A era dos Crypto Ransomwares: um estudo de caso sobre o WannaCry

Guilherme Baesso Moreira[1], Vanusa Menditi Calegario, M.Sc.[2], Julio Cesar Duarte, D.Sc.[1], Anderson F. Pereira dos Santos, D.Sc.[1]

[1]Instituto Militar de Engenharia – Rio de Janeiro – RJ – Brasil

[2]Universidade Federal do Rio de Janeiro - Rio de Janeiro – RJ – Brasil

gbaesso@gmail.com, vmenditi@yahoo.com.br, {duarte,anderson}@ime.eb.br

Abstract. *In a context of growing dependency on computational systems and the Internet, the institutions have been investing more and more resources to ensure the Information Security. Despite the countless efforts, incidents are still growing in frequency and severity, showing that more efficient incident response processes are needed. One of the threats in clear growth is the Crypto Ransomwares. This paper develops a case study of WannaCry – a peculiar ransomware that spread panic in early 2017 – with the goal of identifying opportunities for improvement in the incident response systems and processes.*

Resumo. *Num contexto de crescente dependência dos sistemas computacionais e da Internet, as instituições têm investido cada vez mais recursos para garantir a Segurança da Informação. Apesar dos inúmeros esforços, os incidentes continuam crescendo em frequência [CERT.br 2017] e gravidade, evidenciando a necessidade de processos mais eficientes de resposta a incidentes. Uma das ameaças em franca expansão são os Crypto Ransomwares. Este trabalho realiza um estudo de caso do WannaCry – um ransomware bastante peculiar que causou pânico no início de 2017 – com o objetivo de identificar oportunidades de melhoria nos sistemas e processos de resposta a incidentes.*

1. Introdução e Motivação

Segundo relatório da PwC Brasil, o investimento em Segurança da Informação tem crescido a um ritmo anual de 30% a 40% no país, atingindo cifras de até US$ 8 bilhões. Ao mesmo tempo, ataques cibernéticos causaram perda estimada de até R$ 20 bilhões ao ano na economia brasileira [O Globo 2015].

Embora as companhias tenham aumentado o seu investimento em Segurança da Informação, o número de incidentes continua crescendo [CERT.br 2017]. Inúmeras notícias sobre ataques cibernéticos pelo mundo reforçam a percepção de que o problema continua aumentando em frequência e gravidade. Dentro deste contexto, observa-se que a maioria dos ataques cibernéticos atuais possuem motivações políticas ou financeiras [Kharraz et al. 2015] [Reuters 2017] e muitos são financiados por Estados, como parte da ofensiva de uma verdadeira guerra cibernética [Healey 2016].

Ransomware é um tipo de *malware* que impede ou limita o usuário de acessar seu sistema, até que um "resgate" seja pago. Famílias mais modernas do *malware*, conhecidas como *crypto ransomware*, criptografam certos tipos de arquivos em sistemas

infectados e forçam o usuário a pagar um "resgate" para obter a chave de decriptografia [Trend Micro 2016]. Não por acaso, os ataques com *ransomware* têm crescido fortemente [Economist.com 2017] [AYRAPETOV 2017] e estão se tornando mais sofisticados, passando a ter como alvo não apenas usuários finais, mas também sistemas industriais completos [Formby et al. 2017] [Cobb 2017] [Franceschi-Bicchierai 2016].

