INSTITUTO ENSINAR BRASIL
REDE DE ENSINO DOCTUM

CENTRO UNIVERSITÁRIO DOCTUM DE TEÓFILO OTONI

Artigo apresentado ao curso de Sistemas de Informação do Centro Universitário Doctum de Teófilo Otoni – Unidoctum à disciplina de Trabalho de Conclusão de Curso II como requisito parcial para obtenção de título de Bacharel em Sistemas de Informação.

Linha de Pesquisa V: Redes de Computadores e Segurança da Informação

ANÁLISE DE RANSOMWARE: UM BREVE ESTUDO SOBRE O NOTPETYA E SEUS DANOS

RANSOMWARE ANALYSIS: A BRIEF STUDY ON NOTPETYA AND ITS DAMAGES

Daniel Malheiros Garrocho Alves Pinheiro[1] Lucas Gomes de Souza[2] Marlon de Souza Jardim[3]

Wilbert Viana Barbosa[4]

Resumo: A segurança de dados é um dos aspectos mais críticos da proteção de informações em organizações de todos os tamanhos e setores. Com o aumento da dependência da tecnologia, a ameaça do ransomware se tornou uma preocupação constante. O NotPetya é um exemplo de ransomware que causou danos significativos na escala global. O artigo a seguir tem como objetivo explorar as características desse malware, seu funcionamento e os impactos econômicos e de segurança causados, bem como as medidas de prevenção e mitigação a serem adotadas contra os ataques de ransomware. Como metodologia foi utilizado a revisão de literatura concomitantemente à pesquisa de dados e informações referentes a ataques ransomware NotPetya no mundo desde a sua implementação.

Palavras Chave: NotPetya, Ransomware, Segurança de dados, Análise.

[1] UniDOCTUM – aluno.daniel.pinheiro@doctum.edu.br
[2] UniDOCTUM – aluno.lucas.souza1@doctum.edu.br
[3] UniDOCTUM – aluno.marlon.jardim@doctum.edu.br
[4] UniDOCTUM – prof.wilbert.barbosa@doctum.edu.br

Abstract: Data security is one of the most critical aspects of protecting information in organizations of all sizes and industries. With increasing dependence on technology, the threat of ransomware has become a constant concern. NotPetya is an example of ransomware that has caused significant damage on a global scale. The following article aims to explore the characteristics of this malware, its operation and the economic and security impacts caused, as well as the prevention and mitigation measures to be adopted against ransomware attacks. As a methodology, a literature review was used concomitantly with the research of data and information regarding NotPetya ransomware attacks around the world since its implementation

Key Words: NotPetya, Ransomware, Data security, Analysis.

1 INTRODUÇÃO

O cenário cibernético mundial tem a cada dia sofrido com as ameaças cibernéticas cada vez mais sofisticadas e destrutivas. Entre essas ameaças, o ransomware emerge como uma das mais temíveis, causando danos significativos a organizações e indivíduos em todo o mundo, entre estas está o NotPetya um vírus de alto impacto e grande propagação que se instala e dissemina nos sistemas criando caos e gerando grandes prejuízos às organizações.

Compreender o funcionamento interno e as consequências desses ataques é fundamental para desenvolver estratégias de proteção eficazes. O NotPetya, com seu impacto devastador, servirá como um estudo de caso ilustrativo das ameaças cibernéticas contemporâneas e como a segurança cibernética é uma prioridade crítica na era digital.

A ascensão do NotPetya e outros ransomwares representa uma ameaça significativa e em constante evolução para a segurança digital global. O NotPetya, em particular, destacou-se como uma forma de malware extremamente destrutiva, capaz de causar danos substanciais a organizações em todo o mundo. Esses ataques são caracterizados pela capacidade de bloquear o acesso a dados cruciais, exigindo o pagamento de um resgate para sua liberação. À medida que a tecnologia avança, a sofisticação dos ransomwares aumenta, apresentando desafios constantes para especialistas em segurança cibernética.

O ransomware é um tipo de software malicioso que bloqueia o acesso a arquivos e exige o pagamento de uma quantia em dinheiro para liberar os mesmos. O NotPetya é um exemplo de ransomware que tem causado danos substanciais às empresas em todo o mundo. O objetivo deste trabalho de conclusão de curso (TCC) é realizar uma análise desse tipo de malware, descrevendo sua natureza, meios de difusão, seus efeitos e métodos de proteção eficazes para prevenir ou mitigar os danos causados.

Assim, esse estudo tem como objetivo geral, apresentar a análise do funcionamento do Ransomware NotPetya e os seus danos causados em empresas e usuários.

Objetivos específicos:

- Conceituar o que é NotPetya e Ransomware.
- Apresentar a análise do funcionamento e mecanismos de propagação do Ransomware NotPetya e os danos causados em empresas e usuários a partir de análises encontradas em bases de dados.
- Identificar as medidas de segurança que podem ser tomadas para prevenir ou mitigar os danos causados pelo Ransomware NotPetya.

