Ransomware

Bruna Almeida Osti
Rafael Cortez Sanches
18 de Junho de 2020

Resumo

Esse ensaio tem o objetivo de fazer uma revisão rápida sobre ransomwares. Inicialmente são apresentado os conceitos envolvidos nesse tipo de código malicioso, bem como sua evolução ao longo do tempo. São abordadas técnicas de criptografia utilizadas para sequestrar os dados da vítima, bem como técnicas de ofuscação empregadas para dificultar a detecção do ransomware por softwares antivírus. Por fim, o ensaio enumera técnicas de detecção e medidas preventivas para evitar esse tipo de código malicioso.

1 Introdução

O ransomware é um tipo de malware que impede o acesso aos computadores e aos dados de diversas maneiras, até que a vítima pague pelo resgate dos seus dados, caso contrário os dados se tornam inúteis. O problema é que ele pode criptografar não só os arquivos em uma estação de trabalho, mas viajar pela rede e criptografar arquivos localizados nas unidades de rede mapeadas e não mapeadas, ou seja, pode interromper um departamento ou até mesmo toda a organização (1).

A dependência das tecnologias está ficando cada vez mais comum, as pessoas tendem a organizar o trabalho e a vida pessoal no computador, portanto as informações salvas são valiosas. Os hackers conseguem infectar uma máquina usando: e-mails de phishing, programas não corrigidos, sites comprometidos, publicidade online e downloads de software livre (2).

O crescimento da popularidade das cripto moedas e de outros serviços como MoneyPak, Ukash, e PaySafe tiveram o efeito de aumentar os cibercrimes, pois a possibilidade de não rastreio do dinheiro facilitou as extorsões entre outros cibercrimes, que se tornaram cada vez mais complexos e que conseguem comprometer até milhões de máquinas ao mesmo tempo (3).

Acaba sendo muito efetivo pois instalam medo nas suas vítimas fazendo com que cliquem em um link ou paguem um resgate, e os sistemas dos usuários podem ser infectados com malware adicional, pois exibem mensagens do tipo: ”Todos os arquivos no seu computador foram criptografados. Você deve pagar esse resgate dentro de 72 horas para recuperar o acesso aos seus dados”(4).

Neste trabalho estudaremos um pouco a respeito do ransomware, também conhecido como extorsão digital ou chantagem digital, como esse tipo de método criptografa os arquivos e como se tornou cada vez mais seguro e inquebrável.

2 Evolução do Ransomware

O primeiro ransomware documentado era chamado de AIDS Trojan (1989), criado pelo biólogo Joseph Popp que enviou 20.000 disquetes infectados para os participantes da conferência de AIDS da Organização Mundial da Saúde(OMS). No qual foram identificados como “Informações sobre aids - Disquetes Introdutórios” e continha um questionário interativo que era usado como gatilho para ativar os malwares após aproximadamente 90 reinicializações da máquina da vítima. O funcionamento dele se baseava em criptografar os arquivos utilizando criptografia simétrica simples e ocultar todos os diretórios e nomes de arquivos criptografados localizados na unidade C:\ o que tornava o computador inutilizável (1).

O segundo passo foi em 1996 quando dois pesquisadores escreveram um artigo para a conferência “IEEE Security & Privacy Conference”, no qual sugeriram um programa de prova de conceito que usava criptografia de chave pública para criar um código malicioso para extorquir dinheiro das vítimas (1)(5).

Até 2005 os ataques de ransomware não eram muito utilizados, entretanto surgiram novos tipos de ransomware como por exemplo: Krotten, Archiveus e GPCoder. No qual o GPCoder foi o mais notado, pois utilizava criptografia RSA de 1024 bits (considerada forte naquela época) e recuperava os arquivos das vítimas através de uma

técnica de força bruta difícil. As empresas de antivírus adicionaram a assinatura de cada ransomware descoberto, resultando na interrupção dos ataques naquele momento (1).

