Técnicas de Proteção Contra Ameaças Digitais do Tipo Ransomware em Plataformas Windows

Gabriel F. Pereira1, Rogério A. Casagrande1[1]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) - Criciúma – SC – Brasil

gabrielfernandesfg@hotmail.com, roc@unesc.net

Abstract. *With the advent of an increasingly connected world, many security breaches open up for cyber criminals. Electronic crimes are now the biggest challenge for any company in the world and this problem is reflected in the numbers, reaching trillions of dollars in annual losses. This work aims to carry out an experimental evaluation of tools against Ransomware-type threats. The experiments were conducted using two tools, one specific for protection against Ransomware and an antivirus. For the execution of the tests, two samples of known Ransomwares were used. The results showed that, in general, modern tools have what it takes to protect devices from these threats.*

Resumo. *Com o advento de um mundo cada dia mais conectado, muitas brechas de segurança se abrem para cibe criminosos. Os crimes eletrônicos são hoje o maior desafio de qualquer companhia no mundo e este problema se reflete nos números, chegando na casa de trilhões de dólares em prejuízos anuais. Este trabalho tem como objetivo realizar uma avaliação experimental de ferramentas contra ameaças do tipo Ransomware. Os experimentos foram conduzidos utilizando-se duas ferramentas, sendo uma específica para proteção contra Ransomware e um antivírus. Para a execução dos testes foram utilizadas duas amostras de Ransomwares conhecidos. Os resultados demonstraram que, no geral, ferramentas modernas têm o que é necessário para proteger os dispositivos destas ameaças.*

1. Introdução

A sociedade moderna está cada vez mais conectada e atualmente não estar conectado pode ser um fator exclusivo no panorama recente, pois muitas oportunidades podem ser perdidas. A informação é cada vez mais valiosa, mas, ao mesmo tempo extremamente frágil [Machado 2014].

Isto torna-se ainda mais evidente no ambiente corporativo devido à importância dos dados que podem facilmente ser perdidos através da utilização de programas maliciosos. Programas maliciosos podem ser usados em ataques direcionados para interromper recursos de computação e torná-los indisponíveis [Grégio et al. 2014].

De acordo com [Cybersecurity Ventures 2017], os crimes eletrônicos são hoje o maior desafio de qualquer companhia no mundo e este problema se reflete nos números. Em 2015 o prejuízo anual com este tipo de ameaça já alcançava 3 trilhões de dólares anualmente e estes números continuam crescendo. Outro dado que confirma o aumento destas ameaças é o número de vagas na área de segurança da informação que cresce anualmente, com um milhão em 2016 e expectativa de

crescimento para os anos seguintes.

Um dos tipos mais conhecidos destas ameaças digitais são os Ransomwares, esta ameaça surgiu no final da década de 1980, más realmente se tornou algo relevante após 2005. Isto ocorreu devido às mudanças tecnológicas que aconteceram nesta época [Kevin Savage et al. 2015]. Um dos fatores decisivos nesta mudança foi a evolução de poder computacional dos dispositivos e também a criação de métodos de criptografia mais avançados, fazendo assim com que cada vez se tornasse mais complexo o desbloqueio dos dados em caso de infecção [Liska and Gallo 2017].

A criptografia não surgiu com o advento dos Ransomwares, a mesma já possuiu diversas outras utilidades ao longo da história, já foram criados mecanismos de codificação chamados de códigos, cifras e senhas, sendo muito utilizados para manter a segurança de uma mensagem [Olgin and Groenwald 2011].

Já na computação a criptografia geralmente se utiliza de funções *hash* para garantir a integridade do conteúdo da mensagem, esses *hashs* são gerados através de um calculo matemático, qualquer modificação em seu conteúdo pode facilmente ser detectada, pois novos cálculos matemáticos são necessários para se obter um novo resultado [Ludwig et al. 2020]. A criptografia tem como seu grande objetivo trazer a privacidade dos dados, isto vem através da chave criptografia, que enquanto for secreta, longa e aleatória, dificilmente estes dados serão acessados [Camara and Rocha Jr. 2012].

Os Ransomwares se encaixam em uma categoria de ameaças que atuam com o objetivo de extorquir digitalmente suas vítimas. Eles geralmente podem ser divididos em dois tipos principais. O primeiro tipo age, criptografando e negando acesso aos dados do dispositivo afetado, o segundo tipo restringe e impede o usuário de acessar a dados e arquivos, neste caso não necessariamente as restrições são feitas através de criptografia [Kevin Savage et al. 2015]. Neste tipo de sequestro de dados, é exigido um valor de resgate para que o acesso seja restabelecido ao dispositivo ou dados, e geralmente este pagamento é exigido em criptomoedas Bitcoin para dificultar o rastreio dos criminosos [Gorman and McDonald 2012].

