RANSOMWARE: ORIGENS, CONSEQUÊNCIAS E PREVENÇÃO

Danilo Pereira de Freitas[1], Napoleão Povoa Ribeiro Filho[2]

[1]Estudante do Curso Superior de Tecnologia em Sistemas para Internet – IFTO. e-mail: <danilop.freitas19@gmail.com>
[2]Mestre em Modelagem Computacional de Sistemas – UFT. e-mail: <napoleao@ifto.edu.br>

Resumo: *Ransomware* é um *software* que tem a finalidade de extorquir digitalmente as vítimas, fazendo-as pagar um valor específico, geralmente em *bitcoin*, que é um tipo de moeda digital. Diante disso, percebe-se que ele apresenta grande relevância entre os crimes virtuais praticados nos dias atuais. Esse artigo tem por objetivo identificar os principais motivos que levam os *ransomwares* a ainda conseguirem ter acesso não autorizado aos computadores. Para tanto, buscou-se conceituar *malwares* e *ransomwares*, identificar as falhas que já foram exploradas, os mecanismos de disseminação e por fim, foram apresentadas algumas medidas de precaução contra essas ameaças.

Palavras–chave: cibercrime, malware, ransomware, segurança, vulnerabilidade

1 INTRODUÇÃO

Os *softwares* maliciosos, conhecidos como *malwares*, surgiram em 1971 (COZZOLINO, 2012). De acordo com (CERT.BR, 2012), o termo *malware* (proveniente do inglês *malicious software*) é usado para classificar um *software* destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações. Ainda, Sultan et. al (2018) afirma que tais programas são projetados especificamente para obter acesso e provocar danos no computador da vítima.

No contexto atual, existem *malwares* com grande potencial de infecção, e um deles é um *software* que tem a finalidade de extorquir digitalmente as vítimas, fazendo-as pagar um valor específico geralmente em *bitcoin*, que é um tipo de moeda virtual, conhecido como *ransomware*. O primeiro *ransomware* apareceu em 1989 e ficou conhecido como *Trojan* AIDS (LISKA e GALLO, 2017). Hoje existem diversos tipos e estão distribuídos em várias famílias (tipos de *ransomwares* que possuem o mesmo núcleo de código).

No cenário atual de crimes pela internet, percebe-se que os *ransomwares* tem grande relevância, sendo um dos tipos de *malwares* mais utilizados, pois estão associados diretamente a um possível retorno financeiro que podem gerar para os seus administradores (LISKA e GALLO, 2017). Em virtude das informações apresentadas até aqui, este artigo estabelece a seguinte problemática: por que os *malwares* do tipo *ransomware* ainda conseguem alcançar um alto nível de propagação? Para responder essa pergunta vamos investigar os principais motivos que levam os *ransomwares* a conseguirem um alto grau de disseminação.

ISSN 2179-5649
X JICE©2019

2 JUSTIFICATIVA

Ainda nos dias atuais, o *ransomware* é um grande problema, possui uma grande variedade de tipos e tem um alcance cada vez maior. Tal *malware* infecta (é executado de forma não autorizada) tanto computadores do tipo *desktop* e *laptop* quanto dispositivos móveis. As pessoas envolvidas no desenvolvimento desses *softwares*, que aqui chamaremos de cibercriminosos, estão desenvolvendo técnicas ainda mais sofisticadas com o intuito de impactar os mais diversos sistemas, aumentando o número de possíveis vítimas.

Atualmente existe uma infinidade de variantes de *ransomwares*, todos com o objetivo de obter retorno financeiro dos computadores infectados ao redor do mundo. O número de computadores impactados é muito alto. O FBI (*Federal Bureau of Investigation*), ou Departamento Federal de Investigação dos Estados Unidos que é o equivalente à Polícia Federal do Brasil, estima que o montante total de pagamentos de resgate se aproxima de US$ 1 bilhão por ano (MORGAN, 2019). Esses números revelam a significância do estudo e a necessidade de compreensão do comportamento desse tipo de *software* malicioso.

