RAMON RIULLER DE SOUZA

CRESCIMENTO E EVOLUÇÃO DOS ATAQUES RANSOMWARES

LAVRAS – MG

2022

RAMON RIULLER DE SOUZA

CRESCIMENTO E EVOLUÇÃO DOS ATAQUES RANSOMWARES

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Graduação em Sistemas de Informação, para a obtenção do título de Bacharel.

Prof. Joaquim Quinteiro Uchoa
Orientador

LAVRAS – MG

2022

RAMON RIULLER DE SOUZA

CRESCIMENTO E EVOLUÇÃO DOS ATAQUES RANSOMWARES

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Graduação em Sistemas de Informação, para a obtenção do título de Bacharel.

APROVADA em 08 de Setembro de 2022.

Prof. Paulo Afonso Júnior UFM
Prof. Juliana Galvani Greghi FCO

Prof. Joaquim Quinteiro Uchoa
Orientador

LAVRAS – MG
2022

AGRADECIMENTOS

Primeiro agradeço a Deus por ter me apoiado até aqui. Agradeço também a Nossa Senhora Aparecida por ter sempre me socorrido nas minhas tribulações. Agradeço a minha família por sempre ter me mostrado que o melhor caminho para ter uma vida melhor é o estudo, e por todo apoio nesses anos de curso. Agradeço minha noiva que sempre me deu forças nos momentos difíceis que encontrei ao longo do curso.
Agradeço ao meu orientador Joaquim Quinteiro Uchoa, que com certeza me motivou no curso nas disciplinas que ministrou, e por aceitar e ajudar no desenvolvimento do trabalho. E agradeço também aos outros professores que conheci e fui aluno ao longo do curso, todos foram responsáveis pela minha formação profissional e pessoal.

Se se espera que uma máquina seja infalível, ela também não pode ser inteligente.
(Alan Turing)

RESUMO

O uso da tecnologia se torna cada vez mais frequente no nosso cotidiano, principalmente nos últimos dois anos, quando nos vimos em uma pandemia global causada pelo coronavírus. Como forma de não parar suas atividades, muitas organizações optaram pelo trabalho remoto, aumentando assim o consumo de tecnologias da informação. Porém isso também trouxe um crescimento de uma ameaça que pode ser bem prejudicial, os ataques de Ransomwares. Ataques de Ransomware são aqueles ataques em que a vítima tem os dados de sua máquina criptografados ou o acesso a máquina bloqueado e é pedido um valor de resgate para ter seus dados ou a máquina de volta. Desde sua origem até os dias de hoje, os Ransomwares vem evoluindo e ganhando muito espaço nos ataques cibernéticos nos últimos anos.

Palavras-chave: Ransomware. Tecnologia da informação. Pandemia. Criptografada. Resgate. Ataques cibernéticos.

ABSTRACT

The use of technology becomes more and more frequent in our daily lives, especially in the last two years, when we found ourselves in a global pandemic caused by the coronavirus. As a way of not stopping their activities, many organizations have opted for remote work, thus increasing the consumption of information technologies. However, this also brought the growth of a threat that can be very harmful, the Ransomware attacks. Ransomware attacks are those attacks where the victim has their machine data encrypted or access to the machine blocked and they are asked for a ransom amount to get their data or the machine back. From its origins to the present day, Ransomware has been evolving and gaining a lot of space in cyber attacks in recent years.

Keywords: Ransomware. Information Technology. Pandemic. Encrypted. Rescue. Cyber attacks.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Nos últimos dois anos, a sociedade foi obrigada a se deparar com a pandemia global causada pelo coronavírus, algo que só tinha acontecido há aproximadamente um século atrás, com a gripe espanhola. Muitas pessoas e principalmente organizações começaram a pensar em formas alternativas de manter a rotina de trabalho mesmo durante a pandemia, para não precisarem interromper seus serviços. Como uma das recomendações no pico da pandemia era o distanciamento social, muitas organizações optaram por mudar seu regime de trabalho para remoto. Isso levou a um aumento do uso de serviços como uso de VPNs[1], ambientes virtuais, videochamadas, entre outras.

Um estudo feito pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), mostra que em 2020, 72% dos brasileiros usuários de internet utilizaram serviços públicos ou buscaram informações online sobre direitos do trabalhador. Também mostra que 20% utlizaram serviços de Telemedicina para realizar consultas sem precisarem ir até os consultórios. Com isso houve também um aumento de várias ameaças e ataques cibernéticos. Entre as ameaças mais destacadas, encontram-se os ataques de ransomwares. Ransomwares são um tipo de malware onde a máquina da vítima tem seus dados criptografados ou bloqueados. Na maior parte das vezes, a vítima tem de pagar uma quantia, geralmente em criptomoedas, para reaver seus dados.

Segundo o Relatório de Ameaças Cibernéticas da Sonicwall (SonicWall Capture Labs Threat, 2022), em 2021, o número de ataques de ransomware no mundo chegou a 623,3 milhões, sendo esse número cerca de 105% maior em relação ao ano anterior, como mostra a Figura 1.1. Esse relatório também mostra o crescimento desses ataques no Brasil, que ficou em 4º lugar com mais de 33 milhões de ataques. No ano de 2020 o país estava em nono lugar, com cerca de 3,8 milhões de ataques. Na Figura 1.2 e na Figura 1.3, são apresentados os 10 países que mais sofreram ataques de ransomware nos anos de 2020 e 2021.

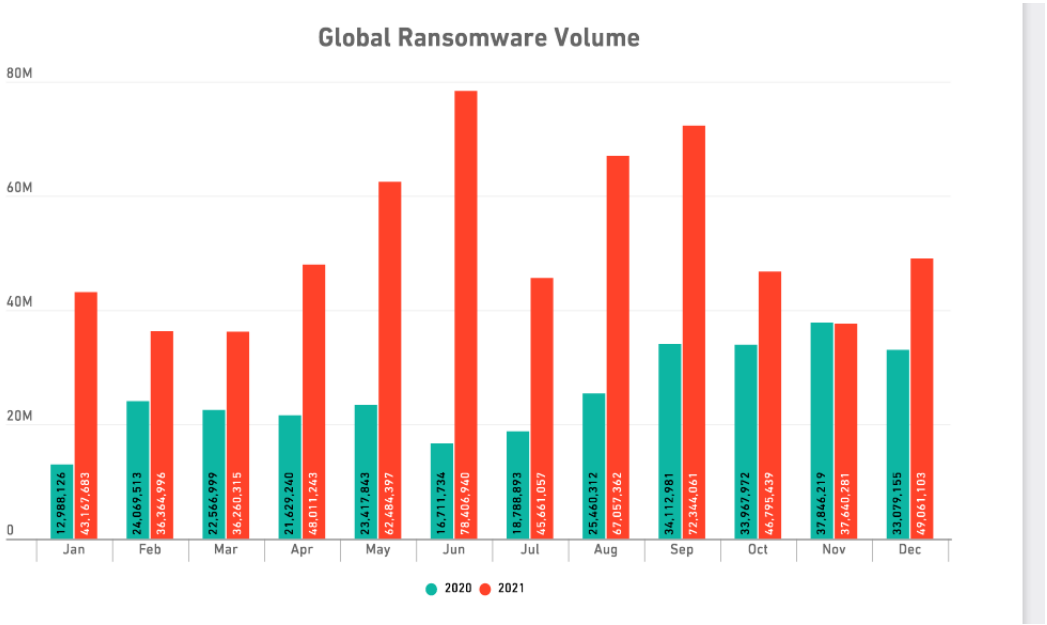
O valor médio de resgate também teve aumento significativo nesse período. Segundo a pesquisa anual da empresa Sophos, o State of Ransomware de 2022 (Sophos,2022), o valor chega a ser 5 vezes maior que no ano anterior, chegando na marca de US $ 800 mil. Ainda de acordo com o mesmo relatório, em 11% das empresas participantes, o pagamento chegou a ser

