UNIVERSIDADE DO SUL DE SANTA CATARINA

DANIEL ROCHA PHILOT

SEGURANÇA DA INFORMAÇÃO:
ATAQUES RANSOMWARE E PROTEÇÃO DE DADOS

Palhoça

2021

DANIEL ROCHA PHILOT

SEGURANÇA DA INFORMAÇÃO:
ATAQUES RANSOMWARE E PROTEÇÃO DE DADOS

Relatório de pesquisa na modalidade de Estudo de Caso apresentado ao Curso de **Tecnólogo em Gestão da Tecnologia da Informação** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientadora: Prof[a.] Patrícia da Silva Meneghel, Dr.

Palhoça

2021

DANIEL ROCHA PHILOT

SEGURANÇA DA INFORMAÇÃO:
ATAQUES RANSOMWARE E PROTEÇÃO DE DADOS

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado, em sua forma final, à aprovação na unidade de aprendizagem de Estudo de Caso, do curso de **Tecnólogo em Gestão da Tecnologia da Informação** da Universidade do Sul de Santa Catarina.

Palhoça, de de 2021.

_____

Professora e orientadora Patrícia da Silva Meneghel, Dr.
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço aos familiares, amigos e professores por todo incentivo, paciência e ajuda dispensados nesse inspirador processo de aprendizado.

Em especial destaco: Ana Luiza dos Santos Rocha, Paula Brasil, Augusto Baade, Eduardo Younes, Mirian Brasil, Rosiane Terra Soares, Prof. Fabio Eduardo Vieira Angelo, Prof. Roberto Fabiano Fernandes, Alan Bittencourt, Sebastião Fonseca, Thiago Simonin e a todos aqueles que já não estão mais presentes, mas que de alguma forma contribuíram na minha decisão em obter essa graduação.

RESUMO

O objetivo deste estudo de caso visa, além de discorrer sobre a definição, características e variantes dessa modalidade de ataque cibernético conhecida como ransomware, analisar os principais casos, os fatores motivadores, as vulnerabilidades exploradas, os impactos e as medidas de segurança que estão amplamente sendo adotadas para proteção contra essa ameaça. Através de uma pesquisa explicativa utilizando uma abordagem qualitativa, busca-se elucidar os efeitos devastadores desse tipo de ataque e seus impactos na sociedade. Por intermédio de um questionário, observa-se as opiniões de especialistas sobre o assunto e suas expectativas para o futuro, tanto com relação aos ataques, quanto às medidas protetivas, avaliando também o nível de maturidade das empresas no que tange a segurança da informação. Por fim, verificou-se uma assustadora previsão com o aumento desses ataques através de novas e sofisticadas variantes, obrigando as organizações a repensarem as estratégias de proteção dos seus dados, levando em consideração o seu valor.

Palavras-chave: Ransomware. Segurança da informação. Tecnologia.

SUMÁRIO

1 INTRODUÇÃO

Cibercriminosos ou crackers são conhecidos como indivíduos ou grupos, dotados de certa especialidade em informática e redes de computadores, que usam seus conhecimentos para invadir e praticar uma série de atividades maliciosas em sistemas de informação de empresas, pessoas ou governos, seja para benefício próprio, em prol de terceiros ou por razões obscuras.

Essas atividades maliciosas, conhecidas como ciberataques, estão se tornando cada vez mais comum e crescentes, devido a difícil rastreabilidade e consequentemente responsabilização e punição dos envolvidos.

> A Internet é uma nova fronteira indomada. Ela inclui quase todo governo, empresa e organização do planeta. Diferente da sua vida diária, no ciberespaço, não existe uma lei real da terra. Atos criminosos que levam a destruição e roubo ocorrem com regularidade. Os criminosos normalmente não são punidos. Às vezes, os atos até mesmo nem são descobertos. (DAVID, KIM, E SOLOMON, MICHAEL G. *FUNDAMENTOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO*. 2014, P.64).

Um tipo de ciberataque que vem ganhando destaque nos noticiários são os provenientes de um software malicioso (malware) conhecido como ransomware. Malware é uma definição abrangente que serve para categorizar desde aplicativos espiões, os spywares usados para monitorar seu comportamento e roubar seus dados, a ransomwares, que capturam o sistema, criptografam seus arquivos e exigem resgate para que você recupere acesso aos seus dados. (GARRET, FILIPE 2021).

Este estudo de caso visa trazer um maior entendimento sobre os ataques ransomware e como os dados podem ser protegidos contra essa ameaça, abrangendo definição, características, variáveis, fatores motivadores, os casos famosos recentes, os impactos gerados e a importância da segurança da informação como prevenção e defesa dentro desse contexto.

1.1 PROBLEMA

De acordo com dados divulgados no primeiro semestre de 2021, pela Check Point Software Technologies LTD, fornecedora de soluções de cibersegurança, os números de ataques de ransomware no Brasil cresceu acima da média global, com um aumento de 92% desde o início de 2021, portanto o presente estudo faz os seguintes questionamentos: O que é um ataque ransomware? Como esses ataques costumam acontecer? Que tipo de vulnerabilidade eles exploram? Quais são os riscos desse tipo de ataque? O que fazer ao ser atacado e como evitar essa ameaça?

1.2 JUSTIFICATIVA

Esse tipo de ciberataque está cada vez mais comum e lucrativo, tendo como vítimas de organizações a pessoas físicas, dado a natureza internacional dessa atividade, os criminosos não temem processos em seus países de origem, tornando-se um negócio bilionário (SCHNEIER, BRUCE, 2020).

> Hoje, o dinheiro está online e, cada vez mais, os criminosos também. Eles roubam de nossas contas bancárias. Roubam informações de cartões de crédito e as usam para cometer fraudes ou roubam informações sobre nossas identidades e as usam. Também bloqueiam nossos dados e cobram um resgate para liberá-los — isso é ransomware. (SCHNEIER, BRUCE. *CLIQUE AQUI PARA MATAR TODO MUNDO.* 2020, p. 63).

Com a popularização do uso de smartphones, crescimento de compras e transações online e armazenamento de praticamente todos os dados em nuvem, a abordagem do tema e suas delimitações servem como pontos de reflexão sobre a vulnerabilidade de dados e informações pessoais, corporativas e governamentais, além da relevância quanto a perda, roubo ou divulgação desses conteúdos e os meios de proteção contra uma das formas de ciberataque mais ameaçadoras da atualidade.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Analisar casos ocorridos de ataques ransomwares em organizações brasileiras, a fim de ter uma compreensão sobre a forma como ocorrem, quais os tipos de vulnerabilidades de ambientes que são favoráveis, além de indicar formas de proteção contra as ameaças.

1.3.2 Objetivos Específicos

a) Definir um ataque ransomware, suas características e variantes;
b) Elucidar os fatores motivadores;
c) Identificar as falhas de segurança mais comuns que propiciam esse tipo de ataque;
d) Expor e analisar dois casos ocorridos nas seguintes organizações: Lojas Renner e Superior Tribunal de Justiça;
e) Compreender os impactos gerados após um ataque;
f) Registrar possíveis soluções reativas e proativas, baseado em opiniões de especialistas da área.

2 REVISÃO DA LITERATURA

O principal elemento que se destaca neste estudo de caso são os dados e no que fere a sua confidencialidade, integridade e disponibilidade, sendo esses considerados os três pilares da segurança da informação (LENTO, LUIZ OTÁVIO BOTELHO, 2011, p 20):

- A confidencialidade envolve a privacidade de dados e informações sensíveis (confidenciais) em ambientes computacionais contra acesso não autorizado (Lento, LUIZ OTÁVIO BOTELHO, 2011, p 23);
- A integridade envolve incorruptibilidade de dados e informações, seja de forma acidental ou intencional oriundos de acesso não autorizado (LENTO, LUIZ OTÁVIO BOTELHO, 2011, p 24);
- A disponibilidade consiste na capacidade de manter dados e informações sempre acessíveis para quem lhe é de direito (LENTO, LUIZ OTÁVIO BOTELHO, 2011, p 24).

Fica convencionado e subentendido que todas as explicações sobre dados que envolvam proteção, perda, roubo, bloqueio, comprometimento, manipulação e vulnerabilidade se referem a dados pessoais (usuários domésticos) ou organizacionais, quando não explicitamente identificados, como arquivos que envolvam textos, planilhas, fotos, vídeos, músicas e outras mais específicas, como conteúdos utilizados por programadores, desenvolvedores e sistemas em organizações, que ficam armazenados em dispositivos destinados a esse fim, como discos rígidos e SSD em computadores, storages e serviços de armazenamento em nuvem como Google drive e Amazon Web Services.

Apesar desse assunto não ser abordado diretamente neste estudo, o armazenamento em nuvem, segundo a Amazon: "é um modelo de computação em nuvem que armazena dados na Internet por meio de um provedor que gerencia e opera o armazenamento físico de dados como serviço". Esses provedores, como a própria Amazon, Google e Microsoft por exemplo, entrega essa capacidade de armazenamento de forma gratuita (limitada) ou paga, seja por um plano de dados ou conforme o uso, sendo também os responsáveis por gerenciar a capacidade, resiliência e segurança desses dados, até certo ponto.

