FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Lucas Miranda Neves

Nicholas de Lucas Bastos Pereira

Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus)

Americana, SP

2020

Faculdade de Tecnologia de Americana

Lucas Miranda Neves
Nicholas de Lucas Bastos Pereira

Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus)

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CETEEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 11 de dezembro de 2020.

Banca Examinadora:

_____
Prof. Maxwel Vitorino da Silva (Presidente)
Mestre
Faculdade de Tecnologia – FATEC Americana

_____
Prof. Diógenes de Oliveira (Membro)
Mestre
Faculdade de Tecnologia – FATEC Americana

_____
Prof. Samuel Tanaami (Membro)
Mestre
Faculdade de Tecnologia – FATEC Americana

Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus)
Ransomware and Phishing during Covid-19 (Coronavirus) pandemic
Ransomware y phishing durante la pandemia de Covid-19 (Coronavirus)

Lucas Miranda Neves[1]
Nicholas de Lucas Bastos Pereira[2]
Orientador: Maxwel Vitorino da Silva[3]

RESUMO

Em 11 de Março de 2020, a Organização Mundial de Saúde declarou a pandemia do Covid-19 (Coronavírus), a qual impactou vários setores da economia e de desenvolvimento social, modificando as relações de trabalho. A tecnologia se tornou protagonista e como foi uma adaptação repentina, acabou deixando brechas, principalmente em empresas, que se tornaram vulneráveis aos ataques de Ransomware e Phishing. Nesse artigo será demonstrado a influência da pandemia em relação ao aumento desses ataques, exibindo as mudanças que sofreram, desde o nível global até o nacional, e um estudo dos que tiveram maior destaque na área de segurança da informação.
Palavras-chave: Covid-19. Ransomware. Phishing. Segurança da Informação.

ABSTRACT

On 11 March 2020, the World Health Organization declared the Covid-19 (Coronavirus) pandemic, in which it impacted various sectors of the economy and social development, changing labor relations. The technology became the protagonist and as it was a sudden adaptation, it ended up leaving loopholes, mainly in companies, which became vulnerable to the attacks of Ransomware and Phishing. In this article, the influence of the pandemic in relation to the increase of these attacks will be demonstrated, exhibiting the changes that have undergone, from the global to the national level, and a study of those that are more prominent in information security.
Keywords: Covid-19. Ransomware. Phishing. Information Security.

INTRODUÇÃO

No final de dezembro de 2019, o governo chinês alertou o mundo sobre um novo Coronavírus (SARS-CoV-2), tendo o nome técnico: Covid-19. Em janeiro de 2020 a Organização Mundial da Saúde (OMS), confirmou uma "emergência de saúde pública de significância internacional", porém, o vírus começou a se espalhar pelo mundo, pois a sua disseminação é fácil e rápida.

O Covid-19, além de ser altamente contagioso pode ser fatal e por isso ele compromete a solidez que as empresas conquistaram antes dessa mudança abrupta, uma vez que, com a chegada desse novo vírus houve uma mudança enorme no cotidiano das pessoas e consequentemente das empresas.

O método que o Brasil e muitos países adotaram foi o isolamento por tempo indeterminado da população, com isso, instituições de ensino (escola e faculdades) decidiram fechar. Empresas que não prestam serviços considerados essenciais foram forçadas a alterar seu meio de execução do trabalho, já que os funcionários não poderiam ir para o local de trabalho de forma física.

Essa mudança repentina fez o mundo corporativo repensar seus processos e o uso da tecnologia foi ainda mais acelerado, sendo atribuído o meio online para múltiplas tarefas. Muitas empresas foram postas em teste, fazendo com que seus sistemas fossem colocados em prova, em relação à segurança

[1,2,3] Faculdade de Tecnologia, Americana - SP
[1] E-mail: lucas.neves14@fatec.sp.gov.br
[2] E-mail: nicholas.pereira01@fatec.sp.gov.br
[3] E-mail: maxwel.silva3@fatec.sp.gov.br

que apresentam quanto a transição de modelo de trabalho, não apenas sobre o software, mas também sobre as pessoas que o operam.

Apesar de o isolamento social ter causado malefícios, um dos pontos positivos foi o aumento significativo da comunicação remota, por meios de contatos tanto entre amigos e familiares, quanto com colegas de trabalho foi possível devido ao grande avanço tecnólogo.

Como exemplo, as plataformas de videoconferência online, que tiverem uma grande demanda de novos usuários se inscrevendo diariamente, tais como: Messenger Room, Google Meet e Microsoft Teams.

Além das ferramentas de comunicações, o estilo de trabalho remoto está sendo algo visado pelas empresas pós pandemia, pois segundo um estudo com 1000 empresas realizado pela IT Barracuda, divulgado no dia 06 de maio de 2020, mostrou que 55% dos entrevistados não tinha interesse em transferir o ambiente de trabalho para o meio remoto dentre os próximos 5 anos, porém, após a mudança mais da metade dos entrevistados (56%) cogitam em manter-se no método remoto de trabalho após o fim do isolamento.

Mas, mesmo esses meios benéficos sendo apresentados diante a pandemia, eles trazem consigo ameaças em questões de segurança cibernética, pois essa massiva procura por esses recursos, faz com que as empresas tenham dificuldades de prover a estabilidade e segurança de suas plataformas, tornando-se alvos suscetíveis aos ataques maliciosos.