[1] VPN: Virtual Private Network é uma conexão a uma rede local feita a partir da rede pública utilizando tecnologias de tunelamento, geralmente usando criptografia.

igual ou maior a US $1 milhão. Em 46% das empresas que tiveram seus dados encriptados a quantia pedida foi paga. Algumas empresas tinham outras formas de recuperar seus dados.

Os principais alvos geralmente são organizações governamentais, empresas de seguros, hospitais, empresas e instituições que armazenam uma grande quantidade de informações, geralmente dados sensíveis como nome dos clientes, documentos, endereço, entre outros.

Figura 1.1 – Comparação dos ataques nos anos de 2020 e 2021



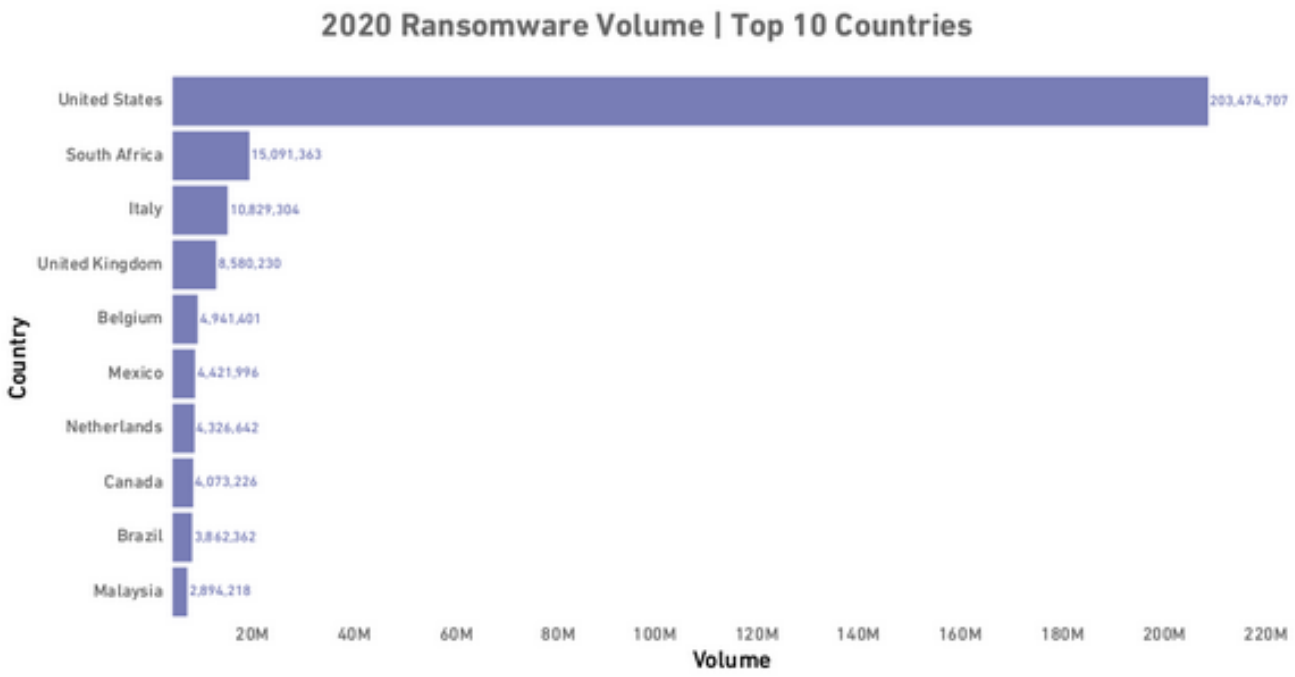
Fonte: SonicWall Cyber Threat Report 2022

O objetivo deste trabalho é entender como esse tipo de malware funciona e também quais as tecnologias, linguagens e métodos são usados para esse tipo de ataque cibernético que não foram encontrada no artigo “Ransomware: Evolution, Mitigation and Prevention”, além de trazer informações mais atuais sobre os ataques de ransomwares.

A metodologia usada para o desenvolvimento do trabalho foi a de pesquisa bibliográfica, utilizando o Google para se fazer as pesquisas com termos chaves como "ataques de ransomware", "ataques de ransomware em 2021", "o que é um ransomware", "principais tecnologias usadas para ransomwares", "principais linguagens usadas para desenvolver ransomwares", sempre tendo como uma das palavras chaves o termo "ransomware", sempre buscando informações mais novas e checando se as fontes são confiáveis.

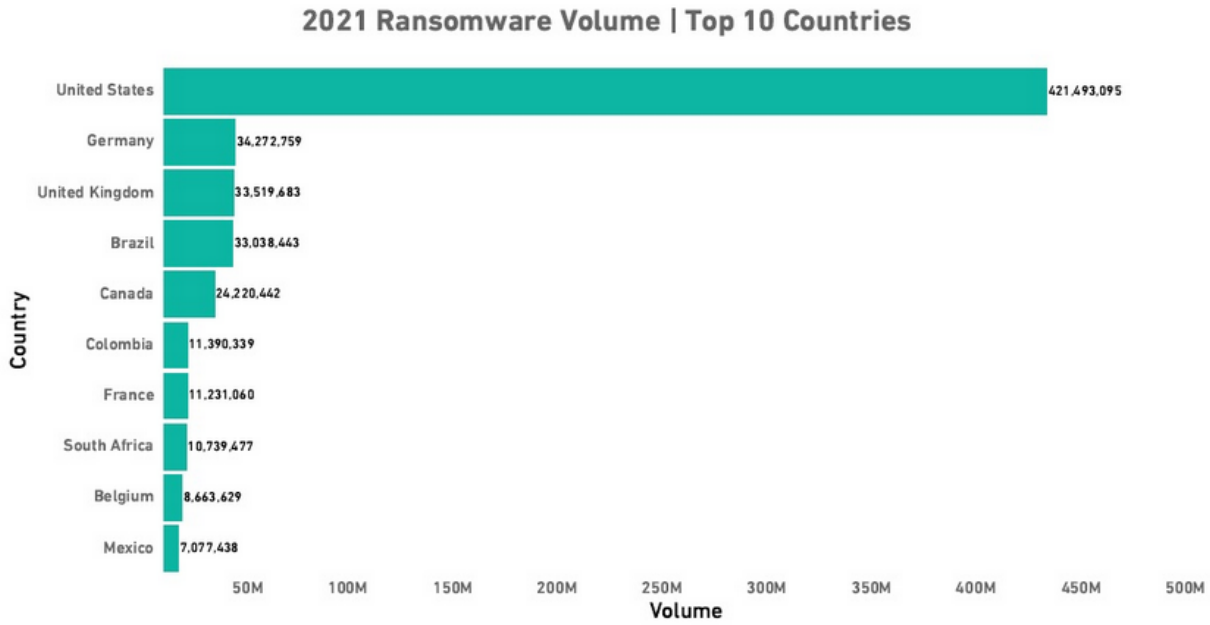
A motivação inicial deste trabalho foi o artigo “Ransomware: Evolution, Mitigation and Prevention ” (Richardson, North, 2017), um artigo que mostra a história do ransomware e sua evolução conforme a tecnologia foi evoluindo, e mostra também alguns ataques e o tipo de ransomware utilizado. O artigo, entretanto, não mostra casos e tecnologias mais atuais que são

