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. História do Ataque

O *ransomware WannaCry* foi um dos ataques mais severos de toda a história da Internet. Em um período de poucas horas, ele afetou inúmeros países em uma escala nunca observada anteriormente. Ocorrido em maio de 2017, a ofensiva atingiu pessoas, empresas e instituições ao redor do mundo, desde hospitais públicos no Reino Unido a grandes corporações na Espanha (e.g. *Santander* e *Telefónica*). Segundo a *Avast*, mais de 200 mil computadores foram infectados em mais de 150 países, estando o Brasil na quinta colocação do ranking dos mais afetados pelo *malware*.

Basicamente, o *WannaCry* afetou inúmeras máquinas que operavam com o sistema operacional *Windows*, aproveitando-se de uma falha de segurança conhecida como *EternalBlue*. Embora a *Microsoft* tenha lançado uma atualização de segurança para corrigir a

falha pouco tempo depois de ser encontrada, muitos computadores não foram atualizados. Dessa forma, criou-se o ambiente perfeito para se aproveitar dessa vulnerabilidade e, assim, promover o ataque que gerou grandes prejuízos à economia global.

De maneira simples, o objetivo desse *ransomware* é criptografar dados de uma determinada máquina, impedindo o acesso a eles por parte do usuário. Para que as informações fossem resgatadas, seria exigido um pagamento em *bitcoins* dentro de uma janela pequena de tempo. Todavia, caso não houvesse o pagamento dentro desse período, o valor cobrado aumentaria. Em vista disso, ao se analisar a ofensiva fica evidente que o objetivo era ser um ataque a inúmeros países, pois existia a opção de mudar a linguagem da mensagem de retorno do vírus.

Infelizmente, até hoje não se sabe quem foi(foram) o(s) autor(es) do ataque, porém existem suspeitas. Uma delas é relacionada ao conhecimento da falha que permitiu o ataque, já que a existência do *EternalBlue* foi divulgada pelo grupo *Shadow Brokers*, em um vazamento de informações da Agência de Segurança Nacional dos Estados Unidos (*National Security Agency* - NSA). Em outras palavras, o governo já tinha conhecimento dessa vulnerabilidade, mas optou por guardar essa informação para si. Além desta, outra hipótese é a de que o *ransomware* foi criado pelo grupo norte coreano *Lazarus*, sendo os principais defensores dessa ideia os governos americano e britânico.

2. Natureza do WannaCry

O *WannaCry* é um *ransomware* conhecido mundialmente, de natureza destrutiva, e sendo bem-sucedido em diversos ataques. A títulos de exemplos, há os casos contra o sistema de saúde público do Reino Unido (*National Health Service* - NHS), contra o banco *Santander* (Espanha) e contra a operadora *Telefónica* (Espanha), citados anteriormente.

Nesse sentido, sua origem provém de uma exploração de vulnerabilidade crítica do *Windows Server Message Block* (SMB) *v1*, que já fora corrigido pela atualização de segurança *MS17-010*. Contudo, por causa de descuidos generalizados em relação à correta manutenção do sistema, o *malware* se alastrou rapidamente, causando grandes prejuízos à economia mundial. De maneira desconhecida até o presente momento, o grupo denominado *The Shadow Brokers* obteve acesso ao *exploit* chamado *EternalBlue*, supostamente criado pela NSA.

Felizmente, o *ransomware* não era do tipo *0day* graças a atualização prévia de segurança por parte da *Microsoft*. Entretanto, a não atualização do *Windows* em diversos computadores ao redor do mundo permitiu que o estrago causado pelo *malware* tivesse proporções gigantescas. Assim, este episódio torna-se um exemplo bastante didático da importância da aplicação de conceitos básicos de segurança, dentre eles a atualização de sistemas e de programas.

No que tange à sua natureza, esse *malware* explora a vulnerabilidade que permite uma execução de código remoto em nível de sistema do protocolo SMB, presente no *Windows*. Por conseguinte, criando um ambiente perfeito para criminosos cibernéticos (*crackers*) realizarem sequestros digitais por meio da criptografia dos dados existentes no computador.

2.1. Explicação e Comportamento de um *Ransomware*

O *ransomware* é nada mais do que um *malware* que sequestra arquivos da vítima, encriptando-os. Dessa forma, é impossibilitado o acesso por parte da vítima aos dados e

geralmente exigindo um valor em *bitcoins* para a liberação dos mesmos.