Ao concluir este trabalho, espera-se que os leitores adquiram uma compreensão mais aprofundada do ransomware NotPetya e estejam mais bem informados sobre as medidas de proteção inovadoras para se defender. Além disso, esta análise pode servir como um exemplo para outros estudos de ransomware e ajudar a melhorar o conhecimento geral sobre segurança cibernética.

2 MARCO TEÓRICO

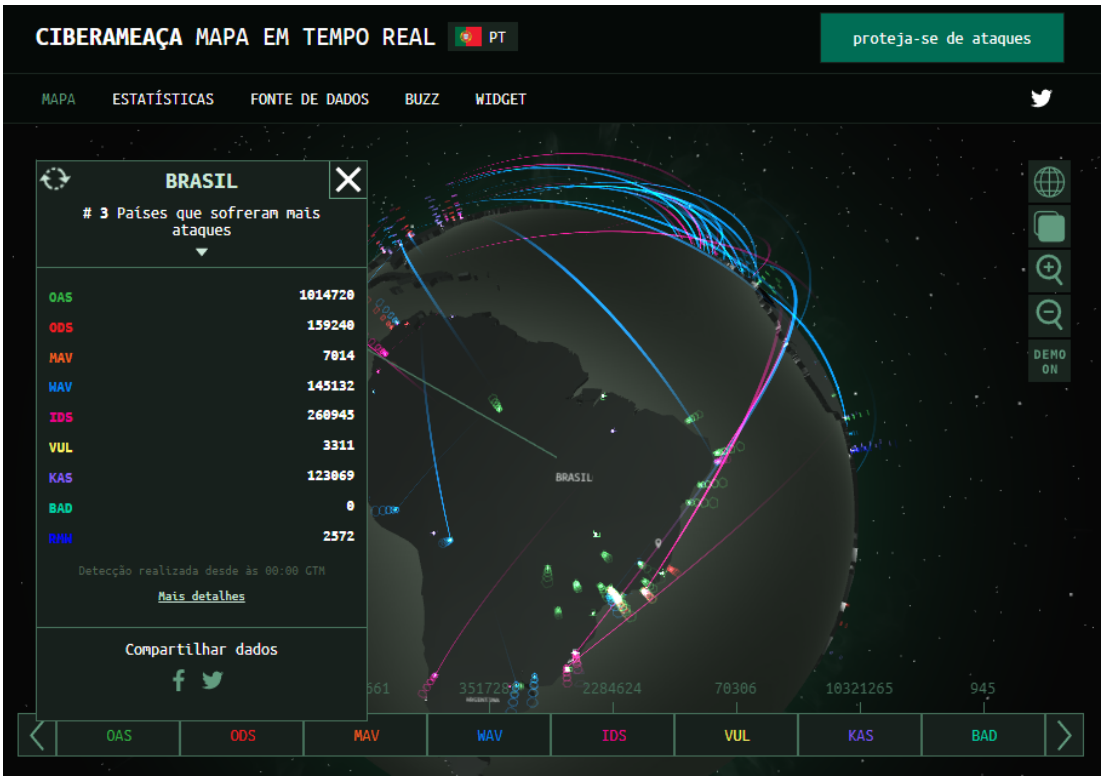
2.1 Proteção de dados

A proteção de dados é uma prática de informações contra acessos não autorizados, alterações, destruição ou divulgação, sendo fundamental para garantir a

confidencialidade, integridade e disponibilidade dos dados e sua violação pode resultar em danos financeiros, legais e de negociação de uma organização ou mesmo de um país (SIM & CHANG, 2017).

O Brasil está entre os países que mais sofrem ataques por ciberameaça ao redor do mundo. Abaixo é possível observar dados em tempo real, disponibilizados pelo Kaspersky, apontando o Brasil na 3ª posição em ataques em tempo real (KASPERSKY, 2023).

Figura 1: Ciberameaça Mapa em Tempo real - Brasil



Fonte: https://cybermap.kaspersky.com/pt (2023)

Por Segurança Cibernética entende-se as ações que visam garantir que os sistemas de informação possam resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (BRASIL, 2019).

As políticas de segurança de dados estabelecem diretrizes para o uso seguro de informações, incluindo a definição de direitos de acesso e responsabilidades. Isso envolve

a implementação de firewalls, antivírus, criptografia e outras tecnologias para proteção ativa de dados.

2.2 Ransomware

O ransomware é um tipo de malware que criptografa os dados de uma vítima e exige um resgate em troca da chave de descrição. Ele se espalhou por meio de anexos de e-mails maliciosos, atualizações de software comprometidos e exploração de vulnerabilidades (CERT.br, 2015). Notório por seu impacto financeiro e operacional, o ransomware é uma das ameaças cibernéticas mais perigosas e disseminadas.

Os cibercriminosos geralmente usam táticas de engenharia social para enganar os usuários a abrir anexos de e-mail ou visitar sites maliciosos. Após a infecção, o ransomware criptografa os dados, tornando-os inacessíveis. O usuário recebe uma mensagem de resgate, exigindo um pagamento em criptomoeda em troca da chave de descrição. Há ainda os ransomwares que se espalham internamente nas redes corporativas, expondo outros sistemas, como o NotPetya (GALOYAN, 2019).