Em 2009, surgiu um novo tipo de ataque de ransomware que ficou conhecido como Vundo, no qual utilizava técnicas de scareware para roubar dinheiro das vítimas convencendo-as a comprarem um software de segurança como XPAntiVirus2009, informando que o computador estava infectado com um vírus. Mudando a função do ransonware para criptografar os arquivos e pedir $U\$$ 40 para decriptografar(1).

Em 2012, o ransomware Raveton passou a atingir provedores de serviços ameaçando usuários que cometiam crimes na internet, se passando pela polícia e bloqueando o computador das vítimas, sob pena de multa para recuperar o acesso (1).

Devido ao sucesso na quantidade de dinheiro considerável recolhido em 2012, começaram a aparecer entre 2013 e 2015 outras abordagens como por exemplo: Cryptolocker, Torrentlocker, Cryptowall, e o Teslacrypt. Esse tipo de malware usa uma criptografia forte (e.g. AES e RSA-2048 bit), levando ao crescimento exorbitante dos pagamentos de ransom que atingiram mais de $325 milhões até 2015(1)

Em 2016, continuou seu processo de evolução adicionando recursos mais avançados como um contador regressivo que aumenta o resgate conforme o tempo que a vítima demorou para pagar. Além disso, foram criadas versões de ransomware que é capaz de se autopropagar através das redes de computadores. Além disso, também foi adicionado formas diferentes para o pagamento do resgate que simplificaram o pagamento. As famílias de ransomware notáveis daquele ano foram Locky, Petya e SamSam (1). Foi um ano memorável pois foram introduzidos 247 famílias novas de ransomware.

É importante observar que algumas variações como Doxware ameaçaram liberar dados pessoais(fotos, vídeos, informações confidenciais, entre outros) da vítima caso não pagasse o resgate (1).

E 2017 foi o ano de ouro segundo os especialistas de segurança, o ataque mais notável foi o ransomware WannaCry. Esse malware suportava 27 linguagens e tinha a habilidade de se propagar através das redes conectadas para infectar servidores e sistemas. O aumento se deve ao grupo de hackers Shadow Broker que lançou o repositório de ferramentas vazado pela NSA que exploram vulnerabilidades em pcs e servidores Windows, além de redes virtuais privadas (VPNs) e sistemas de firewall. As ferramentas foram utilizadas para espalhar ransomware globalmente (1).

Em 2018, a infecção por ransomware caiu 30% em todo o mundo, mas embora o volume tenha diminuído ele se tornou sofisticado e na maioria das vezes tem autopropagação (1). Por outro lado, surgiu o Ryuk que é um trojan de criptografia, os ataques têm como alvos principais as empresas e hospitais dos Estados Unidos e na Alemanha. Está sendo distribuído por conexões RDP (Remote Desktop Protocol) mal protegidas, mas pode ser entregue por outros meios (6).

Em resumo, podemos observar os fatos mais marcantes na história do ransomware através da Figura 1.

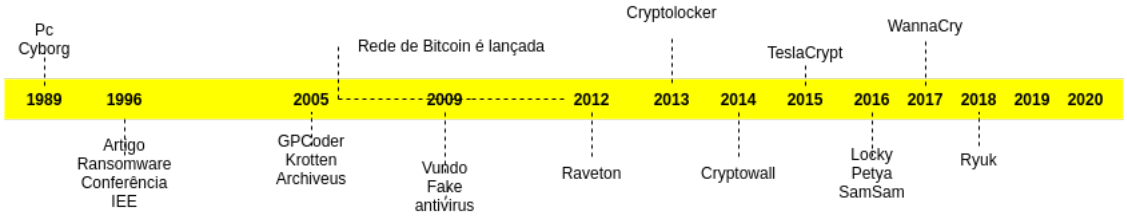

Figura 1: Linha do Tempo - Adaptado (2)

3 Criptografia em Ransomwares

Essa seção aborda técnicas de encriptação utilizadas por um ransomware do tipo crypto-ransomware. Pertencem a esse tipo os códigos maliciosos que criptografam os dados da vítima no disco, de forma que esses fiquem totalmente inutilizáveis até que sejam decriptados com a chave do sequestrador.

