ATAQUES RANSOMWARE

MARKUS CARPEGGIANI DE LEMA[1]
Marcio Freitas[2]

1 INTRODUÇÃO

Este artigo aborda um tema atual, os ataques do tipo ransomware, que são uma preocupação mundial visto que se apresenta em franco crescimento e cada vez mais, possuem um alto grau tecnológico e que afeta a segurança dos dados e as comunicações.

Os prejuízos financeiros, a exposição de dados e a utilização de brechas de segurança nos softwares, sistemas operacionais e nas redes fazem com que diversas empresas de segurança, agentes da lei e as empresas desenvolvedoras de dispositivos e softwares estejam sempre em constante atualização e promovendo correções onde se faça necessário.

Neste trabalho, dividido em quatro partes se faz uma abordagem começando pela compreensão do que vem a ser um ataque ransomware, sua origem e evolução, seu impacto e implicações nos sistemas atingidos.

Na segunda parte se procura explicar as diferenças entre as diversas famílias de ransomwares e suas formas distintas de trabalho e concepção, pois o termo ransomware é genérico e não representa apenas um tipo de ataque criminoso.

Na terceira parte se aborda formas de defesa, e a elaboração de uma estratégia para que se possa evitar este tipo de ataque nas empresas ou mesmo indivíduos.

[1]Aluno Curso Técnico Alcides Maya
[2]Prof. Espec. Alcides Maya. marcio_freitas@alcidesmaya.edu.br

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

E na quarta parte uma rotina ou protocolo para mitigar os danos que possam ocorrer no caso de um ataque bem sucedido, onde backups e a divisão em compartimentos dos departamentos da empresa são opções que ajudam a minimizar os danos.

1.1 Tema

O tema abordado neste artigo é sobre Ataques Ransomware. Esta modalidade de ataque é uma das formas mais preocupantes de todos os ataques que ocorrem na internet, tendo ocorrido seu auge em 2020. Sua crescente sofisticação, aliada ao uso de formas automatizadas de proliferação e contágio, além da dificuldade de solução, chama a atenção para a elaboração de uma estratégia e a criação de protocolos nas empresas a fim de evitar que o mesmo aconteça, e também um guia com os procedimentos necessários caso já tenha ocorrido o dano.

1.2 Problema

Com o crescimento exponencial de sistemas online e toda a infraestrutura tecnológica globalmente conectada, além de dispositivos móveis, este tipo de ataque paralisou as operações das empresas, servidores, provedores de serviços, pessoas físicas e todos os serviços que se utilizam da comunicação e dados digitais, além de dispositivos móveis, acarretando perdas financeiras e também perdas de dados.

1.3 Justificativa

Podemos elencar várias justificativas para este estudo, tais como, o aumento significativo destes ataques, previsão de ser uma tendência ainda em crescimento em 2021, o impacto nas empresas e pessoas que dependem dos meios digitais, a evolução dos tipos de ransomware, a prevenção destes ataques e a solução para a rápida correção dos sistemas atingidos.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

1.4 Objetivos

1.4.1 Objetivo Geral

Uma análise sobre este tipo de ataque, seu impacto, formas de evitar (estratégias) e as soluções (protocolos) que podem ser empregadas.

1.4.2 Objetivos Específicos

Fornecer uma visão geral desta forma de ataque, tipos de ataques ransomware, estratégias de prevenção que podem ser empregadas, e também, soluções que podem ser adotadas de modo a permitir a elaboração de protocolos para a restauração da ordem nos sistemas afetados.

1.5 Metodologia

A metodologia a ser empregada será a de pesquisa descritiva, estudo de caso e pesquisa bibliográfica com o uso de bibliografias disponíveis na internet.

2 REFERENCIAL TEÓRICO

2.1 - Parte I - Compreendendo o Ransomware

2.1.1 O que é o Ransomware

O termo Ransomware foi criado com a junção de Ransom (resgate) + Malware (programa malicioso) sendo “um termo abrangente usado para descrever uma classe de malware que serve para extorquir digitalmente as vítimas, fazendo-as pagar um preço específico” (LISKA, ALLAN, 2019).

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

Conforme Savage, Coogan & Lau, 2015:

> Existem dois tipos básicos de ransomware em circulação. O tipo mais comum hoje é o crypto ransomware, que visa criptografar dados e arquivos pessoais. O outro, conhecido como locker ransomware, é projetado para bloquear o computador, evitando que as vítimas o utilizem.

Essa forma de extorsão tem crescido bastante e já afetou diversas empresas e indivíduos no mundo todo, tendo apresentado índices elevados de prejuízos financeiros e "nunca antes na história da humanidade as pessoas em todo o mundo foram submetidas a extorsão em uma grande escala como ocorre atualmente" (Savage, Coogan & Lau, 2015).

Os diversos tipos de ransomware podem afetar vários sistemas operacionais, incluindo o Windows, Android, Mac OS X & iOS e também o Linux, não havendo limite geográfico para esta ameaça e "é um problema global, alguns países tendem a ser mais afetados do que outros" (SAVAGE ET AL, 2015).

Em uma análise de 12 meses, ficou comprovado que existe uma prevalência para o ataque de alvos situados nos países mais ricos e populosos e a tabela a seguir enumera os 12 países mais afetados pelo ransomware (SAVAGE ET AL, 2015).