2.3 Ransomware NotPetya

O NotPetya, também conhecido como Petya, ExPetr ou Petna, foi identificado pela primeira vez em junho de 2017. Inicialmente, ele foi disfarçado como um ransomware, mas análises posteriores revelaram que seu objetivo principal era a destruição de dados. Este ransomware é fornecido rapidamente através de uma variedade de vetores, incluindo e-mails de phishing, exploração de vulnerabilidades de software e uso de ferramentas de ataque cibernético roubadas da Agência de Segurança Nacional dos Estados Unidos (NSA) (FAYI, 2018).

Quando o NotPetya infecta um sistema, ele criptografa os arquivos do usuário e substitui o registro mestre de inicialização (MBR) do disco rígido, tornando o sistema

inoperável. Em seguida, exige um pagamento em Bitcoin em troca da chave de descrição. No entanto, muitas vítimas relataram que, mesmo após o pagamento do resgate, não receberam a chave de descrição, o que evidencia a verdadeira intenção de destruição de dados por trás do NotPetya (FAYI, 2018).

O NotPetya teve impactos devastadores em organizações em todo o mundo. Além da perda de dados críticos, muitas empresas sofreram danos sofridos em suas operações, o que resultou em perdas financeiras substanciais. Muitas empresas ficam temporariamente incapacitadas de operar devido à destruição de seus sistemas, resultando em perda de receita, muitas destas organizações perderam dados importantes que não puderam ser recuperados. Em alguns casos, as informações fornecidas foram roubadas antes da destruição, o que levou a preocupações com a privacidade e conformidade (GENÇ LENZINI & RYAN, 2018).

3. MATERIAIS E MÉTODOS

A pesquisa e desenvolvimento deste artigo científico basearam-se em uma metodologia de coleta, análise e resumo de informações de fontes diversas, incluindo artigos de bases oficiais, dados de jornais, publicações acadêmicas e demais fontes confidenciais.

Inicialmente foi feita a definição do tema "Análise de ransomware: um breve estudo sobre o NotPetya e seus danos" e a delimitação do escopo, com foco na análise do NotPetya e seus resultados.

Assim, seguiu-se a busca sistemática em bases de dados acadêmicos, para identificar artigos científicos relacionados a ransomware, especificamente o NotPetya. Também foram consultadas fontes oficiais, como o CERT (Computer Emergency Response Team) e a Agência de Segurança Cibernética e Infraestrutura (CISA).

Dados relevantes sobre ataques de NotPetya e suas consequências foram obtidos de fontes confiáveis, incluindo notícias de jornais respeitáveis, relatórios de segurança cibernética e documentos de órgãos governamentais.

Como descritores foram utilizadas as palavras chaves a seguir descritas: “NotPetya”, “Ransomware”, “Ataques cibernéticos”.

Os dados coletados foram submetidos a uma análise de conteúdo sistemática, com a categorização das informações relevantes e identificação de tendências e padrões de ataques de ransomware, seguindo com a sintetização dos principais resultados relacionados ao NotPetya, incluindo seus métodos de propagação, impactos em organizações e as ações de mitigação adotadas.

4. RESULTADOS E DISCUSSÕES

Ransomware tem sido bastante discutido devido ao grande aumento de ataques na última década. Em contrapartida, o NotPetya tem sido pouco discutido por profissionais da área em pesquisas

Os ataques cibernéticos têm evoluído e se tornado mais sofisticados ao longo dos anos, e o ransomware emergiu como uma das ameaças mais perigosas. Ransomware é um tipo de malware que criptografa os arquivos de um sistema e exige um resgate (resgate) em troca da chave descritiva (O'KANE, SEKER, CARLIN, 2018. Entre os numerosos exemplos de ransomware, o NotPetya se destaca como um dos mais destrutivos e impactantes.

A tabela abaixo (Tabela 1), resume os principais tipos de ransomware relacionados ao NotPetya, sua forma de ação:

Tabela 1:

Tipo de ransomware	Forma de Ação	Ferramentas de combate e de ação
(PeTya) ou NotPetya	1. Propagação por meio de anexos de e-mails maliciosos. 2. Exploração de vulnerabilidades, como EternalBlue, para se espalhar internamente nas redes.	1. Atualizações regulares de software para corrigir vulnerabilidades exploradas. 2. Utilização de soluções antivírus e antimalware.

	3. Criptografa arquivos e exige um resgate em Bitcoin.	3. Implementação de firewalls e sistemas de detecção de intrusões. 4. Conscientização do usuário para evitar phishing. 5. Manutenção de backups atualizados para recuperação de dados. 6. Medidas de segurança de rede, como segmentação.
ExPetr (também conhecido como Petya)	Semelhante ao NotPetya, o ExPetr utiliza técnicas de phishing e exploração de vulnerabilidades, como EternalBlue, para se espalhar Utilize anexos de e-mail maliciosos e criptográficos de arquivos da vítima.	

