WannaCry

Arthur Cassemiro da Silva[1], Carlos Eduardo Victoriano Santos Alves[1], João Miguel Bezerra[1], Lucas da Silva Inocencio[1] Luiz Fernando Loureiro Leitão[2], Matheus Laidler Vidal Cunha[2]

[1] Centro de Tecnologia - Universidade Federal do Rio de Janeiro (UFRJ)
Av. Athos da Silveira Ramos, 149 - Rio de Janeiro - RJ - Brasil

[2]Centro de Ciências Matemáticas e da Natureza
Universidade Federal do Rio de Janeiro (UFRJ)
Av. Athos da Silveira Ramos, 274 - Rio de Janeiro - RJ - Brasil

{arthur.cassemiro, carlosvicc, jmiguel.86, lucas.inocencio}@poli.ufrj.br

{luizfllleitao, matheuslaidler}@ufrj.br

{matheuslaidler}@gmail.com

Abstract. *This paper describes the WannaCry ransomware attack, which took place in May 2017. It was a widespread event, causing great damages to several computers running unupdated versions of Microsoft Windows. WannaCry is a famous example of crypto ransomware. In other words, is a type of malicious software (malware) used by cybercriminals to extort money from victims. For the purpose of this work, that episode will be addressed through forensic analysis. Therefore, that attack will be explained by its story, its nature and how was mitigated.*

Resumo. *Este artigo descreve o ataque de ransomware WannaCry, ocorrido em maio de 2017. Foi um episódio difundido, causando grandes danos em diversos computadores rodando versões desatualizadas do Microsoft Windows. O WannaCry é um exemplo famoso de ransomware criptográfico. Em outras palavras, é um tipo de software malicioso (malware) usado por criminosos cibernéticos para extorquir dinheiro das vítimas. Para o propósito deste trabalho, esse episódio será abordado por meio da análise forense. Assim, esse ataque será explicado por sua história, por sua natureza e por como foi mitigado.*

1. Introdução

O *Wannacry* é um *ransomware* que se aproveita de uma falha do *windows* para criptografar os dados das máquinas infectadas até que seja pago um resgate em *bitcoins*. Ele ficou conhecido por ter atingido escala global em 2017, afetando os mais diferentes setores da sociedade, desde computadores pessoais a grandes empresas.

De modo geral, o *WannaCry* funciona apenas se o executável for de fato aberto pela vítima. Todavia, em muitos casos o próprio atacante conseguia realizar essa execução. Por isso, a vulnerabilidade do *Windows* é tão crítica e necessária para o ataque, pois, com ela, o criminoso poderia fazer a execução do código remotamente e ter acesso privilegiado a uma máquina vulnerável. Essa ofensiva pode ser reproduzida em ambiente controlado via máquinas virtuais usando *metasploit framework* e um *Windows 7* vulnerável.

A vulnerabilidade escolhida como alvo dos ataques esteve presente em algumas versões do *Windows* nos anos de 2017 ou anteriores, conforme descrito no *Microsoft Security Bulletim MS 17 - 010 - Critical*. Basicamente, a falha em questão permite que sejam executados códigos remotamente pelo atacante e sem necessitar a autenticação do mesmo. Para isso, utiliza-se o protocolo SMB do *Windows*, que é um protocolo de compartilhamento de arquivos em rede que permite que os aplicativos de um computador leiam e gravem em arquivos e solicitem serviços dos programas do servidor em uma rede. Esse protocolo roda nas portas 139 (originalmente) e 445 (recentemente) e é usado no ataque para que o *WannaCry* seja baixado na máquina e logo após executado.

Outro ponto que tornou o vírus tão conhecido é a capacidade de atacar outros computadores vulneráveis dentro da mesma rede de forma independente. Dessa forma, ele também pode ser considerado como um *worm*.

2. Mitigação

2.1. Atualização do sistema

Os computadores infectados pelo vírus estavam desatualizados, o que permitia o uso do *exploit EthernalBlue* em seu sistema, portanto uma das forma mais efetivas de evitar a infecção e consequentemente os danos causados é mantendo o sistema atualizado. O uso de antivírus pode auxiliar com possíveis problemas ou atuar como um lembrete para atualizações.