Posição	**País**
1	EUA
2	Japão
3	Inglaterra
4	Itália
5	Alemanha
6	Rússia
7	Canadá
8	Austrália
9	Índia
10	Países Baixos
11	Brasil
12	Turquia

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

O fato de o ransomware ter uma finalidade comum, que é o pedido de resgate, eles são diferentes em suas formas de contágio, modo de agir e a cobrança gera desconfiança quanto ao pagamento do resgate, pois não há garantias de que se receberá o acesso aos dados novamente. Segundo Richardson e North (2017):

> Tanto indivíduos quanto empresas enfrentam a decisão de pagar quando não têm backups adequados para se recuperar do ransomware. Como tal, a decisão se resume a duas questões relacionadas. Em primeiro lugar, os dados valem mais do que o resgate? E, em caso afirmativo, qual é o nível de confiança de que o criminoso irá descriptografar os dados se o resgate for pago.

E há situações onde mesmo o resgate sendo pago, os criminosos além de não descriptografar os dados, pedem um segundo resgate como ocorreu em 2016 com o Kansas Heart Hospital que pagou o resgate quando foram infectados com um ransomware não divulgado. Em vez de descriptografar os arquivos, os criminosos exigiram um segundo resgate, que o hospital se recusou a pagar (apud Lemos, 2016).

Embora muitos arrisquem pagando o resgate, os especialistas recomendam o não pagamento e enumeram razões para isso. “Primeira razão, você se torna um alvo maior, pois os criminosos trocam informações entre si” (Richardson & North, 2017). Segundo, conforme o caso do Kansas Heart Hospital, você não pode confiar nos criminosos. Já o ransomware "CryptoWall" tem uma reputação de excelente ‘atendimento ao cliente’. Outras famílias de malware não”(Richardson & North, 2017). “Terceiro, seu próximo resgate será maior. Talvez os criminosos exigem um segundo resgate antes de descriptografar seus dados ou talvez você seja infectado uma segunda vez. De qualquer forma, você pagará mais” (Richardson & North, 2017). Quarto, o pagamento incentiva os criminosos a continuarem a fazer o que estão fazendo (apud Raschid, 2016).

Com o crescente interesse das empresas de segurança, dos agentes da lei, empresas de softwares antivírus, backup e outros voltados à segurança da informação, fez com que os criminosos mudassem a maneira de operar e esconder os rastros de sua atividade criminosa. “À medida que a pressão sobre o ransomware aumentar, os criminosos provavelmente procurarão outras maneiras de bloquear e ofuscar tentativas de rastrear e compreender suas atividades” (Savage, Coogan, & Lau, 2015).

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

O ransomware começou afetando a plataforma Windows, tendo evoluído e migrado para a plataforma da Apple, Android, Linux e já está afetando dispositivos como Smartwatches (relógios inteligentes) através do ransomware Locker.

Segundo Savage, Coogan & Lau, 2015:

> À medida que o mundo muda para a Internet das Coisas (IoT), não há dúvida de que o ransomware também mudará para a IoT. Embora isso possa parecer rebuscado no início, os pesquisadores já conseguiram assumir o controle dos sistemas de computador de um Jeep Cherokee em movimento. Se os pesquisadores podem fazer isso, o ransomware também pode.

Com a pandemia Covid-19, no final de 2019, houve um efeito dramático em nossas vidas em todo o mundo. Mas, além dos perigos óbvios para a saúde humana e um enorme impacto econômico, a pandemia mudou o mundo digital, a forma como trabalhamos e a forma como passamos nosso tempo livre online" (Ivanyuk & Wuest, 2020). Diversos relatórios de várias companhias acusam o ransomware como a principal ameaça e a permanência no posto no ano de 2021.

Conforme Ivanyuk & Wuest (2020):

> **31%** das companhias globais foram atacadas por cibercriminosos pelo menos uma vez ao dia. Ransomware foi responsável por quase **50%** de todos os casos conhecidos - Mais de **1000** companhias tiveram seus dados vazados depois dos ataques com ransomware - Microsoft corrigiu cerca de 1.000 falhas em seus produtos em apenas nove meses. - O tempo médio de vida de uma amostra de malware é de 3.4 dias.

Neste cenário, a empresa Acronis faz previsões com relação a um aumento no ataque a trabalhadores remotos, o vazamento de dados das empresas, um foco dos ataques em Provedores de Serviços, ataques a pequenas empresas, ataques na nuvem, busca por novos alvos e o aumento da automação dos ataques (Ivanyuk & Wuest, 2020).

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

REFERÊNCIAS

IVANYUK, Alexander – WUEST, Candid. **Acronis CyberthreatAcs Report 2020:** Cybersecurity trends of 2021, the year of extortion. Disponível em: https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Threats_Report_2020_EN-US_201201.pdf Acesso em: 02 fev. 2021

LISKA, Allan - GALLO Timothy. **Ransomware:** Defendendo-se da Extorsão Digital. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=gf6ZDwAAQBAJ&oi=fnd&pg=PT3&dq=autores+ransomware&ots=SFZeIGai3K&sig=nEL8fzh_OGtWI9yM7AnDp2aNIbI&redir_esc=y#v=onepage&q&f=false.> Acesso em: 04 fev. 2021.

RICHARDSON, Ronny – NORTH, Max M. **Ransomware:** Evolution, Mitigation and Prevention. Disponível para download em: https://digitalcommons.kennesaw.edu/facpubs/4276/ Acesso em: 02 fev. 2021

SAVAGE, Kevin - COOGAN, Peter, & LAU, Hon. **The Evolution of Ransomware:** Symantec. Version 1.0 - August 6, 2015. Disponível para download em: https://slidelegend.com/the-evolution-of-ransomware-symantec_59b322f11723dd6c7341e7f4.html Acesso em: 03 fev. 2021.