Diferentes variantes e famílias deste tipo de ameaça surgem todos os anos, espalhando os Ransomwares cada vez mais rapidamente [FERREIRA 2018]. Este tipo de ameaça também não se limita há apenas um tipo de sistema operacional ou de dispositivo, podendo ser desde aparelhos android, IOS ou até mesmo Windows, todos podem ser afetados, se limitando apenas a características de cada tipo de sistema [Liska and Gallo 2017].

Conforme “Evolution of Ransomware” [O’Kane et al. 2018], os ataques Ransomware podem ocorrer de 4 maneiras distintas: A primeira infecta o alvo através de um download sem conhecimento do usuário em um site comprometido, a segunda é chamada *de Strategic web compromise*, que são sites contaminados que monitoram os acessos e fazem um levantamento de usuários mais vulneráveis e de suas fragilidades, atingindo muitas vezes usuários que possuem um antivírus desatualizado ou que fazem transações financeiras sem proteção. A terceira maneira é o disparo de e-mails, que

possuem mensagens que induzem o usuário a fazer uma ação e geralmente são distribuídos em larga escala podendo conter ameaças ou links redirecionando para sites maliciosos. E por último, a quarta maneira é a exploração de vulnerabilidades específicas de uma empresa, ou de um sistema específico [Liska and Gallo 2017].

Um Ransomware também pode se utilizar de diversas técnicas para se manter escondido dentro de um sistema infectado e proteger a identidade de seus criadores e distribuidores. De acordo com [Gonzalez and Hayajne 2017], algumas das maneiras são: Encriptar a comunicação com servidores de controle para evitar a detecção no tráfego de rede, pode-se utilizar de técnicas de *Sandbox*, também é possível que que o mesmo se utilize de técnicas de polimorfismo, permitindo assim que o Ransomware mude de forma, mas mantenha sua funcionalidade, dentre outras maneiras.

A informação precisa ser protegida de maneira adequada, principalmente conforme os negócios se tornam cada vez mais conectados. Esta informação está cada vez mais exposta a um crescente número de ameaças e a uma grande variedade de vulnerabilidades [ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS 2005].

Segundo [Oliveira 2001], um dos pontos mais importantes da segurança da informação é o ser humano, onde todo processo se inicia e é finalizado com um.

Nestes casos e cenários pode-se observar que o usuário é na maioria das vezes a porta de entrada é o personagem principal deste tipo de ameaça.

2. Materiais e Métodos

Para a realização dos experimentos foram selecionadas duas amostras de Ransomwares reais: WannaCry, ameaça que ficou mundialmente conhecida no ano de 2017 por afetar diversas companhias e causando grandes perdas financeiras, e Bad Rabbit, ameaça que também se espalhou no ano de 2017, mas que infectou primariamente a Rússia e também a Ucrânia, com alguns relatos de ataques na Alemanha, Turquia, Bulgária e Japão.

Os testes foram realizados utilizando-se de uma máquina virtual, configurada em uma plataforma VMWare Workstation, com 4 gigabytes de memória ram e quatro núcleos.

Todos os acessos externos, como rede e entradas USB... para evitar que qualquer tipo de ameaça se espalhe para a máquina física, também foi optado por desativar o Windows Defender do sistema operacional, para que as ferramentas escolhidas fossem a única linha de defesa do dispositivo

2.1. Máquina Virtual

A ferramenta escolhida para hospedar as máquinas virtuais foi a VMWare Workstation, uma máquina virtual foi criada com uma configuração intermediária, com quatro gigabytes de memória ram, quatro cores e um disco de vinte gigabytes.

As características escolhidas se deram para que a máquina virtual se assemelhasse a uma máquina de uso comum.

O sistema operacional escolhido foi o Windows 10 em sua versão 2004, nenhum software específico além dos selecionados na pesquisa foi instalado na máquina que não fosse padrão do sistema operacional.