Como prova disso a Abnormal, empresa que presta serviços de segurança de e-mail, publicou uma matéria no dia 1 de maio de 2020, dizendo que a plataforma Microsoft Teams foi alvo de ataques phishing com o objetivo de roubar as credenciais do Microsoft 365 de funcionários da empresa.

Dentre estes ataques, os que vem tendo destaque e crescem cada vez mais no Brasil, são os de Ransomware e Phishing. O objetivo do artigo é trazer mais informações sobre eles e mostrar o quanto mudaram em relação ao novo ambiente de vivência proporcionado pelo Covid-19.

1. DESENVOLVIMENTO

Neste capítulo discorre-se sobre os ataques em questão, mostrando as diferenças e relações entre ambos, expondo as mudanças que sofreram de acordo o surgimento da pandemia e como foram efetivos, sendo demonstrado por dados de pesquisas e exemplos da aplicação desses ataques.

1.1. Phishing

Phishing é um método conhecido no mundo virtual, que tem por finalidade a prática criminosa de enganar pessoas para que consiga se obter informações confidenciais delas, como senhas e dados de cartões. Segundo Martins (2017) o phishing é definido como técnicas que combinam Engenharia Social e hacking.

Em sua prática, os criminosos enviam e-mails ou mensagem para as vítimas na qual imitam uma fonte de confiança, como colegas de trabalho, banco ou órgãos governamentais, com isso, as pessoas acreditam que a cópia fraudulenta, criada pelos ladrões se trata de algo legítimo e, como parece ser confiável, a vítima acaba inserindo suas informações pessoais e enviando para os criminosos, permitindo que eles tenham acesso ao sistema verdadeiro, e assim roubando sua identidade virtual.

Durante a pandemia 2020, as formas de phishing que tiverem maior destaque no começo foram páginas falsas sobre assuntos relacionado ao Covid-19, e-mails e mensagens falsas se passando pela OMS, na qual eram anexados arquivos sobre o assunto, mas que baixavam malware ao serem clicados, segundo a Check Point Research. Foi reportado também e-mails que estavam solicitando doações para a OMS e a Organização da Nações Unidas (ONU).

Dentre os ataques de phishing, os mais destacados foram o spear-phishing, vishing e smishing.

- Spear-phishing: É um tipo de phishing que é direcionado a um alvo específico, podendo ser um indivíduo, instituição ou empresa, assim os criminosos juntam informações sobre a vítima e executam o ataque utilizando esses dados obtidos, para que faça parecer o mais

legítimo possível o que está sendo enviado, aumentando as chances do golpe ser bem sucedido. Segundo a Reuters, uma agência internacional de notícias, a OMS foi alvo de ataques desse tipo de phishing.

- Vishing: Junção de Voice (Voz) e Phishing, esse tipo de ataque é aplicado por ligações, tendo contato direto com a pessoa, assim trazendo o uso da engenharia social. O criminoso entra em contato com a vítima por algum meio de comunicação por voz e aplica a persuasão, fazendo acreditar que ele é uma pessoa que o alvo acredita ser, geralmente se passando por gerentes bancários ou órgãos públicos. Na pandemia, o que teve destaque foram ligações se passando por suporte técnico de empresas, uma vez que os funcionários estão em trabalho remoto, facilitando a obtenção e o acesso às informações pessoais tanto dos funcionários, quanto da empresa.
- Smishing: Esse ataque é a aplicação do phishing por meio de *Short Message Service* (SMS), na qual são enviadas mensagens de interesse da pessoa, como dados bancários, notícias atuais ou outras informações pessoais, fazendo a vítima informar seus dados, a página pode ser redirecionada ao acessar o link do SMS, ou é feito o download de um malware que faz a captação dos dados dessa vítima, sendo informações de cartões de créditos ou documentos fiscais. Em relação ao atual momento, esse ataque teve mais destaque em relação a liberação do auxílio emergencial, onde é solicitado informações pessoais para a confirmação dos dados, mas na verdade são criminosos aproveitando um momento frágil para roubar suas informações.

No Brasil, a liberação do auxílio emergencial foi algo que se tornou um chamariz para a prática maliciosa. De acordo resultados de análises divulgados, no dia 07 de julho de 2020, pela IBM X-Force Incident Response and Intelligence Services (IRIS), pelo menos 693 sites maliciosos relacionados ao coronavírus e ao auxílio emergencial foram criados no Brasil.

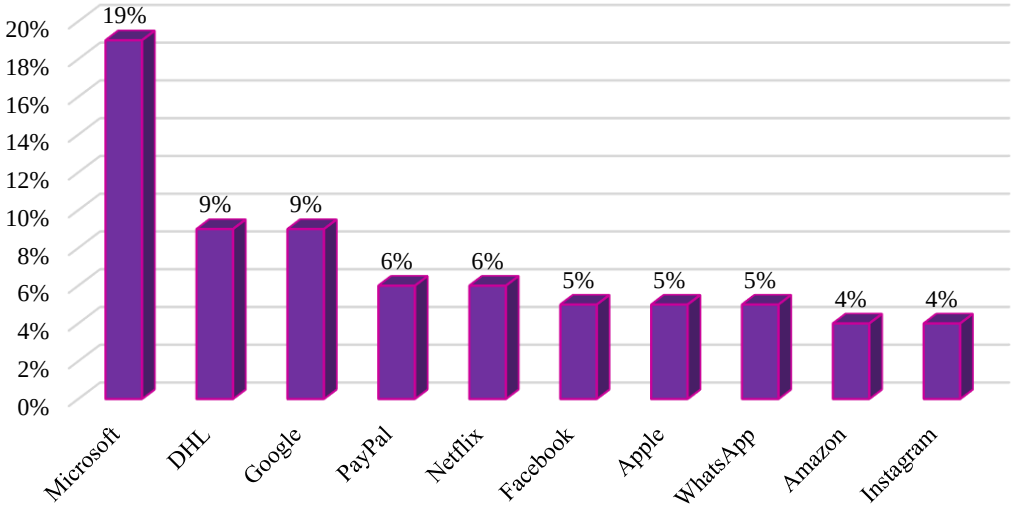
O Google informou que em meados de abril, a plataforma Gmail bloqueou cerca de 18 milhões de e-mails maliciosos relacionados ao Coronavírus. A situação tomou uma proporção tão grande que, a OMS criou uma página para alertar sobre os ataques que estavam sendo aplicados explorando a pandemia do Covid-19.