3 METODOLOGIA

A pesquisa deste trabalho é de caráter exploratório e descritivo, com apresentação de análises qualitativas e quantitativas. Neste sentido, a intenção é identificar na literatura os principais estudos relacionados ao tema proposto, desde a sua criação até os dias de hoje, abordando os riscos e as precauções. Quanto às fontes de dados foram utilizados livros, artigos, relatórios, reportagens e cartilhas relacionadas ao tema.

4 REFERÊNCIAL TEÓRICO

4.1 Origem dos Malwares

A história dos *malwares* se inicia no ano de 1971 com o vírus “Creeper” que se replicou na rede ARPANET, uma precursora da Internet. Conforme Cozzolino (2012), tal *software* foi feito por Bob Thomas para demonstrar a viabilidade de um programa autorreplicante, ou seja, que se duplica sozinho. Era inofensivo, apenas apresentava uma mensagem na tela do computador infectado.

Como exposto no parágrafo anterior, os *malwares* surgiram há quase 50 anos. Desde então, apresentam uma evolução constante, de acordo com o desenvolvimento de novas tecnologias e cada vez mais pessoas utilizando equipamentos conectados na internet. No trabalho de Cardoso (2018) é dito que no final dos anos 80 e início dos anos 90 a internet começava a ganhar força, e foram surgindo novos *malwares* com objetivo de infectar o maior numero de sistemas que conseguissem.

Nessa linha cronológica, percebe-se que os *malwares* se consolidaram de forma muito eficiente de obter algum tipo de vantagem através das redes de computadores. E hoje esses *softwares* estão cada vez mais perigosos. Atualmente existem *softwares* maliciosos dos mais variados tipos, como *worms*, cavalos de troia, *ransomwares* entre outros.

4.2 Conceito de Ransomware

O termo *ransomware* é usado para descrever uma classe de *malware* utilizado para extorquir digitalmente as vítimas, fazendo-as pagar um preço específico. Liska e Gallo (2017) afirma em seu livro que tal *software* é um código malicioso que tem a finalidade de sequestrar os dados do usuário e, posteriormente, solicitar um valor de resgate por esses dados.

O *ransomware* é um dos tipos de *malwares* mais conhecidos do mundo e tem sua origem em um código malicioso conhecido como AIDS, tem esse nome porque foi usado pela primeira vez em uma conferência sobre AIDS (*Acquired Immunodeficiency Syndrome*, ou Síndrome da Imunodeficiência Adquirida), escrito em 1989 por Joseph Popp (CANDIDO et. al, 2018). Sabe-se que esse código substituía o arquivo AUTOEXEC.BAT do sistema operacional Microsoft Windows, e permitia 90 reinicializações do sistema até ocultar os diretórios e alegar que criptografaria os arquivos. Com o passar do tempo foram feitas análises mais detalhadas e descobriu-se que os nomes dos arquivos eram embaralhados com uma criptografia simples de chave simétrica. O código malicioso podia ser removido usando alguns programas como AIDSOUT e CLEARAID (ZAGHETTO, 2017). Mais informações sobre o cavalo de Toria AIDS e sobre os programas usados para remoção do mesmo podem ser encontradas no trabalho de Jim Bates, publicado no *Virus Bulletin*[1]. Desse ponto inicial até o atual estágio em que se encontram os *ransomwares*, é possível perceber o quanto esse tipo de *software* evoluiu e fica cada vez mais complexo e especializado.

Os *ransomwares* são subdivididos em famílias e cada uma tem sua característica. Mas a essência na forma de agir são duas: existem os que criptografam os arquivos que são conhecidos como " Cryptoransomware ", e os que bloqueiam o acesso total do usuário ao sistema "lockerransomware."

Como já se sabe a motivação financeira é um fator crucial para o aumento dos casos de infecções por *ransomwares* nos últimos anos. Com base nessa afirmação retirada do relatório anual de cibercriminalidade apresentado em (MORGAN, 2019), temos a percepção do quanto esse assunto é atual e significativo, gerando transtorno financeiro às suas vítimas e também causando uma sensação de insegurança entre as pessoas menos familiarizadas com o tema em questão.

4.3 Ransomware como um serviço

Uma variante mais recente dos *ransomwares* é o RaaS ou *ransomware* como um serviço. É um modelo de negócio criado por hackers que possibilita que os cibercriminosos iniciantes, sem experiência ou capacidade técnica, consigam produzir e entregar *ransomwares* em um curto período de tempo tirando proveito de recursos existentes para disseminá-los de maneira mais abrangente (SECURITY, 2019).

