Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

O aumento dos ataques cibernéticos em função da pandemia de COVID-19

Henrique Lacerda Alvarenga, Luis Otávio Lourenço de Souza

henrique.alvarenga@fatec.sp.gov.br, luis.souza26@fatec.sp.gov.br

Abstract. *This paper has as objective to relate the coronavírus pandemic to an expressive growth in cyberattacks such as phishing, trojans and ransomwares and also explore the security flaws in applications that had seen an peak in users in function to preventions politics such as social distancing and work from home*

keywords: *coronavírus, phishing, ransomware, trojan, security, cryptography, attacks*

Resumo. *Este artigo busca relacionar a pandemia de coronavírus com o aumento expressivo de ataques cibernéticos como phishing, trojans e ransomwares e também explorar a falta de segurança presente em aplicativos que sofreram com um fluxo elevado de novos usuários devido as políticas de prevenção como o distanciamento social e o trabalho remoto*

Palavras-chave: coronavírus, *trojan, ransomware, phishing*, segurança, criptografia, ataques.

1. Introdução

Com a pandemia do novo coronavírus (Sars-CoV-2), causador da doença COVID-19, pode ser observado um aumento significativo no número de crimes cibernéticos. Foi reportado pela empresa Check Point um total de 200,000 casos por semana de ataques relacionados ao Sars-CoV-2, uma alta de 3900% comparado aos 5,000 ataques por semana antes da pandemia, considerando a alta no uso da internet para ter acesso a serviços antes primariamente presenciais - como um grande número de empresas adotando o modelo de trabalho remoto sem ter um planejamento para lidar com acessos a serviços que anteriormente estavam em um servidor isolado como VPN's[1], segregação de permissões a usuários, falta de treinamento aos colaboradores sobre boas práticas de segurança - como fatores de risco contra ataques cibernéticos,

[1] VPN é uma sigla em inglês para "Rede Virtual Privada, que age criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem te m as credenciais necessárias.

o que abre portas para que os criminosos cibernéticos possam utilizar meios para adquirir dados sensíveis ou implantar *backdoors*[2] em pontos chave dos sistemas possibilitando um ataque de maior escala.

Este artigo procura definir os principais tipos de ameaças virtuais e divulgar ciberataques registrados durante a pandemia do COVID-19, de modo a torná-los conhecidos para ajudar na prevenção de novos incidentes.

2. Phishing

Phishing é um tipo de ataque que consiste no atacante convencer alguém a dar informações sensíveis a eles através de anúncios em *sites*, *e-mail* e até mesmo contato direto com a vítima visando adquirir dados como cartões de crédito, como mostrado na figura 1. Ataques de *phishing* muitas vezes estão relacionados a descontos ou promoções relacionadas a produtos e serviços ou comunicados oficiais do governo oferecendo benefícios a população. Além disso, muitas vezes o *phishing* é utilizado como um catalisador para ataques maiores, como *trojans* e *ransomwares*, instalando uma porta de entrada na rede das empresas afetadas.

FIGURA 1: Exemplo de ataques de *phishing* realizados no aplicativo Whatsapp. Fonte: Olhar Digital, 2020.

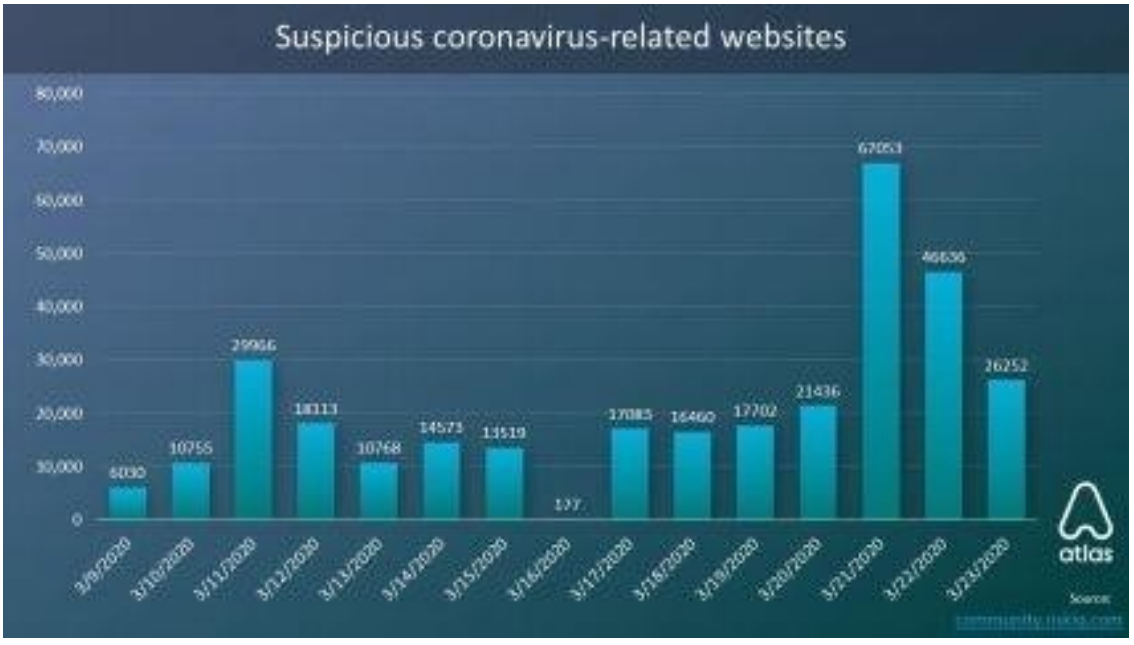
Segundo Radoini (2020) os ataques de *phishing* tiveram um pico, segundo dados adquiridos pelo Google mostrados na figura 2 e analisados pela Atlas VPN, indicam que entre janeiro e março de 2020 ocorreu um aumento de 350% nos *sites* de *phishing* ativos, saltando de 149 mil para 522 mil.