De modo geral, o *WannaCry* funcionava apenas se o executável fosse de fato aberto pela vítima. Todavia, em muitos casos o próprio atacante conseguia realizar essa execução. Por isso, a vulnerabilidade do *Windows* era 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. Por exemplo, essa ofensiva pode ser reproduzida em ambiente controlado via máquinas virtuais usando *metasploit framework* e um *Windows 7* vulnerável.

2.2. Objetivos e Propagação

Sabe-se publicamente que a *Microsoft* corrigiu em 2017 a vulnerabilidade, conhecida como *CVE-2017-014*, através da atualização de segurança MS17-010. Brevemente, esse *exploit* se baseia na execução de código remoto (*Remote Code Execution* - RCE) em nível de sistema do protocolo SMB v1. Logo, ao utilizar este padrão, um (usuário de) aplicativo poderia acessar arquivos e/ou outros recursos em um servidor remoto.

Lamentavelmente, um dos maiores problemas foi sua capacidade de se espalhar na rede para outras máquinas vulneráveis. Dessa forma, ele também foi considerado um *worm*. Nesse ritmo, propagou-se até atingir uma escala global. Resumindo, a ideia desse *ransomware*, também conhecido como *WanaCrypt0r*, é criptografar arquivos no sistema e exibir uma mensagem com wxigência de resgate para ganhos financeiros.

2.3. Crise versus Resgate

Essa confusão generalizada levantou uma questão importante no debate público: deve-se ou não pagar pelo resgate exigido? Isto posto, qual é a alternativa menos prejudicial? Teoricamente, pagar o valor cobrado evitaria mais perdas de ordem financeira e de credibilidade. Entretanto, não pagar o montante desestimularia a continuidade dessa prática criminosa, pelo menos hipoteticamente. De todo modo, é virtualmente impossível analisar com profundidade cada caso e deliberar da melhor maneira cada situação. Portanto, faz-se necessário abordar a problemática através de uma óptica profissional e pragmática.

De modo geral, muitas pessoas pagaram pelo resgate, partindo do pressuposto de que o prometido nas mensagens seria cumprido. Contudo, não havia quaisquer garantias de que o acordo seria cumprido. Por esse ângulo, é essencial ter consciência acerca dos riscos subjacentes a esse tipo de operação. Obviamente, criminosos não se adéquam às regras da vida social. Assim, não há indicativos de posturas moralmente aceitáveis por parte deles nesses tipos de episódios.

Objetivamente, os investimentos prévios em segurança seriam o correto. Dessa maneira, mostra-se importante a realização de backups rotineiros, de modo a evitar que um eventual erro humano provoque danos e prejuízos irreversíveis. Além do mais, é importante salientar que qualquer pessoa de caráter malicioso pode apenas modificar as strings do arquivo executável, possibilitando a modificação da *hash* criptográfica da carteira de bitcoin do grupo para uma carteira própria, neste caso nem o próprio atacante detém acesso a chave criptográfica dos arquivos, impossibilitando que o mesmo libere os dados. De qualquer forma, os parâmetros emocionais relacionados a esses eventos não podem ser desconsiderados, pois eles são fundamentais no sucesso (ou no fracasso) dessas ofensivas. Mais do que isso, deve-se conscientizar os usuários comuns sobre os perigos existentes.

2.4. Aprendizado com Experiências Anteriores

Sem surpresa alguma, esse tipo de evento não se resume ao ocorrido em maio de 2017. Nesse sentido, foi descoberto em 2020 outra vulnerabilidade no protocolo SMB v3, sendo dessa vez apenas para o *Windows* 10. Assim, a própria *Microsoft* publicou que era possível a exploração para a execução de códigos arbitrários no lado do servidor ou no do cliente SMB. Para atacar o primeiro, poder-se-ia enviar um pacote malicioso. Já para atacar o segundo, necessitar-se-ia configurar um servidor SMB v3 malicioso e convencê-lo a se conectar. Portanto, essa vulnerabilidade pode ser usada para alavancar outro programa malicioso, do mesmo estilo do *WannaCry*, porém ela já teve o seu *patch* de atualização, bastando apenas atualizar o sistema para não ficar vulnerável.