Segundo IBM X-Force IRIS, a forma que os criminosos agem é na necessidade das pessoas, que se sentem na carência de confirmação de suas informações junto aos órgãos legais. Eles atuam em meio a esse envio de informações e tem como objetivo obter dados para utilizar em futuras fraudes financeiras ou outros tipos de golpes.

Esse tipo de ataque também teve destaque no âmbito empresarial, uma vez que as empresas foram forçadas a aderir o método de trabalho home office. Um estudo realizado pela IT Barracuda Networks, mostrou que 46% delas sofreu ao menos um incidente de segurança desde o início da pandemia e 51% identificou um aumento no número de tentativas de ataques de phishing por e-mail.

A Check Point Software Technologies, empresa que atua na área de segurança, divulgou em 19 de outubro de 2020, um relatório de Brand Phishing referente ao terceiro trimestre de 2020. Esse relatório mostra as marcas que no período de julho a setembro, foram usadas para propagação de ataques phishing. O Gráfico 1 apresenta as marcas que tiveram maior incidência nas tentativas de ataque.

Gráfico 1: Marcas usadas em ataques de phishing no 3º trimestre de 2020.



Fonte: Microsoft is Most Imitated Brand for Phishing Attempts in Q3 2020. Check Point (2020)

O termo Brand Phishing, traduzindo ao pé da letra "phishing de marca", é realizado na criação de *Uniform Resource Locator* (URL) que imitam os sites oficiais das marcas em questão, a fim de roubar as informações que a vítima tem no sistema oficial da marca propriamente dita.

Além do relatório da Check Point, a Kaspersky também notou que esse tipo de ataque tem se tornado muito comum, mas que obteve novas versões em relação ao trimestre anterior: são e-mails de empresas famosas dizendo que a conta teve um acesso não autorizado, ou também mensagens sobre transações que foram feitas pelo usuário pedindo para que a vítima entre em contato com o número que é disponibilizado no golpe.

1.2. Ransomware

Ransomware pode ser definido como:

> "Ransomware é um termo abrangente usado para descrever uma classe de malwares que serve para extorquir digitalmente as vítimas, fazendo-as pagar um preço específico. As duas principais formas de ransomware são aquelas que criptografam, ofuscam ou impedem o acesso aos arquivos, e aquelas que restringem o acesso ou bloqueiam os usuários dos sistemas. Essas ameaças não estão limitadas a nenhuma área geográfica ou sistema operacional em particular e podem atuar em vários dispositivos." (Liska e Gallo, 2017, p. 16).

Os ataques ransomware são caracterizados por um malware enviado para a vítima, em que ao se obter sucesso, faz com que dados sejam roubados, encriptados, e bloqueados, e por meio de extorsão, é solicitado resgate deles em forma de pagamento. De acordo com Liska e Gallo (2017), o método de pagamento que a maioria dos chantagistas digitais exigem atualmente é por criptomoeda, geralmente Bitcoin, mas não é o único método de pagamento exigido. Vouchers pré-pagos também são muito utilizados pelos criminosos, como MoneyPak, Ukash ou PaySafe.

Um ponto a ser levado em consideração é a dúvida: "devo pagar ou não pelo resgate de meus dados?" Infelizmente essa pergunta não tem uma resposta definitiva, pois, se por exemplo, uma empresa paga o resgate e não vem a reaver suas informações, a "credibilidade" dos criminosos em relação a futuros ataques pode cair, pois as empresas não terão confiança em pagar sendo que não receberam seus dados novamente.

Outro ponto é caso a empresa pague, ela não tem a garantia de que os dados já estão excluídos, então as organizações acabam virando verdadeiros reféns dos criminosos. Em alguns casos também o software acaba sendo tão ruim que mesmo sendo pago o resgate e entregue a chave correta para a desencriptação, o programa pode não funcionar e a empresa terá um prejuízo ainda maior.