[2] Backdoor é uma porta de acesso ao sistema, que foi criada a partir de um programa instalado que não foi autorizado pelo proprietário do sistema e que permite o acesso ao computador por pessoas não autorizadas

FIGURA 2: *sites* maliciosos identificados pelo google
Fonte: Atlas VPN, 2020.

Esses dados mostram mais de 349 mil *sites* maliciosos ligados ao COVID-19 entre os dias 9 e 23 de março como indicado na figura 3 e tendo picos nos dias 21 com 67,053 casos e dia 22 com 46636 *sites* detectados pelo RiskIQ (Empresa focada em segurança cibernética fundada em 2009) utilizando palavras chaves relacionadas ao coronavírus, tratamentos e vacinas.

FIGURA 3: *sites* suspeitos relacionados ao coronavírus. Fonte: Atlas VPN, 2020.



2.1. Ataques a hospitais e trabalhadores da saúde

Alguns dos ataques mais comuns direcionados a área da saúde, segundo Barnett e Okuda (2020), estão relacionados a *e-mails* nos quais o remetente afirma ser alguma organização conhecida como a Organização Mundial de Saúde (OMS) pedindo por doações ou suporte financeiro, ou se passa por algum centro de pesquisa e prevenção fornecendo informação sobre como combater o COVID-19. Alguns *e-mails* podem carregar documentos anexados que dizem conter informações vitais, mas na verdade estão embutidos com códigos maliciosos.

Outro tipo de estratégia que os atacantes estão utilizando é a da se passar por fornecedores médicos, eles enviam mensagens alegando que suas entregas foram barradas e demandam uma ação da equipe do hospital para completar a mesma, o corpo da mensagem carrega um *link* que envia o destinatário a um *site,* o qual instala um programa malicioso na máquina, os dois tipos de *malware* mais utilizados nesse ataque são *trojans* e *ransomwares*.

2.2 Desinformação

Segundo um artigo da Interpol (2020), em fevereiro a OMS (Organização Mundial de Saúde) anunciou que junto à pandemia de COVID-19 estava ocorrendo também uma pandemia de desinformação. Segundo uma pesquisa feita pelo Instituto Reuters (Centro de estudos sobre questões que afetam as agências de notícias globalmente, da universidade de Oxford na Inglaterra, 2020) listou os tópicos relacionados ao vírus que aparecem mais comumente com o aumento de notícias falsas, sendo eles: As ações dos órgãos públicos, como o vírus se espalha e taxas de transmissão comunitária, teorias da conspiração e desenvolvimento da vacina. Segundo Reuters, 27% dos países participantes na *Global Cybercrime Survey* (Pesquisa global sobre crimes cibernéticos) confirmaram a circulação de informações falsas relacionadas ao COVID-19 e 21% apresentaram uma preocupação sobre esse fato.

Os ataques de *phishing* são favorecidos com o aumento dessas falsas informações sendo compartilhadas, principalmente por conta das redes sociais expondo usuários mais leigos a *links* maliciosos que contém *malwares* e outros *softwares* maliciosos ou até mesmo *scams*[3] prometendo curas, investimentos seguros em setores que não foram afetados pelo coronavírus ou produtos com baixo estoque e alta demanda devido a pandemia.

3. *Trojans* ou Cavalos de Tróia

Conforme definido por Josh Fruhlinger (2019), um *Trojan* ou Cavalo de Tróia consiste em uma variedade de *malwares* que se disfarçam aparentando ser um programa legítimo e inofensivo, com o propósito de enganar os usuários a o deixarem passar por suas defesas. Como muitos *malwares*, os propósitos dos *Trojans* são atacar os computadores dos usuários e inutilizar seus serviços ou tomar posse de informações sigilosas.