Mas como é feito a segurança desses dados pelos serviços de armazenamento em nuvem? A criptografia é um método de segurança amplamente utilizado para proteção de dados e consiste em processos de codificação e decodificação de arquivos. Para David, Kim, e Solomon, Michael G. (2014, p.11) “Codificação é o processo de transformar dados de texto claro para texto cifrado. Dados em texto claro são aqueles que qualquer um pode ler. Texto

cifrado são os dados misturados que resultam da encriptação de texto claro [impossibilitando sua leitura]. O provedor ou criador da criptografia possui uma chave, que é um pedaço de informação que controla todos os processos da criptografia (codificação e decodificação), arbitrando quem pode ou não ter acesso a determinados dados, tornando essa ferramenta valiosa na segurança da informação, mas em contrapartida, perigosa quando utilizada por cibercriminosos (DAVID, KIM, E SOLOMON, MICHAEL G, 2014).

Em se tratando de tecnologia da informação, imprevistos são esperados, mesmo que frustrantes do ponto de vista do usuário e preocupantes (ou até catastróficos) do ponto de vista organizacional: Computadores e smartphones apresentam lentidão e travamentos. Aplicativos param de funcionar. Sites na internet não carregam devidamente seus conteúdos. Quando tudo parece ter perdido o controle, por vezes basta reiniciar o programa, computador ou dispositivo, independente da causa, às vezes perde-se dados importantes, obrigando em alguns cenários sua salvaguarda compulsiva, através de backups de arquivos em outros locais ou usar sistemas que fazem essa tarefa de forma automatizada. (SCHNEIER, BRUCE, 2020).

Esses imprevistos estão relacionados ao fato de que a maioria dos softwares são desenvolvidos de maneira inadequada, salvo raras exceções, pois um software de qualidade demanda maior tempo e investimento para ser criado, algo que não é compatível com as necessidades do mercado, em que custo e prazo de entrega são mais importantes do que a qualidade, levando também em consideração o nível de exigência da maioria dos consumidores, que não estão muito dispostos a pagar o preço por algo melhor desenvolvido. Devido a isso, softwares modernos apresentam uma infinidade de defeitos, falhas ou erros de código que provocam seu mau funcionamento [bugs] e que não foram resolvidos durante seu processo de desenvolvimento (SCHNEIER, BRUCE, 2020).

Vulnerabilidades são definidas segundo a segurança da informação, como qualquer ponto fraco em um sistema que possibilite que uma ameaça cause danos a ele. Uma ameaça é qualquer ação que possa danificar um ativo (DAVID, KIM E SOLOMON, MICHAEL G., 2014). Alguns bugs também são vulnerabilidades, pois viabilizam sua exploração, através da execução de comandos arbitrários e até o controle total de suas funções, abrindo brechas para diversos tipos de ameaças, como os ciberataques. Apesar de não ser possível definir com clareza quais bugs também são vulnerabilidades e quais vulnerabilidades são exploráveis, é fato que todo sistema possui milhares de vulnerabilidades exploráveis, tornando apenas a questão da invasão como simples ou não (SCHNEIER, BRUCE, 2020).

> O software do qual dependemos — aquele que está rodando em nossos computadores, telefones, veículos e aparelhos médicos conectados à Internet, em sistemas que controlam nossa infraestrutura essencial — é inseguro sob vários pontos de vista. Essa não é simplesmente uma questão de encontrar algumas vulnerabilidades e consertá-las; existem muitas para isso. É um fato da vida do software com que teremos que conviver em um futuro próximo. (SCHNEIER, BRUCE, 2020, P. 18).

A situação se agrava com a popularização dos dispositivos IoT (A Internet das Coisas), um conceito que se refere à interconexão digital de objetos cotidianos com a internet (MOHAMMADI ZANJIREH, MORTEZA & LARIJANI, HADI, 2015) para controle remoto e outras funcionalidades, de domésticas a industriais. Tais objetos, como geladeiras, termostatos, smart tvs, sensores industriais e até automóveis, são regidos por softwares, muita das vezes, feitos sob encomenda e suscetíveis aos mesmos bugs e vulnerabilidades citados anteriormente.

Segundo o relatório de janeiro de 2017 do Gartner Inc, líder mundial em pesquisa e aconselhamento imparcial em tecnologia, até 2020 os dispositivos conectados em todas as tecnologias atingirão 20,6 bilhões. A correção das vulnerabilidades desses dispositivos, que porventura tenham sido lançadas pelo fabricante, é uma questão que pode passar despercebida, seja pela falta de compreensão da necessidade, seja pela complexidade envolvida na atividade, tanto para um usuário doméstico, quanto em um meio corporativo, sendo nesse último, o mais preocupante, visto que pouco adiantaria manter uma rede de computadores com todos os seus componentes com as últimas correções de vulnerabilidades aplicadas e esquecer daquele dispositivo IoT que utiliza a mesma rede, como por exemplo um termostato ou sensor de presença, deixando o ambiente vulnerável a ciberataques.

> Todos os computadores podem ser infectados por um malware. Todos os computadores podem ser comandados por um ransomware. Todos os computadores podem ser arrastados para uma botnet — rede de dispositivos infectados com malwares — controlada remotamente. Todos os computadores podem ter seus dados apagados remotamente. A função pretendida deste computador embarcado ou o dispositivo IoT no qual o computador é construído não faz diferença. Hackers podem explorar dispositivos IoT da mesma forma que atualmente exploram desktops e notebooks. (SCHNEIER, BRUCE, 2020, p. 23).

3 PROCEDIMENTOS METODOLÓGICOS

3.1 CARACTERIZAÇÃO DO ESTUDO

A pesquisa é de caráter explicativo com uma abordagem qualitativa, visando buscar as causas e efeitos de um ataque ransomware e identificar medidas protetivas.

3.2 CAMPO DE ESTUDO

Este trabalho utiliza como base uma investigação bibliográfica sobre ataques ransomware em livros e sites na Internet, analisando dois casos ocorridos em organizações brasileiras, além de buscar opiniões de especialistas da área de segurança da informação, analisando os fatores motivadores desses ataques e a importância na preservação de dados pessoais e corporativos.

3.3 INSTRUMENTOS PARA COLETA DE DADOS

Análise de materiais pesquisados, questionários direcionados a especialistas em segurança da informação e observação participante com a relação aos assuntos abordados.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

4.1 DEFINIÇÃO, CARACTERÍSTICAS E VARIANTES DE RANSOMWARE

A Kaspersky, empresa especializada em soluções para segurança da informação, explica que ransomware é a junção de dois termos em inglês "ransom" e "malware", sendo que a primeira significa “resgate”, definindo-o então como “um software malicioso que pode bloquear o seu computador, exigindo um resgate para desbloqueá-lo”.

Suas variantes e formas de ataque são bem diversificadas, que vão desde o bloqueio parcial (Scareware) ou total (Screen lockers) das funções de um sistema operacional, até a modalidade que o popularizou: a criptográfica, que envolve a criptografia parcial ou total dos dados de uma maneira praticamente impossível de ser decodificada, devido a utilização de algoritmos complexos na criação das chaves criptográficas. Porém o que todas elas têm em comum são um pedido de resgate, que são gerados automaticamente pelo malware durante sua ação e consiste em uma nota em arquivo texto ou imagem inserida em locais no sistema de fácil visualização pela vítima. Essa nota geralmente é um texto informando o que aconteceu com os dados e instruções de pagamento para resgatá-los, normalmente exigido em uma moeda virtual, como o bitcoin. Na maioria dos casos existe um prazo para esse pagamento, sob algum tipo de ameaça em caso de não cumprimento. Geralmente todas as negociações são feitas através de troca de e-mails (TUPINAMBÁ, MARCOS, 2021, p. 18).

Figura 1: Exemplo de uma nota gerada em desktops após um ataque ransomware.

Fonte: https://www.arquer.com.br/techterra/golpe-pode-vir-em-forma-de-curriculo-falso-o-virus-dilma-locker/

O Dilma Locker é um ransomware criptográfico brasileiro, criado em 2017 e segundo o TechMundo, site sobre tecnologia e política, é disseminado através de e-mails com anexos do malware disfarçado sob um pretenso documento de currículo.