Figura 1.2 – 10 países que mais sofreram ataques em 2020



Fonte: SonicWall Cyber Threat Report 2021

Figura 1.3 – 10 países que mais sofreram ataques em 2021



Fonte: SonicWall Cyber Threat Report 2022

utilizadas, pois é um artigo de 2017, então foi proposto fazer o trabalho com base nesse artigo e completar com informações que não foram encontradas no artigo e que são releventes para o assunto.

As principais fontes utilizadas foram os relatórios da Sonicwall 2020 e 2021 (SonicLab), que é uma empresa de cibersegurança muito conceituada que oferece soluções em cibersegurança e anualmente solta o relatório com as principais ameaças identificadas no ano. Também o relatório da Sophos de 2021, que assim como a Sonicwall, também é uma empresa de soluções em cibersegurança e lançam o relatório também anualmente com as ameaças identificadas no ano. E ainda da Sophos o whitepaper “The State of Ransomware 2022”. E como falado anteriormente, o Google para informações específicas sobre os ransomwares e sobre casos de ataques de ransomwares.

2 RANSOMWARE

Ransomware é um tipo de malware que criptografa os dados ou bloqueia a máquina da vítima, impedindo-a de tentar salvar alguma informação durante o ataque. O acesso ao sistema ou aos dados só são liberados mediante um pagamento de uma quantia, geralmente em criptomoedas, para dificultar ou impedir o rastreamento do criminoso. Entretanto, mesmo com o pagamento, o usuário afetado não tem certeza se realmente terá os dados ou o acesso ao sistema de volta.

Pode-se classificar o Ransomware em dois tipos: os Crypto Ransomwares, que são os mais comuns usados em ataques, são aqueles que criptografam os dados e arquivos da máquina(Figura 2.1). O segundo tipo são os Locker Ransomware, que bloqueiam geralmente as funções básicas da máquina ou o dispositivo, como por exemplo o mouse, acesso a área de trabalho e também parte do teclado, deixando a pessoa interagindo apenas com a tela de resgate (Figura 2.2). Esse tipo de ransomware geralmente somente bloqueia, geralmente os dados e arquivos não são alterados, muito utilizado para ataques em dispositivos IoTs, onde não se tem dados para serem criptografados.

Figura 2.1 – Imagem da tela de resgate de um Cripto Ransomware

Fonte: F-Secure Weblog

Em nenhum dos dois tipos se tem a certeza que, após o pagamento, a vítima receberá a chave para poder recuperar seus dados de volta. Em alguns casos é pedido até um segundo pagamento, com quantias maiores que a pedida anteriormente. Também não se sabe se o criminoso pode ter obtido alguma cópia dos dados que possa depois ser vendida ou exposta.

Os ataques acontecem, geralmente, por meio de técnicas para fazer a coleta de informações, como phishing, que é uma técnica que cria cópias de sites de uso do alvo ou email falsos que permitem a instalação ou o download do ransomware na máquina alvo. Podem, também, ser exploradas vulnerabilidades na rede, como redes wifi abertas, dispositivos bluetooth ou ou-

Figura 2.2 – Imagem da tela de resgate de um Locker Ransomware

Fonte: KnowBe4

tros conectados na rede da empresa e também sistemas desatualizados. Uma prática também usada é a engenharia social, em que o criminoso faz contato com colaboradores da empresa se passando por algum funcionário de sistema ou algum serviço que a organização utiliza para extrair informações sobre a empresa e suas vulnerabilidades, usando essas informações para montar o ataque.

2.1 Ransomware como serviço

Inicialmente os ataques de ransomwares eram individuais, os criminosos personalizam ou desenvolvem seus próprios ransomwares e realizam os ataques por conta própria. Porém com o recente aumento dos ataques e como muitos alvos preferiam pagar o resgate, começou a surgir um novo tipo de mentalidade: o Ransomware como serviço.

Ransomware como serviço é um modelo em que os ataques não são mais feito de maneira individual, mas sim por organizações criminosas, em que elas desenvolvem o ransomware e os comercializam como um produto, alugando o software por uma parte do resgate que será pedido pelos criminosos.

Segundo o Sophos 2022 Threats Report (SophosLab, 2022), esse tipo de ataque vai continuar a dominar o cenário de ameaças por ataques de ransomware, visto que esse modelo é vantajoso para que os especialistas na criação dos ransomwares melhorem seus produtos, e os especialistas em atacar os clientes, possam somente se concentrar exclusivamente em sua tarefa.

3 EVOLUÇÃO DO RANSOMWARE

O Ransomware, apesar de estar em evidência nos últimos anos, é um malware que já é conhecido a muito tempo. O artigo “Ransomware: Evolution, Mitigation and Prevention ” (Rchardson, North, 2017) faz uma linha do tempo da evolução do Ransomware, porém pelo artigo ser de 2017, falta algumas informações mais atuais que foram colocadas também nessa sessão, para complementar as informações presente no artigo.

Em 1989, Joseph L. Poop, um biólogo de Harvard, foi responsável pelo primeiro ransomware, com o nome de AIDS Trojan. Ficou assim conhecido pelo grande interesse em informações sobre a AIDS na época. Ele distribuiu disquetes para os assinantes da conferência Internacional sobre AIDS da Organização Mundial da Saúde juntamente com as instruções necessárias para instalar o programa com o nome de AIDS (AIDS Info Disk), que na verdade era um cavalo de Tróia, tendo o contrato de licença que dizia que o usuário concordava em pagar US $378 dólares. Porém quando o sistema atingia a nonagésima inicialização ele ativava o Trojan, criptografando os arquivos da máquina da vítima e pedindo um valor de US $189 dólares. Como era usado a criptografia simétrica, uma criptografia simples, logo conseguiram quebrar e descriptografar o arquivo.