[3] Scams é um tipo de ataque que consiste em falsamente oferecer um produto ou serviço.

3.1. Ataques a Instituições Bancárias utilizando *Trojans* durante a pandemia do COVID-19

Desde o início da pandemia do novo coronavírus (Sars-CoV-2) pôde ser observado um aumento significativo nas transações financeiras por meios eletrônicos. De acordo com uma pesquisa realizada pela Capgemini e Efma (2020) com 11.200 correntistas de 11 países e 80 executivos globais de bancos de varejo - incluindo o Brasil -, o uso de aplicativos bancários cresceu para 55%, comparado aos 47% antes do decreto da pandemia. No entanto, conforme um balanço feito em 2020 pela Febraban (Federação Brasileira de Bancos), ocorreu também um aumento de 70% nas tentativas de golpes financeiros no Brasil.

Segundo um levantamento feito pela empresa de soluções de segurança cibernética Check Point (2020), durante o primeiro semestre de 2020 os três principais *malwares* usados em ataques cibernéticos direcionados às instituições bancárias foram com o uso de *trojans* como Trickbot, Ramnit, Dridex e Agent Tesla. Dessa forma, esses ataques têm como objetivo roubar credenciais de usuário e/ou informações financeiras fazendo o uso de *trojans* em conjunto com outros malwares como *Ransomwares*. Porém, existem também *malwares* sofisticados como o Emotet que utilizam múltiplos métodos para se auto-propagar e também distribuir outros *softwares* maliciosos como os *ransomware*s.

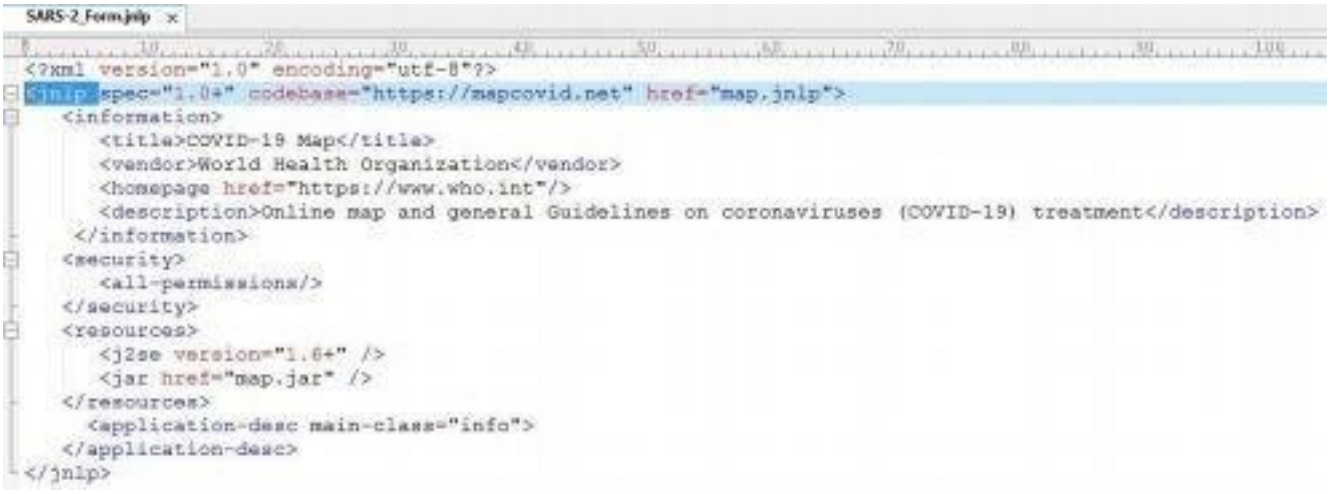
3.2 Trickbot

Conforme definido pela empresa MalwareBytes (2020), Trickbot é um *trojan* bancário que alveja máquinas com sistemas operacionais Windows. Desenvolvido em 2016, o *malware* é construído por meio de módulos acompanhados por um arquivo de configurações. Cada módulo de um Trickbot executa tarefas específicas como propagação, roubo de credenciais, criptografia, etc. Trickbots normalmente se propagam em *emails* de *phishing*, anexos de *emails* e URL's incorporadas, como mostrado na figura 4.

De acordo com a comunidade de *experts* de segurança da Microsoft (Microsoft Security Intelligence, 2020), o Trickbot é o *malware* mais prolífico que usa como isca temáticas sobre a COVID-19.

FIGURA 4: Código de um formulário relacionado a COVID-19 anexado a um e mail spam, a linha destacada baixa e executa o Trickbot "map.jnlp".

Fonte: Trustware, 2020.