Diversos incidentes relacionados à infecção por *ransomware* vieram a público nos últimos anos [Gibbs 2016] [Winton 2016] [Smith 2016], porém o mais emblemático talvez tenha sido o WannaCry, devido a algumas características peculiares: **(i) Gerou grande impacto e pânico internacional** – infectou mais de 200 mil computadores em 150 países, interrompeu a operação de hospitais e empresas, e é visto como um dos maiores incidentes da atualidade [Reuters 2017]; **(ii) Kill Switch** -– esta não é uma característica propriamente nova em *malware*, mas no caso do WannaCry foi fundamental na contenção do ataque inicial, tendo evitado a propagação da epidemia e transformado o jovem pesquisador que o identificou numa celebridade; **(iii) Utilizou um código roubado da NSA** e trouxe polêmica sobre o tema de agências de defesa armazenarem código malicioso de vulnerabilidades não divulgadas; **(iv) Levou a Microsoft a desenvolver, extraordinariamente, atualizações para o Windows XP**, sistema operacional cujo suporte foi descontinuado em 8 de abril de 2014; **(v) Apesar do impacto, o *malware* não possui qualidades inovadoras**, pelo contrário: possui baixa complexidade e reaproveitou código de ameaças anteriores.

Estas características tornam o WannaCry um ótimo candidato para um estudo de caso. Além disso, o alcance e velocidade do ataque mostram a necessidade de uma melhor preparação para se responder rapidamente a futuras ameaças.

2. Objetivos

O objetivo é realizar um estudo de caso do WannaCry e, no contexto de um trabalho maior de dissertação de Mestrado, contribuir com a identificação de oportunidades de melhoria nos sistemas e processos preventivos e responsivos, subsidiando a construção de um *framework* de apoio para o desenvolvimento e operação de iniciativas de resposta a incidentes de Segurança da Informação.

3. Metodologia

Foi desenvolvida uma pesquisa de caso exploratória em uma empresa listada na Fortune 500 (lista com as 500 maiores empresas do mundo, segundo a revista Fortune), realizando um estudo analítico de combinação de padrão [Yin 2015] que compara as observações empíricas deste estudo com descobertas de trabalhos relacionados.

Os dados da pesquisa foram obtidos de documentações internas sobre o incidente, entrevistas informais com atores chave, bem como de informações publicamente disponíveis. Também foi realizada revisão bibliográfica de trabalhos relacionados que auxiliam na convergência das teorias defendidas.

4. Estudo de caso

Esta seção descreve detalhes sobre a ameaça e as observações do estudo de caso. Como se trata de um estudo de caso único e não foram encontrados outros estudos disponíveis com o mesmo nível de detalhes, as comparações se limitam a dados e estatísticas obtidos em fontes de dados abertas.

4.1. Visão geral do ransomware WannaCry

A ameaça é composta por duas partes: (i) Módulo *worm* – componente responsável pela propagação da ameaça e instalação do módulo *ransomware*; (ii) Módulo *ransomware* – componente responsável pelas atividades de extorsão da ameaça. [Symantec 2017]

(i) Módulo *worm*

O módulo *worm* utiliza o *exploit* EternalBlue para explorar duas vulnerabilidades do serviço SMBv1 no Windows (CVE-2017-0144 e CVE-2017-0145), e assim disseminar o módulo *ransomware*. Estas vulnerabilidades impactam todas as versões do Windows que tenham o SMBv1 habilitado, porém a Microsoft publicou em 14/03/2017 atualizações para corrigi-las. O *exploit* EternalBlue fazia parte de um conjunto de ferramentas e arquivos roubados da NSA pelo grupo *hacker* Shadow Brokers e foram publicadas na internet em abril de 2017, após tentativas infrutíferas de vender o material vazado.

Quando executado, o módulo *worm* tenta contactar um dos domínios a seguir. Caso algum deles esteja alcançável, a execução é interrompida imediatamente. Esta funcionalidade atua como uma chave de desligamento (*kill-switch*), permitindo que a ameaça seja parada e, provavelmente, foi incluída para burlar sistemas de defesa que utilizam *sandboxing*, pois estes sistemas costumam responder a requisições para qualquer URL.

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Estes domínios não estavam registrados quando a ameaça foi lançada. Um pesquisador registrou os domínios assim que os descobriu, fazendo com que esta versão da ameaça parasse de se disseminar. Posteriormente, surgiram versões da ameaça com variações nestas URLs e até mesmo sem o recurso de *kill-switch*.