Em maio de 2005 apareceu o primeiro ransomware moderno, conhecido como Trojan GPcoder. Ele usava uma técnica de criptografia simétrica personalizada, mas era fraca e fácil de quebrar. Era espalhado via spam enviado por um email com um anexo dizendo ser um pedido de emprego. Sua maior parte foi desenvolvida por criminosos russos e destinada a ataques a vítimas de países vizinhos como Bielorrússia, Ucrânia e Cazaquistão.

Em março de 2006 apareceu o Trojan.Cryzip, que copiava arquivos para arquivos protegidos com senhas e apagava o arquivo original. O problema era que o código incluía a senha, ficando assim fácil de recuperar. Nesse mesmo ano apareceu também o Trojan.Archievus, que funcionava semelhante ao Cryzip, porém no lugar do resgate, ele exigia que as vítimas comprassem medicamentos de algumas farmácias onlines específicas e enviassem o identificador do pedido para liberar a senha.

Em 2007, começou a aparecer um novo tipo de ransomware, o Locker ransomware, que bloqueava a máquina, muitas vezes mostrando uma imagem imprópria, exigindo um pagamento para retirar. O pagamento era feito por SMS ou por ligação para um telefone de taxa premiada, onde a pessoa liga ou manda uma mensagem para um número passado pelo criminoso, geralmente descartável, onde ele passa as instruções para o pagamento.

Em 2008 apareceu uma variação do GPCoder chamada GPCoder AK, usando uma chave RSA de 1024 bit, deixando um arquivo com instruções em cada subdiretório que encriptava os arquivos e exigia pagamento de US $100,00 a US $200,00 em e-gold ou Liberty Reserve, que era um sistema online de pagamentos que baseava suas moedas no preço do ouro.

Em 2011 houve um aumento de ataques ransomwares, principalmente devido a maior visibilidade de meios de pagamentos anônimos como criptomoedas, cartões pré-pagos,entre outros, que tem uma complexidade de rastreio maior do que as formas de pagamentos comuns. Nesse ano foram identificadas mais de 100.000 amostras de ransomwares pelos pesquisadores de cibersegurança.

Em 2012 foi lançado um kit de ferramentas chamado de Citadel, feito para produzir e distribuir ransomwares. Ele tinha um custo de cerca de US$3.000,00. No mesmo ano, também foi lançado o Lyposit, que foi produzido para desenvolver ransomwares que se passavam por mesagens de órgão que tem ligação com a lei de acordo com a região configurada na máquina. Um exemplo é o Reveton, que mostrava uma mensagem que aquela máquina fazia parte de atividades ilegais.

Em 2013, o hacker conhecido como Slavik, lançou o que seria talvez um dos mais famosos ransomware, o CryptoLocker. Ele usava chaves públicas e privadas para encriptar e descriptografar os arquivos das vítimas, sendo originalmente distribuído por um botnet de Trojan bancário. Esse botnet era chamado Gameover Zeus, e a principal forma de ser distribuído era por email que pareciam vir de UPS ou Fedex. Sua versão original consegue encriptar mais de 67 tipos de arquivos, inclusive todos do pacote Office da Microsoft.

Em 2016, foi descoberto o JavaScript-only, um ransomware baseado em JavaScript, que foi usado para infectar vários sistemas como MacOS e Linux. Em fevereiro do mesmo ano, ele infectou milhares de sites WordPress.

Em 2017, pode se dizer que o ransomware ficou mais conhecido, visto que se teve um dos ataques que causou prejuízos em várias organizações em diversos países e talvez o mais conhecido, o WannaCry[1]. Foi detectado primeiro em fevereiro de 2017, que se propagava por meio de SPAMS ou outras máquinas infectadas que estivessem na mesma rede. O WannaCry utilizou a vulnerabilidade EternalBlue/MS17-010, que se refere a um protocolo de Server Message Block, permitindo a execução de um programa remoto ou criar uma backdoor para um futuro ataque. Dentre as organizações afetadas estavam o Serviço Nacional de Saúde do Reino

[1] Informação retirada de:https://olhardigital.com.br/especial/wannacry/ e https://pt.wikipedia.org/wiki/WannaCry

Unido, uma fábrica da Nissan na França, a Portugal Telecom e a empresa de energia também de Portugal. No Brasil tivemos ataques ao Tribunal de Justiça de São Paulo, a Vivo, o Hospital Sírio-Libanês, NEXTEL, NET, entre outras. Segundo a Kaspersky, estima-se que afetou cerca de 230 mil computadores no mundo, causando perdas que somam cerca de US $4 bilhões.

Em 2018, apareceu o Ryuk[2], que foi noticiado pela primeira vez quando uma editora americana de jornais, a Tribune Publishing, e também o New York Times, disseram ter sido infectadas por esse ransomware, visto que as duas editoras compartilhavam a mesma gráfica em Los Angeles. O Ryuk é um ransomware que precisa que seja baixado primeiro um outro malware, que pode ser por meio de spams ou phishing, que quando acessados baixam ferramentas que instalam esse malware. Depois que foi feito o download, esse mesmo malware baixa o Ryuk e o instala. Estima-se que até o início de 2021, esse ransomware causou um prejuízo de US $150 milhões segundo a Top Business Tech.

Nos últimos anos também se teve um crescimento considerável de ataques de ransomwares em dispositivos IoTs, visto que esses dispositivos muitas vezes não suportam atualizações ou regras muito pesadas de segurança. Esse tipo de ataque se classifica mais como do tipo Locker Ransomware, pois somente bloqueia o dispositivo, tirando o controle do usuário daquele dispositivo. É utilizado geralmente um vírus chamado de "Jackware"[3], que tenta assumir o controle de qualquer dispositivo conectado. Isso se torna extremamente perigoso, visto que o criminoso pode assumir o controle não só de um dispositivo, mas de uma casa toda, já que está cada vez mais comum o conceito de "casa inteligente". Pensando também que com o avanço da tecnologia para carros autônomos, eles podem conseguir tomar o controle desses carros, podendo ameaçar inclusive a vida de motoristas e passageiros.

O primeiro ataque de um Jackware foi em 2010, quando se interrompeu o programa de armas nucleares do Irã, destruindo várias centrífugas. Em 2015 Charlie Miller e Chris Valasek, conseguiram hackear um Jeep Cherokee em movimento na rodovia, para mostrar a falha de segurança do modelo. Os dois são hackers éticos, e a experiência mostrou que basicamente quem conseguisse encontrar o IP do veículo conseguia acessar desde limpadores de parabrisa, ar condicionado, como funções mais importantes como funcionamento dos freios, desligar o motor, câmbio, entre outras.

---

[2] Informação retirada de:https://pt.tbtech.co/blockchain/security- and-data/ryuk-ransomware-evolution-requires-strategies-to-outpace-attackers/

[3] Informação retirada de: https://www.cisoadvisor.com.br/jackware-e-dez-vezes-mais-perigoso-que-o-ransomware/

4 ATAQUES NOS ÚLTIMOS ANOS

Como vimos, tivemos muitos ataques de ransomwares nesses últimos anos, e muitos deles acabam ganhando destaque na mídia e noticiários por razões como valores ou instituições afetadas. Como são muitos ataques e a grande maioria não é noticiada com detalhes por opção da própria organização afetada para não prejudicá-la e terceiros, ou por não se ter conhecimento, a seguir serão listados alguns ataques que ocorreram nesse período de pouco mais de dois anos.