3.3 Ramnit

Ramnit é definido como uma família de *trojans* cujo objetivo é se infiltrar em sistemas operacionais para abrir *backdoors* e agir como um distribuidor para outros *malwares.*

Seus principais meios de distribuição são anexos de *email* infectados, *softwares* pirateados, e anúncios maliciosos em *sites*.

Quando dentro de um computador, o Ramnit pode infectar arquivos “.dll”, ".exe" e ".HTML", injetando código malicioso nestes arquivos. Ao abrir qualquer arquivo infectado, o código do Ramnit é executado e podem ser instalados diversos *malwares* no sistema do usuário.

3.4 Dridex

O trojan Dridex pode ser definido como uma variação sofisticada de *malware* bancário distribuído em plataformas *Windows* e se proliferando por meio de campanhas de *spam* com o objetivo de roubar credenciais bancárias por meio de *WebInjects* [4] redirecionando as credenciais enviadas pelo usuário para um servidor remoto controlado pelo atacante.

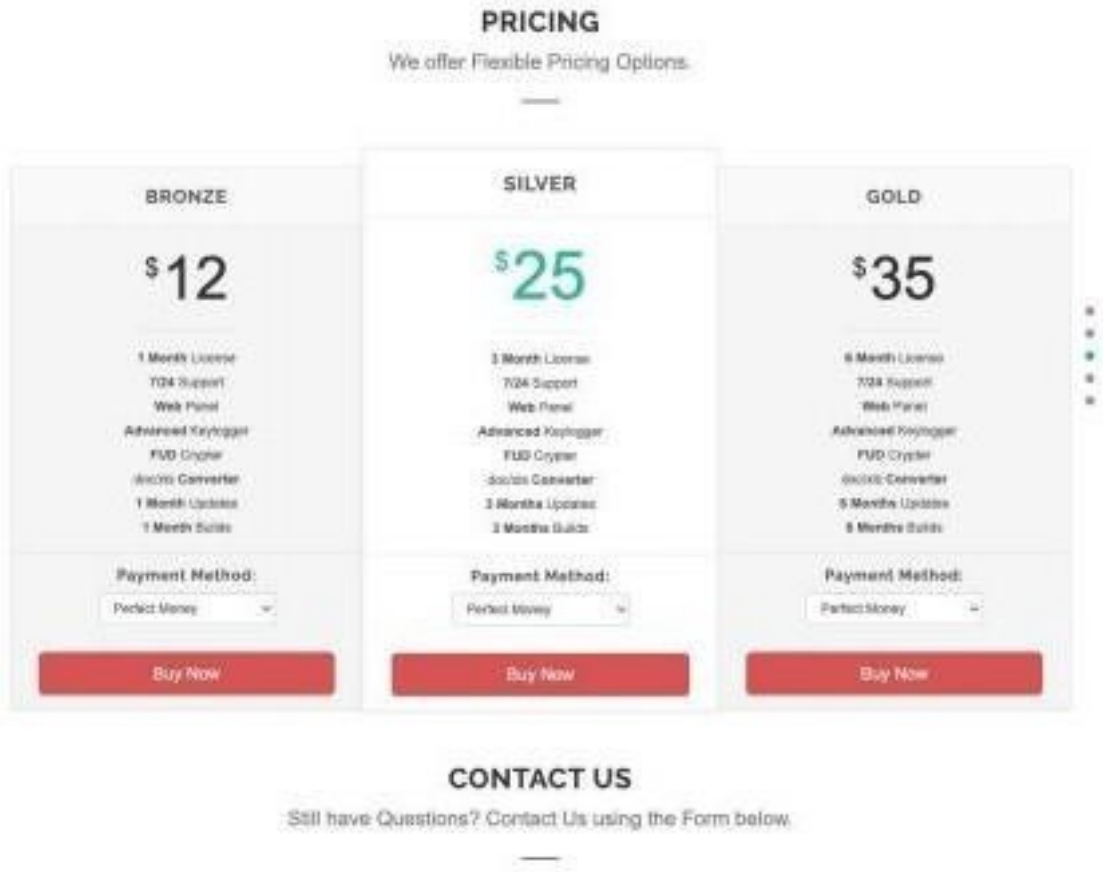
Segundo a empresa de soluções de segurança Check Point, atualmente o Dridex afeta 4% de todas as organizações globalmente.

3.5 Agent Tesla

Apresentada originalmente como um *software* legítimo, Agent Tesla é uma ferramenta de acesso remoto (RAT) que utiliza *keyloggers* para tomar controle da máquina do usuário. O *malware* era vendido em seu próprio site (agora *offline*) á partir de 12 dólares mensais e podia ser comprado por qualquer pessoa e usado livremente, conforme pode ser observado na figura 5. Os desenvolvedores do *malware* também forneciam suporte por meio de um servidor Discord (Popular aplicativo de voz-sobre-ip gratuito), inclusive providenciando dicas sobre suas utilizações para os usuários.