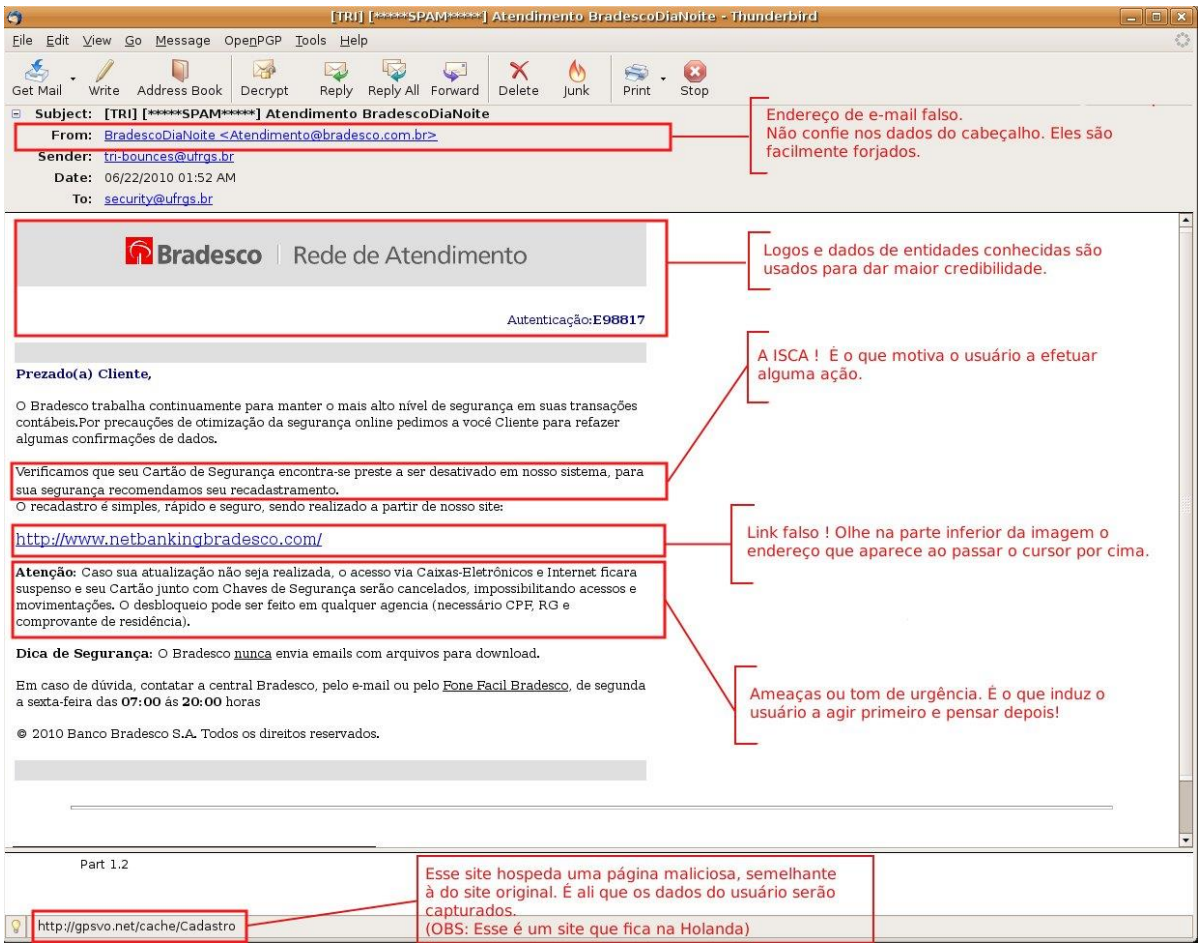
Figura 2: Instruções de pagamento e resgate de dados do Dilma Locker deixados nas pastas dos arquivos criptografados.

Fonte: https://twitter.com/PolarToffee/status/905552193956302848/photo/1

A modalidade criptográfica atua de duas formas, sendo que uma pode complementar a outra. A primeira envolve a criptografia dos dados e um pedido de pagamento do resgate sob a promessa de envio da chave para descriptografar os arquivos. Da mesma forma que acontece em um sequestro de pessoas na realidade, o pagamento do resgate não é garantia de devolução, pois trata-se de uma negociação com um criminoso. Na segunda forma, o cibercriminoso, podendo ou não criptografar os dados, os envia para servidores remotos, chantageando a vítima e exigindo alguma compensação financeira para não tornar público informações sigilosas (TUPINAMBÁ, MARCOS, 2021, p. 18). Um exemplo é o Egregor, considerado pelos pesquisadores da Kaspersky como uma das formas mais agressivas de ataque, dando apenas 72 horas para que suas vítimas paguem o resgate solicitado, caso contrário, os dados criptografados serão roubados e disseminados na Web.

Dentre as diversas formas de disseminar um ransomware, a mais utilizada é através do envio massivo de e-mails com anexos e links infectados a diversos destinatários. Cibercriminosos geralmente enviam mensagens através de um bot de e-mail, que se trata de um programa que automatiza essa tarefa de forma pré-definida e repetitiva, realizando envios para destinatários e domínios aleatórios ou direcionados, em caso de empresas ou pessoas que se tornam foco de ataques por razões específicas dos envolvidos. Conhecido como phishing, esses e-mails geralmente possuem o remetente forjado com nome de alguma pessoa ou instituição conhecidas, simulando, muitas das vezes, no corpo do e-mail, o site ou formato da empresa original. O objetivo é oferecer alguma vantagem, benefício ou informação importante, induzindo a vítima a clicar em um link ou abrir um anexo que possui um programa ou script malicioso em oculto, que uma vez executado, o malware é instalado automaticamente no sistema de maneira imperceptível pelo usuário. (DAVID, KIM E SOLOMON, MICHAEL G., 2014).

Figura 3: Exemplo de um e-mail com phishing.



Fonte: http://www.ufrgs.br/tri/Documentos/mensagens-fraudulentas-phishing

Existem também diversos sites maliciosos na Web que induzem usuários desatentos a clicarem em links infectados ou a realizar download de programas com o ransomware embutido, usando a mesma técnica de atração utilizada nos e-mails.

Outra forma de invasão, e talvez a mais complexa, ocorre por intermédio da exploração de vulnerabilidades de segurança existentes em sistemas. A complexidade está relacionada ao nível técnico envolvido em tal atividade. Uma disseminação de ransomware por e-mail pode ser criado por qualquer curioso com conhecimentos básicos em informática, bastando pesquisar como fazer nos locais corretos ou contratando um RaaS (Ransomware-como-serviço), que são kits de ransomwares comercializados no mercado negro (Deep Web). Já a invasão de um sistema requer conhecimentos avançados em programação, característica de hackers. Uma vez invadido um sistema a partir de uma vulnerabilidade explorada, seja por um código em um site ou aplicação, seja por uma porta aberta em um servidor, o invasor estará livre para executar quaisquer ações, dentre elas, implementar um ransomware no sistema, bloqueando todos os dados locais e quiçá em toda a rede interna que esse sistema está interligado. Apesar de existir essa ação isolada, existem também ferramentas e bots utilizados por cibercriminosos para exploração dessas vulnerabilidades de maneira automatizada. O WannaCry foi dos mais eficazes ransomwares já construídos por não depender da ação de um usuário para sua disseminação, aproveitando uma vulnerabilidade em sistemas operacionais Windows sem atualizações de segurança e replicando-se automaticamente entre computadores do mundo inteiro (TUPINAMBÁ, MARCOS, 2021).

> O ransomware é cada vez mais comum e lucrativo. Vítimas vão de organizações [...] a pessoas físicas. O Kaspersky Lab informou que as invasões a empresas triplicaram e a quantidade de variantes de diferentes ransomwares aumentou em 11 vezes, durante 9 meses de 2016. A Symantec descobriu que a quantia de resgates saltou de US$294, em 2015, para US$679, em 2016, para mais de US$1.077, em 2017. A Carbon Black informou que as vendas totais de software de ransomware no mercado negro aumentou 25 vezes de 2016 a 2017, para US$6,5 milhões. O ransomware agora vem com instruções detalhadas sobre como pagar, e alguns dos criminosos por trás do ransomwares até têm linhas telefônicas para dar assistência às vítimas. (Se você está pensando que uma linha de apoio é um risco para os criminosos, lembre-se da natureza internacional dessa atividade. Os criminosos não temem processos em seus países de origem.) Em suma, trata-se de um negócio bilionário. (SCHNEIER, BRUCE, 2020, p. 64).

Segundo o safeatlast.co, os ataques ransomware custou às empresas mais de 8 bilhões de dólares no ano de 2020, alguns efeitos incluem:

- Tempo de inatividade como resultado de infraestrutura comprometida;
- Perda de produtividade como resultado do tempo de inatividade;

- Esforços de recuperação dispendiosos que potencialmente superam o próprio resgate;
- Danos a longo prazo nos dados e na infraestrutura de dados;
- Danos à reputação anterior de uma empresa como segura;
- Perda de clientes e, nos piores casos, o potencial de danos pessoais se a empresa negociar em serviços públicos, como serviços de saúde.

4.2 CASO LOJAS RENNER

Conforme divulgado em diversos portais de notícias, como o G1 e InfoMoney, a varejista de moda conhecida como Lojas Renner teve seu site e-commerce e aplicativo móvel indisponibilizados entre os dias 19 e 22 de agosto de 2021, após um ataque ransomware. Também foram afetados os sistemas de pagamentos por meios digitais das lojas físicas e as atividades da Camicado e Ashua, empresas que pertencem ao mesmo grupo.

Figura 4: Informação divulgada pela Renner em seu site após o ataque.

Fonte: https://www.cisoadvisor.com.br/ransomexx-assina-ataque-as-lojas-renner/

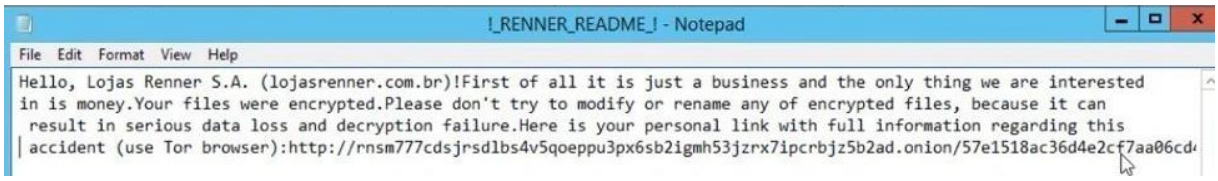
Abaixo um trecho do comunicado oficial da companhia após o evento e publicado no Security Report, site de notícias e reportagens voltados à segurança da informação:

"LOJAS RENNER S.A. ("Companhia"), em observância ao disposto na Instrução da Comissão de Valores Mobiliários ("CVM") n.º 358, de 30 de janeiro de 2002, conforme alterada, vem

informar aos seus acionistas e ao mercado em geral que, nesta data, sofreu um ataque cibernético criminoso em seu ambiente de tecnologia da informação, que resultou em indisponibilidade em parte de seus sistemas e operação e prontamente acionou seus protocolos de controle e segurança para bloquear o ataque e minimizar eventuais impactos."