Além de utilizar técnicas de criptografia para sequestrar os dados da vítima, os crypto-ransomwares também

FAMILIES	Propagation Strategy	Date Appeared	Cryptographic Techniques	C and C Server
REVETON	Accused of illegal activities	2012	RSA and DES	Using MoneyPak
GPCODE	Email Attachments	2013	660-bit RSA and AES	Tor Network
CRYPTOLOCKER	compromised websites and email attachments	2013	2048-bit RSA	Tor Network
CRYPTOWALL	compromised websites and email attachments	2013	2048-bit RSA	Tor Network
FILECRYPTO	compromised websites and email attachments	2013	2048-bit RSA	Tor Network
TELSACRYPT	compromised websites and email attachments	2013	2048-bit RSA	Tor Network
CTB-LOCKER	Email Attachments	2014	Elliptic Curve Cryptography	Onion Network
CRYPTO M IX	Spear-phishing Email	2014	2048-RSA and AES-256 and ROT-13	P-2-P Network
CERBER	compromised websites and email attachments	2013	2048-bit RSA and RC4	Hardcoded IP range
PETYA	Link in an Email purporting to be a job application	2016	Elliptic Curve Cryptography and Salsa	Tor Network
SATANA	Email Attachments	2016	256-bit AES in ECB	Hardcoded IP Address
JIGSAW	Word Document with Javascript	2016	RSA and AES	Onion Network
SHADE	Spam Email	2015	RSA-3072 and AES-256	Fixed Server as C and C server
WANNACRY	Samba Vulnerability	2017	RSA and AES combination	Onion Network

Tabela 1: Lista das diferentes famílias de ransomwares com seus respectivos meios de transmissão, propagação e tipo de criptografia (7)

utilizam técnicas criptográficas para ofuscar o código malicioso empregado no ataque, deixando-o mais protegido de sistemas antivírus.

3.1 Criptografia aplicada aos dados da vítima

Para encriptar os dados da vítima em disco, ransomwares têm utilizados diversos algoritmos de criptografia ao longo do tempo, tanto os de criptografia simétrica quanto assimétrica. Alguns desses códigos maliciosos até mesmo usam ambos, o que torna a recuperação dos dados ainda mais inviável. A Tabela 1 apresenta diversas famílias de malware e os respectivos algoritmos de criptografia utilizados por elas.

Uma vez que os dados da vítima estão criptografados, cópias das chaves utilizadas são enviadas ao atacante por meio de conexões com servidores de *Command and Control* (C&C), que também recebe os dados da vítima. O envio dessas informações geralmente se dá por um canal seguro da *deep web*, como por exemplo a rede Tor.

3.1.1 Estudo de caso: WannaCry

Um dos casos mais recentes de infecção em massa por ransomwares foi provocado pelo malware batizado de *WannaCry*, o qual se propagou rapidamente pela web através do *EternalBlue*, um *exploit* de uma vulnerabilidade de um serviço de compartilhamento de arquivos e impressoras do Microsoft Windows, o *Server Message Block* (SMB).

O *WannaCry* utiliza o método de criptografia simétrica AES para encriptar os arquivos da vítima, sendo que para cada um desses arquivos uma chave diferente é gerada e utilizada para encriptação. Essas chaves, por sua vez, são encriptadas com o algoritmo assimétrico RSA através de uma chave pública, a qual é distribuída junto com o executável do malware. Uma vez que todos arquivos estão indecifráveis, as chaves criptografadas são enviadas para o C&C do atacante e o pano de fundo da Área de Trabalho é alterado para mostrar a mensagem de resgate à vítima. (8)

Como a maioria dos ransomwares, o *WannaCry* solicita uma transferência de um certo valor em criptomoeda para a conta do atacante. As chaves para descriptografar os arquivos só são recuperadas caso essa transferência seja computada.