Alternativamente, na ausência de um pacote de atualização, uma das estratégias de defesa possíveis seria o bloqueio da porta TCP 445 no *firewall* de perímetro da empresa. São boas práticas a implementação de soluções de segurança confiáveis e recorrentes atualizações, porém as vezes devemos achar caminhos que evitam o estrago de um 0day.

2.5. Conclusões

Diante do exposto, entende-se que a utilização de *ransomwares* para infecção de máquinas é altamente lucrativa para as quadrilhas cibernéticas. Nessa lógica, o *WannaCry* foi ainda mais exitoso, pois explorou a vulnerabilidade CVE-2017-014 com RCE. Além disso, ao invés de infectar um único computador, ele se autor-replicou e infectou outros computadores em escala global. Por causa disso, o *WannaCry* também é considerado um *worm*. Entretanto, em hipótese alguma deve-se pagar pelos resgastes exigidos, seja pela falta de garantia de retorno, seja pela fomentação da estrutura criminosa ou seja pela modificação da chave criptográfica no executável. Logo, o profissional de segurança deve estar sempre alerta quanto às atualizações e os pacotes de segurança.

3. Mitigação e Proteção

As políticas de mitigação e proteção de riscos devem estar no cerne das prioridades da organização. Sem elas, todo o ambiente de trabalho restante fica vulnerável à ação de programas maliciosos e demais possibilidades de ataques criminosos. Assim, elas serão descritas no presente documento em três partes: backups. sistemas atualizados e políticas de segurança.

3.1. Backups

É imperativo fazer backups com regularidade. Nesse sentido, a janela de tempo ideal para realizá-los é de uma semana, e a depender do ramo de atuação da organização (e.g. instituições financeiras), faz-se necessário haver backups diários. Além disso, é fundamental tanto a existência de redundância quanto à localização estar fora do ambiente de atuação diária da companhia. Portanto, os dispositivos de armazenamento externo só devem estar conectados aos computadores da empresa enquanto os processos de backup estejam sendo realizados.

3.2. Sistemas Atualizados

Uma excelente prática de proteção do ambiente digital da organização é a atualização rotineira dos sistemas, notadamente o sistema operacional (e.g. *Microsoft Windows*) e

as suítes de antivírus (e.g. *Norton*, *Kaspersky* e *McAfee*). Dessa maneira, diminuem-se drasticamente os riscos de contaminação por *ransomwares* e/ou demais *malwares*. Logo, o investimento em licenças dos softwares citados anteriormente não deve ser norteada pelo custo em si do produto, mas por sua efetividade em cumprir os objetivos designados.

3.3. Políticas de Segurança

A parte mais frágil de toda a cadeia produtiva é a humana. Isto posto, a primeira política de segurança a ser implementada é a de treinamento de todos os funcionários da companhia para a correta utilização dos meios digitais disponíveis. Destarte, eles serão detalhados nas próximas sub-seções.

3.3.1. *Phishing Scam*

O *phishing scam* é a maneira mais comum de infecção de computadores. Inicialmente, deve-se orientar os usuários comuns sobre os riscos de clicar em links suspeitos (muitas vezes maliciosos), descrevendo como ocorre o ataque de *phishing*. Por conseguinte, faz-se necessário alertar que links oriundos de e-mails suspeitos e/ou links de sites não confiáveis não devem ser acessados em dispositivos conectados à(s) rede(s) da empresa. Em vista disso, uma boa prática de segurança é a limitação de acesso ao sistema por parte dos funcionários que não operam os sistemas de segurança da organização.

3.3.2. Dispositivos de Armazenamento

As possibilidades de infecção de computadores não se resumem àquelas oriundas de malwares que se propagam pela Internet. Infelizmente, os sistemas da companhia podem ser atacados por softwares maliciosos presentes em dispositivos de armazenamento externo portados por funcionários da organização. Assim sendo, existem duas alternativas para a mitigação desse risco: bloqueio de permissão para a execução de arquivos não instalados previamente ou a migração de todo o ambiente digital para a nuvem. Em vista disso, cabe à organização decidir qual solução se adéqua mais às suas necessidades.