Uma captura de tela, da suposta nota de resgate deixada nas estações de trabalho da Renner, circulou na internet, sendo também publicadas em diversos sites de notícias, porém sem comprovação da veracidade.

Figura 5: Suposta nota de resgate deixada nas estações de trabalho da Renner após o ataque:



Fonte: https://thehack.com.br/urgente-lojas-renner-podem-ter-sido-vitimas-de-ransomware-site-sai-do-ar/

De acordo com o CISO Advisor, site de notícias sobre cibersegurança, foi utilizado um ataque conhecido como RansomEXX para invadir os sistemas da Renner. O mesmo utilizado em ataques a Embraer, Grupo Ultra e no Tribunal de Justiça Federal como será visto no próximo caso.

Segundo a Kaspersky, o RansomEXX é altamente direcionado. Amostras do malware analisadas exibem um nome codificado da organização atacada. Foi observado também que o grupo utiliza o nome das vítimas tanto no endereço de e-mail usado para fazer a chantagem, quanto na extensão dos arquivos criptografados.

Apesar das Lojas Renner não terem divulgado qual foi o vetor de entrada do ransomware, de acordo com Ledivino Natal da Silva, CEO da empresa de segurança Stefanini Rafael, especula-se que pode ter sido tanto um ataque de phishing, quanto por uma exploração de alguma vulnerabilidade em seus sistemas ou servidores. Vitor Gasparini, Sales Engineer da Trend Micro, reforça afirmando que 90% dos casos de infecções por ransomware ainda se originam por e-mails falsos (phishing), mas não descartando a hipótese desse ataque ter sido originado a partir da exploração de vulnerabilidades em servidores antigos, que podem ter sistemas desatualizados e suscetíveis a invasões.

De acordo com a revista Exame, informações não oficiais dizem que os bancos de dados da Renner teriam sido criptografados e os criminosos estariam exigindo um resgate pelas informações, algo em torno de 1 bilhão de reais em criptomoedas, mas que a empresa teria feito

um acordo e pago apenas 20 milhões de dólares. Contudo, a Renner, em comunicado, negou essa informação e alegou que seus principais bancos de dados permaneciam intactos e que apenas seus sistemas foram restaurados a partir backups existentes.

Embora a Renner não tenha divulgado os prejuízos gerados, esse ataque com certeza causou grandes impactos financeiros e que ainda poderá ecoar nos próximos anos, dado a repercussão e a sensação de insegurança geradas nos consumidores e até em outros varejistas.

4.3 CASO SUPERIOR TRIBUNAL DE JUSTIÇA

No dia 03 de novembro de 2020, o Superior Tribunal de Justiça (STJ) sofreu um ataque de ransomware, conforme amplamente noticiado, inclusive pelo próprio STJ. Em nota oficial um dia após o incidente, foram emitidas as seguintes declarações:

" O Superior Tribunal de Justiça (STJ) detectou, no dia 3 de novembro de 2020, um ataque hacker durante o período da tarde, quando ocorriam sessões de julgamento. Verificou-se que um vírus estava circulando na rede de informática do tribunal e, como medida de precaução, os links para a rede mundial de computadores foram desconectados, o que implicou no cancelamento das sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e de telefonia da Corte. O presidente do Superior Tribunal de Justiça, ministro Humberto Martins, de imediato, solicitou providências à Polícia Federal, por meio de notícia criminis, para que procedesse às devidas investigações. [...] Em paralelo, a equipe da STI do STJ, juntamente com empresas prestadores de serviços de tecnologia do tribunal, a exemplo da Microsoft, iniciou os procedimentos de recuperação dos ambientes dos sistemas de informática do Tribunal da Cidadania. [...] O Tribunal também está contando com a colaboração do Centro de Defesa Cibernética do Exército Brasileiro, para auxiliar a Secretaria de Tecnologia da Informação e Comunicação do tribunal na restauração dos sistemas de informática. O STJ esclarece que o ataque hacker bloqueou, temporariamente, com o uso de criptografia, o acesso aos dados, os quais, todavia, estão preservados nos sistemas de backup do tribunal. Permanecem íntegras as informações referentes aos processos judiciais, contas de e-mails e contratos administrativos, mantendo-se inalterados os compromissos financeiros do tribunal, inclusive quanto à sua folha de pagamento."

Fonte: https://www.conjur.com.br/2020-nov-05/stj-processos-preservados-conta-inteligencia-exercito

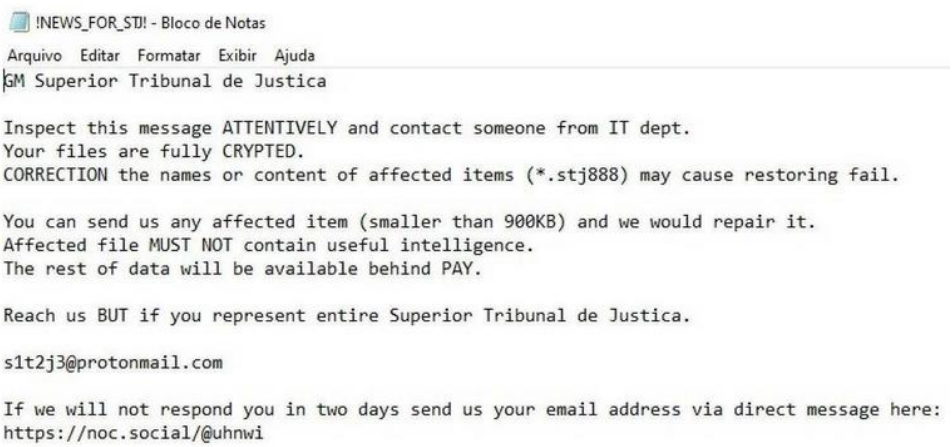
Devido ao STJ não ter registrado em sua página convencional suas declarações acerca do incidente, apenas comunicados em pop-ups, essas informações só se encontram disponíveis

nos principais canais de notícias online, como a Conjur, site especializado em notícias ligadas a temas jurídicos.

Segundo o Correio Braziliense, após o ataque, todo o acervo de processos da Corte foi criptografado, já de acordo com o CISO Advisor, foram mais de 1.200 servidores infectados e com seus dados comprometidos, incluindo os backups, porém conforme publicado na Conjur, o STJ informou que o backup do sistema não foi afetado pelo ato, o que permitiu a posterior restauração dos arquivos.

Ainda em divulgação no site do STJ, as atividades afetadas só voltaram à normalidade no dia 10 de novembro, exatamente oito dias após o ataque. Apesar da assessoria de imprensa do STJ não ter declarado qual tipo de ataque sofreu e qual foi o vetor de entrada, o site Bleeping Computer, voltado a notícias de tecnologia, informou que dado às características da nota supostamente deixada nas estações que tiveram seus dados criptografados, o ataque provavelmente foi o RansomEXX, a mesma variante que atacaria as Lojas Renner 10 meses depois.

Figura 6: Suposta nota deixada nas estações de trabalho do STJ após o ataque:



Fonte: https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/

A nota contém as recomendações, em inglês, de como entrar em contato e realizar o pagamento. Diferente de outras notas desse tipo de ataque, não foi informado o valor para o resgate dos arquivos criptografados.

Conforme Fernando Amatte, pesquisador da Cipher, empresa de cibersegurança, esse incidente poderia ter sido evitado com o "mapeamento eficiente dos ativos, patches, vulnerabilidades e riscos" presentes nos sistemas do STJ. Além disso, "testes periódicos, equipe especializada em segurança, cuidado especial com sistemas legados e principalmente manter os sistemas atualizados" é indispensável para evitar problemas como esse.

Com o bloqueio do acesso a todos os documentos do STJ após o ataque, consequentemente foram suspensas todas as sessões de julgamento e prazos processuais, além de todos os sistemas do STJ terem sido retirados do ar por precaução, se tornando mais um caso em que os prejuízos gerados, dessa vez à sociedade, foram imensuráveis.

O restabelecimento oito dias depois não minimiza os impactos do ataque, visto que ocorreu o acesso a processos sigilosos, além de dados sensíveis que foram coletados pelos cibercriminosos, fato esse que gerou grande temor na comunidade jurídica, de acordo com o Migalhas, portal de notícias jurídicas, políticas e econômicas.