3.1.2 Estudo de caso: CriptoWall 3.0

Segundo Cabaj (9) o ransomware Cryptowall geralmente é distribuído utilizando sites que não são confiáveis ou até e-mails de plishing. Utiliza nomes de domínio ao invés de endereços de ip. Portanto, requere um serviço de nome de domínio (DNS) para funcionar direito. Analisando o tráfico das máquinas infectadas foi revelado que primeira ação feita pelo CryptoWall 3.0 foi aprender o endereço de ip do computador da vítima, usando um serviço de público disponível (e.g., myexternalip.com).

A comunicação CryptoWall utiliza mensagens HTTP POST direcionadas aos scripts carregados nos servidores da Web invadidos (proxy servidores). Essa comunicação é encriptada utilizando o algoritmo RC4, e a chave é incorporada na requisição HTTP. Quando decriptado, um simples protocolo de texto é revelado.

Durante a primeira troca de dados, o malware reporta o único identificador e o endereço de ip da máquia para o C&C, com a capacidade de receber informações.

Na segunda troca de dados, a resposta contém o endereço TOR do site do ransom, o código pessoal da vítima e a chave pública do RSA-2048 bit que é utilizado para encriptar os dados. A chave pública e privada são geradas fora da máquina infectada e do proxy.

Na terceira troca de dados, é enviado para a vítima um PNG contendo instruções, o qual será mostrado mais tarde como provedor.

Se a conexão for bem sucedida, a máquina infectada agora tem capacidade de recepção de todos os dados. Então a comunicação é interrompida apenas enquanto está acontecendo o processo de encriptação dos dados.

Finalmente, o processo de troca de dados contém um número da quantidade de arquivos encriptados que serão mostrados para a vítima com a instrução para decriptação dos dados.

3.2 Criptografia aplicada a ofuscação

Para que um ransomware possa infectar o sistema alvo, seu código malicioso precisa ser executado nesse sistema. Caso o atacante não tenha total controle desse sistema, uma solução é convencer algum usuário ou administrador do sistema alvo a executar o código malicioso, o que é muito mais fácil se o executável estiver **disfarçado** como um executável útil, como por exemplo um programa editor de texto. Por esse motivo, é comum atacantes inserirem o código malicioso dentro de um executável útil antes de o enviar ao sistema alvo. (10)

Disfarçar o executável dessa forma, no entanto, não é o suficiente para garantir o sucesso de um ataque. Aplicações anti-vírus comumente encontradas tanto em organizações quanto em computadores pessoais são capazes de encontrar código malicioso por meio de técnicas de detecção estática. Essas aplicações varrem as memórias do sistema calculando hash de trechos de código suspeitos, comparando-os com informações de malwares conhecidos. Uma solução utilizada pelos atacantes é encriptar o código malicioso antes de inseri-lo em uma aplicação inofensiva, o que dificulta a detecção estática por parte de aplicações anti-vírus.

4 Técnicas de ofuscação

Essa seção apresenta técnicas utilizadas tanto por ransomwares quanto por outros tipos de malware para evitar sua detecção por softwares antivírus e por sistemas de detecção de intrusão.

4.1 Criptografia e Polimorfismo

Conforme apresentado na seção 3, alguns malwares costumam esconder seu código binário com criptografia, com o objetivo de evitar mecanismos de detecção estática. No momento o oportuno, o malware decripta a parte oculta de seu próprio código e a executa.

Para evitar que sistemas anti-vírus identifiquem o código decriptador do malware por meio de técnicas de análise estática, como assinatura de bytes, os atacantes criam um número ilimitado de códigos decriptadores para utilizar nesses malwares, de forma que essas diversas versões de código não tenham elementos em comum para serem identificados por softwares anti-vírus.