[4] Webinjects são módulos usados em malwares para injetar código HTML ou javascript antes da página ser renderizada

FIGURA 5: Planos e Recursos do Agent Tesla. Fonte: Sentinel Labs, 2020.



Como a maioria dos *trojans* abordados neste artigo, o Agent Tesla se prolifera por campanhas de *email* maliciosas, *spam* e anúncios fraudulentos. Uma vez baixado, o Agent Tesla utiliza de *keyloggers* - método usado para armazenar teclas digitadas pelo usuário - para ter acesso à informações confidenciais do usuário.

3.6 Emotet

Identificado pela primeira vez em 2014, o trojan Emotet foi originalmente projetado para roubar credenciais bancárias, com suas últimas versões apresentando capacidades avançadas de distribuição de outros *malwares* e prevenção de detecção. Seu principal método de transmissão também são os *emails* com anexos contendo *script*s ou *links* maliciosos que podem baixar o *trojan* no dispositivo do usuário.

Definido pela Cybersecurity & Infrastructure Security Agency (Departamento Governamental de Segurança Interna dos Estados Unidos, 2020) como um dos *malwares* mais custosos e destrutivos, o Emotet está entre os mais avançados *trojans* disponíveis atualmente. Suas características o permitem se espalhar rapidamente usando características de *worms* e seus ataques já chegaram a gerar o gasto de mais de 1 milhão de doláres por incidente. Sua estrutura modular também é de difícil remediação: O Emotet possui módulos para recuperar senhas

antigas do usuário e usá-las para obter acesso, também consegue enviar cópias de si mesmo em *emails* de *phishing,* e finalmente usa *bypasses* para se escrever dentro de discos compartilhados, o que pode significar uma infecção de vários servidores e clientes. Finalmente, o Emotet pode inserir código em processos importantes como *explorer.exe* para persistir no sistema.

Até Outubro de 2020, o Emotet é o *trojan* mais presente e o que cresce no Brasil, impactando 15,64% das organizações no país, também mantém a liderança globalmente impactando 14% de todas as organizações segundo pesquisa realizada pela Inforchannel.

4. Ransomwares

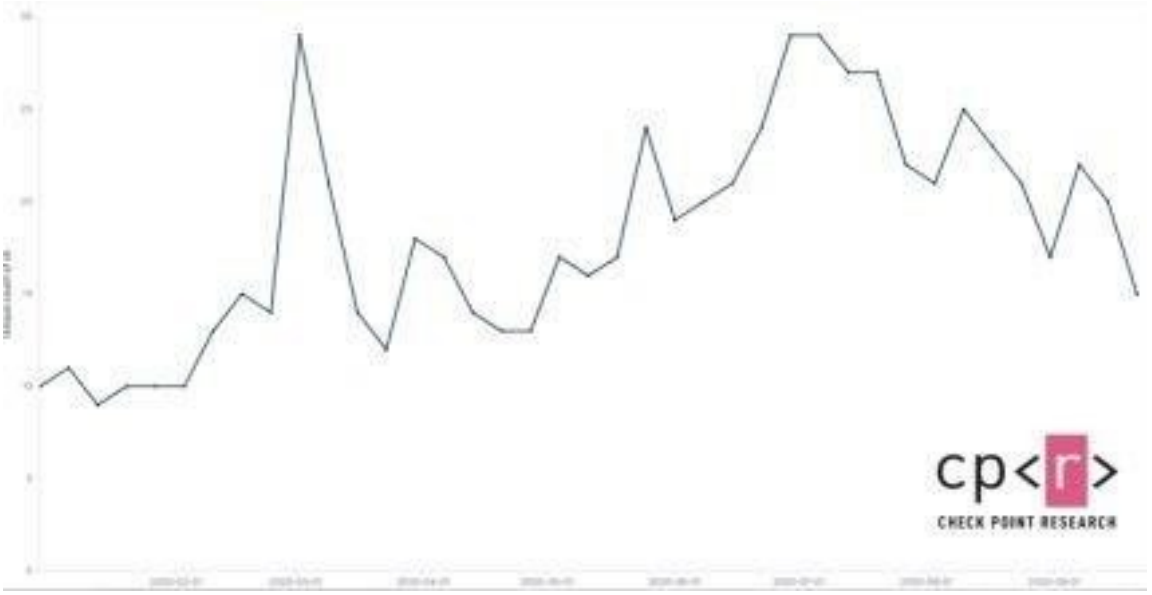
Segundo a empresa russa de soluções em segurança Kaspersky (2020), *ransomware* é um *software* malicioso que ao infectar a máquina criptografa arquivos importantes ou o próprio disco rígido e mostra mensagens demandando o pagamento de uma taxa para liberar os arquivos afetados, o que não significa que os dados permanecerão em sigilo ou que os mesmos serão de fato liberados, podem também transformar a máquina em um "computador-zumbi" utilizado para minerar criptomoedas. Muitas vezes são instalados por consequência de um ataque de *phishing* e podem vir também camuflados em outros aplicativos.