4.4 OPINIÕES DE ESPECIALISTAS

Baseado em um questionário com perguntas abertas sobre ransomware e proteção de dados, entrevistou-se três especialistas em segurança da informação através do mensageiro eletrônico Whatsapp, com objetivo de buscar opiniões baseadas em suas experiências ou na troca de informações em suas redes relacionadas à segurança da informação, onde a colaboração e ajuda mútua são características desse tipo de profissional. Todos os especialistas pertencem a empresas distintas e não tiveram contato entre eles e nem com informações deste estudo antes de sua publicação. Abaixo segue uma breve apresentação dos especialistas:

> **Alan P. Bittencourt** é engenheiro de sistemas sênior, com certificações Linux (Red Hat RHCE, LPI-2 e Plesk) e especializado em firewalls (Iptables, Fortgate e ISA Server). Atuou durante 12 anos em um dos maiores datacenters da América latina, efetuando análises de vulnerabilidades em ambientes e executando os procedimentos necessários para a correção de brechas de segurança nos mais variados dispositivos e sistemas sob sua administração.
>
> **Sebastião A. Fonseca** é analista de segurança da informação, com diversas certificações na área como COMPTIA SECURITY+ e ETHICAL HACKER C|EHV10, com experiência de mais de 5 anos em cyber segurança, tendo como especialidade o tratamento e prevenção de ataques, análise de vulnerabilidade de segurança e análise de riscos de incidentes.
>
> **Thiago Simonin** é especialista em cyber segurança com certificações na área como COMPTIA SECURITY+, ISFS em ISO/IEC 27002 e soluções antivírus como a DDI da Trend Micro e ESM Analyst Siem da McAfee. Possui experiência de mais de 10 anos na área de segurança da informação, atuando em empresas de TI como analista e outras como consultor.

Dentre os níveis de ameaça estipulados [crítico, alto, médio ou baixo], todos classificaram um ataque ransomware como crítico, sob a justificativa de envolver sequestro e perda de dados por conta dos métodos de criptografia utilizados que são praticamente inquebráveis, além da indisponibilidade de operação e dano à imagem.

Também por unanimidade, os especialistas apontaram a falta de conscientização dos usuários quanto ao uso adequado dos sistemas como principal porta de entrada para as ameaças. Parte desse problema muita das vezes ocorre por ineficientes e equivocadas políticas de segurança adotadas em uma organização, como a falta ou aplicação incorreta do princípio do menor privilégio, que preza por delegar somente os acessos necessários para que usuários e sistemas possam realizar as atividades requeridas, sem mais, nem menos. Outro problema também apontado foi a ausência ou falta de frequência no processo de patch management nos ambientes, que trata as atualizações em um sistema operacional, plataforma ou aplicação e envolve a identificação de correções e aprimoramentos, processo de aplicação dessas atualizações e posteriores validações.

Questionados sobre quais medidas corretivas são consideradas cruciais para a proteção contra ataques ransomware, todos declararam a conscientização dos usuários como ponto principal desse processo. Sebastião Fonseca inclui que deveriam existir campanhas de esclarecimento focadas principalmente em ataques phishing e na utilização de políticas de segurança baseadas em guias como o NIST, que fornece uma metodologia para padronizar de definir melhores práticas as questões relacionadas à cibersegurança, também afirma a necessidade de antivírus instalados em estações de trabalho que monitore comportamentos verificados em ransomwares conhecidos e que não permita a criptografia de arquivos em massa. Outras questões que apresentaram conformidade entre os especialistas foi no que se refere à aplicação correta do princípio de menor privilégio. Segundo Alan Bittencourt, os ambientes de redes deveriam ser segregados por perfis de operação e uso, com a utilização de regras de firewall mais restritivas, somente liberando acesso a portas essenciais. Todos também sinalizaram a necessidade de uma rotina de patch management mais efetiva e com maior frequência.

Diferente dos demais, Thiago Simonin distinguiu usuários domésticos a ambientes corporativos para emitir suas recomendações. Manter o sistema operacional sempre atualizado, se possível, deixando o recurso de atualização no automático, ter uma boa solução de antivírus e não sair clicando em todo o link recebido, principalmente oriundos de e-mails e rede sociais, desconfiar sempre de tudo e checar diretamente com os envolvidos em caso de dúvidas e sempre que possível, salvar os dados importantes em um HD externo, são as dicas fornecidas para os

usuários comuns. Já no ambiente corporativo, ele inclui que além da prevenção de ataques, as empresas também têm que se preocupar com um plano de recuperação condizente com o negócio, porque nenhum ambiente é 100% seguro. Além de uma política eficiente e frequente de backups de acordo com a importância dos dados, mantendo cópias em mídias arquiváveis e um ambiente de contingência (Disaster Recovery) que viabilizaria a restauração de todo um ambiente em questão de minutos.

Outro assunto abordado se refere a percepção do nível de maturidade das empresas brasileiras, tanto as de TI, como as de outras áreas com relação à segurança da informação. Todos declararam que o nível está de mediano a baixo e o principal problema está na resistência das organizações em investir adequadamente em segurança da informação, sendo na maioria dos casos, devido à falta de compreensão ou negligência, que vai desde a alta diretoria até gestores, sobre os riscos dessas ameaças e os imensuráveis prejuízos financeiros que uma invasão pode causar. Alan Bittencourt inclui que boa parte das empresas brasileiras trabalham em evoluções e controles reativos, sendo as reações baseadas em incidentes ocorridos em seus ambientes ou em players concorrentes de segmento, já Thiago Simonin afirma que as empresas ainda enxergam os sistemas de informação como custo e não como uma necessidade crucial para o negócio.

Por fim, perguntou-se aos especialistas quais eram suas expectativas com relação à evolução dos ataques ransomware. Sebastião Fonseca acredita no surgimento de mais grupos especializados nesse tipo de ataque, como o Darkside e REvil. Alan Bittencourt concluiu dizendo que a tendência é que os ataques aumentem em quantidade e evoluam na maneira que são implementados. À medida que ambientes vão adotando políticas de segurança mais rigorosas, cibercriminosos desenvolverão novas técnicas e ferramental de ataque. Seguindo um pensamento semelhante, Thiago Simonin também acredita que novas ameaças surgirão conforme os ambientes vão se tornado mais seguros, elevando o nível de sofisticação dessas invasões. Complementa ainda informando que existem grupos que são financiados por iniciativas privadas e até por governos para a prática do cibercrime, com isso, os crackers sempre estarão um passo à frente da indústria de Cibersegurança, pesquisando e desenvolvendo novos métodos e técnicas de invasão e exploração de vulnerabilidades, como o uso de Inteligência Artificial (Machine Learning), por exemplo.

5 CONSIDERAÇÕES FINAIS

A proteção dos dados tem se tornado um tema mais complexo dado ao aumento exponencial de diversos ataques direcionados a organizações com o objetivo de obter ganhos financeiros através do acesso, manipulação e bloqueio de informações sigilosas.

Este estudo, além de esclarecer o que é ransomware e suas características, mostrou que nenhuma organização está livre de ter seus dados comprometidos por conta de um ataque, nem mesmo órgãos governamentais, que deveriam seguir à risca todos os princípios da segurança da informação. Através dos casos apresentados, foi possível ter uma visão dos impactos gerados durante e após esses ataques e como as organizações lidaram com esses eventos.

Também se verificou a baixa maturidade das empresas com relação à segurança da informação, que ainda a enxerga como custo ou despesa, ao invés de investimento e atividade essencial para o negócio.

Observou-se que a principal porta de entrada desses ataques são os usuários e os ambientes vulneráveis, tornando necessário constantes iniciativas de conscientização dos usuários quanto a utilização dos recursos de TI e a restrição do acesso apenas à execução das suas funções (princípio do menor privilégio), além de políticas de verificação e aplicação de pacotes de segurança frequentes, com o objetivo de manter todas as plataformas atualizadas, sendo medidas amplamente recomendadas para se evitar todo o tipo de ataques.

Outra questão que as empresas devem se preocupar é com um plano de recuperação condizente com as necessidades do negócio, porque nenhum ambiente é totalmente imune a ataques. Backups frequentes e ambientes de contingência são boas práticas a serem adotadas.

Por se tratar de um negócio bilionário, a previsão é que os ataques ransomware aumentem em quantidade e qualidade, além do fortalecimento dos grupos de cibercriminosos, ficando notório a importância de investimentos constantes na área da segurança da informação.

A era da informação, apesar de trazer facilidades da interconexão, em que pessoas acessam e compartilham informações através da internet de maneira rápida através do seus computadores ou dispositivos móveis, também viabiliza a exposição e perda da privacidade de dados, tornando extremamente necessário que todos os seus usuários, sem exceção, entendam conceitos importantes sobre segurança da informação e aprendam a lidar na prática com a segurança dos dados, tornando-se esse o verdadeiro desafio, principalmente no que se refere a dados de propriedade corporativa.

REFERÊNCIAS

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação**: livro didático. 1 ed. Rio de Janeiro: LTC, 2020. 377 p.

SCHNEIER, Bruce. **Clique Aqui Para Matar Todo Mundo**: livro didático. 1 ed. Editora Alta Books, 2020. 199 p.

LENTO, Luiz Otávio Botelho. **Segurança da Informação:** livro didático. 3 ed. rev. e atual. Palhoça: Unisul Virtual, 2011. 234 p.

TUPINAMBÁ, Marcos. **Segurança Digital – Proteção de dados nas empresas:** livro didático. 1 ed. Editora Atlas, 2021. 247 p.

CUSNIR, Danielle. **A problemática dos ciberataques em um contexto de cooperação jurídica internacional**. 2018. 66f. Tese (Bacharel em Direito) - Curso de graduação em Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

SERPRO**. Você sabe o que é um ataque de ransomware?** Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2021/ataque-de-ransomware. Acesso em: 15 ago. 2021.

Minuto da Segurança**. Tudo sobre Ransomware, da história à decisão de pagamento!** Disponível em: https://minutodaseguranca.blog.br/tudo-sobre-ransomware-da-historia-a-decisao-de-pagamento/. Acesso em: 15 ago. 2021.