2.2. Criação manual do *Mutex*

Para evitar que um vírus seja executado múltiplas vezes em uma maquina, é pratica comum de vários *malwares* criar um *Mutex* único e parar a execução caso esse *Mutex* seja encontrado. No *WannaCry*, para que uma máquina já infectada e que tenha pago o resgate não seja infectada novamente é adotada essa prática. Portanto, uma das técnicas iniciais mais efetivas adotadas por pesquisadores foi a criação manual deste *Mutex* (Global\MsWinZonesCacheCounterMutexA) como prevenção antes da instalação de um *patch* ou atualização para corrigir o problema.

2.3. Backups externos

O backup é um procedimento que deve ser feito regularmente para evitar que falhas de funcionamento das máquinas ou acidentes físicos possam afetar os arquivos. Com isso, mesmo que a máquina seja afetada pelo *WannaCry*, os dados podem ser recuperados. É importante ressaltar que os backups devem ser armazenados externamente (idealmente com redundância) para garantir que eles não sejam juntamente afetados.

2.4. Recomendações Gerais

Caso o sistema esteja infectado, o pagamento do resgate não é recomendado, tendo em vista que neste caso não há garantia de que seus arquivos sejam devolvidos do sequestro após pagamento de resgate, até porque não é nada complexo de mudar a carteira bitcoin do executável (mesmo que no início tenha tido algumas supostas devoluções como forma de ganhar ”confiança”). Com tudo isso em mente, podemos perceber mais um motivo do tamanho da importância dos backups regulares estarem em dia.

Para evitar a infecção e a disseminação desse malware pela rede, todos os sistemas devem estar atualizados com os últimos patches lançados, assim como as assinaturas de seu antivírus. Além disso, um firewall bem configurando é sempre imprescindível, bloquear conexões de entrada para portas SMB (139 e 445) impedirá a disseminação do malware para eventuais sistemas ainda vulneráveis, sistemas esses que nem deveriam estar ativos na rede. Percebemos, assim, a importância da atualização dos sistemas e programas.

Podemos observar também que caso algum vírus não queira infectar uma máquina que já foi contaminada (Mutex), então teremos mais uma forma de fazer um 'bypass' para futuras tentativas de invasões, fazendo a máquina se passar por uma já infectada anteriormente.

3. Técnicas e ferramentas

Podemos dividir o processo de análise forense em quatro etapas: Coleta, extração, análise e apresentação.

3.1. Coleta

A coleta é a cópia de evidências do local original para um ambiente sob controle das autoridades ou pesquisadores, se possível, para a continuação da investigação. Isso é feito para garantir a integridade dos dados originais e evitar que a própria ánalise forense interfira nos resultados. No caso em questão, o ataque foi simulado, por nós, em uma máquina virtual, utilizando a ferramenta *Oracle VM VirtualBox*, ideal para simular o ataque de forma segura e local. Em seguida, a coleta de dados foi feita com a ferramenta *Forensic Toolkit (FTK) Imager*. O *FTK Imager* é um software forense criado pela empresa Access Data que possui funcionalidades para criar imagens de disco, realizar despejos (dumps) de memória e até mesmo recursos básicos de análise pericial em imagens de disco nos formatos aceitos pela ferramenta. O motivo da escolha dessa ferramenta foi sua simplicidade de uso, por ser razoavelmente completa além de ser gratuita.

3.2. Extração

A extração corresponde à fase de obtenção das informações da máquina. Nela, a imagem é submetida a uma requisição de informações detalhadas. As ferramentas utilizadas nessa etapa foram o *autopsy* (para a imagem do disco) e o *volatility* (para o *memory dump*). O autopsy é uma ferramenta com diferentes módulos, o que torna possível verificar arquivos afetados pelo vírus, linha temporal de eventos, palavras chaves de busca, etc. Com ela, podemos introduzir o arquivo encontrado na parte de coleta e obter informações relevantes com base nos módulos selecionados.

A outra ferramenta é o *volatility*, software gratuito usado para análise forense em memória RAM ou memórias voláteis em geral, e possui inúmeros comandos úteis para a identificação, captura e análise de *malwares*, desta forma, pode ser analisado o comportamento da RAM em um sistema infectado.

3.3. Análise

A análise consiste em estudar as informações extraídas e tirar conclusões válidas para o cenário proposto. Como o comportamento do vírus, o que ele afeta e se os métodos de mitigações são válidos.