3.3.3. Implementação de VPN

A implementação de redes virtuais privadas (VPNs) é outra excelente prática de proteção do ambiente digital corporativo. Nesse sentido, ela promove uma série de benefícios, tais como a proteção do tráfego de dados por meio de criptografia segura (existência de uma chave criptográfica), o disfarce de paradeiro e o não comprometimento de segurança devido ao trabalho remoto. Em relação à primeira, torna-se virtualmente impossível que os dados sejam acessados por atacantes externos, haja vista que o tempo para quebrar via *brute force* um bom algoritmo de criptografia está na casa de milhões de anos. Já em relação à segunda, o mascaramento da localização real dos dispositivos conectados à rede privada dificulta o planejamento de ataques maliciosos coordenados contra à organização. Em relação à última, a implementação de VPNs confere segurança ao trabalho remoto, permitindo que os funcionários da empresa possam trabalhar a partir de diferentes ambi-

entes sem aumentar os riscos de acessos indevidos a dados sensíveis. Logo, esta política deve ser tratada como prioridade máxima de segurança por parte da companhia.

4. Análise Forense

4.1. Vetores de Ataque

Vetores de ataque são as formas que um atacante encontra de conseguir acesso a uma máquina, sejam elas utilizando vulnerabilidades ou utilizando alguma falha humana que possibilite a execução deles.

4.1.1. Principais Maneiras de Contaminação

Para que o ataque seja efetivado, o *ransomware* inicialmente precisa ser instalado no computador de alguma forma. Logo, as possibilidades de contaminação decorrem da maneira que o *malware* alcança (infecta) a máquina. A principal delas é o download por meio de cliques em links suspeitos, como os presentes em e-mails e sites não confiáveis. Esta péssima prática, combinada a falta de atualizações tanto do sistema operacional quanto das soluções de segurança, comprometem de maneira significativa o ambiente digital da companhia, pois aumenta a chance de programas maliciosos serem instalados indevidamente.

Além do supracitado, o *ransomware* também pode ser baixado erroneamente por funcionários, caso estes acessem sistemas da empresa sem utilizar VPN. Notadamente, ao utilizar redes públicas e/ou utilizar o mesmo dispositivo de armazenamento externo (e.g. pendrive, HD externo) para armazenar tanto dados pessoais quanto corporativos.

4.1.2. Vulnerabilidades Utilizadas

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*. Embora já existisse um *patch* para essa vulnerabilidade quando o *WannaCry* começou a ser utilizado, os sistemas atacados não estavam atualizados.

Basicamente, a falha em questão permite que sejam executados códigos remotamente pelo atacante e sem necessitar a autenticação do mesmo. Assim, 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 na porta 445 e é usado no ataque para que o *WannaCry* seja baixado na máquina e logo após executado.

4.2. Execução e Cifragem

4.2.1. Execução

Ao ser executado, o *WannaCry* inicia uma série de ações, sendo elencados aqui os passos mais importantes e contextualizá-los. É interessante perceber que, mesmo sendo um

ataque de grandes proporções, o *malware* em si não apresenta estratégias complexas ou inteligentes de ataque, tampouco tentativas de obfuscação relevante.

Ao ser executado, ele inicialmente tenta se conectar a um domínio (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com nas amostras originais), que não era registrado, e só continua a execução se houver uma falha na conexão. Esse comportamento pode ser explicado como uma implementação de um *kill-switch* (que seria registrar o domínio) ou, mais provavelmente, uma tentativa de identificar se o programa está sendo executado em uma máquina virtual de teste, onde o *host* retornaria um endereço mesmo com o domínio não registrado. Como esse domínio estava definido *hardcoded*, qualquer um que fizesse o registro do domínio conseguiria, de fato, frear o avanço ao menos dessa versão (e foi exatamente isso que um pesquisador da *MalwareTech* fez enquanto investigava o *WannaCry*).

Em seguida, ele cria um *mutex* no registro do *Windows*, para que o *WannaCry* não rode mais de uma vez na mesma máquina. A criação "artificial" deste *mutex* foi, inclusive, uma das formas de proteger a máquina e impedir a execução do *malware*. A partir deste momento, ele inicia o processo de cifragem do arquivo e abre uma ligação "*Command and Control*" utilizando a rede Tor com os atacantes. Quando concluída a cifragem dos arquivos, ele abre uma janela avisando que o computador foi atacado e indicando o endereço da carteira de *bitcoins* para ser feito o pagamento do resgate.