Canaltech**. Ciberataques de ransomware crescem no Brasil acima da média global**. Disponível em: https://canaltech.com.br/seguranca/ciberataques-de-ransomware-crescem-no-brasil-acima-da-media-global-189251/ Acesso em: 15 ago. 2021.

Filipe Garrett. **O que é malware? Veja significado, tipos e saiba remover.** Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 15 ago. 2021.

Amazon. **O que é armazenamento em nuvem?** Disponível em: https://aws.amazon.com/pt/what-is-cloud-storage/. Acesso em: 03 set. 2021.

Check Point. **Check Point's 2021 Cyber Security Report.** Disponível em: https://pages.checkpoint.com/cyber-security-report-2021.html Acesso em: 08 set. 2021.

Gartner. **Newsroom Press Releases** Disponível em: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Acesso em: 22 set. 2021

TechMundo. **Lojas Renner confirma ataque cibernético.** Disponível em: https://www.tecmundo.com.br/seguranca/121800-acredite-quiser-dilma-locker-o-novo-ransomware-brasileiro.htm. Acesso em: 03 out. 2021.

Security Report. **Lojas Renner confirma ataque cibernético.**
Disponível em: https://www.securityreport.com.br/destaques/lojas-renner-confirma-ataque-cibernetico/#.YVJjF31v9hF. Acesso em: 08 set. 2021.

Kaspersky. **RansomEXX e Egregor: famílias de ransomware intensificam ataques.**
Disponível em: https://www.kaspersky.com.br/blog/ransomexx-egregor-ransomware-ataques/16712/. Acesso em: 22 set. 2021.

Cisoadvisor. **Renner confirma ataque. RansomExx reivindica autoria.**
Disponível em: https://www.cisoadvisor.com.br/ransomexx-assina-ataque-as-lojas-renner/. Acesso em: 22 set. 2021.

Exame. **Após ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos.**
Disponível em: https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/. Acesso em: 22 set. 2021.

Safeatlast. **22 Shocking Ransomware Statistics for Cybersecurity in 2021.**
Disponível em: https://safeatlast.co/blog/ransomware-statistics/#gref. Acesso em: 22 set. 2021.

The Hack. **STJ é vítima de ransomware e tem seus dados e os backups criptografados.**
Disponível em: https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/. Acesso em: 25 set. 2021.

Conjur. **STJ diz que processos estão preservados e conta com a inteligência do Exército.**
Disponível em: https://www.conjur.com.br/2020-nov-05/stj-processos-preservados-conta-inteligencia-exercito. Acesso em: 25 set. 2021.

Correio Braziliense. **Ataque de hackers ao STJ é o mais grave da história no país.**
Disponível em: https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html. Acesso em: 25 set. 2021.

STJ. **Comunicado.**
Disponível em https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx. Acesso em: 25 set. 2021.

G1. **STJ diz que sistema de informática do tribunal foi alvo de ataque hacker e pede investigação da PF.**
Disponível em https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque. Acesso em: 25 set. 2021.

Bleeping Computer. **Brazil's court system under massive RansomExx ransomware attack**
https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/ -de-hackers-ao-sistema-do-tribunal.ghtml. Acesso em: 25 set. 2021.

MIGALHAS. **Migalhas de Proteção de Dados.**
Disponível em https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios. Acesso em: 25 set. 2021.

APÊNDICES

APÊNDICE A – Questionário

O questionário a seguir procura opiniões dos especialistas da área, podendo ser baseado em suas experiências ou na troca de informações em suas redes de contatos relacionados à segurança da informação, onde a colaboração e ajuda mútua são características desse tipo de profissional.

1) Dentre as diversas ameaças virtuais existentes hoje, em que nível de ameaça [Crítica, alta, média ou baixa] você classificaria os ataques por ransomware? Se possível, justifique.

2) O safeatlast.co estimou em 2018 que 77% das empresas sujeitas a um ataque de ransomware estavam atualizadas em sua tecnologia de segurança de terminais, do seu ponto de vista ou experiência, quais são as principais causas que viabilizam um ataque ransomware?

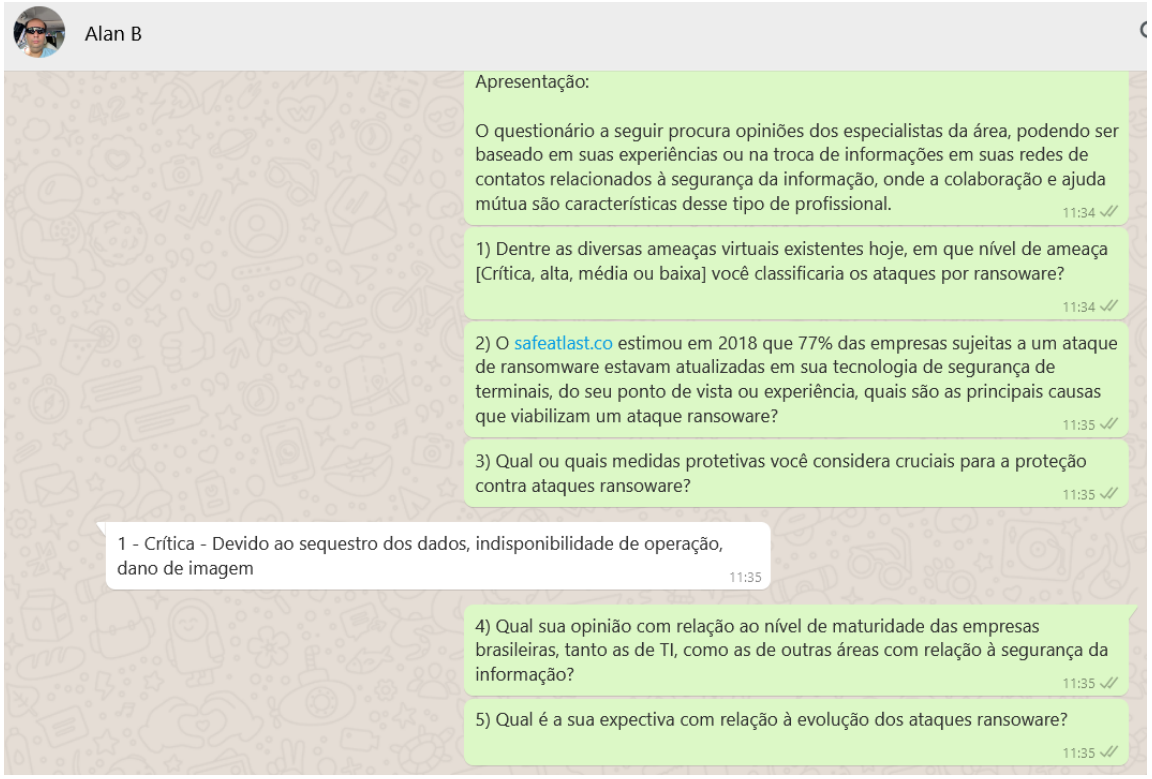
3) Quais medidas protetivas você considera cruciais para a proteção contra ataques ransomware?

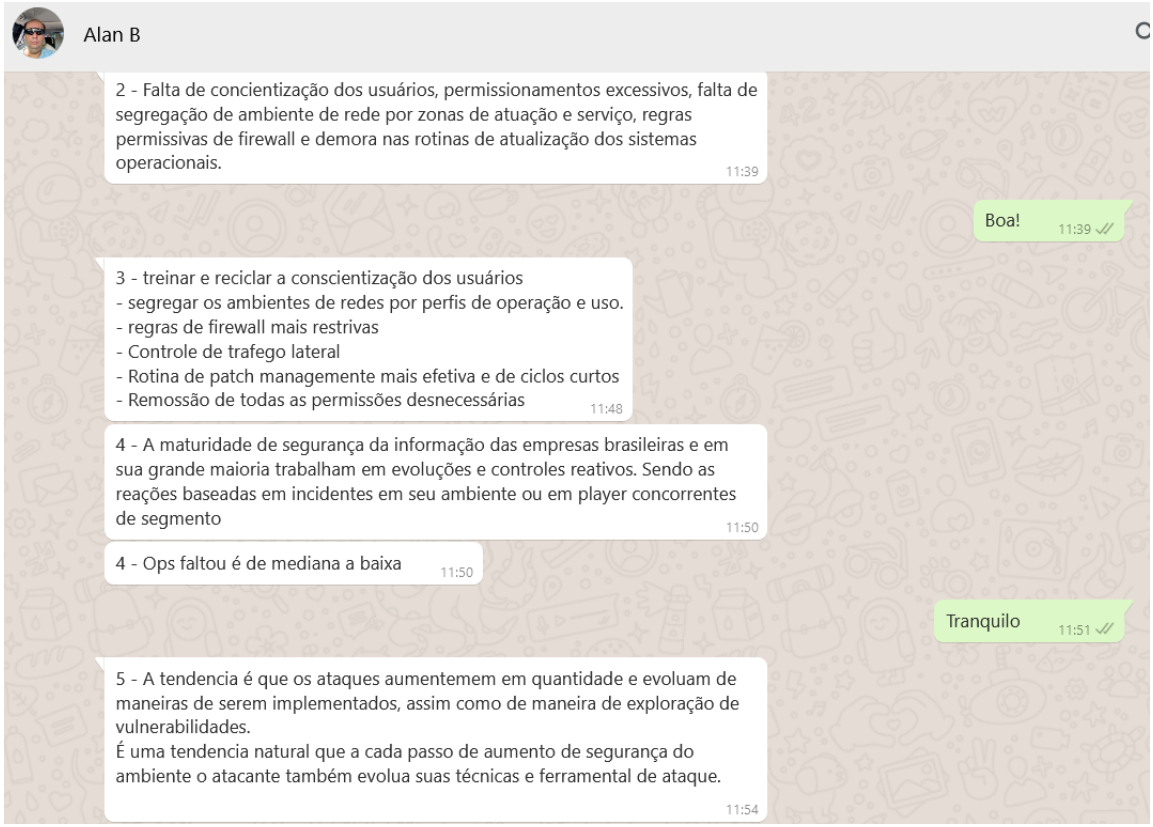
4) Qual sua opinião com relação ao nível de maturidade das empresas brasileiras, tanto as de TI, como as de outras áreas com relação à segurança da informação?