Fonte: SOLON, HERN (2018)

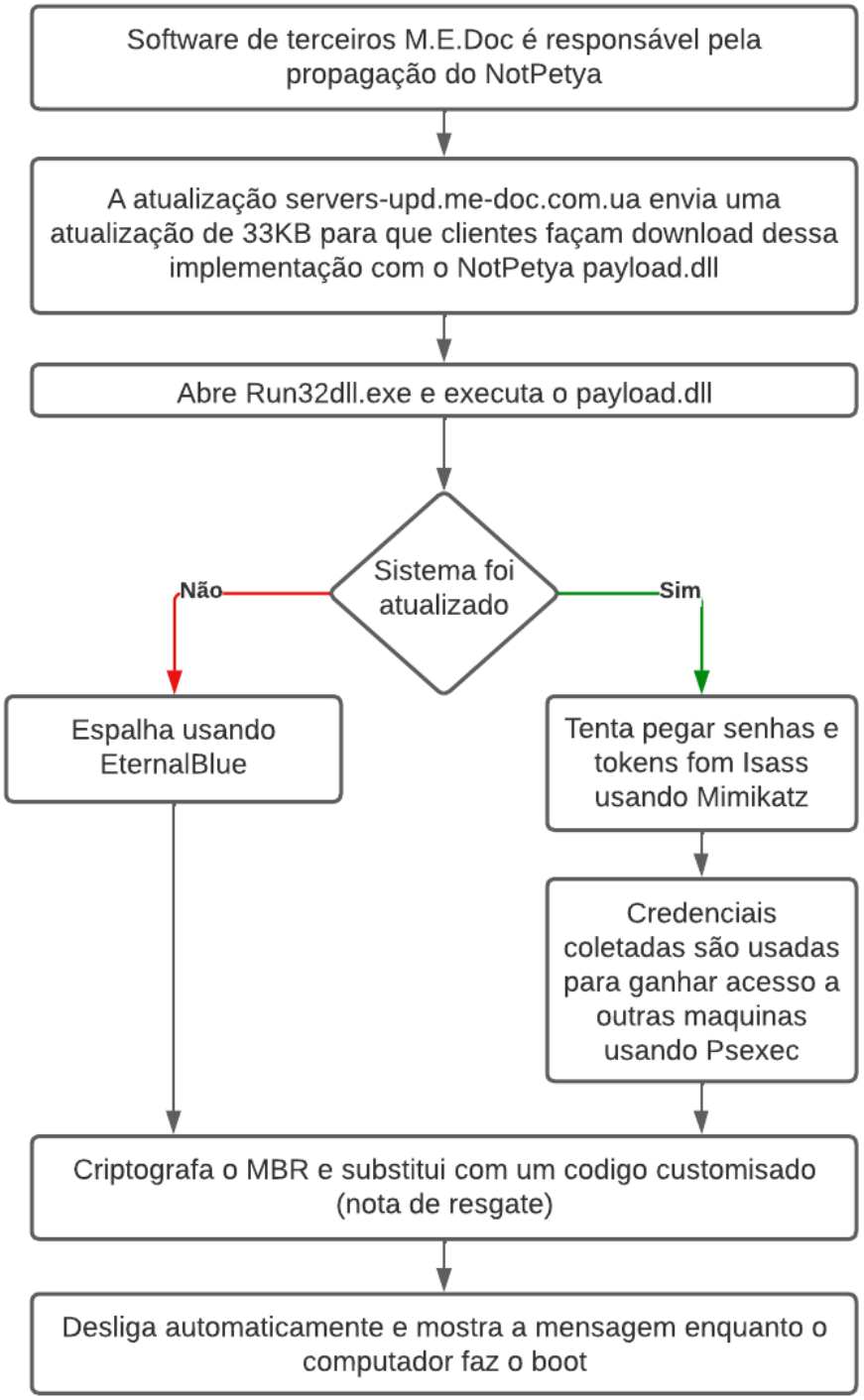
4.2 ESTRUTURA DO NOTPETYA

O NotPetya, também conhecido como Petya, ExPetr ou Petna, é um ransomware notório que ficou amplamente conhecido devido a seus impactos em organizações e empresas em todo o mundo (NOCETTI, 2018; CISA, 2017).

Figura 2: Ação de infecção NotPetya

Fonte: Kaspersky (2017)- Tradução Livre

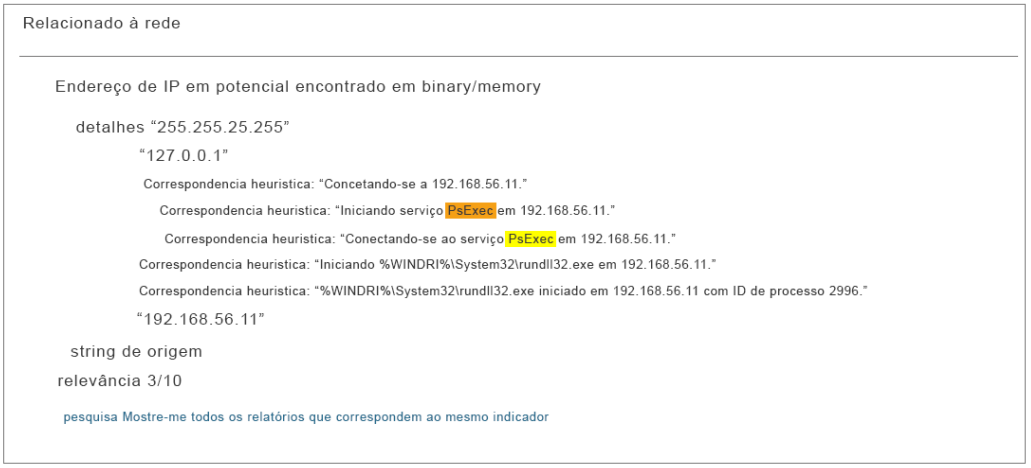
Fluxograma 1: Fluxo do Ransomware NotPe



Fonte: SAI e KUMAR, 2019 - Tradução livre.