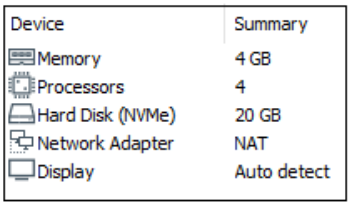

Figura 1. Configuração do dispositivo

2.2. Ransomwares escolhidos

Para a realização dos testes foram escolhidas duas amostras de Ransomwares específicos e já conhecidos pelo público geral, isto foi adotado para que os testes fossem o máximo possível de um ambiente real.

O primeiro escolhido foi o WannaCry, Ransomware mundialmente conhecido no ano de 2017 em sistemas operacionais do tipo Windows, afetando milhares de dispositivos neste mesmo ano, escolhido por ter sido mundialmente conhecido.

O Ransomware utiliza-se de criptografia do tipo assimétrica. De acordo com [BERRY; HOMAN; EITZMAN 2017], o mesmo se utiliza de uma lista de chaves do tipo Rivest-Shamir Adleman (RSA) para realizar a encriptação dos dados e arquivos da vítima, sendo que esta lista possui chaves públicas e genéricas.

A ameaça realiza a encriptação de todos os dados, evitando arquivos de sistema ou outros arquivos que podem comprometer o funcionamento do dispositivo, logo após ele irá se comunicar com um servidor do tipo *Onion* utilizando-se de um servidor Tor sendo executado na porta 9050.

Caso a conexão ocorra com sucesso, o mesmo registra o sistema da vítima com o servidor Onion, faz a transferência das chaves utilizadas na encriptação dos dados e apaga qualquer cópia das mesmas que possam estar salvas no sistema.

Se a vítima realizar o pagamento exigido pela ameaça, o mesmo se comunica com o servidor Onion, obtém a chave privada que será utilizada na descriptografia e realiza o processo em todos os arquivos que previamente foram bloqueados.

A segunda amostra utilizada foi do Ransomware BadRabbit, uma ameaça também difundida no ano de 2017, mas ficando mais conhecida apenas em países da Europa.

2.3. Ferramentas de defesa

Quanto ao quesito prevenção, há muitas maneiras de se evitar os ataques, como é relatado por [Saxena and Soni 2018], algumas são bastante simples para se aplicar, como por exemplo manter o sistema operacional utilizado sempre atualizado.

O SO atualizado por si só já conseguirá prevenir não apenas de ameaças do tipo Ransomware, mas também de muitas outras ameaças cibernéticas. Manter um antivírus no dispositivo e mantê-lo atualizado também é uma maneira efetiva para manter o sistema prevenido contra estas ameaças. Geralmente as ferramentas de antivírus já possuem cadastrados em suas bases de dados os Ransomwares já conhecidos e maneiras de detectá-los caso eles invadam o dispositivo.

Uma outra maneira de proteção é ter sempre cópias de segurança dos arquivos, que não irá prevenir a invasão do dispositivo pelo Ransomware, mas irá garantir que a perda pelo ataque seja mínima. Outra estratégia simples que pode ser utilizada é evitar abrir e-mails suspeitos, sendo este um dos maiores vetores de Ransomwares.

Há também estratégias mais específicas para combate de deste tipo de ameaça segundo [Saxena and Soni 2018], algumas delas são:

a) monitorar chamadas em Application Programming Interface (APIs): alguns Ransomwares se utilizam de interfaces específicas do sistema operacional para realizar o bloqueio de arquivos, uma ferramenta de monitoramento de chamada nestas APIs pode auxiliar na detecção de Ransomwares ao detectar uso indevido das mesmas;

b) monitorar o sistema de arquivos: um Ransomware geralmente tem o comportamento de encriptar os arquivos do sistema da maneira mais rápida possível, algum tipo de monitoramento no sistema de arquivos do sistema procurando por este comportamento pode auxiliar na detecção de um ataque que já esteja em andamento;

c) arquivos de isca: muitas famílias de Ransomwares utilizam-se deste processo agressivo de encriptação dos arquivos da vítima, tornando possível a utilização das técnicas descritas acima para a detecção dos mesmos. Mas alguns Ransomwares já prevendo estas técnicas se utilizam de técnicas para que as mesmas não funcionem.

A estratégia mais comum é ao atacar o sistema da vítima simular um comportamento comum no sistema de arquivos e em chamadas de API, assim tornando as técnicas descritas acima inúteis, então se utilizar de arquivos de isca pode ser uma estratégia muito promissora para detectar estes ataques a sistemas. Geralmente

ferramentas de defesa se utilizam da assinatura das ameaças para detectar a ameaça no dispositivo, através da utilização de APIs para a detecção se faz possível detectar o Ransomware no dispositivo a partir do dia um [Cheng et al. 2019].