5) Qual é a sua expectativa com relação à evolução dos ataques ransomware?

APÊNDICE B – Respostas dos especialistas

Segue abaixo os prints coletados do mensageiro instantâneo Whatsapp com as respostas dos especialistas em segurança da informação.





Sebastiao André
visto por último hoje às 19:12

1) Dentre as diversas ameaças virtuais existentes hoje, em que nível de ameaça [Crítica, alta, média ou baixa] você classificaria os ataques por ransoware?

- Crítica

2) O safeatlast.co estimou em 2018 que 77% das empresas sujeitas a um ataque de ransomware estavam atualizadas em sua tecnologia de segurança de terminais, do seu ponto de vista ou experiência, quais são as principais causas que viabilizam um ataque ransoware?

- Phishing, não realizar atualizações de forma frequente o suficiente para que o ambiente tenha o minimo de vulnerabilidades possiveis e há não utilização do principio de least privilege. Os dois primeiros normalmente são utilizados como ponto de entrada nas empresas, as vulnerabilidades as vezes ainda permitem a escalação de privilegio, o que nos leva ao ultimo ponto, onde o atacante não conseguir o privilegio necessario através da vulnerabilidade pode conseguir através de usuários que tem privilegios que não deveriam ter ou a uatilização de usuarios padrão no ambiente.

3) Qual ou quais medidas protetivas você considera cruciais para a proteção contra ataques ransoware?

- Ter antivirus que monitore comportamentos verificados em ransowares conhecidos e que não permita a criptografia de arquivos em massa, ter ferramentas que possibilitem um processo eficiente de detecção e correção de vulnerabilidades, campanhas de concientização contra ataques de phishing e utilizar politicas de segurança baseadas em guias como NIST.

Sebastiao André
visto por último hoje às 19:12

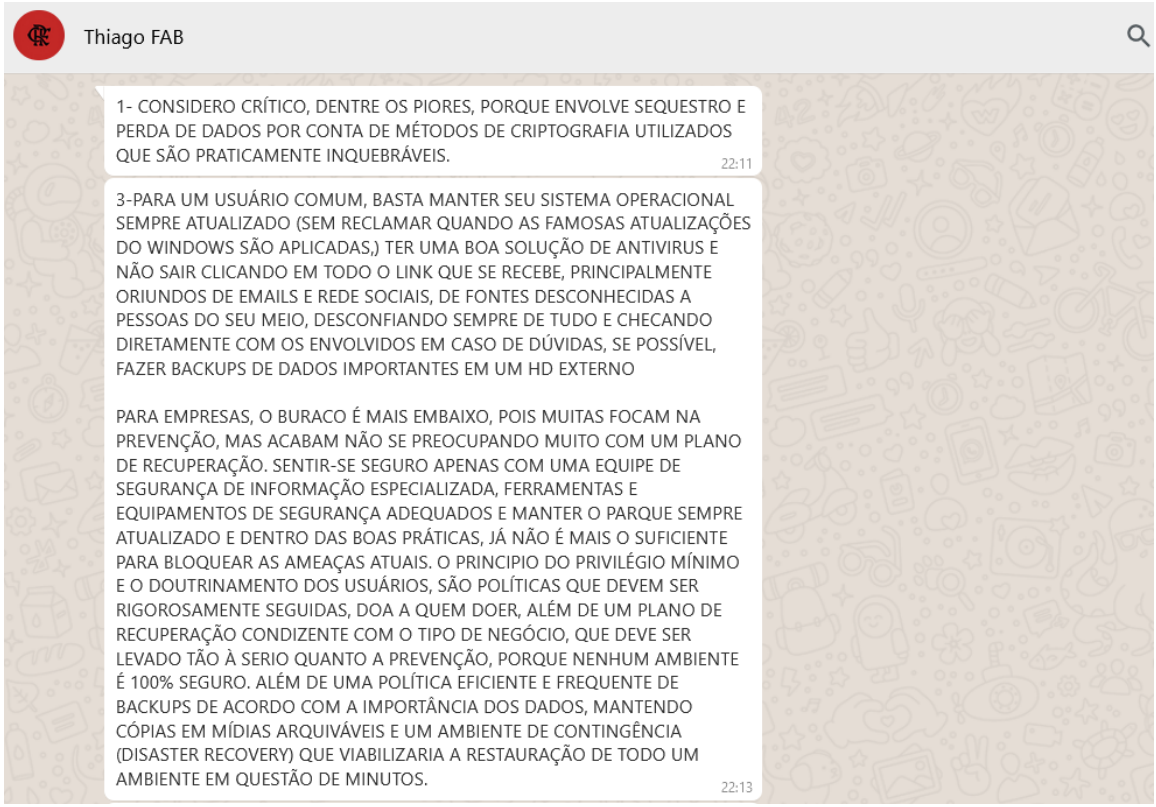
4) Qual sua opinião com relação ao nível de maturidade das empresas brasileiras, tanto as de TI, como as de outras áreas com relação à segurança da informação?

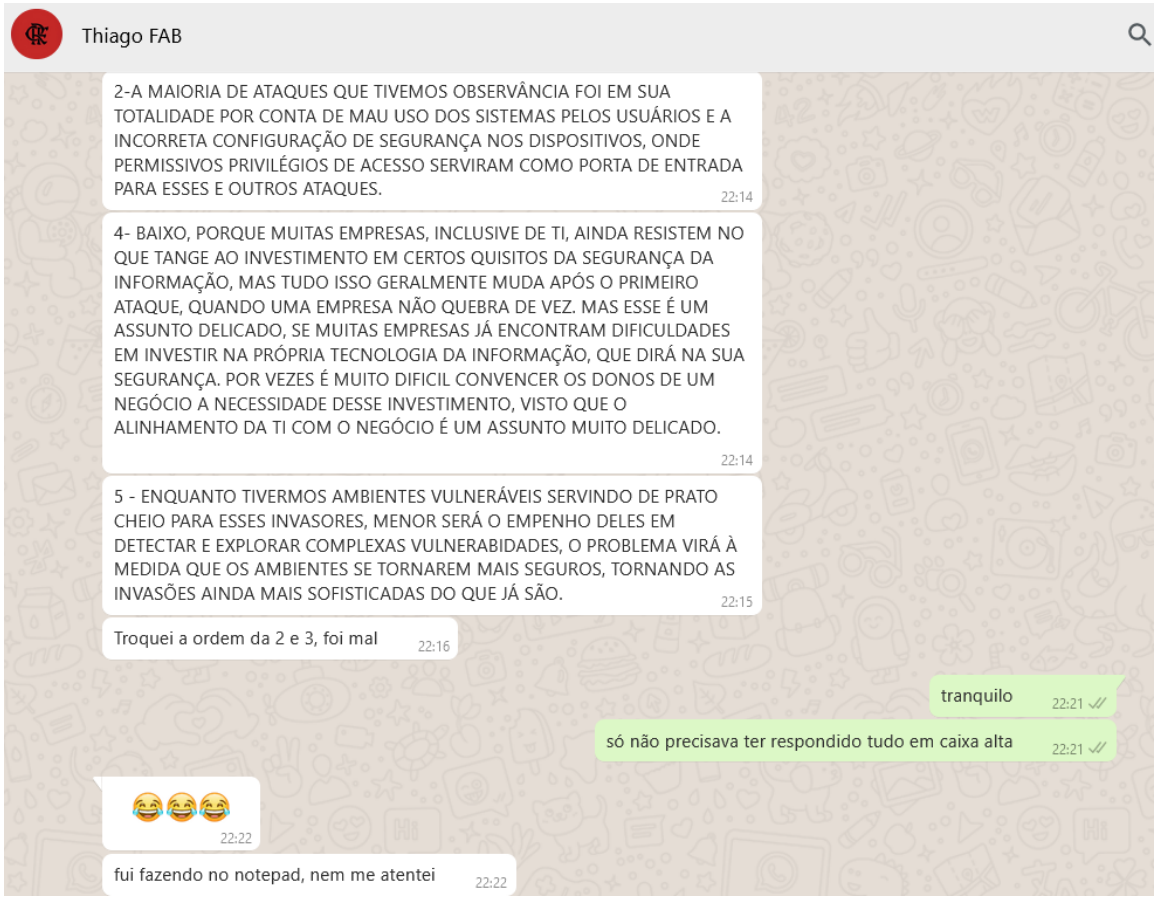
- O nível de maturidade das empresas brasileiras ainda é muito baixo. Um dos fatores que pode ajudar nessa falta de maturidade é o de não se entender o real risco das ameaças ciberneticas e dessa forma verem o custo disso como muito alto.