As diferentes versões dos decriptadores são geradas pela inserção de código inútil e pela substituição de registradores e de instruções. Dessa forma, um mecanismo de mutação consegue produzir binários com assinaturas diferentes toda vez que o malware infecta uma nova vítima, como pode ser visto na figura 2. (11)

4.2 Detecção de Sandbox

Uma das técnicas utilizada para detectar um ransomware é executá-lo em um ambiente *sandbox*: uma instância minimalista e controlada do sistema protegido. Através da análise comportamental do executável dentro da *sandbox*, pode-se identificar se ele possui características maliciosas ou não por meio de técnicas de análise dinâmica.

Para evitar esse tipo de detecção por análise dinâmica, malwares costumam fazer um *fingerprinting* do sistema antes de se comportarem efetivamente como um código malicioso. Dependendo do nível de acesso do executável ao

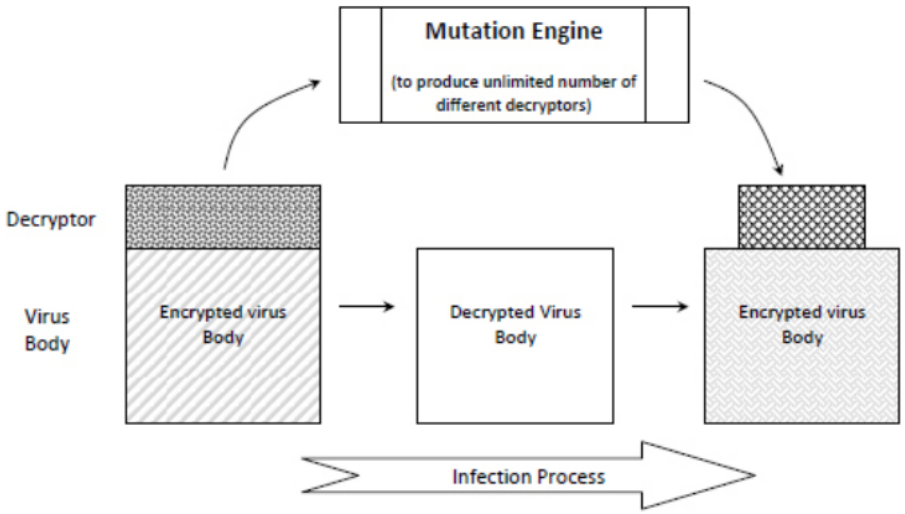

Figura 2: Mecanismo de mutação para malware polimórfico (11)

sistema, o hardware pode ser analisado quanto ao seu comportamento, com o objetivo de identificar se está sendo rodado em uma máquina virtual. Com essa mesma finalidade, também podem ser analisados a memória do sistema e o disco. (12)

Caso seja identificado que o código está sendo executado em um ambiente *sandbox*, o malware simplesmente não realiza o seu trabalho normal, passando-se por um executável inocente no processo de análise. Esse comportamento defensivo dificulta a detecção do malware por aplicações antivírus.

5 Técnicas de Detecção de Malwares

Nesta seção serão abordados alguns métodos de detecção utilizados pelos anti-malwares, visando identificando ações e arquivos maliciosos, os bloqueando antes que possam causar danos.

É importante observar que os malwares estão sempre evoluindo e existem táticas como as citadas anteriormente na seção de técnicas de ofuscação que buscam passar as ameaças despercebidas, portanto, os provedores de softwares anti-malwares precisam incorporar várias camadas de proteção pois cada algoritmo tem seus pontos fracos e fortes e ao combinar ferramentas as taxas de detecção de ameaças tendem a aumentar.

5.1 Detecção baseada em assinatura

Esse método utiliza aspectos chave do arquivo, examinando se existem impressões digitais de malwares já conhecidos. Desta forma, podemos o verificar se a assinatura é uma série de bytes ou um hash criptográfico do arquivo (13).