Em janeiro de 2020, um ataque à empresa Travelex, uma empresa de câmbio, fez com que a empresa desligasse todos os sistemas e sites em 30 países. O ataque foi feito pelo grupo Sodinokibi (conhecidos também por REvil) alegando ter entrado na rede da empresa antes e extraido dados durante 6 meses. Foram pagos $2,3 milhões em Bitcoin e o sistema foi recuperado.

Em março de 2020, a Communication Power Industries, uma fabricante de eletrônicos e também equipamentos militares, sofreu um ataque após o administrador do domínio da empresa clicar em um link malicioso e afetou inclusive os backups da empresa. Por causa dessa ação, foi pago meio milhão de dólares para recuperar o sistema.

Em maio de 2020, o escritório de advocacia Grubman Shire Meiselas Sacks, que tem sede em Nova York e cuida de celebridades como Madonna, Lady Gaga, Bruce Springsteen entre outros, foi afetada por um ataque de ransomware. Os criminosos ameaçaram divulgar os dados se não fossem pagos $21 milhões de dólares, e quando a firma se recusou a pagar eles dobraram o valor do resgate. A firma chamou o FBI para investigar o caso.

No mês de março de 2021, a seguradora CNA Financials, uma das maiores seguradoras dos EUA, sofreu um ataque de ransomware do grupo Evil Corp, que atingiu e interrompeu as redes, chegando a deixar a empresa quase sem operações durante 6 semanas. Foi pago um resgate de $40 milhões de dólares.

A Colonial Pipeline Company sofreu um ataque em maio de 2021, que interrompeu o abastecimento de combustível para grande parte do sudeste dos EUA, que poderia se estender até o norte de Nova York. Como eles não tinham políticas de seguranças muitos rígidas, os criminosos entraram facilmente pelas VPNs da empresa. A empresa pagou um resgate de $4,4 milhões de dólares.

Também em maio de 2021 ocorreu um ataque a empresa JBS, uma das maiores fornecedoras de carne do mundo. O ataque foi na divisão norte-americana, a JBS USA, que foi causado pelo grupo REvil. As pessoas logo esgotaram os produtos da empresa das prateleiras devido ao

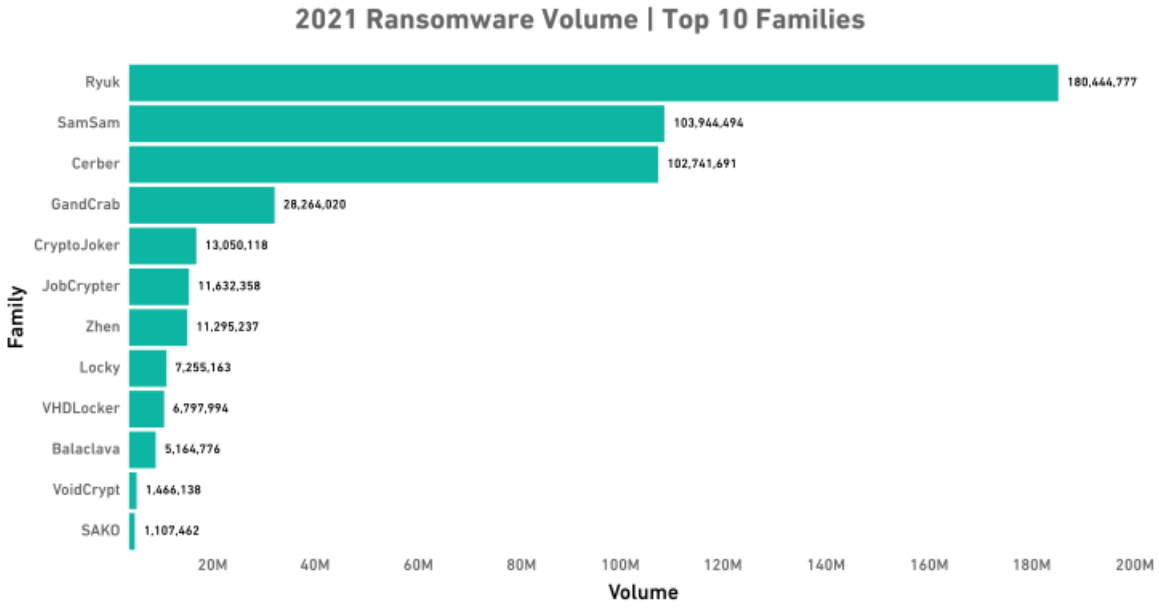
ataque ter atingido a cadeia de abastecimento da empresa. Foram pagos $11 milhões de dólares para evitar vazamento de dados da empresa, clientes e colaboradores.

No Brasil, em 2021, também tivemos muitos ataques durante o ano, geralmente focados em e-commerce, como os ataques as lojas Renner, que indisponibilizaram todo o site da loja em todo o país. O ataque foi feito pelo grupo RansomExx. Em novembro de 2020 houve um ataque do mesmo grupo, mas desta vez, o alvo foi o STJ, criptografando quase mil máquinas virtuais. O ataque visava também os backups em disco local, uma vez que com os backups criptografados a vítima não teria escolha a não ser pagar o resgate. Em dezembro de 2021, um ataque de ransomware sofrido pela PF e PRF apagou dados de várias informações dos agentes de segurança que tinham dívidas ativas e também condutores que tinham seus dados nas plataformas desses órgãos.

5 CRESCIMENTO DAS ASSINATURAS DE RANSOMWARE

No ano de 2021, os pesquisadores do SonicWall Capture Labs Threat, encontraram cerca de 1000 ransomwares diferentes nos ataques, mostrando o quanto é difícil montar uma ferramenta para prevenção, pois são escritos em linguagens diferentes, possuem códigos diferentes, entre outras diferenças. Além disso, foram identificadas também mais de 300 famílias de ransomwares nesses ataques, sendo que as principais são Ryuk, SamSam e Cerber, que foram responsáveis por 62% dos ataques do mesmo ano, como mostra a figura 5.1.