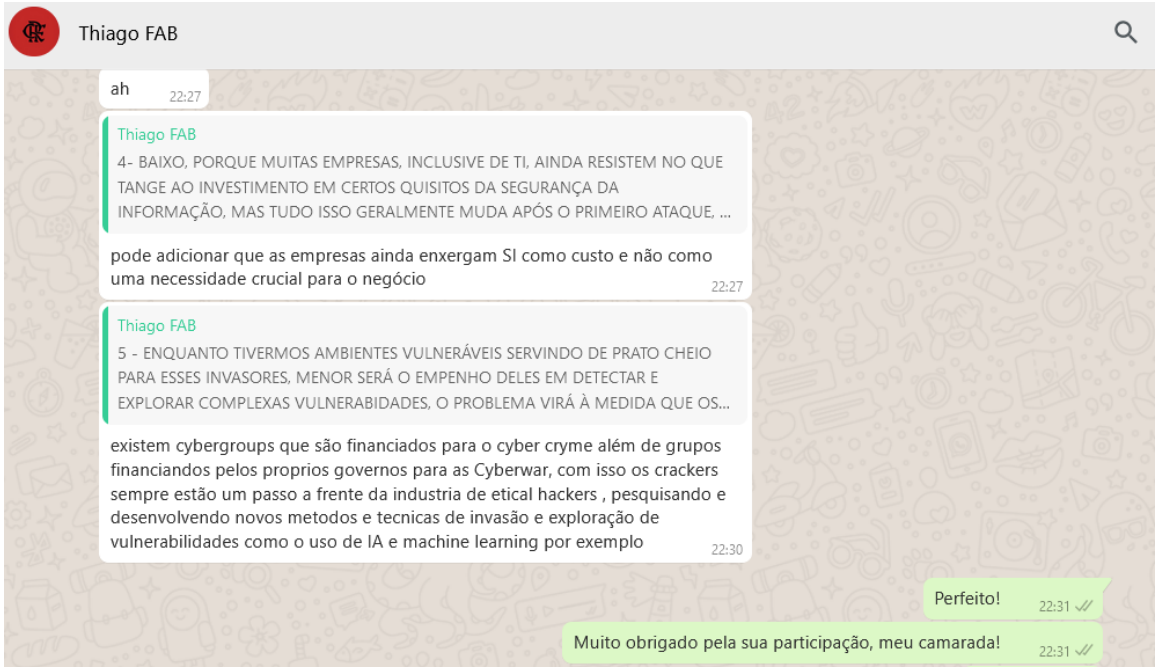
5) Qual é a sua expectiva com relação à evolução dos ataques ransoware?

- De surgirem cada vez mais grupos especializados apenas nesta segmentação, como já é o caso do Darkside e REvil.

19:36


Thiago FAB
1- CONSIDERO CRÍTICO, DENTRE OS PIORES, PORQUE ENVOLVE SEQUESTRO E PERDA DE DADOS POR CONTA DE MÉTODOS DE CRIPTOGRAFIA UTILIZADOS QUE SÃO PRATICAMENTE INQUEBRÁVEIS. 22:11
3-PARA UM USUÁRIO COMUM, BASTA MANTER SEU SISTEMA OPERACIONAL SEMPRE ATUALIZADO (SEM RECLAMAR QUANDO AS FAMOSAS ATUALIZAÇÕES DO WINDOWS SÃO APLICADAS,) TER UMA BOA SOLUÇÃO DE ANTIVIRUS E NÃO SAIR CLICANDO EM TODO O LINK QUE SE RECEBE, PRINCIPALMENTE ORIUNDOS DE EMAILS E REDE SOCIAIS, DE FONTES DESCONHECIDAS A PESSOAS DO SEU MEIO, DESCONFIANDO SEMPRE DE TUDO E CHECANDO DIRETAMENTE COM OS ENVOLVIDOS EM CASO DE DÚVIDAS, SE POSSÍVEL, FAZER BACKUPS DE DADOS IMPORTANTES EM UM HD EXTERNO
PARA EMPRESAS, O BURACO É MAIS EMBAIXO, POIS MUITAS FOCAM NA PREVENÇÃO, MAS ACABAM NÃO SE PREOCUPANDO MUITO COM UM PLANO DE RECUPERAÇÃO. SENTIR-SE SEGURO APENAS COM UMA EQUIPE DE SEGURANÇA DE INFORMAÇÃO ESPECIALIZADA, FERRAMENTAS E EQUIPAMENTOS DE SEGURANÇA ADEQUADOS E MANTER O PARQUE SEMPRE ATUALIZADO E DENTRO DAS BOAS PRÁTICAS, JÁ NÃO É MAIS O SUFICIENTE PARA BLOQUEAR AS AMEAÇAS ATUAIS. O PRINCIPIO DO PRIVILÉGIO MÍNIMO E O DOUTRINAMENTO DOS USUÁRIOS, SÃO POLÍTICAS QUE DEVEM SER RIGOROSAMENTE SEGUIDAS, DOA A QUEM DOER, ALÉM DE UM PLANO DE RECUPERAÇÃO CONDIZENTE COM O TIPO DE NEGÓCIO, QUE DEVE SER LEVADO TÃO À SERIO QUANTO A PREVENÇÃO, PORQUE NENHUM AMBIENTE É 100% SEGURO. ALÉM DE UMA POLÍTICA EFICIENTE E FREQUENTE DE BACKUPS DE ACORDO COM A IMPORTÂNCIA DOS DADOS, MANTENDO CÓPIAS EM MÍDIAS ARQUIVÁVEIS E UM AMBIENTE DE CONTINGÊNCIA (DISASTER RECOVERY) QUE VIABILIZARIA A RESTAURAÇÃO DE TODO UM AMBIENTE EM QUESTÃO DE MINUTOS. 22:13


Thiago FAB
2-A MAIORIA DE ATAQUES QUE TIVEMOS OBSERVÂNCIA FOI EM SUA TOTALIDADE POR CONTA DE MAU USO DOS SISTEMAS PELOS USUÁRIOS E A INCORRETA CONFIGURAÇÃO DE SEGURANÇA NOS DISPOSITIVOS, ONDE PERMISSIVOS PRIVILÉGIOS DE ACESSO SERVIRAM COMO PORTA DE ENTRADA PARA ESSES E OUTROS ATAQUES. 22:14
4- BAIXO, PORQUE MUITAS EMPRESAS, INCLUSIVE DE TI, AINDA RESISTEM NO QUE TANGE AO INVESTIMENTO EM CERTOS QUISITOS DA SEGURANÇA DA INFORMAÇÃO, MAS TUDO ISSO GERALMENTE MUDA APÓS O PRIMEIRO ATAQUE, QUANDO UMA EMPRESA NÃO QUEBRA DE VEZ. MAS ESSE É UM ASSUNTO DELICADO, SE MUITAS EMPRESAS JÁ ENCONTRAM DIFICULDADES EM INVESTIR NA PRÓPRIA TECNOLOGIA DA INFORMAÇÃO, QUE DIRÁ NA SUA SEGURANÇA. POR VEZES É MUITO DIFICIL CONVENCER OS DONOS DE UM NEGÓCIO A NECESSIDADE DESSE INVESTIMENTO, VISTO QUE O ALINHAMENTO DA TI COM O NEGÓCIO É UM ASSUNTO MUITO DELICADO. 22:14
5 - ENQUANTO TIVERMOS AMBIENTES VULNERÁVEIS SERVINDO DE PRATO CHEIO PARA ESSES INVASORES, MENOR SERÁ O EMPENHO DELES EM DETECTAR E EXPLORAR COMPLEXAS VULNERABIDADES, O PROBLEMA VIRÁ À MEDIDA QUE OS AMBIENTES SE TORNAREM MAIS SEGUROS, TORNANDO AS INVASÕES AINDA MAIS SOFISTICADAS DO QUE JÁ SÃO. 22:15
Troquei a ordem da 2 e 3, foi mal 22:16
tranquilo 22:21
só não precisava ter respondido tudo em caixa alta 22:21
😂😂😂 22:22
fui fazendo no notepad, nem me atentei 22:22


Thiago FAB
ah
22:27
Thiago FAB
4- BAIXO, PORQUE MUITAS EMPRESAS, INCLUSIVE DE TI, AINDA RESISTEM NO QUE TANGE AO INVESTIMENTO EM CERTOS QUISITOS DA SEGURANÇA DA INFORMAÇÃO, MAS TUDO ISSO GERALMENTE MUDA APÓS O PRIMEIRO ATAQUE, ...
pode adicionar que as empresas ainda enxergam SI como custo e não como uma necessidade crucial para o negócio
22:27
Thiago FAB
5 - ENQUANTO TIVERMOS AMBIENTES VULNERÁVEIS SERVINDO DE PRATO CHEIO PARA ESSES INVASORES, MENOR SERÁ O EMPENHO DELES EM DETECTAR E EXPLORAR COMPLEXAS VULNERABIDADES, O PROBLEMA VIRÁ À MEDIDA QUE OS...
existem cybergroups que são financiados para o cyber cryme além de grupos financiando pelos proprios governos para as Cyberwar, com isso os crackers sempre estão um passo a frente da industria de etical hackers , pesquisando e desenvolvendo novos metodos e tecnicas de invasão e exploração de vulnerabilidades como o uso de IA e machine learning por exemplo
22:30
Perfeito!
22:31
Muito obrigado pela sua participação, meu camarada!
22:31