Além disso, deve ser levado em consideração os custos de reparação. Muitas vezes, para restaurar o que foi perdido por meio de backups fica mais caro que pagar o próprio resgate, ou também

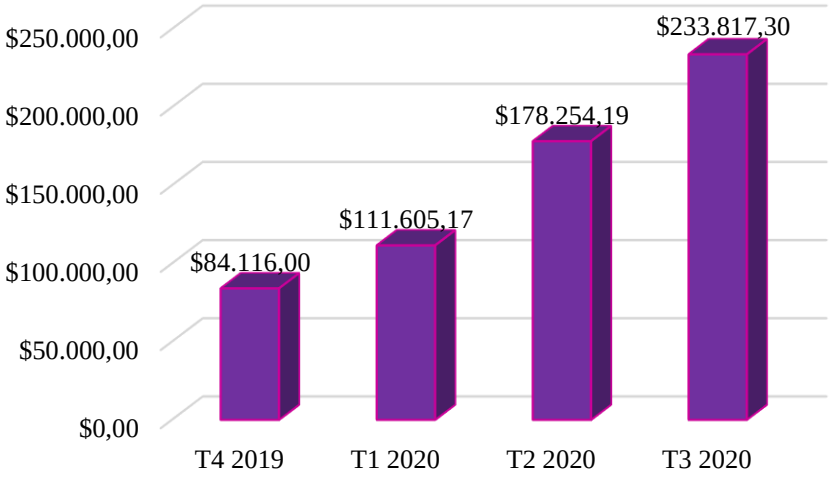
um arquivo importante não foi colocado no seu serviço de backup. Tudo isso deve ser pensado antes da organização ou usuário responder essa questão.

Geralmente o valor solicitado para o resgate variam por grupos e vítimas, como exemplo o grupo de Ransomware Sodinokibi, a ZDNet, site que faz coberturas de notícias globais e análises sobre tendências e oportunidades locais e globais da indústria de TI, diz que o grupo adequa o valor do resgate dependendo da vítima, o maior preço de resgate conhecido que foi solicitado por esse grupo foi de 42 milhões de dólares, já o menor foi cerca de 1.500 dólares.

Segundo Liska e Gallo (2017), há algumas variantes que atacam corporações que cobram dezenas de milhares de dólares, e que existem ransomwares que com o passar do tempo o preço sugerido é aumentado, para causar mais terror para as suas vítimas.

Em uma pesquisa publicada em novembro de 2020 pela Coveware, empresa especializada em proteção e recuperação de golpes relacionados a ransomware, o pagamento médio do resgate de ransomware no último trimestre de 2020 teve uma crescente de 31% chegando à marca de 233.817 dólares. O Gráfico 2 ilustra um comparativo do valor de pagamento médio de resgate de ransomware nos últimos quatro trimestres.

Gráfico 2: Pagamento médio de resgate – Trimestral.



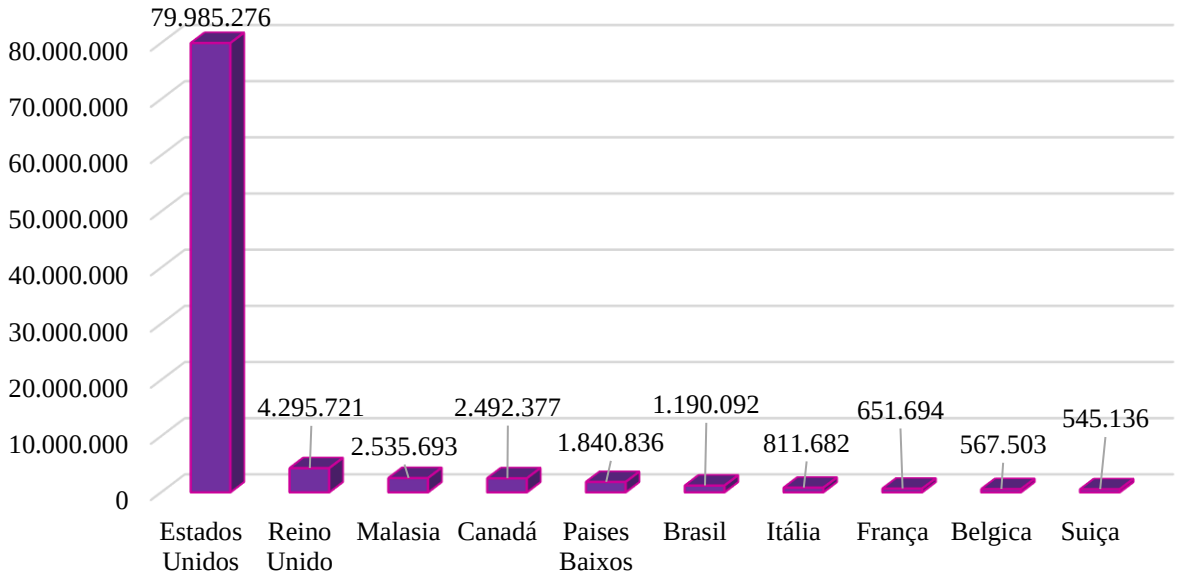
Fonte: Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues. Coveware (2020).

Mesmo sendo um ataque já conhecido, os riscos que ele pode causar e as maneiras de prevenção, na pandemia de 2020 juntamente ao phishing esse método teve uma crescente em sua execução, tendo destaque no ambiente brasileiro, trazendo riscos econômicos para o país. Em grande parte, isso ocorreu pela drástica mudança no cenário de trabalho.

Um agravante para esse ataque é a facilidade que ele pode ser obtido, pois existe um serviço chamado *Ransomware as a Service* (RaaS), que é um modo fácil de usuários comuns terem acesso a ransomwares. Segundo Liska e Gallo (2017) com a chegada do navegador que deixa a navegação anônima *The Onion Router* (TOR), uma economia clandestina e que tem força (conhecida como Dark Web), os hackers que são habilidosos, conseguem vender os seus serviços para outras pessoas, então um indivíduo que deseja atacar outrem pode simplesmente pedir um ransomware customizado ao seu modo, para atacar a pessoa que desejar.