Esse método já foi um elemento essencial nos antivírus e continua integrando muitas ferramentas, embora sua eficácia esteja diminuindo.

O problema deste método é que não é possível verificar assinaturas que ainda não foram apontadas como suspeitas. Portanto, abre uma brecha para as ações dos criminosos que ainda não foram desmascarados.

5.2 Detecção baseada em heurística

Esse método visa uma detecção generalizada de malwares, analisando estatisticamente os arquivos e encontrando suspeitas (13).

Esta ferramenta pode simular a execução de um arquivo e observar o comportamento do mesmo, pois se houver mais de um atributo suspeito é o suficiente para classificar o arquivo como malicioso.

O problema deste método é que a tecnologia pode sinalizar arquivos que são legítimos como suspeitos.

5.3 Detecção comportamental

Este método analisa o processo de execução de um programa, no qual busca identificar malwares ao investigar comportamentos suspeitos (14).

A detecção comportamental pode até mesmo impedir que arquivos adicionais sejam criptografados. Entretanto, assim como acontece no modelo heurística, cada ação sozinha não é suficiente para classificar um programa como malware. No entanto, se juntas as detecções, essas iniciativas podem ser bons aliados na indicação de arquivos maliciosos.

Existem dois tipos de detecção comportamental, a estática e a dinâmica. Ambos coletam informações dos dados, interpretam, usam algoritmos de combinação, utilizam modelos de comportamentos e procuram o padrão da assinatura, o que diferencia os dois é que o primeiro faz a verificação formal, verificando as especificações lógicas, algébricas e semânticas, enquanto o segundo faz uma verificação baseada em simulação, roda heurísticas e verifica com as referências respectivamente.

5.4 Detecção baseada em Nuvem

Esse método detecta malwares ao coletar dados de computadores protegidos, entretanto a análise é realizada na própria infraestrutura do provedor, portanto não é uma análise local (15).

A investigação geralmente é feita através da análise de detalhes relevantes sobre os arquivos e seus contextos de execução, enviando-os para o processamento em nuvem, incluindo a execução do potencial arquivo malicioso, e analisando suas ações.

É interessante acrescentar que a maioria dessas ferramentas incluiu as tecnologias de inteligência artificial e machine learning na infraestrutura de análise de malware, isso é importante porque permite que a ferramenta aprenda com casos anteriores, e automaticamente.

5.5 Detecção de malwares invisíveis (sem arquivos)

Esse método de detecção é um dos avanços mais recentes das tecnologias de detecção, os malwares são detectados com base em um script/comando que são executados em um endpoint (16).

Uma observação importante é que um comando/script malicioso funciona através de uma aplicação de script, que já está instalado no endpoint, utilizando os privilégios do usuário atual para performar suas ações.

6 Prevenção de Infecção

Como citado anteriormente o ransomware é construído para passar despercebido no sistema, por isso, melhor que detectá-lo seria prevení-lo. A seguir citaremos algumas formas de prevenção da infecção pelo malware segundo o site ”The No More Ransom”(17).

1. Backup: Tenha um sistema de recuperação de forma que você possa substituir os dados em caso de infecção. A melhor forma é ter duas cópias de backup, uma em cloud e outra armazenada fisicamente (hd externo, outro computador, etc). Além disso, não é aconselhado deixar o computador ligado quando ninguém estiver usando.
2. Antivírus: atualize sempre o antivírus e não desligue as ‘funcionalidades de heurística’, pois é utilizado para identificar um malware que ainda não foi detectado formalmente.
3. Atualizações: Quando o sistema operacional ou as aplicações oferecem uma nova atualização, instale. Se tiver atualizações automáticas ative. Isso é importante pois as atualizações corrigem e previnem problemas.
4. Não confie em ninguém: Qualquer conta pode ser comprometida e links maliciosos podem ser enviados através de contas de amigos. Nunca abra anexos em emails, pode ser phishing.
5. Ative a opção ”Mostrar extensões de ficheiros conhecidos”nas definições do Windows. Isso torna a detecção de ficheiros com extensões ”.exe”, ”.vbs”e ”.scr”enviados em anexos em emails. O tipo de ataque por scammers

usa extensões para disfarçar ficheiros maliciosos, por exemplo teste.doc.src.