O NotPetya possui capacidade de auto replicação e movimentação lateral (Figura 3), por meio do uso dos exploits Eternal Blue e EternalRomance, juntamente a componentes como PSEXEC, WMI e Mimikatz, que possibilitam que ele se colete as credenciais em uso na máquina, com uma ou mais permissões e se autentique em outras máquina, gerando a replicação em larga escala (BORGES, 2017).

Figura 3: Processo de replicação lateral do NotPetya



Fonte: Borges (2017) - Tradução Livre

4.3 DANOS CAUSADOS PELO NOTPETYA

O NotPetya surgiu inicialmente em 2016, mas seu ataque mais notório ocorreu em junho de 2017, quando foi enviado rapidamente por meio de uma atualização maliciosa do software contábil atualizado chamado MeDoc. O malware foi projetado para explorar a vulnerabilidade EternalBlue no Windows, o que permitiu uma rápida propagação (NOCETTI, 2018; CISA, 2017).

O ataque causou danos financeiros e operacionais substanciais em diversas organizações. Empresas dos setores como transporte, logística, saúde e muitas outras foram afetadas, enfrentando perdas graves devido à interrupção de operações e, em alguns casos, à perda permanente de dados (FAYI, 2018).

Além das perdas financeiras e operacionais, o NotPetya também afetou infraestruturas críticas em diferentes países, o que levou a implicações geopolíticas,

sendo a Ucrânia um dos centros mais afetados, com o desenvolvimento de conflitos políticos direcionadas entre a Rússia e a Ucrânia (EL PAÍS, 2017).

O quadro abaixo traz a lista dos países afetados pelo NotPetya no ataque em 2017.

Quadro 1: Países afetados pelo NotPetya

PAÍSES AFETADOS PELO NOTPETYA ENTRE 27 E 28 DE JUNHO 2017				
OESTE EUROPEU	**LESTE EUROPEU**	**ÁSIA E OCEANIA**	**AMÉRICA**	**ORIENTE MÉDIO**
REINO UNIDO	UCRÂNIA	INDIA	ESTADOS UNIDOS	TURQUIA
FRANÇA	RÚSSIA	CHINA	BRASIL	ISRAEL
ESPANHA	POLÔNIA	COREIA DO SUL	CHILE	
DINAMARCA	BIELORRÚSIA	AUSTRÁLIA	ARGENTINA	
ALEMANHA	LITUÂNIA	NOVA ZELÂNDIA		
NORUEGA	ROMÊNIA			
PAÍSES BAIXOS				

Fonte: MASCARENHAS (2017) adaptado pelos autores.

Uma análise das tendências de ransomware em 2021 e 2022 revela um cenário de ameaças cibernéticas em constante evolução:

- Ataques à cadeia de abastecimento: Os atacantes estão cada vez mais optando por ataques à cadeia de abastecimento, ampliando o impacto de seus ataques. Isso foi evidenciado pelo ataque Kaseya em 2021, que afetou uma ampla gama de clientes provedores de serviços gerenciados (KERNER, 2023).

- Extorsão Dupla: O ransomware não se limita mais à criptografia de dados; os invasores agora também exfiltram dados sensíveis. Isso cria uma pressão

adicional sobre as vítimas, que enfrentam a ameaça de vazamento de informações se não pagarem o resgate (KERNER, 2023).

- Ransomware como serviço (RaaS): A comercialização do ransomware facilita o acesso de criminosos à ameaça (KERNER, 2023).

- Ataques a sistemas não corrigidos: A exploração de vulnerabilidades descobertas em sistemas não corrigidos continua a ser uma tática predominantemente entre os atacantes, destacando a importância das atualizações de segurança (KERNER, 2023).

- Phishing: O e-mail de phishing permanece uma das principais formas de infecção por ransomware em 2022 (KERNER, 2023).

As estatísticas de ransomware para 2021 e 2022 destacam a gravidade do problema, em 2021 o ransomware afetou 66% das organizações, com um aumento de 78% em relação a 2020, conforme relatado pelo “The State of Ransomware 2022” da Sophos. Ainda em 2021, o FBI recebeu 3.729 reclamações sobre ataques de ransomware, resultando em US$ 49,2 milhões em perdas financeiras. Os setores mais envolvidos incluíram bens e serviços industriais, tecnologia, construção, assistência médica e educação. Em relação aos custos, o valor médio do resgate foi de US$ 812.360, mas os custos totais de um ataque de ransomware foram estimados em US$ 4,5 milhões, considerando a identificação e a resolução de notificação. Em 2022, os ataques de ransomware representaram 25% dos ataques cibernéticos divulgados, de acordo com o Relatório de Investigação de Violações de Dados da Verizon (KERNER, 2023).