Com o surgimento do *The Onion Router* (TOR), um *software* de código aberto que garante total privacidade ao navegar na internet, ficou mais fácil para os hackers mais habilidosos oferecerem seus serviços a outras pessoas (ABRAMS, 2018). Devido a isso, o RaaS tem ganhado espaço no mercado clandestino, permitindo a hackers colocarem anúncios de seus serviços em vários sites TOR.

1 BATES, J. **AIDS Information Version 2.0**. 1990. Disponível em: https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf. Acesso em: 22 out. 2019.

4.4 Famílias de Ransomwares

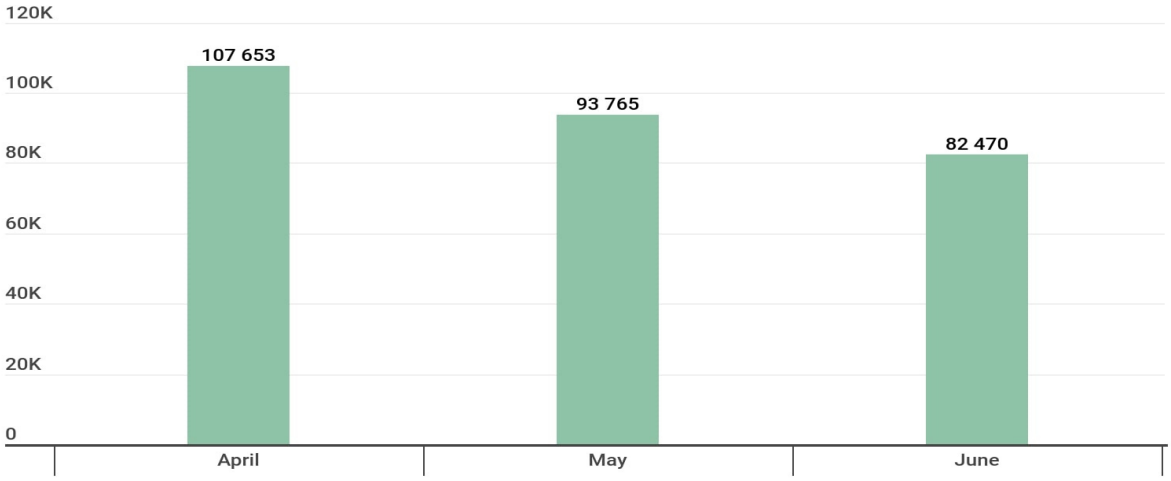
Um *ransomware* pode obter diversas variantes de um mesmo código. Essas variantes, por possuírem o mesmo núcleo de *software*, são chamadas de família de *ransomwares*. Existem duas gerações principais de famílias. A primeira era distribuída de forma desordenada, havia pouca organização entre as várias equipes de cibercriminosos dos primeiros *ransomwares*. Já na segunda geração o cenário começou a mudar e as equipes passaram a ser bem mais organizadas (LISKA e GALLO, 2017). De acordo com Hull et. al (2019), existem diversas famílias com originalidade e nível de infecção alto, como exemplo temos Cerber, Chimera, CTB-Locker, DonaldTrump, Jigsaw, Petya, Reveton, Santana, TeslaCrypt, TorrentLocker, WannaCry, CryptoLocker, Odin, Shade, Locky, Spora, CryptorBit, CryptXXX e CryptoWall.

Por exemplo, Cerber é considerada a primeira família de *ransomware* da segunda geração. Ela tem como características: uma equipe bem financiada, um ciclo curto de lançamento de versões e uma equipe que está constantemente investigando novos métodos para evitar que ele seja detectado. Suspeita-se que seus criadores são da Rússia. O *ransomware* não criptografava vítimas com computadores na Rússia e os primeiros anúncios clandestinos para os serviços Cerber foram postados em fóruns russos (HELP, 2016).

4.5 Casos reais de infecção por Ransomwares

Os casos reais de infecções por *ransomwares* são muitos. Na figura 1 temos o número de usuários atacados por *Trojans* (programa malicioso, que se infiltra na máquina disfarçado de um programa comum e legítimo) de *ransomware* no segundo trimestre de 2019.