6. Se descobrir um processo estranho em execução no computador desligue-o imediatamente da internet, isso irá prevenir que a infecção se espalhe por outros sistemas.

Alguns conselhos adicionais para o ransomware "WannaCry":

- Desative a função "smb v1": isso prevenirá do ransomware se espalhar pela rede.
- Instale os patches da Microsoft: também prevenirá o espalhamento do ransomware.

7 Considerações Finais

Podemos observar a complexidade dos ransomwares que evoluíram com o tempo e as tecnologias disponíveis e passaram a ser quase impossíveis de serem revertidos, isso se dá pelas técnicas de encriptação e ofuscação utilizadas nos programas e continuam causando muito prejuízo à empresas.

Em contrapartida, existem técnicas de detecção dos malwares que apesar de não serem totalmente eficazes, permitem que se utilizados em conjuntos possam detectar boa parte dos malwares.

Mas a realidade é que apesar de existir muitas técnicas de detecção dos malwares, a prevenção é sempre a melhor arma contra esse tipo de armadilha. Manter dois backups é sempre a melhor alternativa, além da utilização de um bom anti-vírus e de seguir recomendações de segurança fornecidas por entidades especializadas. É importante nunca confiar em ninguém e tomar sempre cuidado com o download de arquivos, pois aparecem novos malwares que não são conhecidos continuadamente.

Referências

[1] N. A. Hassan, *Ransomware Revealed.* Apress, 2019.

[2] L. Miller, *Ransomware Defense for Dummies - Cisco Version.* Hoboken, New Jersey: John Wiley Sons, Inc., 2017.

[3] A. Liska, *Ransomware : defending against digital extortion.* Sebastopol, CA: O'Reilly Media, 2016.

[4] Berkley, "Perguntas freqüentes - ransomware."

[5] A. Young and M. Yung, "Cryptovirology: Extortion-based security threats and countermeasures," 09 1996.

[6] GoldSparrow, "Ryuk ransomware."

[7] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," in *2018 IEEE Security and Privacy Workshops (SPW)*, IEEE, May 2018.

[8] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of wannacry ransomware," in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 454–460, 2017.

[9] K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: The case of CryptoWall," *IEEE Network*, vol. 30, pp. 14–20, Nov. 2016.

[10] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking.* Apress, 2014.

[11] B. Bashari Rad, M. Masrom, and S. Ibrahim, "Camouflage in malware: From encryption to metamorphism," *International Journal of Computer Science And Network Security (IJCSNS)*, vol. 12, pp. 74–83, 01 2012.

[12] Xu Chen, J. Andersen, Z. M. Mao, M. Bailey, and J. Nazario, "Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," in *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, pp. 177–186, 2008.

[13] A. Mujumdar, G. Masiwal, and D. B. B. Meshram, "Analysis of signature-based and behavior-based anti-malware approaches," 2013.

[14] G. Jacob, H. Debar, and E. Filiol, "Behavioral detection of malware: from a survey towards an established taxonomy," *Journal in Computer Virology*, vol. 4, pp. 251–266, Feb. 2008.

[15] S. Salam, D. Maged, and D. Mahmoud, "Malware detection in cloud computing," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 4, 2014.

[16] Microsoft, "Out of sight but not invisible: Defeating fileless malware with behavior monitoring, amsi, and next-gen av."

[17] N. M. Ransom, "conselhos de prevenção."