Em julho de 2020, a SonicWall divulgou um relatório de ameaças cibernéticas, na qual é disposto um gráfico dos 10 países que mais sofreram ataques até a data de divulgação do relatório, com o Brasil estando na sexta posição. O Gráfico 3 apresenta os dados coletados pela SonicWall dos números de ataques ransomware até julho de 2020.

Gráfico 3: Países com ataques ransomware até julho/2020.



Fonte: 2020 SonicWall Cyber Threat Report. SonicWall (2020).

Um dos destaques em relação a grandes empresas que sofreram esse ataque durante a pandemia foi a Light, que é uma empresa privada de geração, distribuição, comercialização e soluções de energia elétrica no Rio de Janeiro - RJ.

O incidente que a empresa de energia elétrica Light sofreu ocorreu em 16 de junho de 2020, sendo também um ataque do tipo ransomware. Segundo a revista Veja, os criminosos solicitaram US$7 milhões, totalizando cerca de R$ 37,4 milhões, na qual pediram recebimento pela criptomoeda Monero, que vem recentemente sendo utilizada nesse tipo de ataque. Embora o ataque não tenha influenciado na distribuição de energia, todos os processos administrativos foram inviabilizados.

Em nota, a Light confirmou o ataque:

> "[A Light] sofreu, nesta terça-feira (16/6), um ataque de vírus em seus computadores. O corpo técnico da empresa vem elaborando diagnósticos, ações e recomendações que estão sendo seguidas por seus colaboradores."

A empresa também veio a relatar a seguinte informação:

> "No momento, os serviços de atendimento ao cliente estão enfrentando dificuldades técnicas. Estamos trabalhando para resolver o problema o mais rápido possível."

Essas ameaças além de acarretar consequências para o usuário que foi vítima por um descuido da empresa, pode também colocar ela e seus clientes em risco.

Outro grande aqui no Brasil foi ao Superior Tribunal de Justiça (STJ), em que confirmou no dia 05 de novembro de 2020, quinta-feira, ter sido alvo de um ataque hacker que criptografou todos os dados e fez com que o tribunal suspendesse sessões e tirasse o site do ar.

Dois dias antes da confirmação (03 de novembro de 2020), o STJ identificou um vírus circulando na rede do tribunal. Como medida preventiva, foi desconectado o acesso à Internet, fazendo com que sessões de julgamento fossem cortadas e bloqueando o funcionamento dos sistemas de informática e comunicação da Corte.

Desde o ocorrido, a equipe de tecnologia do STJ vem trabalhando nas restaurações de informações, contando com a ajuda do Centro de Defesa Cibernética do Exército Brasileiro, da Microsoft e de outras empresas prestadoras de serviços de tecnologia para a Corte.

Em uma nota compartilhada com Tilt, canal sobre tecnologia do UOL , o tribunal afirmou:

> "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".

O STJ retoma suas operações aos poucos no dia 10 de novembro de 2020, terça-feira.

Em questão de dados no meio empresarial, a Tabela 1 apresenta uma análise feita pela Sophos, empresa que desenvolve e fornece softwares e hardwares de segurança. Nela foi obtido as informações de como ransomware penetra em uma organização.

Tabela 1: Como os ataques de ransomware entram na rede.

COMO O RANSOMWARE ENTRA NA ORGANIZAÇÃO	% Incidentes
Via download de arquivo / e-mail com link malicioso	29%
Via ataque remoto no servidor	21%
Por e-mail com anexo malicioso	16%
Instâncias na Nuvem pública configuradas incorretamente	9%
Por meio de nosso protocolo de área de trabalho remota (RDP)	9%
Por meio de um fornecedor que trabalha com nossa organização	9%
Por meio de um dispositivo USB / mídia removível	7%
Outro	0%
Não sabe	0%
Total	**100%**

Fonte: Firewall Best Practices to Block Ransomware. Sophos (2020).

A pesquisa foi realizada com pessoas na qual a empresa foi atingida por ataques do tipo ransomware, tendo a base de análise a resposta de 2538 entrevistados.

2. MÉTODOS PREVENTIVOS

Neste capítulo será abordado métodos para prevenção dos ataques descritos, segmentando uma sessão para cada um deles, com intuito de facilitar o entendimento e tornar mais objetivo em questão ao tema, além de atender ambos os meio de trabalho, tanto presencial quanto remoto.

2.1. Ataques Phishing

Como já definido, o Phishing é uma junção de engenharia social e técnicas de hacking, e em relação a segurança da informação, o lado humano sempre será o elo mais fraco, sujeito a vulnerabilidades e fácil de ser explorado pelos hackers. Se tratando de Phishing que é um golpe que funciona apenas se a vítima acreditar no conteúdo do e-mail ou mensagem, clicar no link, fornecer dados ou baixar o arquivo infectado, a empresa pode evitar ser atacada com simples passos:

- Definir uma política de segurança: Uma empresa deve ter uma política de segurança para definir o que pode ser acessado e baixado, e como a mudança do ambiente foi forçada, muitas empresas devem revisar a política caso não seja abordado o tema de home office. Um

exemplo é definir que os usuários podem apenas acessar o ambiente de trabalho por dispositivos disponibilizados pela empresa, já que neles podem ser aplicadas regras que um aparelho pessoal não teria.