Figura 1 – Número de usuários atacados por *Trojans* de *ransomware*, segundo trimestre de 2019



Fonte: Kaspersky (2019)

Para um melhor entendimento sobre esse *malware*, a seguir serão apresentados alguns dos mais famosos casos acontecidos nos últimos anos. Para cada caso, serão mencionadas algumas características de cada família de *ransomware*.

4.5.1 TeslaCrypt

O TeslaCrypt tinha um modo inteligente de agir, se passando por arquivos auxiliares associados a jogos de computadores e conteúdo para *download* que eram armazenados localmente no computador pelos usuários. Ele foi usado em campanhas (ataques de *ransomwares*) do início de 2015 até maio de 2016 (CIO, 2019).

Apesar de não ser a família de *ransomware* mais amplamente implementada, o TeslaCrypt gerou muito lucro ao seu criador. Estima-se que tenha gerado cerca de 500 mil dólares (LISKA e GALLO, 2017), no período de apenas um ano. Em maio de 2016 surpreendendo a todos, o seu criador disponibilizou a sua chave privada (senha utilizada para descriptografar arquivos) para o mundo e se desculpou pelos danos causados. Para atingir tamanha proporção ele tinha a capacidade de se autorreplicar, o que é uma característica dos *worms*.

Seus criadores decidiram cessar suas operações, pois os números de computadores infectados e resgates obtidos atingiram proporções muito grandes, atraindo atenção à nível mundial, o que poderia ocasionar maiores investigações sobre os criminosos.

4.5.2 WannaCry

Talvez o *ransomware* mais bem-sucedido seja o cryptoworm WannaCry. Como é mostrado em (AVAST, 2019), ele chegou à manchete em maio de 2017 quando afetou mais de 230.000 computadores em centenas de países, incluindo o Serviço Nacional de Saúde do Reino Unido, hospitais na Ucrânia e estações de rádio na Califórnia. O Brasil, inclusive, foi um dos países mais afetados.

O WannaCry se auto propagava e explorou uma vulnerabilidade do *Windows* que foi publicada pela primeira vez no Boletim de Segurança da Microsoft MS17-010 (documento onde a Microsoft publica as atualizações de segurança), lançado em meados de março de 2017. A Microsoft declarou que essa atualização era crítica para todas as versões suportadas do sistema operacional *Windows*. Como apresentado em (AVAST, 2019), a Microsoft já havia disponibilizado um *patch* (programa de computador criado para atualizar ou corrigir um *software*) para tratar o problema, mas muitos usuários não atualizaram o sistema e acabaram sendo vítimas do ataque em massa.

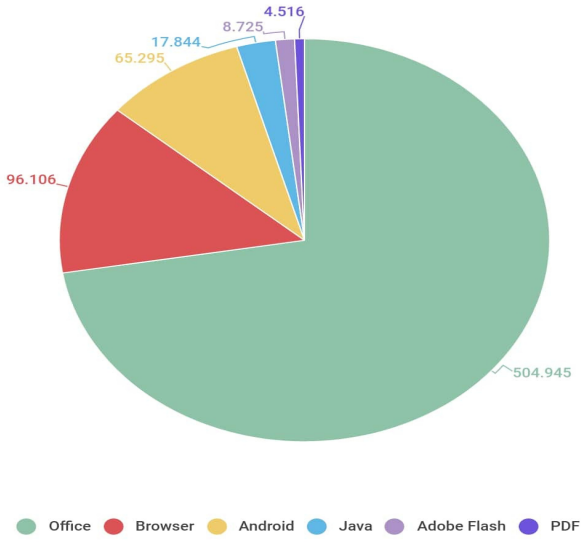
4.6 Falhas que os *ransomwares* já exploraram

As falhas são inúmeras e uma delas está no próprio usuário final, que na maioria das vezes não tem o cuidado necessário para navegar na grande rede, podendo clicar em links de páginas mal intencionadas ou baixar e executar arquivos maliciosos, ocasionando assim a infecção do sistema. Os *ransomwares* se aproveitam de falhas em diversos *softwares* como Internet Explorer, Pacote Office, Silverlight, Google Chrome, Mozila Firefox, Apple Safari, Adobe PDF, Adobe Flash e em vários outros que possam ter contato direto ou indireto com a internet. Para conseguirem se infiltrar nos sistemas operacionais usam kits de *exploit*, que são pacotes de códigos criados para explorar vulnerabilidades específicas de um *software* em particular. Na figura 2 vemos quais são os *softwares* mais explorados pelos *ransomwares*.