Ataques notáveis de ransomware em 2021 e início de 2022 incluíram (KERNER, 2023):

- Ataque à Acer.
- Ataque à CNA Financial.
- Ataque ao Oleoduto Colonial.

- Ataque à JBS USA.
- Ataque a Kaseya.
- Ataque ao Grupo de Transmissão Sinclair.
- Ataques a serviços públicos e instituições de ensino.

Abaixo (Quadro 2) segue uma simulação de como o ransomware NotPetya opera em um nível conceitual, juntamente com a ação de resolução do problema que deve ser aplicada em caso de uma infecção real.

Quadro 2: Simulação conceitual ransomware NotPetya

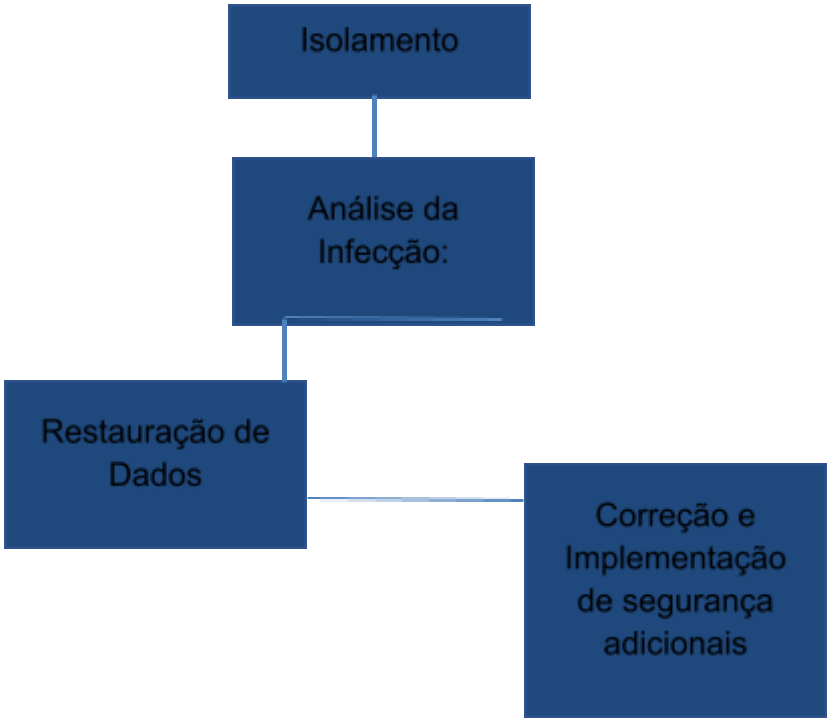
Distribuição
O ransomware NotPetya é distribuído através de um vetor de ataque, como um e-mail de phishing ou uma atualização de software falsa. Um usuário desavisado clicou em um link ou baixou um arquivo malicioso, iniciando o processo de infecção.
Exploração de Vulnerabilidade e propagação
O NotPetya pode explorar uma vulnerabilidade no sistema, como o EternalBlue, para se propagar lateralmente pela rede. O malware se espalha para outros sistemas e dispositivos na mesma rede, criptografando arquivos e exibindo uma mensagem de resgate.
Criptografia de Dados
O NotPetya criptografa os arquivos do sistema, tornando-os inacessíveis para o usuário. Uma mensagem de resgate é exibida na tela, exigindo o pagamento de um resgate em Bitcoin em troca da chave de descrição.

Fonte: FAYI (2018)

4.4 CUIDADOS CONTRA O NOTPETYA

Um ponto central a ser comentado neste cenário de ataques NotPetya são as ações de recuperação e proteção. O usuário é compelido a pagar um resgate pelas informações, contudo, grande parte das empresas que fizeram o pagamento não receberam a chave de acesso, remontando a falta de confiabilidade dos crimes cibernéticos no fornecimento de chaves de descrição após o pagamento. Assim, o mais indicado é que o usuário não faça o pagamento do resgate e proceda com ações de isolamento e correção. ((GENÇ LENZINI & RYAN, 2018).

O fluxograma a seguir traz as ações de controle e resolução contra ataques NotPetya.



A primeira ação a ser tomada a partir da infecção pelo NotPetya é o isolamento da máquina ou sistemas infectados da rede para evitar a propagação adicional de malwares. Feito isso, deve-se analisar a tecnologia, quais sistemas e dados foram afetados e como o ransomware foi incluído. O próximo passo é a restauração dos sistemas e dados a partir dos backups é a melhor abordagem, que deve ser feita após a remoção completa do

malware. Por fim, deve-se seguir a correção de quaisquer vulnerabilidades de segurança, como as exploradas pelo NotPetya, aplicando atualizações e patches em sistemas e softwares. Implementando medidas de segurança adicionais, como firewall, antivírus, prevenção contra intrusões, filtragem de e-mails e treinamento de conscientização em segurança cibernética para evitar futuras infecções (FAYI, 2018).