- Treinamento e conscientização: A empresa deve oferecer um treinamento referente a como a engenharia social atua nessas situações, tipos de ataques, bem como métodos de defesas para que o funcionário possa lidar com esse novo ambiente, como utilizar o hardware da empresa no ambiente doméstico, também dicas de segurança da informação como por exemplo a mudança de senhas a cada X dias (que deverá ser definido na política de segurança).
- Segurança na rede: A rede deve ser protegida, o acesso deve ser feito através de *Virtual Private Network* (VPN), é recomendado ter uma lista branca de sites que podem ser acessados, desabilitar portas que não serão usadas, permitir apenas as aplicações importantes para o funcionamento da máquina, e a rede sempre deve ser monitorada.
- Auditoria: Deve ser aplicado testes para verificar se as medidas que foram tomadas anteriormente foram eficazes. Pode ser utilizado como exemplo ferramentas que simulam Phishing, com elas é obtido estatísticas de quantos acessos tiveram e há até algumas que podem até dizer o porquê de os usuários terem clicado no link falso.
- O ponto principal que deve ser levado em consideração, em relação aos novos assuntos que surgiram durante a pandemia é a desconfiança, na qual deve ser checado primeiro a fonte original da informação, assim o risco de os golpes terem efeito é minimizado.
- Sempre que um link for enviado é recomendado verificar a veracidade do site ou sistema que está sendo acessado de acordo com o e-mail encaminhado através de pesquisas, pois se ele for falso, haverá relatos de outras pessoas na internet em relação a esse ambiente.
- Nunca compartilhar informações pessoais ou de conhecidos na Internet, pois mesmo que o local de compartilhamento pareça seguro, eles também estão propícios a serem alvos de ataques cibernéticos.
- Validar as informações recebidas com as fontes que já são contactadas, por exemplo, em um envio de e-mail do banco para confirmar suas credenciais, antes de fazer o processo, contate o gerente bancário e confirme essa informação. Ações como essas, simples de serem aplicadas, fazem com que o assalto de informações seja evitado e garantem a sua proteção.

2.2. Ataques Ransomware

O ataque ransomware por sua vez é mais complexo, pois há muitas variantes e cada uma com sua peculiaridade, algumas escolhem apenas um tipo de arquivo para bloquear, outras roubam os arquivos e depois criptografam, há também outras que apagam o arquivo e fazem com que o usuário pague pensando que esse arquivo ainda está disponível na sua máquina. Apesar do principal meio de propagação desse ataque ser por phishing, seus métodos de transmissão são variáveis e todos têm a falta de atenção da vítima em comum.

Para as empresas, há várias opções que ajudam a inibir esses tipos de ataques, e algumas delas podem gerar conflitos entre os usuários que utilizam a máquina com os profissionais da área de TI, contudo, para que o sucesso seja garantido deve ser levado em consideração o balanceamento entre essas duas áreas, para Liska e Gallo (2017), “Quanto mais envolvidos com as mudanças estiverem os líderes e os usuários, maiores serão as chances de eles concordarem com elas.”.

Os dois primeiros pontos citados na seção de phishing também são utilizados para o ransomware, como demostrado na Tabela 1, a maioria dos ransomwares entram nas organizações por meio de links e downloads de arquivos vindos de e-mails maliciosos.

Além dessas dicas em comum, a empresa também deve:

- Investir em atualizações na segurança: Nada adianta os usuários serem treinados para lidar com os problemas da engenharia social e consequentemente com o ransomware se o equipamento que ele manuseia é desprotegido e desatualizado. Muitos donos e gerentes de empresas não gostam quando é dito que a empresa tem que investir em segurança e equipamentos, mas esse ponto é um fator decisivo para que a empresa consiga lidar com esse tipo de ataque.
- Navegadores de sites devem ser protegidos contra-anúncios, patches devem ser aplicados, o firewall precisa estar ativo e configurado, ele deve restringir o acesso dos usuários que utilizam VPN, deixando apenas o acesso permitido para endereços IP que forem permitidos.
- O *Remote Desktop Protocol* (RDP), ou seja, Protocolo de Área de Trabalho Remota teve um crescente no tempo da pandemia e, segundo Tabela 1, de 2.538 entrevistados nas organizações, 221 foram atacados por ransomware por meio do RDP.
- Maus hábitos em relação a senhas é comum no âmbito empresarial, já que se a empresa tem uma política que seja minimamente responsável, é adotado a troca de senhas periodicamente, porém, para o funcionário isso é um problema. Também é recomendado que as senhas sejam fortes e que haja autenticação de dois fatores, para todo tipo de programa e ferramenta de gerenciamento e compartilhamento de arquivos, para que nenhuma delas corram o risco de serem vítimas de ataques ransomware direcionados por força bruta.
- Ter cópias de backups dos seus dados: Como citado no início do tópico, o ransomware consegue deixar o dado indisponível e alguns até excluem as informações. Então uma solução que toda empresa deve aplicar é o costume de realizar backups diários, ou semanalmente. Segundo a Tabela 1 com base na pesquisa da Sophos, dos 2538 que responderam que foram atacados 56% usaram backups para recuperar os arquivos que foram encriptados, então backups podem reduzir os custos que seriam pagos para o resgate dos arquivos.
- Escolher os arquivos que devem ser guardados também é de suma importância, já que não há necessidade de guardar arquivos que sejam temporários ou que não sejam sensíveis para a organização, assim é o custo de armazenamento e a tarefa de backup são otimizados
- Serviços de armazenamento em nuvem como Dropbox, Google Drive e Amazon Cloud Drive são bons aliados para empresas que precisem de uma solução em relação a backups, mas deve ser destacado que se os arquivos de backups estiverem com a opção de sincronia nos arquivos há chances de os arquivos serem criptografados e então a empresa ainda vai ser refém dos invasores, por isso é importante drives compartilhados não estarem ativados, e que os backups sejam feitos na nuvem e em mídias físicas.
- Investir em prevenção e detecção: Outro ponto imprescindível para o sucesso na detenção desse tipo de ataque é a prevenção e detecção, em outra pesquisa da Sophos com 5.000 gerentes de TI em 26 países diz que as vítimas do ransomware gastam mais tempo em resposta do que prevenção, ou seja, depois de já sofrerem o ataque é que a ação de reparo acontece, já os que não foram atingidos focaram mais em prevenção.

