o serviço manual. E todo impacto em uma planta de uma rede industrial vai afetar todo o processo da cadeia de produção.

Slide-11: Ransomware nas redes industriais - ICS

E os ataques na infraestrutura crítica e nas redes industriais não são muito documentados. Há uma razão muito forte para evitar essa divulgação, que está relacionado ao impacto do dano à imagem da empresa. Mas nessa linha do tempo podemos verificar que ao longo dos anos temos presenciado inúmeros ataques, com sucesso, tanto na infraestrutura crítica como nas redes industriais.

Slide-12: Ransomware nas redes industriais - ICS (cont.)

Essa parte superior do diagrama representa a rede corporativa de uma empresa, que é normalmente o foco das reportagens na mídia, como dos recentes ataques de ransomware.
Na parte de baixo do diagrama está representada uma rede industrial, presente na infraestrutura crítica como sistema de transportes (trens, aviões, metrô, etc), sistemas de fornecimento de energia, usinas nucleares, estações de tratamento de água, indústria do agro-negócio, indústrias petroquímicas, e todas as indústrias de uma maneira geral.
Na parte inferior da rede industrial temos o nível do campo, onde ficam os sensores e os instrumentos das plantas das indústrias, mais acima temos nível de comprole, com os controladores lógicos programáveis controlando esses sensores e instrumentos, e mais acima temos nível de supervisão, onde estão os chamados sistemas supervisórios, conhecidos também como sistemas SCADA, que controlam as unidades de produção de forma automatizada, porque nos dias atuais não tem mais condições de controlar processos tão complexos de forma manual.
A rede corporativa nós conhecemos bem, e quanto às redes industriais, eu compartilho com vocês minha percepção sob o aspecto da ameaça de ataque por ransomware, e nesse sentido, esse é o cenário ideal em que a rede industrial está completamente separada da rede corporativa. Dessa forma a rede estaria imune aos agentes externos que poderiam levar riscos à essa rede extremamente complexa de se gerenciar.

Slide-13: Ransomware nas redes industriais - ICS (cont.)

Até que um colaborador tem a brilhante idéia de trazer um pen drive pra fazer uma atualização do sistema porque o acesso à rede corporativa e à internet não é possível, e dessa forma ele traz a atualização sem saber que está expondo a rede à riscos de ataques.

FIESP: Painel 2 – Palestra Ransomware

Slide-14: Ransomware nas redes industriais - ICS (cont.)

Ou então quando mão de obra especializada em sistemas SCADA vem fazer manutenção no ambiente do cliente, trazendo seus computadores, pen drives, discos externos, etc. Porque esses sistemas são de missão crítica, rodando 24/7 e eles requerem manutenção periódica.

Slide-15: Ransomware nas redes industriais - ICS (cont.)

Ou então quando a alta gerencia pressiona a área de TI para ter acesso aos dados de produção, e solicita a criação de um link de acesso para essas redes industriais, em alguns casos isso é feito via acesso a um drive lógico na rede industrial, em outros um servidor web na rede industrial para ser acessado pela rede corporativa que, se for hackeada, uma das primeiras ações do hacker será fazer os movimentos laterais para encontrar um serviço que tiver maior criticidade para a empresa, como por exemplo um sistema SCADA.

Slide-16: Ransomware nas redes industriais - ICS (cont.)

Ou ainda o pior cenário, quando a rede industrial é exposta diretamente na internet. Normalmente esse cenário é desconhecido pela gestão de TI das empresas, que não tem gestão dos processos industriais, a exceção de algumas poucas empresas com mais maduridade em seus sistemas de gestão.

Slide-17: Ransomware nas redes industriais - ICS (cont.)

E da mesma forma que usamos o google para encontrar informações do que procisamos na internet, existem serviços especializados em buscar dispositivos nas redes industriais, expostos para a internet, como o ZoomEye que é um motor de busca que faz a varredura de portas abertas nesses dispositivos e análise de fingerprint. Na data de ontem que eu fiz a pesquisa, 20/06, haviam quase 800 milhões de dispositivos disponíveis para acesso e mais de 132 milhões de recursos web.

Slide-18: Ransomware nas redes industriais - ICS (cont.)

E a consequência disso é que um indivíduo mal intencionado pode facilmente ter acesso a uma central de controle industrial exposta na internet, explorar as inúmeras vulnerabilidades desse ambiente, que normalmente não está sob gestão de segurança da informação das equipes corporativas de TI, e da pra imaginar as consequências de um ransomware ou um malware acançando uma central de controle de uma rede industrial.

Slide-19: Ransomware: Padrões observados

Há alguns padrões que observamos no comportamento dos ataques via ransomware, mas dois pontos eu chamo a atenção: primeiro, com relação aos vetores de infecção, percebemos que o fator humano é ainda o principal ponto de falha nos ataques via ransomware. No caso do WannaCry, a campanha inundava o ambiente de e-mails das empresas na ordem de 5 milhões de e-mails/hora, e a capacidade de penetração se deu principalmente em virtude das aberturas dos anexos nos e-mails phishing.