- Aplicação dos patches de correção do boletim Microsoft MS17-010.
- Aplicação de assinaturas de detecção e vacinas de fabricantes
- Bloquear ou desabilitar o protocolo SMB onde for possível - Portas 137 e 138 UDP e TCP 139 e 445.
- Interrupção do uso da rede de usuários (rede física e Wifi) para evitar a disseminação
- Validação do processo de *backup* na empresa, com segmentação de rede, e testes periódicos em ambos.
- Uso de *virtual patching* para sistemas legados.
- Adoção do gerenciamento sobre o uso de Psexec, wmi e powershell.
- Adoção da monitoração de logs do S.O., rede e tecnologias de segurança (BORGES, 2017)

A segurança dos dados é uma prioridade fundamental para qualquer organização, dada a crescente ameaça à segurança do ransomware e outras ameaças cibernéticas. Proteger os dados da organização envolve uma abordagem multifacetada, incluindo treinamento, tecnologia, políticas e procedimentos sólidos, com atualizações regulares de software para mitigar vulnerabilidades, conscientização dos funcionários para evitar técnicas de engenharia social, backups para a recuperação de dados e medidas de segurança de rede, como firewalls e sistemas de detecção de intrusões, adaptados às ameaças em constante evolução são cruciais para manter a segurança dos dados em um ambiente digital cada vez mais complexo (LIKA et al, 2018).

BARBAS (2022) cita em especial no contexto das organizações, a governança na Segurança da Informação e Cibersegurança, como o sistema de controle das atividades de segurança em uma organização, pontuando como ações de eficácia a retirada da

concentração exclusiva de responsabilidade de segurança nas equipas de TI, um envolvimento maior dos gestores nas decisões estratégicas de segurança, a disposição de recursos para implementação de políticas de segurança aprovadas, a avaliação prévia de segurança em projetos, com relatórios de monitoramento da eficácia dos controles de segurança.

O NotPetya serviu como um alerta para a importância da segurança cibernética robusta e preventivas, como um incentivo para o fortalecimento da segurança de dados nas organizações, incluindo a aplicação de atualizações de segurança, o treinamento de funcionários em conscientização cibernética e a manutenção de backups e planos de recuperação de desastres. Além disso, a colaboração com organizações de segurança cibernética e o compartilhamento de informações sobre ameaças são essenciais para a prevenção e a resposta a ataques de ransomware, possibilitando o monitoramento das táticas e ferramentas utilizadas pelos ransomwares, visto que estes podem evoluir com o tempo, exigindo uma busca constante por melhores práticas e soluções atualizadas de segurança cibernética.

CONSIDERAÇÕES FINAIS

Como ficou evidente no estudo, o NotPetya é um tipo de ransomware que ganhou notoriedade em 2017, sendo uma variante mais sofisticada e destrutiva do ransomware NotPetya, que se espalha principalmente através de redes locais e utiliza várias técnicas, como phishing e aproveitamento de vulnerabilidades, para infectar sistemas e criptografar os arquivos do usuário, exigindo um resgate em troca da chave de descriptografia.

O esclarecimento conceitual, inicialmente, delineou as definições essenciais de NotPetya e Ransomware, estabelecendo uma base sólida para as investigações subsequentes.A análise aprofundada dos mecanismos de propagação e dos danos causados revelou o seu impacto em diferentes esferas em âmbito global, proporcionando uma compreensão holística dos desafios enfrentados por organizações e indivíduos.

O NotPetya foi responsável por causar grandes danos a empresas e infraestruturas em todo o mundo. Além de criptografar arquivos, o ransomware também corrompe o Master Boot Record (MBR), tornando o sistema operacional inacessível. O impacto do ransomware NotPetya acende um alerta sobre os riscos dos ataques cibernéticos e da

vulnerabilidade dos dados em todos os setores da sociedade. O NotPetya interrompeu operações em setores essenciais, como saúde, logística e transporte, demonstrando a vulnerabilidade da infraestrutura crítica a ataques cibernéticos, Para além disso gerou implicações geopolíticas em larga escala, o que ressalta o alto grau de comprometimento que uma invasão deste tipo de sistema pode levar.

Os danos financeiros causados por este tipo de sistema são significativos, e pode levar grandes organizações a enfrentar perdas substanciais devido à interrupção das operações e à recuperação de dados, afetando toda a cadeia de funcionamento. Além disso, o pagamento de resgates nem sempre garantiu a recuperação bem-sucedida dos dados, aprofundando ainda mais os prejuízos.

A experiência do NotPetya destaca a importância da prevenção e mitigação de ameaças cibernéticas, reforçando a necessidade constante de atualizações e Patching, além de ações de conscientização do usuário, com treinamento de funcionários e demais usuários do sistema. Também a necessidade de manutenção de backups atualizados e planos de recuperação de desastres para minimizar os danos em caso de infecção.