Para Dmitry Bestuzhev (2020), diretor da equipe global de pesquisa e análise da Kaspersky na América Latina, a soma desses costumes que deixavam a empresa vulnerável, com a situação em que as corporações passaram ao adequar os seus funcionários com equipamentos para o trabalho remoto sem soluções de segurança, e a adoção do RDP sem nenhum treinamento de boas práticas para cibersegurança fazem com que os riscos de ataques contra corporações aumentem.

Os investimentos em ferramentas de monitoramento de rede, especialistas de segurança da informação e em ferramentas que barram ransomwares e vários outros tipos vírus devem ser grandes.

Ainda na pesquisa citada anteriormente a Sophos (2020) apresenta que mais de 35% dos gerentes que foram vítimas de ransomware no último ano disseram que a contratação e retenção de

profissionais em segurança de TI que sejam qualificados é o maior desafio enfrentado por eles, e 53% disseram que um desafio expressivo.

Em outras palavras, um profissional de segurança da informação que seja qualificado deve ser levado em consideração, tendo em vista que esses ataques são difíceis de lidar e necessitam de muito conhecimento em prevenção e detecção.

Usuários comuns também não estão fora da mira, já que para o atacante é algo simples atacar qualquer pessoa, pois seu ataque segundo Liska e Gallo (2017) se caracteriza por apenas dois passos:

1. Mandar o ataque por algum meio.

2. Receber o pagamento da vítima.

É de suma importância ressaltar que: para que o ataque ransomware funcione é preciso que o usuário interaja com ele, seja por download de arquivos em links, ou por simplesmente abrir um documento PDF que esteja infectado. É necessário duvidar de e-mails, mensagens e propagandas suspeitas, ter o hábito de guardar suas informações em outros discos e até em nuvem.

Ter antivírus instalado na máquina e buscar proteger a sua rede, não esquecendo de sempre deixar o seu firewall habilitado e configurado, em outras palavras prevenção e detecção.

3. CONCLUSÃO

O principal objetivo para a realização deste estudo foi o de demonstrar a significativa mudança que os ataques do tipo phishing e ransomware sofreram em seu método de execução durante a pandemia, principalmente em empresas que trocaram a sua ambientação de trabalho físico para online.

Neste trabalho foram apresentados resultados por meio de exemplos reais e dados estatísticos, que foram analisados e descritos de forma que se pudesse comprovar a mudança citada e efetuar o desenvolvimento dos métodos preventivos.

Foi constatado que muitas empresas pretendem continuar no estilo de trabalho remoto após o término da pandemia, tanto quanto muitas não veem a hora de voltar em seu antigo processo presencial. Com isso os métodos preventivos foram feitos no intuito de atender ambas as situações, a fim de beneficiar a todos.

Para futuros trabalhos pretende-se de realizar um aprofundamento técnico em decorrência do tema, com um objetivo de depurar mais sobre a aplicação dos ataques, analisando os vírus utilizados, os meios de acesso e a identificação em uma rede corporativa.

4. REFERÊNCIAS

AYRES, Nathalie. Vacina contra o coronavírus: 8 principais dúvidas respondidas pela OMS. **Veja**, 2020. Disponível em: <https://saude.abril.com.br/medicina/vacina-contra-o-coronavirus-8-principais-duvidas-respondidas-pela-oms/>. Acesso em: 08 de nov. de 2020.

BOSS, Alex. The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails. **NIST**, 2020. Disponível em: <https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click>. Acesso em: 10 de nov. de 2020.

CARVALHO, Lucas. STJ confirma que hacker criptografou dados, mas processos têm backup. **UOL**, São Paulo, 05 de nov. de 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/11/05/site-do-stj-sai-do-ar-apos-ataque-hacker-saude-tambem-investiga-invasao.htm>. Acesso em: 13 de nov. de 2020.

CONTEH, N. Y.; SCHMICK P. J. **Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks.** International Journal of Advanced Computer Research, Vol 6(23). 2016.

COVID-19 causa nova onda de ataques cibernéticos. **Crypto Id**, 2020. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/covid-19-causa-nova-onda-de-ataques-ciberneticos/>. Acesso em: 10 de out. de 2020.

CYBERSECURITY: The human challenge. **Sophos**, 2020. Disponível em: <https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx>. Acesso em: 14 de nov. de 2020.

HACKERS invadem sistema da Light e pedem resgate de US$ 7 milhões. **Minuto da Segurança**, 2020. Disponível em: <https://minutodaseguranca.blog.br/hackers-invadem-sistema-da-light-e-pedem-resgate-de-us-7-milhoes/>. Acesso em: 27 de jun. de 2020.

HARVEY, Cynthia. 10 Cyberattacks on the Rise During the Pandemic. **InformationWeek**, 2020. Disponível em: <https://www.informationweek.com/strategic-cio/security-and-risk-strategy/10-cyberattacks-on-the-rise-during-the-pandemic/d/d-id/1338155?page_number=6>. Acesso em: 17 de jul. de 2020.