4.2.2. Cifragem

O WannaCry, assim como outros *ransomwares* recentes, utiliza uma combinação de estratégias de cifragem (simétrica e assimétrica) utilizando os algoritmos AES e RSA respectivamente. A cifragem é feita localmente, isto é, a máquina infectada não precisa de conexão com a internet, já o processo de decifragem requer conexão. Para entender melhor esse processo, façamos uma análise de possíveis estratégias:

- **Cifragem assimétrica local (RSA):** A cifragem seria feita no alvo, utilizando uma chave pública, mas a chave privada teria que ser enviada para o atacante, o que exigiria conexão externa, ou armazenada no alvo, onde poderia ser encontrada e utilizada para recuperar os arquivos. Além disso, seria um processo demorado, principalmente para arquivos grandes.
- **Cifragem simétrica local (AES):** Essa estratégia aumenta a velocidade do processo, sendo inclusive a estratégia efetivamente usada para cifragem dos arquivos pelo WannaCry, mas não resolve a questão da chave para decifragem que continua exposta ou exigindo conexão.
- **Chave pré-compartilhada (RSA ou AES):** Independente de utilizar RSA ou AES, as chaves poderiam ser geradas previamente. No entanto, isto implicaria que, depois de pago o resgate, o atacante precisaria enviar a chave de decifragem, que poderia ser usada para decifrar qualquer computador infectado. Outra possibilidade, seria o alvo enviar os arquivos cifrados e o atacante devolver os arquivos decifrados, algo impraticável.
- **Cifragem simétrica local (AES) + assimétrica dupla (RSA):** Neste modelo, o atacante gera previamente um par de chaves assimétricas (*prePriv* e *prePub*, por exemplo) e envia a chave pública (*prePub*) juntamente com o *malware*. No

alvo, é gerada um novo par de chaves assimétricas (*alvoPriv* e *alvoPub*, por exemplo) e a chave privada *alvoPriv* é cifrada usando a chave pública *prePub* pré-compartilhada. Em seguida, a cifragem dos arquivos é feita utilizando o AES e a chave de decifragem é cifrada usando a chave pública *alvoPub*. Dessa forma, a cifragem é feita de forma rápida e sem necessidade de conexão externa, caso o resgate seja pago, basta o atacante receber a chave *alvoPriv* (cifrada usando a chave *prePub*), decifrá-la (usando a *prePriv* secreta) e enviar de volta para o alvo.

4.3. Comunicação com os Atacantes

O ataque se origina por *phishing*, geralmente um e-mail pedindo para que pessoa clique no arquivo em anexo e uma vez executado ele se propaga por aquela rede. Contudo, após isso, não há mais uma comunicação com os atacantes, ha somente as mensagens predeterminadas do e-mail e programa.

4.3.1. IPs e a trajetória de ataque

Com a máquina já infectada, o *exploit* permite que o atacante transmita pacotes para qualquer sistema na internet com acesso a porta 445, assim permitindo a ligação de *Command and Control* pela rede *Tor*.

Sistemas contaminados pelo vírus vasculham por endereços IPs que estão no alcance da máquina contaminada e verificam se a máquina tem a porta 445 aberta para a infecção. Com a nova contaminação concluída, será iniciada uma nova busca por IPs, assim o ataque não necessita de interação humana depois da primeira infecção. Usando uma análise de rede é possível notar tal comportamento de forma mais clara, onde a máquina contaminada faz uma requisição DNS ao domínio *kill-switch* e com a resposta o vírus é iniciado, começando o tráfico SMB e executando buscas por nova máquinas.

4.3.2. Resgate em *Bitcoin*

Sobre o ataque original, como comentando nas seções anteriores, era exigido um valor de 300 dólares em *bitcoins* como regaste do sequestro de dados, sendo este aumentado para 600 dólares dentro de um prazo de 3 dias e perda total dos dados dentro de um prazo de 7 dias. É importante salientar que os dados eram de fato decriptografados, pois isto levava a uma maior confiança e o lucro para os atacantes. Contudo, o *ransomware* poderia ser facilmente modificado, devido sua simplicidade e por ser um *exploit* publico, trocando os *bytes* do executável para direcionar para outra carteira de *bitcoins*, assim simulando o original, mas sem possuir o deciframento.

5. References

[Olhar digital]*Wanncry: 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*