Figura 5.1 – 10 maiores famílias nos ataques de 2021

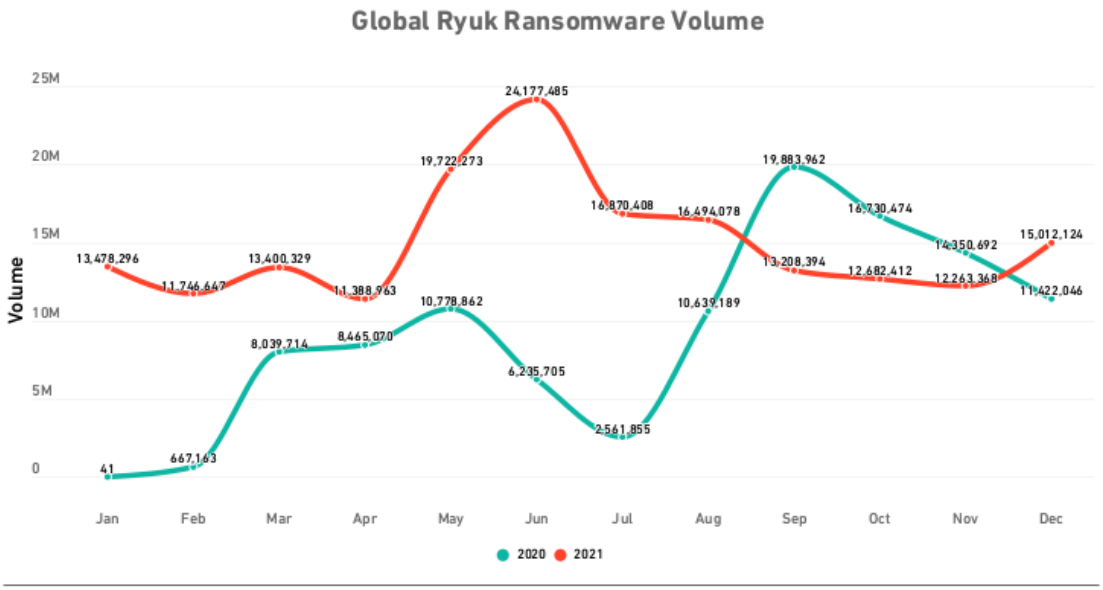


Fonte: SonicWall Cyber Threat Report 2022

Em 2021, foi identificado 180,4 milhões de acessos de ransomwares da família Ryuk, um crescimento em relação ao ano anterior de 64% e também representa 30% de todos as tentativas de ataques, mas também representa uma redução, já que no ano anterior era de 36%. O pico desse aumento foi no mês de junho de 2021, com 24,2 milhões de acessos, aproximadamente 9,32 acessos por segundos. Ele se espalha principalmente por phishing e spearphishing, que é um ataque de phising focado em uma empresa ou em alguma pessoa em específico, mas também pode se espalhar pela rede por credenciais já comprometidas ou por malware já ativo no sistema, como por exemplo o Trickbot ou o Emotet.

Porém, ele não conseguia se espalhar por redes sozinho. Entretanto, no início de 2021, foi descoberto pela ANSSI da França, uma variante que conseguia se espalhar sozinho pela rede por uma conta de domínio com privilégios e desabilitar a conta ou alterar a senha não adianta.

Figura 5.2 – Números de acessos do Ryuk em 2020 e 2021



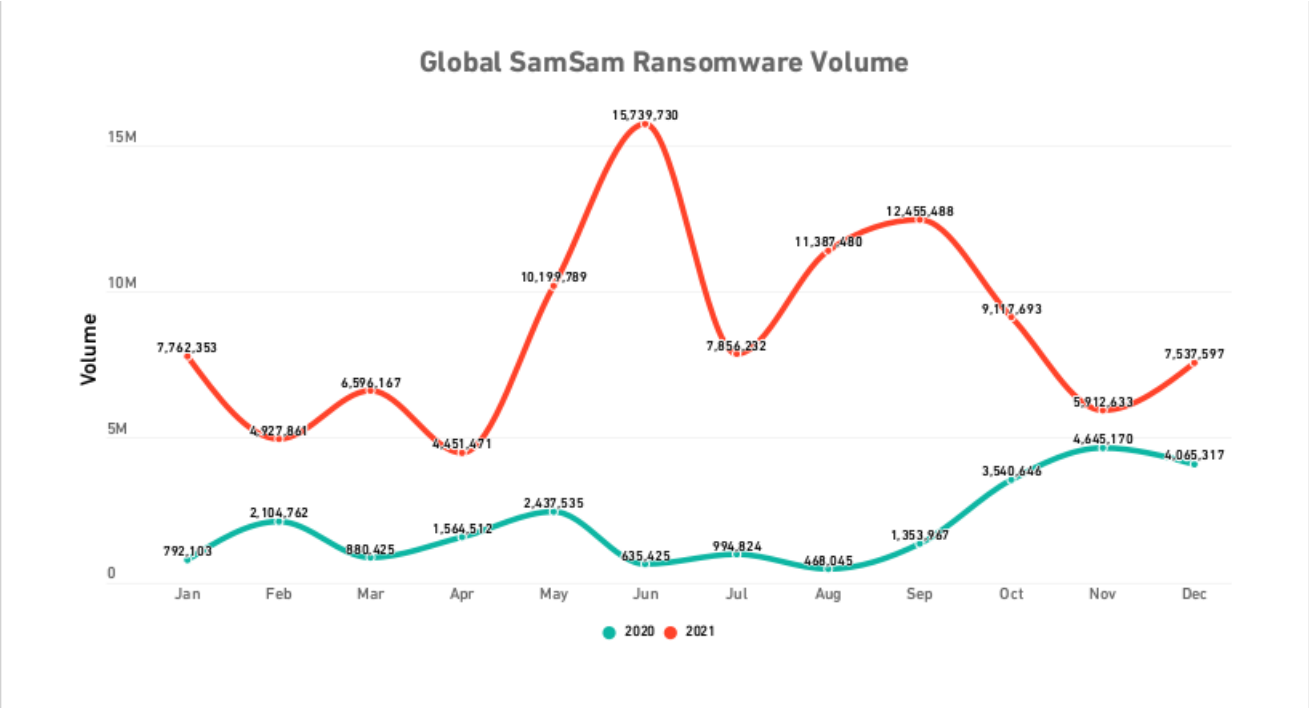
Fonte: SonicWall Cyber Threat Report 2022

SamSam teve um grande crescimento no ano de 2021, saltando de 23,5 milhões em 2020 para 104 milhões de acessos no ano de 2021, representando 16,7% de todos os acessos de ransomwares no ano de 2021. Em nenhum mês de 2021 de acessos de SamSam foi menor que o de 2020, tendo seu pico no mês de junho, com 15,7 milhões de tentativas. Diferente do Ryuk, que é um Ransomware As A Service (RaaS), o SamSam não é vendido no mercado negro, mas sim desenvolvido e atualizado de forma privada. O grupo por trás do SamSam é conhecido por buscar menções sobre seus ataques na internet, quando é relatado um ataque, eles lançam uma nova versão, ajudando a garantir o sucesso do SamSam por 7 anos.

O Cerber liderava o ranking dos ataques até a chegada do Ryuk. Em 2019 ele representava 33% dos acessos, que caiu para aproximadamente 13% em 2020. Em 2021 ele teve um crescimento de 158% em relação a 2020, representando 16,5% de todos os ataques de 2021. Foi desenvolvido em março de 2016 e foi um dos primeiros modelos de RaaS. Geralmente se espalha por kits de exploits, spams infectados, sites infectados, downloads de softwares falsos e propagandas maliciosas.