HARVEY, Cynthia. 10 Cyberattacks on the Rise During the Pandemic. **InformationWeek**, 2020. Disponível em: <https://www.informationweek.com/strategic-cio/security-and-risk-strategy/10-cyberattacks-on-the-rise-during-the-pandemic/d/d-id/1338155?page_number=7>. Acesso em: 17 de jul. de 2020.

KHAN, N. A., BROHI, S. N.; ZAMAN, N. **Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.** TechRxiv, 12 de maio de 2020. Disponível em: <https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792/1>. Acesso em: 26 de set. de 2020.

KULIKOVA, Tatyana; SIDORINA, Tatyana. Spam and phishing in Q3 2020. **Kaspersky**, 2020. Disponível em: <https://securelist.com/spam-and-phishing-in-q3-2020/99325/>. Acesso em: 15 de nov. de 2020.

LISKA, Allan; GALLO, Timothy. **Ransomware:** Defendendo-se da extorsão digital. 1. ed. São Paulo: Novatec, 2017. 223 p. ISBN 978-85-7522-551-6.

MACEDO, Jefferson; SINGLETON, Camille. COVID-19 Cybercrime Capitalizing on Brazil's Government Assistance Program. **Security Intelligence**, 2020. Disponível em: <https://securityintelligence.com/posts/covid-19-cybercrime-capitalizing-on-brazils-government-assistance-program/>. Acesso em: 03 nov. de 2020.

MAIS da metade das empresas sofreu ataques-phishing durante pandemia. **CIO**, 2020. Disponível em: <https://cio.com.br/noticias/mais-da-metade-das-empresas-sofreu-ataques-phishing-durante-pandemia/>. Acesso em: 04 de nov. 2020.

MARTINS, Gabriel da Silva. **Segurança Digital:** O Guia para a segurança na internet. 1. ed. [S.I.]: Brutal Security, 2015. E-book. 413 p. Disponível em: <https://www.amazon.com.br/Seguran%C3%A7a-Digital-Guia-seguran%C3%A7a-internetebook/dp/B016H5PF1A.> Acesso em: 15 jun. de 2020.

MICROSOFT is Most Imitated Brand for Phishing Attempts in Q3 2020. **Check Point**, 2020. Disponível em: <https://www.checkpoint.com/press/2020/microsoft-is-most-imitated-brand-for-phishing-attempts-in-q3-2020/>. Acesso em: 31 de out. de 2020.

MICROSOFT Teams Impersonation. **Abnormal Security**, 2020. Disponível em: <https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/>. Acesso em: 15 de nov. de 2020.

NEVES, Andressa. Como evitar se tornar uma vítima de ransomware? Confira nossas dicas. **Canaltech**, 2017. Disponível em: <https://canaltech.com.br/seguranca/como-evitar-se-tornar-uma-vitima-de-ransomware-confira-nossas-dicas/>. Acesso em: 13 de set. de 2020.

O que é smishing e como se proteger? **Kaspersky**, 2020. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>. Acesso em: 17 de jul. de 2020.

O que significa uma 'emergência de saúde pública internacional' da OMS. **Veja**, 2020. Disponível em: <https://veja.abril.com.br/saude/o-que-significa-uma-emergencia-de-saude-publica-internacional-da-oms/>. Acesso em: 10 de out. 2020.

RANGER, Steve. Ransomware: Gangs are shifting targets and upping their ransom demands. **ZDNet**, 2020. Disponível em: <https://www.zdnet.com/article/ransomware-gangs-are-shifting-targets-and-upping-their-ransom-demands/#ftag=RSSbaffb68>. Acesso em: 05 de nov. de 2020.

RANSOMWARE Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase. **Coveware**, 2020. Disponível em: <https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report?rq=q2%202020>. Acesso em: 12 de set. de 2020.

RANSOMWARE Demands continue to rise as Data Exfiltration becomes common, and Maze subdues. **Coveware**, 2020. Disponível em: <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>. Acesso em: 18 de nov. de 2020.

RANSOMWARE Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020. **Coveware**, 2020. Disponível em: <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>. Acesso em: 12 de set. de 2020.

RANSOMWARE. Costs Double in Q4 as Ryuk, Sodinokibi Proliferate. **Coveware**, 2020. Disponível em: <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate?rq=84%2C116>. Acesso em: 12 de set. de 2020.

RODRIGUES, Renato. Brasil é líder empresas atacadas por ransomware na epidemia: Cibercrime aproveitou a transferência de funcionários para regime de home office para intensificar ataques. **Kaspersky**, 2020. Disponível em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/>. Acesso em: 15 jun. de 2020.

SANHOTRA, Rajan. Report: Firewall Best Practices to Block Ransomware. **Sophos**, 2020. Disponível em: <https://news.sophos.com/en-us/2020/08/18/report-firewall-best-practices-to-block-ransomware/>. Acesso em: 14 de nov. de 2020.

SHI, Fleming. Surge in security concerns due to remote working during COVID-19 crisis. **Barracuda**, 2020. Disponível em: <https://blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/>. Acesso em: 04 de nov. de 2020.

SOBRE a doença. **Ministério da Saúde**, 2020. Disponível em: <https://coronavirus.saude.gov.br/sobre-a-doenca#o-que-e-covid>. Acesso em: 10 de nov. de 2020.