Nesta etapa, foi feita também uma análise estática do executável. Nesta inspeção (utilizando o comando *strings* no *linux*) encontramos, dentre outras coisas, o *Mutex* utilizado, o comando para dar permissão para o executavél (*icacls . /grant Everyone:F /T /C /Q && attrib +h .*, diversos executáveis embutidos no executável principal (isso pode facilitar a análise dinâmica posterior) e referências à *Windows Crypto API* (utilizada para gerar as chaves de cifragem).

A criptografia é feita em uma cópia do arquivo original da vítima, o arquivo original é apagado, sobrando apenas os criptografados. Desta forma, o uso de programas de recuperação de arquivos, como *recuva*, pode ser um meio de tentar recuperar estes arquivos.

Com a ferramente wireshark podemos monitorar o trafego da rede e bloquear padrões de requisições e resposta não usuais.

3.4. Apresentação

A apresentação resume-se a apresentar de forma imparcial os resultados obtidos através da análise, onde, com base nessa etapa, serão tomadas as decisões cabíveis dentro do problema proposto.

4. Correções e efetividades

Existe um programa criado pelo *aguinet*, chamado *wannakey*, que explora uma falha do windows e permite recuperar os números primos da chave privada RSA que são utilizados pelo *Wannacry*, sendo assim funcionaria apenas para computadores que não foram desligados ou reiniciados após o ataque, pois a chave só é destruída ao ser desalocada da memória. Isto não é um erro dos autores, mas um exploit das funções CryptDestroyKey e CryptReleaseContext da API de criptografia do Windows.

O ataque que tornou o *wannacry* conhecido foi altamente destrutivo, porém muito mais sistemas poderiam ser afetados caso não fosse encontrado um grande ”calcanhar de Aquiles” do *ransomware*. Quando o *wannacry* infecta uma máquina, uma requisição a uma URL era feita e caso fosse atendida o vírus não agia. Porém o domínio da URL era inexistente, então não afetava diretamente na execução do vírus, entretanto, quando pesquisadores descobriram esse fato, o domínio e a URL foram criadas, sendo usadas para atender a requisição do vírus e assim minimizando o ataque de forma significativa.

Após um tempo, nova versões do Wannacry não apresentavam esse falha altamente proveitosa, complicando a mitigação e prevenção desse ataque. Esse comportamento pode ser considerado análogo a evolução biológica presente nos vírus orgânicos que afetem os seres vivos, mesmo que seja resultado de alteração humana. Em outras palavras, possa ser que a competição entre defensores e *malwares* atacantes possa ser modelada de forma similar a evolução decorrente da interação entre os seres vivos.

5. Referências

[Olhar digital]*Wannacry: Entenda o que foi o ataque que afetou mais de 200mil PCS*

[Kaspersky]*Ransomware WannaCry: All you need to know*

[Malwareytes]*What was wannacry?*

[BBC]*Cyber-attack: US and UK blame North Korea for WannaCry*

[SecureWorks]*WannaCry Ransomware Analysis*

[Medium]*Ransomware encryption techniques*

[Medium]*Can files locked by WannaCry be decrypted: A technical analysis*

[Malwaretech]*How to Accidentally Stop a Global Cyber Attacks*

[Kaspersky]*CVE-2020-0796: Nova vulnerabilidade no protocolo SMB*

[Convergência Digital]*WannaCry: ransomware ainda requer atenção*

[Microsoft]*MS17-010: Atualização de segurança para o servidor Windows SMB: terça-feira, 14 de março de 2017*

[Kaspersky]*CVE-2020-0796: Nova vulnerabilidade no protocolo SMB*

[Petter Lopes]*WANNACRY, um RANSOMWARE que sequestrará a economia*

[Rathod & Sharma]*DIGITAL FORENSIC ANALYSIS OF RANSOMWARE INFECTED WINDOWS SYSTEM*

[LogRhythm Labs]*A Technical Analysis of WannaCry Ransomware*

[Donny]*Memory Analysis of WannaCry Ransomware*

[fabrimagic72]*malware-samples*

[Zimba & Mulenga]*A DIVE INTO THE DEEP: DEMYSTIFYING WANNACRY CRYPTO RANSOMWARE NETWORK ATTACKS VIA DIGITAL FORENSICS*

[aguinet]*wannakey*

[Como recuperar e descriptografar arquivos criptografados por Wanna Crypt?]*easeus*

[DEVCOM]*Cybersecurity Awareness Workshop Series WannaCry*