Outro ponto que chama a atenção é o processo de geração das chaves criptográficas do ransomware. Que fica armazenado em servidor remoto, normalmente hospedado na rede TOR.

Então, bloquear os serviços de proxy como TOR, I2P, domínios “.onion” e endereços IP’s

maliciosos (blacklist) constitui uma ação valiosa para minimizar a probabilidade de infecção por ransomware.
Esse site do ransomware tracker (https://ransomwaretracker.abuse.ch/feeds/) fornece uma lista atualizada a cada 5 minutos de sites e endereços IP's que servem de propagação de ransomware, e é uma boa prática construir blacklists baseados nessas fontes.

Slide-20: Ransomware: Engenharia Social x Hackers

No contexto do ransomware e do tema Engenharia Social, eu trouxe uma experiência que aconteceu comigo no mês passado para compartilhar com vocês.
Recebi um telefonema de uma empresa, aqui da região da Paulista, que disse que eu tinha sido recomendado para lidar com um problema de ransomware que eles estavam enfrentando.
E o cenário era o seguinte: a empresa tinha sido alvo de infecção por ransomware. A empresa terceirizada que cuidava do backup, constatou que o backup mais recente que eles conseguiriam restaurar era de outubro de 2016.
Eles estavam muito inclinados a pagar pelo resgate, mas consideramos tentar uma abordagem de negociação, que nada mais era do que utilizar Engenharia Social para tentar sensibilizar o criminoso do outro lado, em outro país.
A conversa se iniciou, e eu comecei dizendo que não sabia o que era biticoin, que a cidade era pequena e que eu morava distante da cidade, mas conseguia me comunicar com eles porque havia um posto de serviços de saúde, que quando funcionava o serviço de internet eu conseguia utilizar pra conversar com eles e fui sustentando essa conversa durante os dias que conversava com eles via o terminal do ransomware Nemesis que eles disponibilizavam para negociações.
E para minha surpresa, depois de trez dias de conversas, a mensagem do hacker: No need to pay. This is a gesture of goodwill. (Não precisa pagar. Isso é um gesto de bondade.).
Passou as instruções para decriptar os dados e ainda deu várias sugestões em como tornar o ambiente mais seguro.
Somente para reforçar que a Engenharia Social é uma ferramenta poderosa e pode funcionar até mesmo com os hackers.

Slide-21: Recomendações para Backup

Importânte: No caso de um ataque por ransomware, o backup será a melhor alternativa para restaurar os dados.
A empresa está monitorando o sistema de backup? Se o serviço é terceirizado, quem monitora?
Em relação aos backups, mantenha-os atualizados e monitore os logs diariamente.
Quanto aos tipos de backup, considere o automático e se existir espelhamento de servidores, considere o espelhamento passivo para o cenário envolvendo ransomware.
Com relação a frequência, considere backup diário na medida que os dados são alterados.
Mas e se o backup falhar? Possui alguma redundância?
Os casos que tive conhecimento de pagamento do ransomware ocorreram quando a empresa descobriu que seu sistema de backup não estava funcionando.

Slide-22: Recomendações gerais aos usuários

Faça backup regularmente e mantenha o backup separado do computador, como um disco rígido externo.
Mantenha os sistemas de proteção atualizados, eles precisam ser atualizados diariamente.
Adquira somente software original e licenciado.

FIESP: Painel 2 – Palestra Ransomware

Pense muitas vezes antes de abrir um anexo de e-mail.
Tome cuidado com as mídias removíveis que você conecta em seu computador.

Slide-23: Recomendações Corporativas

Manter Antivírus/Anti-Ransomware atualizados e monitorar os logs diariamente.
Promova regularmente a auditoria de software para revisão dos sistemas. Considere fazer uso do Windows AppLocker, um recurso da rede Microsoft que permite controlar quais programas podem ser utilizados na empresa. Programas não autorizados serão bloqueados.
Revise periodicamente as políticas de segurança da informação da empresa. Antes a preocupação era a rede, hoje temos a preocupação com a nuvem, os dispositivos IoT, entre outros, e a política de segurança da empresa está contemplando essa evolução?
Simule testes de invasão não intrusivos para avaliar possíveis vulnerabilidades que possa estar expondo os ativos da empresa em risco.
E o principal : Treine seus usuários. O fator humano continua sendo um dos principais pontos de falha.

Slide-24: FIM

Bem pessoal, o tema na verdade é bem extenso, era isso que eu queria compartilhar com vocês, e acredito que os pontos apresentados são de grande relevância para a indústria em relação às ameaças que foram apresentadas, e também as que ainda estão por vir.

Muito obrigado pela atenção, e um excelente dia a todos.