No sentido de tentar minimizar os efeitos dos softwares maliciosos, foi criado o CVE (*Common Vulnerabilities and Exposures*, ou vulnerabilidades e exposições comuns), que é uma

iniciativa colaborativa de diversas organizações de tecnologia e segurança. Nessa iniciativa são criadas listas de nomes padronizados para vulnerabilidades e outras exposições de segurança. Conforme análise apresentada em Liska e Gallo (2017), o padrão mais explorado de 2015 foi o CVE-2012-0158, que é uma vulnerabilidade do Microsoft Word.

Figura 2 – Explorações usadas por cibercriminosos, por tipo de aplicativo usado, segundo trimestre de 2019



Fonte: Kaspersky (2019)

Em 2019 as explorações em falhas no pacote Microsoft Office continuam aumentando, passando de 67% para 72% no segundo trimestre. De acordo com (KASPERSKY, 2019), as vulnerabilidades do pacote Office mais exploradas nos últimos anos foram CVE-2017-11882, CVE-2018-0798, CVE-2018-0802, CVE-2017-8570 e CVE-2017-8759.

4.7 Mecanismos de disseminação utilizados pelos *ransomwares*

De acordo com Zaghetto (2017), o principal meio para disseminação dos *ransomwares* se dá através de e-mails, e precisam da interação com o usuário para serem executados e assim conseguirem se infiltrar na máquina. Diante dessas informações, os atacantes passaram a usar nomes de empresas conhecidas em seus e-mails fraudulentos. Com isso aumentaram as chances de um usuário confiar e clicar no *link*. Além desse, existem outros métodos, como o spam de restituição, que usa logos comuns e informações pessoais para fazer as pessoas acreditarem que estão recebendo uma restituição.

De acordo com Saísse (2016), *ransomwares* podem ser propagados de diversas maneiras, seja por intermédio de acesso aos sites suspeitos que liberam o código malicioso apenas com a visita do usuário ou por arquivos disfarçados que normalmente são divulgados em redes sociais ou enviados por e-mail aparentando algo comum, de interesse público. Ainda podem ser liberados via instalação de aplicativos vulneráveis em dispositivos móveis ou computadores.

Para encontrar novas vítimas, os meios de disseminação são muitos, e vão se adequando de acordo com as novas tecnologias. Com esse objetivo, e de acordo com Sultan et. al (2018), os criminosos virtuais passaram a usar kits de *exploit*, para entregarem *malwares* usando redes de

malvertisement (propagandas maliciosas) que servem para redirecionar os usuários para sites que vão disseminar ***softwares*** indesejados para assim, infectar o hospedeiro.

4.8 Medidas que os usuários podem tomar para se precaver contra os *ransomwares*

Como apresentado em Saísse (2016), a força tarefa internacional (união entre a Polícia Nacional Holandesa, a Europol, a Intel Security e a Kaspersky para combater o *ransomware*), elencou seis tópicos para prevenção e reação ao *ransomware*, que são os seguintes:

1 - *Backup*: é a cópia dos arquivos importantes, sempre faça.

2 - Antivírus: são *softwares* que combatem os programas maliciosos, tenha um bom antivírus.

3 - Atualização Contínua: é importante que seu sistema operacional esteja sempre atualizado.

4 - Desconfie Sempre: nunca clicar em links sem ter certeza de que seja legitimo.

5 - Exibir Extensões de Arquivos: define seu formato, nunca baixe um executável.

6 - *Off-line*: se perceber algum arquivo suspeito, desligue o dispositivo e a internet.

5 CONSIDERAÇÕES FINAIS

Como apresentado anteriormente, os *ransomwares* se tornaram um negócio que movimenta muito dinheiro. E como ainda existem inúmeras vulnerabilidades nos *softwares*, os criminosos acabaram se aprofundando de maneira intensa em busca de explorá-las. Contudo, os estudiosos, as companhias especializadas em segurança cibernética e as forças policiais e de inteligência estão em constante cooperação para combater este inimigo comum e destrutivo.