De acordo com Upatham e Treinen (2020) os casos de ataques de *ransomware* aumentaram 148% entre janeiro e março de 2020 tendo seus picos mais notáveis relacionados a dias importantes no ciclo de notícias relacionadas a COVID-19, sugerindo que os atacantes estão utilizando as informações urgentes para investir contra a população vulnerável e sendo seus principais alvos a indústria financeira tendo em março 52% de todos os ataques vistos através do VMware Carbon Black (*software* de segurança para armazenamento em nuvem) relacionados a si e 70% desses ataques sendo de um *malware*
de mineração de criptomoedas.

No setor de saúde também foi observado um aumento expressivo nesse tipo de ataque tendo como alvos principais pequenos prestadores de serviços e grandes centros médicos, que devido ao COVID-19 operaram com capacidade máxima em sua maioria. Além do *phishing* grupos buscam vulnerabilidades presentes em serviços de VPN para infectar uma rede e lateralmente através da mesma coletar credenciais administrativas para por fim implantar os *softwares* nocivos nos sistemas, criptografando todas as informações desta rede segundo Lawrence Abrams (ABRAMS,2020), visando auxiliar os centros de saúde a Microsoft disponibilizou gratuitamente acesso a um sistema de segurança que envia notificações sobre as vulnerabilidades encontradas nos dispositivos presentes na rede.

Um dos *softwares* que foram mais utilizados para ataques no setor da saúde foi o Ryuk, que diferente de outros *ransomwares* como o WannaCry que ficou famoso em 2018 e busca infectar o maior número de máquinas pedindo um resgate pequeno, foca em infectar uma grande organização e pedir um grande valor de resgate, vem sendo observado pela companhia de *software* Check Point, ilustrado pela figura 6 que desde julho de 2020 ataques relacionados a este *software* tiveram um pico e chegou a alvejar cerca de 20 organizações semanalmente.

FIGURA 6: Ataques por semana utilizando Ryuk, em todos os setores.
Fonte: Check Point, 2020.



Ainda houve um crescimento no número de ataques utilizando o Ryuk que tem como alvo organizações de saúde, sendo o setor mais alvejado nos Estados Unidos da América, chegando a afetar um dos maiores provedores de serviços médicos do país o Universal Health Services. O ataque ocorreu dia 27 de setembro de 2020 travando computadores e sistemas telefônicos em diversos estabelecimentos da UHS, segundo Zack Whittaker (2020) uma pessoa que teve conhecimento do incidente afirmou que as telas dos computadores exibiram uma mensagem ligada ao Ryuk e após isso foram ordenados a desligarem os computadores e não ligarem novamente e que levariam alguns dias para que eles estivessem operacionais novamente.

5. Aplicativos de chamada de vídeo

Desde o começo das políticas de isolamento social impostas por órgãos governamentais foi registrado um crescimento no uso de aplicativos de videoconferência, alguns desses contém falhas graves de segurança que foram expostas com o aumento de usuários ativos visto que os mesmos não estavam preparados para o aumento de dados sensíveis vindos destes usuários. Falhas que permitiam usuários a se conectarem a chamadas sem serem convidados, problemas com senhas não seguras, repasse não autorizado de dados a outras companhias, falta de criptografia *end-to-end* ou simplesmente servidores não preparados para o alto fluxo de usuários, com a competitividade criada pela alta demanda de serviços desse tipo, grande parte dessas falhas foram rapidamente corrigidas porém algumas persistiram por tempo suficiente para comprometer um alto número de usuários.

5.1. Zoom

Zoom é um aplicativo de videoconferências fundado em 2011 e lançado em janeiro 2013 por Eric Yuan, durante os anos seguintes o aplicativo foi ganhando uma popularidade estável de um milhão de usuários em maio de 2013, para 10 milhões

um ano depois em junho de 2014 e então 40 milhões em fevereiro de 2015 porém em 2020 devido a pandemia do novo coronavírus chegou a 300 milhões de reuniões diárias em abril de acordo com dados de Iqbal (2020).

Com o aumento expressivo de usuários, foram se revelando algumas falhas cruciais em relação a segurança presentes no aplicativo.

5.1.1 Envio de dados não autorizados ao Facebook

Uma matéria escrita por Cox (2020) na revista VICE, indica que o aplicativo estava mandando dados de usuários ao Facebook, algo que não consta na política de privacidade do Zoom, mesmo que ele não tenha uma conta na rede social, uma inspeção no aplicativo mostra que ao abrir ele envia detalhes sobre o usuário como modelo do aparelho utilizado, fuso horário e cidade a qual ele está se conectando e um identificador de propaganda criado pelo dispositivo, o qual empresas utilizam para anúncios direcionados.