O *worm*, verificando que as URLs não estão responsivas, registra-se como um serviço no Windows e tenta instalar o módulo *ransomware* como um arquivo de sistema (%windir%\tasksche.exe). O módulo *ransomware* está embutido no próprio binário do *worm*, portanto não precisa ser baixado pela internet, como ocorre com outras ameaças.

O módulo *worm* tenta, em seguida, baixar uma ferramenta para conexão à rede anônima TOR e tenta se conectar a alguns domínios TOR. Estes domínios são utilizados apenas para rastrear as infecções e prover um endereço de pagamento Bitcoin único, bem como as chaves de decriptografia, caso a vítima pague pelo resgate. Esta funcionalidade, porém, possui um bug e não é executada corretamente.

O *worm*, então, tenta se propagar, realizando *scan* por portas 445 abertas nos seguintes endereços: (i) IPs da mesma subrede do computador infectado; (ii) **IPs gerados aleatoriamente** – este foi considerado um dos principais vetores de infecção global do WannaCry. Uma vez identificado um computador com a porta 445 aberta, o *worm* tenta explorar as vulnerabilidades já informadas e, caso obtenha sucesso, o novo computador será infectado e todo o ciclo recomeça.

(ii) Módulo ransomware

Ao ser executado, o módulo *ransomware* instala-se como um serviço, que será executado sempre que o computador for reiniciado. Os nomes das pastas e do serviço criados utilizam uma sequencia aleatória de caracteres. Inicia-se a rotina de criptografia:

- O módulo procura por vários tipos de extensões de arquivos específicas: documentos, multimídia, bancos de dados, arquivos compactados, etc.;
- Cada arquivo é criptografado com um chave simétrica AES individual. Cada chave AES é criptografada individualmente usando criptografia assimétrica RSA, com chave de 2048 bits;
- Os arquivos criptografados têm a extensão ".WCRY" adicionada ao seu nome original. Exemplo: "foto.jpg" é criptografado para "foto.jpg.WCRY";
- O módulo tenta deletar *shadow copies* (Cópia de Sombra de Volume do Windows, uma espécie de *backup* integrado no sistema operacional) dos arquivos criptografados, de maneira a impedir a recuperação dos arquivos originais pelos usuários;
- Concluída a rotina de criptografia, são extraídos arquivos com as instruções de pagamento em diversos idiomas, além do próprio binário que permite descriptografar amostras de arquivos, e é exibida a "mensagem de resgate".

A lógica de pagamento do módulo *ransomware* previa a geração de um endereço Bitcoin único para cada usuário infectado, utilizando a rede TOR, porém, devido a um *bug* apenas três endereços Bitcoin são disponibilizados e compartilhados com todas as vítimas, de maneira que **o atacante não tem como determinar quem pagou pelo "resgate"**.

Estas características são de apenas uma das variantes da ameaça. Outras variantes foram descobertas após o ataque inicial e podem surgir novas derivações do *ransomware*.

4.2. O estudo de caso

As informações coletadas foram inicialmente descritas em ordem cronológica, com detalhamento dos fatos e ações tomadas. Em seguida as ações foram agrupadas em fases, de acordo com o processo de resposta a incidentes proposto por [Grispos 2016].

4.2.1. Preparação

A fase de preparação consiste na criação de um time de resposta a incidentes e o provisionamento de ferramentas e recursos que permitam responder adequadamente aos incidentes de Segurança da Informação.

A empresa do estudo de caso possui, há mais de 10 anos, uma gerência responsável por aspectos estratégicos e técnicos de Segurança da Informação na companhia e é responsável pela resposta a incidentes. Equipes formais dedicadas para detecção e resposta a incidentes de Segurança da Informação foram estabelecidas aproximadamente 8 meses antes do incidente com o WannaCry.