Os *ransomwares* podem ser classificados em Cryptoransomware e lockerransomware. É comum que vários desses *malwares* utilizem o mesmo código base, o que faz com que os mesmos sejam classificados como uma família. Normalmente *ransomwares* se associam a outros *softwares* maliciosos para se disseminar e exploram falhas específicas de *software* para infectarem os computadores.

Os principais motivos para que os *ransomwares* ainda tenham um alto índice de infecção é a sua constante evolução como “negócio”, a alta capacidade técnica dos cibercriminosos e a facilidade que eles têm em disponibilizar seus serviços para “hackers” leigos. Entretanto, existem medidas simples que, se bem observadas minimizam bastante a possibilidade desse tipo de *malware* causar algum tipo de transtorno.

REFERÊNCIAS

ABRAMS, L. **Princess Evolution Ransomware is a RaaS With a Slick Payment Site**. 2018. Disponível em: https://www.bleepingcomputer.com/news/security/princess-evolution-ransomware-is-a-raas-with-a-slick-payment-site/. Acesso em: 26 set. 2019.

AVAST. **Wannacry**. 2019. Disponível em: https://www.avast.com/pt-br/c-wannacry. Acesso em: 16 ago.2019.

BATES, J. **AIDS Information Version 2.0**. 1990. Disponível em: https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf. Acesso em: 22 out. 2019.

CARDOSO, E. **Uma breve história dos malwares**. 2018. Disponível em: https://wardocardoso.com/malwares/artigo-uma-breve-historia-dos-malwares/. Acesso em: 20 jul. 2019.

CERT.BR. **Cartilha de Segurança para Internet**. 2012. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 03 jun. 2019.

CIO. **Os 6 maiores ataques dos últimos 5 anos**. 2019. Disponível em: https://cio.com.br/os-6-maiores-ataques-de-ransomware-dos-ultimos-5-anos/. Acesso em :04 jun. 2019.

COZZOLINO, M. F. (2012). **Detecção de variantes metamórficas de malware por comparação de códigos normalizados**.

HELP, N. S. 2016. **The inner workings of the Cerber ransomware campaign**. Disponível em: https://www.helpnetsecurity.com/2016/08/17/inner-workings-cerber-ransomware-campaign/. Acesso em: 26 set. 2019.

HULL, G., JOHN, H., and ARIEF, B. (2019)**. Ransomware deployment methods and analysis: views from a predictive model and human responses**. Crime Science, 8(1):2. Disponível em: https://doi.org/10.1186/s40163-019-0097-9. Acesso em: 02 jul. 2019.

KASPERSKY. **IT threat evolution Q2 2019. Statistics.** Disponível em: https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/. Acesso em: 18 set. 2019.

LISKA, A. GALLO, T. **Ransomware: Defendendo-se da Extorsão Digital.** São Paulo: Novatec, 2017.

MORGAN, S. **The 2019 official annual cybercrime report.** Herjavec group. Disponível em: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report. Acesso em: 05 jun. 2019.

SAÍSSE, R. C. **Ransomware: Sequestro de dados e extorsão digital.** 2016. Disponível em: http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/. Acesso em: 25 jun. 2019.

SECURITY, R. **Dark Web é o lugar onde negócios Ransomware as a Service são fechados e multiplicados**. 2019. Disponível em http://www.securityreport.com.br/overview/dark-web-e-o-lugar-onde-negocios-de-ransomware-as-a-service-sao-fechados-e-multiplicados/#.XZNwcFVKiM9. Acesso em: 26 set. 2019.

CANDIDO, J. W., BORGES, J. H. G., and FLORIAN, F. 2018. **Segurança da informação com foco na propagação iminente de ransomware nas corporações.** Simpósio de Tecnologia da Fatec.

SULTAN, H., KHALIQUE, A., ALAM, S. I., and TANWEER, S. (2018). **A survey on ransomware: Evolution, growth, and impact**. International Journal of Advanced Research in Computer Science.

ZAGHETTO, C. 2017. **Ransomware: Este problema também pode ser seu.** Tecnologias em projeção.