Ao concluir este trabalho, acreditamos que proporcionamos aos leitores não apenas uma análise abrangente do NotPetya, mas também insights valiosos sobre as práticas inovadoras de proteção. Almejamos que este estudo não seja apenas um fechamento deste tópico, mas um ponto de partida para futuras investigações e aprimoramentos na área de segurança cibernética. Este trabalho, assim, não apenas preenche uma lacuna no entendimento do NotPetya, mas serve como uma contribuição para o conhecimento contínuo e aprimoramento da segurança digital em um mundo cada vez mais interconectado.

REFERÊNCIAS

BARBAS, João Manuel Assis. **Segurança da Informação e Cibersegurança**: A indispensabilidade da Governação. IDN – Instituto de Defesa nacional, jul. 2022. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/42136/1/PINHO Alexandre_Segurancaedefesadociberespaco_IDNBrief_Julho_2022.pdf. Acesso em 20 de setembro de 2023

BRASIL. Presidência da República/Gabinete de Segurança Institucional. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, 2019.

BORGES, Carlos. A ficha técnica do "ransomware" Petya. NEC, Jun. 2017. Disponível em: https://blog.nec.com.br/a-ficha-tecnica-do-ransomware-petya. Acesso em 20 de setembro de 2023

CERT.BR. Cartilha de Segurança para Internet - Ransomware, 2015. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em setembro de 2003.

CISA - CYBERSECURITY E INFRASTRUCTURE SECURITY AGENCY. SA. Alerta (TA17-181A) Petya Ransomware, US-CERT, 2017. Disponível em: https://www.us-cert.gov/ncas/alerts/TA17-181A . Acesso em 7 de setembro de 2023.

EL PAÍS. **Poderoso ciberataque afeta grandes empresas de todo o mundo**. Madri, junho de 2017. Disponível em: https://brasil.elpais.com/brasil/2017/06/27/internacional/1498568187_011218.html. Acesso em 05 de outubro de 2023.

FAYI, Sharifah Yaqoub A.O que é Petya/NotPetya Ransomware e quais são suas remediações. **In**: Tecnologia da Informação - Novas Gerações. Série - Avanços em Sistemas Inteligentes e Computação - AISC, volume 738. 2018.

GALOYAN, Albert. **Segurança cibernética no âmbito das relações internacionais**. Trabalho de conclusão de curso de Relações Internacionais da Universidade de Brasília. Brasília, 2019.

GENÇ, Z.A., LENZINI, G., RYAN, P.Y.A. No Random, No Ransom: A Key to Stop Cryptographic Ransomware. In: Giuffrida, C., Bardin, S., Blanc, G. (eds) **Detection of Intrusions and Malware, and Vulnerability Assessment**. DIMVA 2018. Lecture Notes in Computer Science(), vol 10885. Springer, Cham, 2108. Disponível em: https://doi.org/10.1007/978-3-319-93411-2_11. Acesso em 07 de setembro de 2023.

LIKA, RA. MURUGIAH, D. BROHI E, SN. RAMASAMY, D. "NotPetya: Cyber Attack Prevention through Awareness via Gamification," **Conferência Internacional de 2018 sobre Computação Inteligente e Empresa Eletrônica (ICSCEE)** , Shah Alam, Malásia, 2018, pp. 6, doi: 10.1109/ICSCEE.2018.8538431.

KERNER, Sean Michael. **Tendências, estatísticas e fatos de ransomware em 2023**. Techtarget, janeiro de 2023. Disponível em: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts . Acesso em 15 de outubro de 2023.

SIM, Q. CHANG, AJ. Ameaças e contramedidas para segurança de sistemas de informação: um estudo intersetorial. Inf. Gerenciar. 2007.

SOLON, Olivia. HERN, Alex. Ataque de ransomware Petya: o que é e como pode ser interrompido?, The Guardian, 2017. Disponível em:

https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how . Acesso em 11 de outubro de 2023.

MASCARENHAS, Jacinto. **Ransomware 'Petya'**: lista completa de países afetados pelo enorme ataque cibernético global. IBT - International Business Times, junho de 2017. Disponível em: https://www.ibtimes.co.uk/petya-ransomware-full-list-countries-affected-by-massive-global-cyberattack-1628086. Acesso em 15 de setembro de 2023.

NOCETTI, J. Géopolitique de la cyber-conflictualité. **Politique étrangère**, vol. 83, nº 2, été 2018. Disponível em : https://www.ifri.org/fr/publications/politiqueetrangere/articles-de-politique-etrangere/geopolitique-de-cyber. Acesso em 11 de outubro de 2023.

O'KANE, Philip. SEKER, Sakir Sezer, CARLIN, Domhnall. **Edição Especial**: Privacidade, Garantia de Dados, Soluções de Segurança para Internet das Coisas (PASS4IoT), vol 7, 5ª edição, setembro de 2018. Disponível em: https://doi.org/10.1049/iet-net.2017.0207. Acesso em 05 de outubro de 2023.

SAI, R. L. P.; KUMAR, T. P. Reverse engineering the behavior of NotPetya ransomware. **International Journal of Recent Technology and Engineering**, v. 6, p. 574-578, 2019.