5.2 Invasão de chamadas

Muitos usuários do aplicativo relataram que suas reuniões foram sequestradas por indivíduos anônimos que espalharam imagens de cunho pornográfico ou racista, o Departamento Federal de Investigação dos Estados Unidos da América (FBI, 2020) divulgou uma nota advertindo a população a ser cautelosa com as reuniões criadas no Zoom,
fornecendo dicas de segurança.

5.3 Resposta das companhias

Segundo informações fornecidas pela Fundação Mozilla (2020) em Outubro grande parte das falhas existentes devido a uma fraca política de segurança foram corrigidas pelos aplicativos que viram um aumento significativo no número de usuários em 2020 devido a pandemia de COVID-19, também foram tomadas medidas para que se dificultasse a invasão de chamadas ou reuniões. Porém, a fundação aponta que em alguns casos os aplicativos ainda apresentam brechas como a falta de uma autenticação em duas etapas garantindo mais segurança ao usuário em relação a sua conta no aplicativo, armazenamento e compartilhamento de informações pessoais do usuário.

6. Conclusão

Com o aumento massivo de pessoas conectadas à internet, ocorreu também o aumento na movimentação de grupos *hackers* visando explorar o medo e pânico criado pela a pandemia e a falta de preparo das instituições para lidar com o grande fluxo de usuários conectando-se entre si e remotamente aos servidores de suas empresas devido ao distanciamento social e o trabalho remoto que foi implementado em grande parte das empresas, mostrando falhas tanto de segurança como de infraestrutura. Boa parte dessas instituições buscaram tanto corrigir as falhas existentes em seus sistemas como atualizar suas políticas de segurança.

Nesse momento é de suma importância que as empresas se conscientizem

e com isso passem orientações a seus colaboradores visando prevenir e mitigar os riscos de invasões a seus servidores e aos dados existentes no mesmo.

Referências

C. John. “Google Registers a 350% Increase in Phishing Websites Amid Quarantine”. Disponível: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing websites-amid-quarantine, Março/2020. Acesso: Junho/2020.

Barnett, D. and Okuda, S. “Phishing in the Time of COVID-19: How to Recognize Malicious Coronavirus Phishing Scams”. Disponível: https://www.eff.org/pt br/deeplinks/2020/03/phishing-time-covid-19-how-recognize-malicious-coronavirus phishing-scams, Março, 2020. Acesso: Junho/2020.

Fruhlinger, J. “What is a Trojan? How this tricky malware works”. Disponível: https://www.csoonline.com/article/3403381/what-is-a-trojan-horse-how this-tricky-malware-works.html, Junho/2019. Acesso: Junho/2020.

TI INSIDE. “Trojan Dridex entra no ranking global de Top 10 malware mais procurado em março”. Disponível: https://tiinside.com.br/13/04/2020/dridex-o-trojan-bancario bem-posicionado-no-ranking-global-de-top-10-malware-mais-procurado/. Acesso: Junho/2020.

Munhoz, F. “Tentativas de golpes envolvendo bancos sobem 70% na pandemia”. Disponível: https://agora.folha.uol.com.br/grana/2020/06/tentativas-de-golpes envolvendo-bancos-sobem-70-na-pandemia.shtml, Junho/2020. Acesso: Junho/2020.

Flach, N. “Usuários de internet banking passam de 49% para 57% após pandemia de covid”. Disponível: https://exame.com/negocios/usuarios-de-internet-banking-passam de-49-para-57-apos-pandemia-de-covid/, Junho/2020. Acesso: Junho/2020.

IMPERVA. “Phishing attacks”. Disponível: https://www.imperva.com/learn/application security/phishing-attack-scam/. Acesso: Junho/2020.

Upatham, P. and Treinen, J. “Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted”. Disponível: https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike in-ransomware-attacks-finance-industry-heavily-targeted/, Abril/2020. Acesso: Junho/2020.

Kapersky, “What is Ransomware?”. Disponível: https://www.kaspersky.com/resource center/definitions/what-is-ransomware. Acesso: Junho/2020.

Cox, J. “Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account”. Disponível: https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends data-to-facebook-even-if-you-dont-have-a-facebook-account, Março/2020. Acesso: Junho/2020.

Scroxton, A. “Banking trojans roar back to prominence in May” Disponível: https://www.computerweekly.com/news/252484667/Banking-trojans-roar-back-to prominence-in-May, Junho/2020. Acesso: Julho/2020

Check Point, “Coronavirus Pandemic Drives Criminal and Political Cyberattacks across Networks, Cloud and Mobile”. Disponível: https://pages.checkpoint.com/cyber-attack

2020-trends.html, 2020. Acesso: Outubro/2020.