2.4. Avaliação Experimental

Para a realização desta pesquisa foram selecionadas duas ferramentas, uma ferramenta genérica, neste caso um antivírus é uma ferramenta criada especificamente para a defesa de sistemas contra ameaças do tipo Ransomware.

A ferramenta específica escolhida foi o ZoneAlarm Anti-Ransomware, está ferramenta é desenvolvida especificamente para ameaças do tipo Ransomware, de acordo com ZoneAlarm, a ferramenta possui compatibilidade com todos os antivírus do mercado, há funcionalidade de restauração de arquivos encriptados.

A ferramenta trabalha analisando comportamentos suspeitas no dispositivo, ao detectar um Ransomware a ferramenta realiza o bloqueio e restauração dos arquivos afetados pelo mesmo.

Segundo algumas análises, a ferramenta é bastante efetiva, possuindo alguns pontos positivos, como, proteção com sucesso de amostras reais de Ransomwares, simplicidade no uso e uma boa limpeza de rastros de ameaças no sistema.

A ferramenta genérica escolhida foi o McAfee Antivírus, uma ferramenta de defesa mundialmente conhecida, sendo utilizada por mais de 500 milhões de dispositivos. Segundo a própria desenvolvedora da ferramenta, ela é capaz de defender não apenas o usuário, mas toda a família contra os últimos vírus, ameaças, *spywares* e Ransomwares conhecidos, mantendo a privacidade e a identidade do usuário.

Ele também possui uma camada específica de proteção contra Ransomwares, chamada de Ransom Guard. A proteção em tempo da ferramenta já é responsável pela detecção de boa parte dos Ransomwares conhecidos, esta camada de proteção adicional vem em casos onde a proteção comum não é suficiente.

O Ransom Guard monitora arquivos suspeitos, ao detectar tentativas de encriptação de arquivos o mesmo realiza cópias de segurança dos mesmos e continua analisando o comportamento. Ao confirmar que se trata de um Ransomware, o mesmo é colocado em quarentena e os arquivos encriptados são restaurados através da cópia de segurança.

2.4.1. Definição dos testes

Para a realização dos testes uma premissa precisou ser estabelecida, a desativação da ferramenta Windows Defender. Este trabalha como um antivírus integrado diretamente com o sistema operacional, o mesmo tem como objetivo a remoção de ameaças, trojans, spywares e etc. A escolha se deu para que fosse possível avaliar única e exclusivamente o desempenho da ferramenta escolhida sem interferência de outras ferramentas de defesa do próprio sistema operacional.

Foram definidos cinco cenários para a realização dos testes, com o intuito de se aproximar ao máximo de uma utilização real de um dispositivo que foi infectado por uma dessas ameaças: Primeiro, a ferramenta McAfee com uma amostra do Ransomware WannaCry; o segundo foi a mesma ameaça com a mesma ferramenta, mas com a varredura da ferramenta desativada; o terceiro cenário foi a utilização da ferramenta ZoneAlarm Anti Ransomware com uma amostra da ameaça Wanna Cry; no quarto cenário uma amostra do Ransomware BadRabbit foi testada com a ferramenta específica ZoneAlarm AntiRansomware e no último a ferramenta McAfee Antivírus foi testada com a segunda amostra, o Bad Rabit.

Os testes foram realizados da seguinte maneira: uma das duas ferramentas foi instalada no dispositivo, após isso uma cópia da amostra de Ransomware foi colocada no equipamento e logo após a mesma foi executada para que fosse possível verificar a efetividade da ferramenta.

Cada ferramenta foi testada com cada amostra de Ransomware cinco vezes. A análise posterior dos resultados se deu de maneira qualitativa, observando-se alguns pontos específicos, como: se a ferramenta alerta o usuário da infecção que está ocorrendo, o tempo que a ferramenta leva para alertar o usuário, a clareza da informação que está sendo passada para o usuário e o comportamento da ferramenta perante aos arquivos afetados, verificando se após o ataque todos os arquivos se mantêm sem nenhum tipo de criptografia ou comprometidos.

2.4.2 Resultados

Todas as ferramentas foram testadas com as amostras selecionadas e algumas variações foram realizadas para se entender possíveis diferenças. Um ponto importante a ser mencionado é o fato de que todas as amostras foram inseridas no dispositivo de forma compactada, para prevenir detecção precoce.