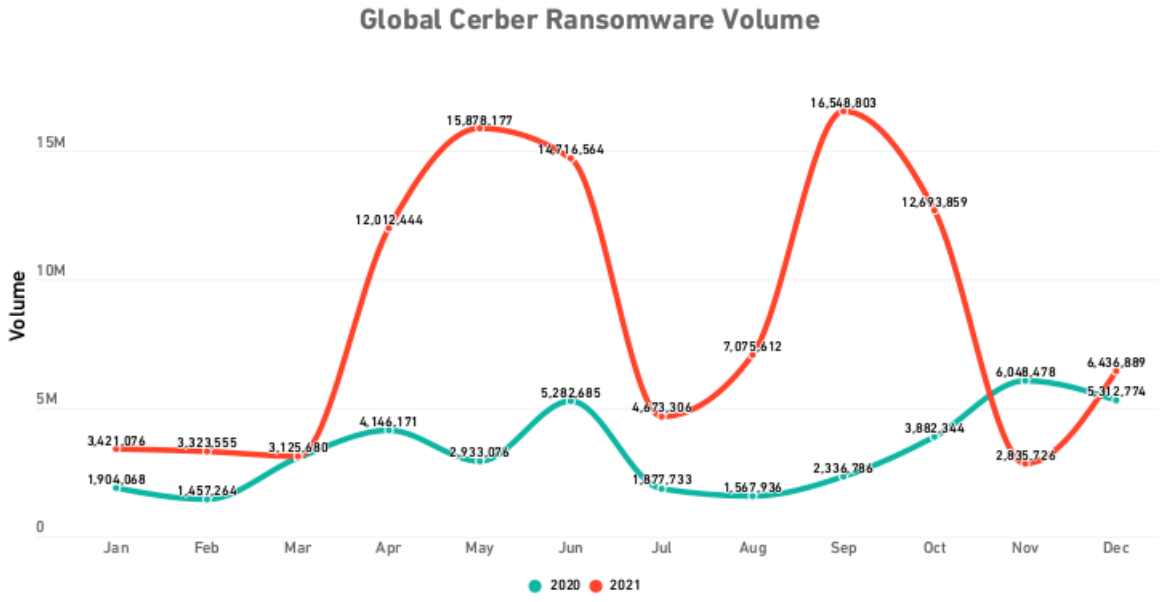
Em fevereiro de 2021, o Departamento de Justiça dos Estados Unidos, indiciou 3 atacantes norte coreanos por ajudar a espalhar o WannaCry, que foi um ransomware propagado pelo exploit EternalBlue, roubado pelo grupo The Shadow Brokers da Agência de Segurança Nacional dos Estados Unidos, conseguindo mais de US$ 1,3 bilhões em dinheiro e criptomoedas. Em 2020, foi identificado pela SonicWall, 233.000 acessos do WannaCry, e em 2021 100.000.

Figura 5.3 – Números de acessos do SamSam em 2020 e 2021



Fonte: SonicWall Cyber Threat Report 2022

Figura 5.4 – Números de acessos do Cerber em 2020 e 2021



Fonte: SonicWall Cyber Threat Report 2022

6 LINGUAGENS E TECNOLOGIAS MAIS USADAS

Cada vez mais, os cibercriminosos utilizam linguagens poucos usadas ou exóticas para desenvolver seus ransomwares para tentarem passar despercebidos por ferramentas de segurança, ocultar sua entrada no sistema, e outros fatores que podem ajudar a identificar o ataque. Geralmente os cibercriminosos utilizam as linguagens Go, Rus, DLang, Nim, para desenvolverem droppers, um programa utilizado para instalar ransomwares e outros malwares mais antigos, que estão embrulhados nesses programas. Há uma certa preferência pela linguagem Go, pois ela é compilada para todos os principais sistemas operacionais, sendo assim uma arma poderosa para infiltrar em qualquer sistema, e também por sua confiabilidade, por ser fácil de usar e pela eficiência.

Um grupo de cibercriminosos chamados “Hive”, recentemente estão focando os seus ransomwares na linguagem Rust, por ser mais eficaz para sistemas Linux, para ampliar seus o alcance para servidores, principalmente virtualizados por ferramentas como VMware. O Cetir gov (Centro de Prevenção, Tratamento e Resposta a Incidentes de Governo), emitiu um alerta no site governo, para um ransomware chamado Conti:"O Centro de Prevenção, Tratamento e Resposta a Incidentes de Governo (CTIR Gov) vem observando o aumento significativo de casos envolvendo o Ransomware Conti em países da América Latina. ". Os principais fatores de entrada do ransomware Conti são além das que já se são conhecidas nesse tipo de ataque, vulnerabilidades como 2017 Microsoft Windows Server Message Block 1.0 server vulnerabilities, "PrintNightmare"vulnerability (CVE-2021-34527) in Windows Print spooler service e "Zerologon"vulnerability (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems para escalar privilégios.

No final de 2021, uma lista de vulnerabilidades, que começou a ser montada por Allan Liska, membro da CSIRT (equipe de resposta a incidentes de segurança em computadores) da Recorded Future e diversos outros colaboradores, serviu de um ponto inicial para diversas organizações reverem suas infraestruturas de redes e checar se possui alguma das vulnerabilidades listadas. A figura 6.1 mostra essa lista de vulnerabilidades e seus sistemas.

O esforço de Liska e seus colaboradores fez com que outras entidades também montassem uma linha de defesa contra ataques de ransomware. Em setembro de 2021 a ISA se juntou à Microsoft, Google Cloud, Amazon Web Services, ATT, Crowdstrike, FireEye Mandiant, Lumen, Palo Alto Networks e Verizon para formar uma parceria colaborativa de defesa cibernética com foco em defesa de infraestrutura crítica de ransomware ou outras ameaças cibernéticas.

Figura 6.1 – Diagrama de vulnerabilidades usadas em ataques de ransomwares

Fonte: Seginfo

7 FORMAS DE PREVENÇÃO

Como vimos, os ransomwares são uma ameaça para as organizações e os danos causados são graves, tanto financeiramente como materialmente, pois muitas vezes coloca em risco os dados de seus clientes. Para se prevenir desse tipo de ameaça, pode se manter backups, em nuvem ou cópias físicas, em caso de cópias físicas, devem ficar armazenadas em uma máquina diferente do servidor, para não correr risco de serem perdidas também em um ataque e poderem ser restauradas sem causar nenhum dano no sistema ou dados criptografados.

É preciso também fazer um treinamento dos funcionários sobre conscientização dos riscos de crescentes ameaças cibernéticas, como o ransomware, mostrando aos funcionários como esse tipo de ameaça é crescente e os danos que pode causar para a organização. Com mostrando maneiras de se evitar esse tipo de ameaça, diminuem as chances da organização ser infectada por esse tipo de ameaça.

Deve-se manter antivírus atualizados, pois cada vez que um tipo de vírus como malwares e ransomwares são detectados e se conhece as formas de utilizá-lo, normalmente eles são atualizados com essas informações. Portanto os antivírus sempre estarão atualizados para evitar os vírus conhecidos por mais recentes que sejam.