RiskIQ, “RISKIQ I3 INTELLIGENCE BRIEF: Ransomware in Health Sector 2020: A Perfect Storm of New Targets and Methods”. Disponível: https://www.riskiq.com/wp content/uploads/2020/04/Ransomware-in-Health-Sector-Intelligence-Brief-RiskIQ.pdf, Abril/2020. Acesso: Outubro/2020.

Abrams, L. “Microsoft is Alerting Hospitals Vulnerable to Ransomware Attacks”. Disponível: https://www.bleepingcomputer.com/news/security/microsoft-is-alerting hospitals-vulnerable-to-ransomware-attacks/, Abril/2020. Acesso: Outubro/2020.

Gallagher, R. and Bloomberg. “Hackers ‘without conscience’ demand ransom from dozens of hospitals and labs working on coronavirus”. Disponível: https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/, Abril/2020. Acesso: Outubro/2020.

Whittaker, Z. “Healthcare giant UHS hit by ransomware attack, sources say”. Disponível: https://techcrunch.com/2020/09/28/universal-health-services-ransomware/, Setembro/2020. Acesso: Outubro/2020.

Check Point, “Check Point Research: COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020”. Disponível: https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1- 2020/. Acesso: Novembro/2020.

Malwarebytes. “Trojan.TrickBot”. Disponível: https://blog.malwarebytes.com/detections/trojan-trickbot/. Acesso: Novembro/2020.

CISO Advisor. “Trickbot é o malware mais prolífico durante pandemia da covid-19”. Disponível: https://www.cisoadvisor.com.br/trickbot-e-o-malware-mais-prolifico durante-pandemia-da-covid-19/, Abril/2020. Acesso: Novembro/2020.

Malwarebytes. “Emotet”. Disponível: https://pt.malwarebytes.com/emotet/. Acesso: Novembro/2020.

Lopera, D. “TrickBot Disguised as COVID-19 Map”. Disponível: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trickbot-disguised as-covid-19-map/, Junho/2020. Acesso: Novembro/2020.

Meskauskas, T. “Guia de remoção do vírus Ramnit”. Disponível: https://www.pcrisk.pt/guias-de-remocao/9399-ramnit-virus, Julho/2020. Acesso:

Novembro/2020.

INTERPOL. “INTERPOL report shows alarming rate of cyberattacks during COVID 19”. Disponível: https://www.interpol.int/News-and-Events/News/2020/INTERPOL report-shows-alarming-rate-of-cyberattacks-during-COVID 19#:~:text=INTERPOL%20report%20shows%20alarming%20rate%20of%20cyberatta c ks%20during%20COVID%2D19,-4%20August%202020&text=An%20INTERPOL%20assessment%20of%20the,corporat ions%2C%20governments%20and%20critical%20infrastructure, Agosto/2020. Acesso: Novembro/2020.

Rigues, R. “Ataques de ransomware no Brasil cresceram 3,5 vezes desde janeiro, diz pesquisa”. Disponível: https://olhardigital.com.br/coronavirus/noticia/ataques-de ransomware-no-brasil-cresceram-3-5x-desde-janeiro-diz-kaspersky/98583, Março/2020. Acesso: Novembro/2020.

Walter, J. “Agent Tesla | Old RAT Uses New Tricks to Stay on Top”. Disponível: https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/, Agosto/2020. Acesso: Novembro/2020

Meskauskas, T. “Guia de remoção do vírus Agent Tesla”. Disponível: https://www.pcrisk.pt/guias-de-remocao/9252-agent-tesla-rat, Junho/2020. Acesso: Novembro/2020.

Check Point. “Global Surges in Ransomware Attacks”. Disponível: https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/, Junho/2020. Acesso: Outubro/2020.

Inforchannel. “Os malwares Emotet e Trickbot têm causado um aumento nos ataques de ransomware”. Disponível: https://inforchannel.com.br/os-malwares-emotet-e-trickbot tem-causado-um-aumento-nos-ataques-de-ransomware/, Novembro/2020. Acesso: Novembro/2020.

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Henrique Lacerda Alvarenga,
Luis Otávio Lourenço de Souza

O aumento dos ataques cibernéticos em função da pandemia de COVID-19

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

Americana, 14 de dezembro de 2020.

Banca Examinadora:

_____
Marcus Vinícius Lahr Giraldi (Presidente)
Especialista
Fatec Americana Ministro Ralph Biasi

_____
José Mario Balan (Membro)
Especialista
Fatec Americana Ministro Ralph Biasi

_____
Maria Cristina Aranda (Membro)
Doutora
Fatec Americana Ministro Ralph Biasi