Compreendendo todos os testes foi possível obter 5 cenários distintos:
O primeiro cenário foi a ferramenta McAfee Antivírus sendo testada com o Ransomware WannaCry, após instalação da ferramenta a amostra foi inserida no dispositivo e descompactada, o resultado obtido foi que logo após a descompactação a ferramenta já foi capaz de detectar a assinatura do Ransomware, o colocou em quarentena e alertou o usuário, como pode ser visto na figura 3.

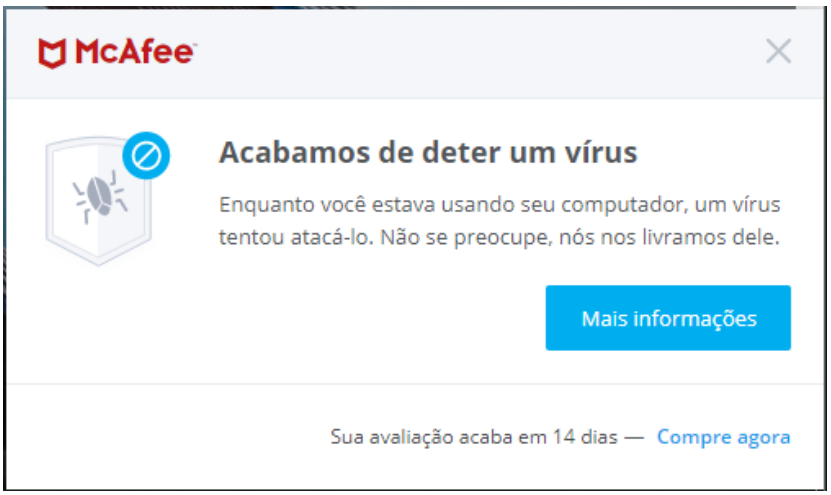

Figura 2. Cenário 1 de infecção por Ransomware

No segundo cenário a detecção em tempo real da ferramenta foi desativada e novamente uma amostra compactada foi inserida no dispositivo, neste teste foi possível obter o resultado esperado, sem esta funcionalidade da ferramenta a mesma fica completamente incapacitada de detectar quaisquer tipos de ameaça. Após a descompactação a ameaça foi executada e em poucos segundos todos os arquivos do dispositivo foram encriptados que uma tela pedindo um resgate em bitcoin foi mostrada para o usuário, como mostra a figura 4.

Figura 3. Cenário 2 de infecção por Ransomware bem sucedida

No terceiro cenário a ferramenta ZoneAlarm AntiRansomware foi testada também com o Ransomware WannaCry, após instalação da ferramenta a amostra foi inserida no dispositivo e descompactada, logo após a descompactação a ferramenta já foi capaz de detectar a assinatura do Ransomware e alertou o usuário, neste cenário a ferramenta de número dois se diferencia da primeira por não colocar o arquivo executável em

quarentena logo após sua detecção, sendo ainda possível executar o arquivo, o resultado pode ser observado na figura 5.

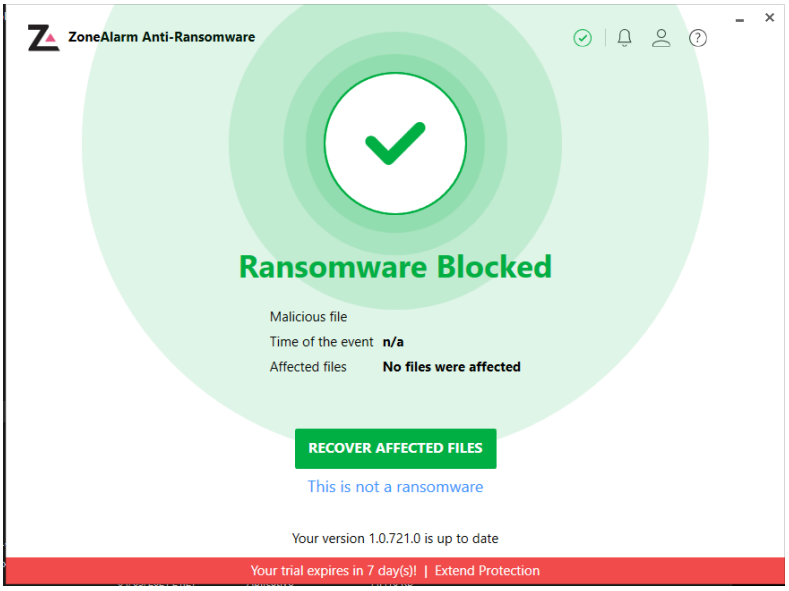

Figura 4. Cenário 3 de infecção por Ransomware mal sucedida

No quarto cenário, a amostra de Ransomware foi substituída, a amostra testada foi da ameaça BadRabbit com a ferramenta ZoneAlarm AntiRansomware, este Ransomware se diferencia de seu predecessor WannaCry por não ser tão conhecido como o mesmo.