Pode-se também implantar ou atualizar de políticas de seguranças como proxies de rede, evitando que qualquer pessoa possa se conectar na rede ou que algum arquivo malicioso entre na rede sem ser percebido, e para evitar que qualquer usuário também instale programas que não se conheça a origem.

8 CONCLUSÃO

Como podemos ver ransomware é uma ameaça crescente e difícil de ser identificada, pois só se sabe do malware na hora em que ele já consegue se estabelecer e criptografar os dados. Pode causar não só danos financeiros nas organizações como também danos materiais, pois compromete a integridade dos dados e mesmo que se pague o resgate e consiga recuperar os dados, não se tem certeza se o cibercriminoso obteve alguma cópia deles.

Neste trabalho foi feito uma pesquisa bibliográfica de artigos e informações mais recentes sobre ransomware, partindo do artigo “Ransomware: Evolution, Mitigation and Prevention” (Rchardson, North, 2017), que foi publicado em 2017. Nos preocupamos em falar da evolução dos ataques de ransomware desde sua criação, colocar as tecnologias usadas recentemente e também colocar os principais ataques de ransomware nos últimos anos. Além disso também foram apresentadas algumas formas de prevenção desse tipo de ataque.

Como trabalhos futuros pode ser feito um levantamento maior das tecnologias e linguagens utilizadas, visto que não foi encontrado muitas informações sobre a linguagem em que os principais ransomwares são escritos, também não se tem muitas informações sobre os ataques que foram cometidos aqui no Brasil, como valores ou até mesmo o ataque em si, pois muitas organizações não divulgam para não comprometer sua integridade.

REFERÊNCIAS

SONICWALL CAPTURE THREATS LABS, Sonicwall Threat Report 2022. Sonicwall. 1. ed. California, 2022.

SOPHOS LABS; SOPHOS MANAGED THREAT RESPONSE; SOPHOS RAPID RESPONSE; SOPHOSAI. Sophos 2022 threat report. Sophos. 1. ed. Abingdon, 2021.

SOPHOS LABS. The State of Ransomware 2022. Sophos. 1. ed. Abingdon, 2022.

MCLAUGHLIN, Daniel, 'Golden era' for cyber attacks as criminals take advantage of pandemic, 15 jan. 2022. Disponível em: https://www.irishtimes.com/life-and-style/golden-era-for-cyber-attacks-as-criminals-take-advantage-of-pandemic-1.4775522. Acessado em: 04 jul. 2022.

BLANCAS, Juan, Ataques cibernéticos ransomware em hospitais, 04 jan. 2022. Disponível em: https://emaster.cloud/Blog/ataques-ciberneticos-ransomware-em-hospitais. Acessado em: 04 jul. 2022.

RICHARDSON, Ronny and North, Max M., "Ransomware: Evolution, Mitigation and Prevention". 2017. Faculty Publications. 4276. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276. Acessado em: 04 jul. 2022.

DA REDAÇÃO, Ransomware: 105% mais ataques em 2021, diz a SonicWall, 14 mar. 2022. Disponível em: https://www.cisoadvisor.com.br/ransomware-105-mais-ataques-em-2021-diz-a-sonicwall/. Acessado em: 04 jul. 2022.

DIGITAL, Convergência, Ataques ransomware: Empresas pagam, em média, R$ 4 milhões de resgate, 29 abr. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Ataques-ransomware%3A-Empresas-pagam%2C-em-media%2C-R%24-4-milhoes-de-resgate-60147.html?UserActiveTemplate=mobile. Acessado em: 04 jul. 2022.

TERRA, Ataques ransomware e a evolução dos ciberataques, 11 abr. 2019.Disponível em: https://www.terra.com.br/noticias/dino/ataques-ransomware-e-a-evolucao-dos-ciberataques, 672ed3e3c39b5914764e973a592815cdlg7s9i0q.html. Acessado em: 04 jul. 2022.

TADEU, Erivelto, Ataque ao STJ visava servidores de backup, nova tendência entre hackers, 05 fev. 2021.Disponível em: https://www.cisoadvisor.com.br/ataque-ao-stj-visou-servidores-de-backup-nova-tendencia-entre-hackers/. Acessado em: 05 jul. 2022.

GRUSTNIY, Leonid, A saga do ransomware, 9 abr. 2021. Disponível em: https://www.kaspersky.com.br/blog/history-of-ransomware/17280/. Acessado em: 05 jul. 2022.

LAB, Kaspersky, Reconhecendo um ransomware – diferenças entre cavalos de Troia de criptografia, . Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-attacks-and-types. Acessado em: 05 jul. 2022.

DA REDAÇÃO, Hackers descobrem linguagens 'exóticas' para criar malware, 28 jul. 2021. Disponível em: https://www.cisoadvisor.com.br/hackers-passam-a-usar-linguagens-exoticas-para-criar-malware/. Acessado em: 05 jul. 2022.

DEMARTINI, Felipe, Ransomware muda de linguagem de programação para ampliar ataques, 28 mar. 2022. Disponível em: https://canaltech.com.br/seguranca/ransomware-muda-de-linguagem-de-programacao-para-ampliar-ataques-212612/. Acessado em: 05 jul. 2022.

CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO, Alerta 13/2022, Alerta sobre o Ransomware Conti, 28 abr. 2022. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2022/ alerta-13-2022. Acessado em: 05 jul. 2022.

PESQUISADORES compilam lista de vulnerabilidades mais usadas por gangues de ransomware, 04 out. 2022. Disponível em: https://seginfo.com.br/2021/10/04/pesquisadores-compilam-lista-de-vulnerabilidades-mais-usadas-por-gangues-de-ransomware/. Acessado em: 05 jul. 2022.

WANNACRY, 14 jul. 2022. Disponível em: https://pt.wikipedia.org/wiki/WannaCry. Acessado em: 05 jul. 2022.

DIGITAL, Redação Olhar, Entenda o ciberataque que afetou mais de 200 mil PCs em 150 países. Disponível em: https://olhardigital.com.br/especial/wannacry/. Acessado em: 05 jul. 2022.

STEVENS, Ambar Donovan, A evolução do ransomware Ryuk requer estratégias para superar os invasores, 17 nov. 2021.Disponível em: https://pt.tbtech.co/blockchain/security-and-data/ryuk-ransomware-evolution-requires-strategies-to-outpace-attackers/. Acessado em: 05 jul. 2022.

REDAÇÃO, Hackers "brincam"com falha de segurança e controlam Cherokee à distância, 22 jul. 2015. Disponível em: https://motor1.uol.com.br/news/124472/hackers-brincam-com-falha-de-seguranca-e-controlam-cherokee-a-distancia/. Acessado em: 05 jul. 2022.

Do R7, Serviços públicos online tiveram aumento de demanda na pandemia, 02 out. 2020. Dísponivel em: https://noticias.r7.com/tecnologia-e-ciencia/servicos-publicos-online-tiveram-aumento-de-demanda-na-pandemia-29062022. Acessado em: 05 jul. 2022.