Após a descompactação do arquivo já foi possível perceber um comportamento diferente, a ferramenta não detectou nenhum tipo de ameaça neste momento. Após isto o Ransomware foi executado com sucesso na máquina virtual e alguns arquivos foram inscritos, a ferramenta sendo testada em questão possui uma funcionalidade específicas para casos onde não é possível detectar a ameaça por sua assinatura.

A ferramenta quando não tem certeza de uma ameaça deixar a mesma realizar a encriptação de alguns arquivos para se certificar, e neste cenário foi possível ver esta funcionalidade em ação, após alguns segundos em execução o Ransomware foi detectado e a ferramenta disponibilizou a possibilidade da recuperação dos arquivos encriptados, como pode ser visto na figura de número 6.

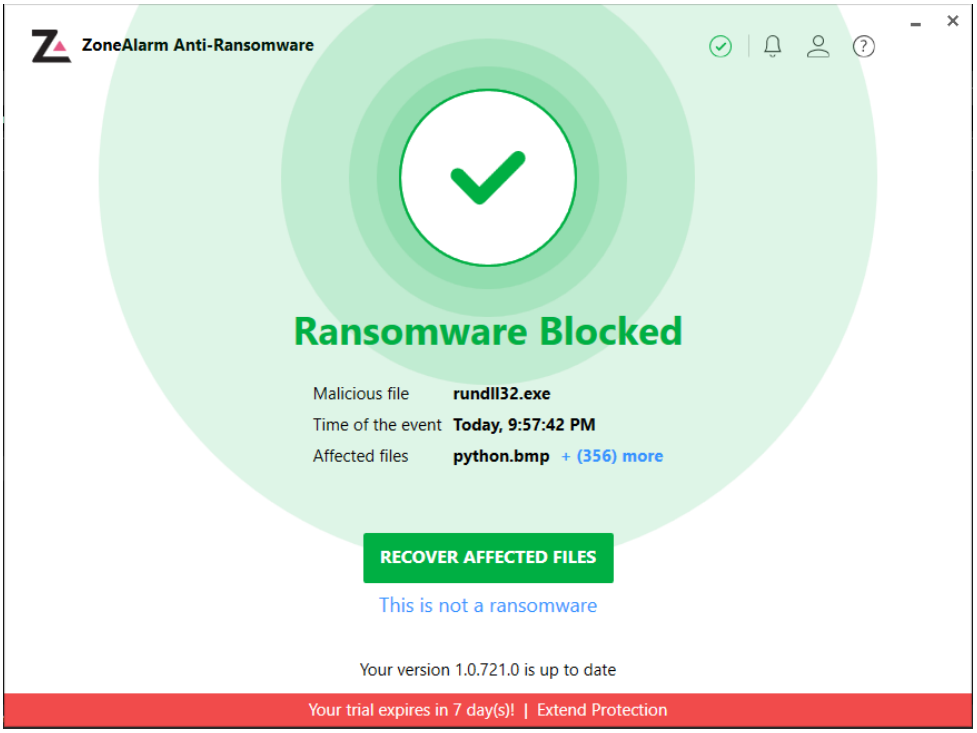

Figura 5. Cenário 4 possibilidades de recuperação de arquivos

No quinto e último cenário de testes a amostra do Ransomware BadRabbit foi testada juntamente com a ferramenta de defesa McAfee Antivírus. Neste cenário como em todos os outros a amostra foi colocada zipada em uma máquina virtual, logo após a mesma foi descompactada. Neste cenário de testes logo após a descompactação a ferramenta de defesa já foi capaz de detectar a ameaça e rapidamente moveu a mesma para sua quarentena, realizando assim a proteção completa do dispositivo. Na figura 7 é possível verificar o retorno da aplicação para o usuário.

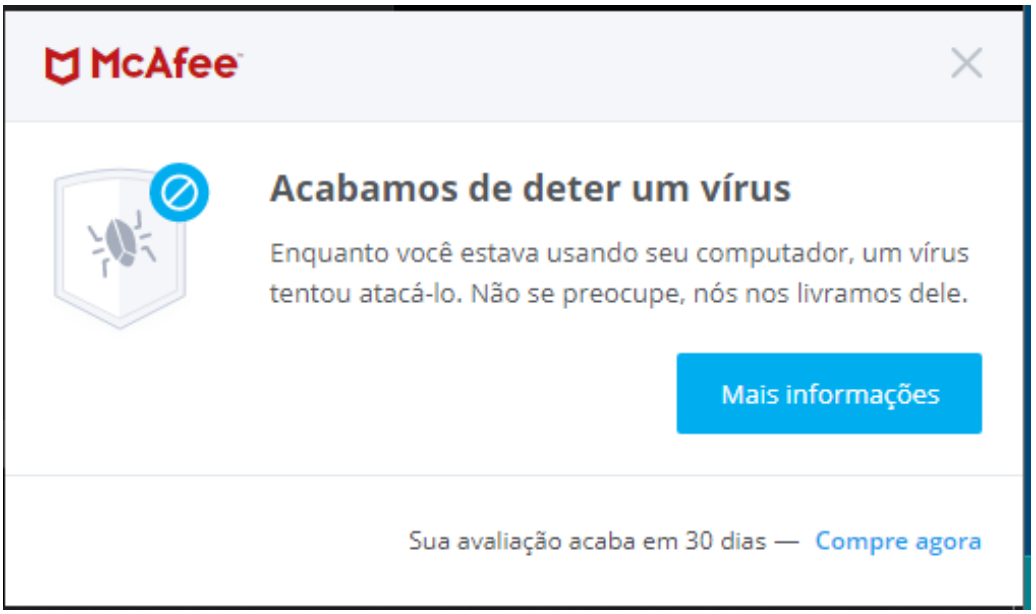

Figura 6. Cenário 5 detecção de ameaça pela ferramenta

2.5. Discussão dos resultados

Com os resultados apontados por esta pesquisa foi possível verificar alguns pontos importantes: o primeiro deles é de que os sistemas operacionais modernos por si só já possuem ferramentas pré instaladas para evitar a propagação deste tipo de ameaça. No caso desta pesquisa o sistema escolhido foi o Windows 10, que possui integrado com sua versão base a ferramenta Windows Defender, que por si só já consegue detectar muitos Ransomwares que porventura possam infectar o dispositivo. Por este motivo o Windows defender foi desativado para que a pesquisa pudesse ser concluída.

De acordo com alguns dos cenários testados na pesquisa foi possível também identificar que Ransomwares mais conhecidos têm mais chances de serem detectados tanto por ferramentas específicas quanto por ferramentas genéricas. Como foi possível verificar no cenário quatro da pesquisa, onde o Ransomware BadRabbit não foi detectado em um primeiro momento, a detecção ocorreu apenas após o Ransomware realizar a encriptação de diversos arquivos no dispositivo.

Enquanto em todos os cenários em que a ameaça escolhida foi o WannaCry, independente da ferramenta de defesa a ameaça foi detectada logo após a descompactação da mesma, sem dar chances para a ameaça causar problema no dispositivo.

Com estes cenários foi possível verificar que para usuários comuns uma ferramenta genérica como um antivírus é mais do que suficiente para proteger completamente o dispositivo desta ameaça e de possivelmente outros tipos.

Mas isso não elimina a necessidade de outros métodos de defesa como a realização de backups de arquivos importantes com frequência e evitar o acesso a sites suspeitos, entre outras várias medidas de segurança.

2.5. Conclusão

Este tipo de ameaça, já assola todos os tipos de dispositivos a muitos anos, causando grandes prejuízos financeiros tanto para pessoas quanto para empresas. Causando não apenas perdas financeiras como já posto por este trabalho, mas também perdas pessoais, como documentos ou fotos familiares.

Com o intuito de proteger os usuários deste tipo de ameaça ao longo dos anos diversas estratégias e também ferramentas foram desenvolvidas. Este trabalho teve como objetivo principal verificar a possível efetividade de algumas destas ferramentas na defesa dos dispositivos Windows contra estas ameaças.

A presente pesquisa pode constatar alguns pontos importantes para a defesa de dispositivos contra ameaças do tipo Ransomware. O primeiro ponto a se notar é de que todas as ferramentas testadas foram capazes de proteger os arquivos do dispositivo, mesmo nos casos onde a ameaça não foi detectada na descompactação. A ferramenta utilizada no momento pode com sucesso realizar o backup de todos os arquivos encriptados pela ameaça, posteriormente recuperando quando a ameaça for detectada.

Um segundo ponto a ser denotado refere-se a defesa deste tipo de ameaça através de ferramentas nativas do próprio sistema operacional. Com o passar dos anos, o sistema operacional Windows evoluiu suas ferramentas de defesas, como o Windows Defender, que age no dispositivo do usuário como uma ferramenta genérica de proteção, trazendo bons níveis de proteção contra ameaças mais comuns. Uma evidência disto foi a necessidade da desativação da ferramenta para a realização dos testes com as ferramentas escolhidas para compor a pesquisa.

Se faz possível concluir que com o passar dos anos as ameaças evoluíram muito, mas que as ferramentas de defesa e os sistema operacional também teve uma grande evolução na defesa contra este tipo de ameaça. Durante a pesquisa foi possível verificar que usuários que se utilizam apenas das ferramentas padrão dos sistemas operacionais já tem um elevado nível de segurança contra Ransomwares e que dispositivos que possuem uma ferramenta genérica ou uma ferramenta específica, possuem um nível ainda maior de defesa, sendo pouco provável que qualquer tipo de Ransomware venha a infectar o dispositivo. É importante denotar que ferramentas mais específicas trazem consigo funcionalidades que não são encontradas em ferramentas do sistema operacional, como a recuperação de arquivos infectados, que foi possível ser verificada em um dos cenários testados durante a pesquisa.

Um último ponto a se perceber se refere a utilização de estratégias de defesa juntamente com ferramentas ativas de defesa, como a realização de backups rotineiros de arquivos importantes, para evitar que ameaças muito recentes que possivelmente não sejam detectadas por ferramentas não sejam capazes de trazer perdas tão grandes para usuários ou empresas.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2005). NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. . http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf.

BERRY, Alex; HOMAN, Josh; EITZMAN, Randi. Threat Research: WannaCry Malware Profile. [S. l.], 23 maio 2017. Disponível em: https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware profile.html. Acesso em: 4 out. 2020.

Camara, D. P. B. A. e Rocha Jr., V. C. (2012). Combinando Criptografia e Biometria: Sistemas de Regeneração de Chave. *Revista de Tecnologia da Informação e Comunicação*, v. 2, n. 2, p. 26–38.

Cheng, B., Liu, J., Chen, J., et al. (2019). Behavior-Obfuscation ResistanceMalware Detection. *Computer Journal*, v. 62, n. 12, p. 1734–1747.

Cybersecurity Ventures (2017). Cybercrime Damages $6 Trillion By 2021. *Cybersecurity Ventures*, p. 1–18.

Gonzalez, D. e Hayajne, T. (2017). Detection and Prevention of Crypto-Ransomware. *IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*,

Gorman, G. O. e McDonald, G. (2012). Ransomware : A Growing Menace. *Symantec*, v. 1, p. 16.

Grégio, A. R. A., Afonso, V. M., Filho, D. S. F., Geus, P. L. De e Jino, M. (2014). Toward a Taxonomy of Malware Behaviors. *Computer Journal*, v. 58, n. 10, p. 2758–2777.

Kevin Savage, Coogan, P. e Lau, H. (2015). Symantec SECURITY RESPONSE The evolution of ransomware. p. 57.

Liska, A. e Gallo, T. (2017). *Ransomware*. O'Reilly Media.

Ludwig, L., Rebelatto, M. G. e Da Silva, S. J. R. (2020). O estado da arte das criptografias modernas: uma revisão sistemática da literatura. *Revista Brasileira de Computação Aplicada*, v. 12, n. 2, p. 46–53.

MACHADO, Rodrigues, F. N. Segurança da informação - princípios e controle de ameaças - 1a edição - 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536531212/.

O'Kane, P., Sezer, S. e Domhnall, C. (2018). Evolution of ransomware. *IET Networks (Volume: 7 , Issue: 5 , 9 2018)*,

Olgin, C. de A. e Groenwald, C. L. O. (2011). Engenharia {Didática}: uma experiência com o tema criptografia. *Jornal Internacional de Estudos em Educação Matemática*, v. 4, n. 2, p. 158–190.

Oliveira, W. (2001). *Segurança da Informação Técnicas e Soluções*.

Saxena, S. e Soni, H. (2018). Strategies for Ransomware Removal and Prevention. *Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB-18)*,