4.2.2. Identificação

A fase de Identificação está relacionada à detecção ou reporte de incidentes numa organização. A detecção do incidente, no caso estudado, deu-se no dia 12/05/2017, que, por convenção, será referenciado como **dia 1**. As seguintes ações ocorreram:

(i) Na **manhã do dia 1**, a equipe de monitoração detectou um serviço com nome "estranho" (conjunto aleatório de caracteres) em um servidor virtual; (ii) A equipe contatou o responsável pelo servidor; (iii) Foi detectado que o servidor estava infectado pelo

ransomware WannaCry e a equipe de resposta a incidentes foi acionada; (iv) Uma hora depois, foram confirmados 12 servidores virtuais, no mesmo segmento de rede, infectados; (v) Agentes HIPS (sistema de prevenção de intrusão nos *hosts*) detectaram tráfego suspeito oriundo de filiais. Posteriormente, foi identificado que os agentes HIPS já possuíam "assinatura" que identificava e bloqueava a exploração das vulnerabilidades no SMBv1, **um importante elemento de contenção ao ataque**.

4.2.3. Contenção

A fase de contenção consiste nas ações para evitar que um incidente sobrecarregue recursos, aumente o seu dano ou seja disseminado. As seguintes ações foram implementadas:

DIA 1: (i) Os primeiros servidores infectados detectados faziam parte de uma mesma subrede, que foi isolada com o objetivo de conter a propagação a partir deles; (ii) Foram bloqueadas as portas exploradas pelo *ransomware* nas conexões com redes de filiais; (iii) Segmentos onde a TI não possuía autonomia para atuar, mas que apresentaram tráfego suspeito, foram isolados; (iv) *Hosts* não isolados que não foram contemplados nos casos anteriores foram desligados, quando possível; (v) Foi configurado o bloqueio da execução de binários previamente conhecidos do *ransomware* (amostras da companhia e do próprio fornecedor de antivírus); (vi) Foi iniciada nova distribuição das atualizações que corrigiam as vulnerabilidades, com reinicialização obrigatória; (vii) A primeira "vacina" foi disponibilizada pelo fornecedor de antivírus.

DIA 2: (i) Foram identificados 3 mil *hosts* com risco potencial de contaminação – com antivírus desatualizado e sem as atualizações de segurança. Em decisão conjunta com corpo gerencial, o time de resposta a incidentes optou por desconectar da rede estes equipamentos como medida para evitar a propagação do *ransomware*;

DIA 3: (i) No fim do dia foi instalado um servidor Web interno e o DNS da companhia foi configurado para direcionar as chamadas às URLs do "*kill switch*" para este servidor, criando-se então um *honey pot* (uma espécie de armadilha para coletar informações sobre a ameaça). Este último recurso, embora simples, foi extremamente eficiente no tratamento do *ransomware*, por duas razões: a. Interrompeu o ataque (da variente original); b. Criou um mecanismo para identificar a origem de *hosts* infectados, gerando insumo para posterior tratamento (atuou como um recurso de IDENTIFICAÇÃO).

4.2.4. Erradicação

A fase de erradicação envolve a implementação de soluções para prevenir novas ocorrências do incidente. As seguintes ações de erradicação foram realizadas:

DIA 4: (i) Foram bloqueadas as extensões do WannaCry nos servidores de arquivos, com o objetivo de coibir ações de criptografia do *ransomware* em arquivos de rede; (ii) Foi iniciada rotina para detecção de máquinas suspeitas/vulneráveis e tratamento (24x7); (iii) Equipes de suporte local foram instruídas a aplicar os procedimentos necessários nos casos de máquinas suspeitas antes que elas pudessem ser religadas.

Ações da rotina de tratamento: a. Aplicação das atualizações de Sistema Ope-

racional; b. Atualização do antivírus c. Reinicialização forçada dos equipamentos; d. Execução do *scan* completo do antivírus. Critérios adotados no tratamento: **Estações administradas**: tratamento remoto; **Estações não administradas**: desconectadas da rede; **Servidores**: delegado tratamento emergencial para os respectivos responsáveis; **Servidores sem identificação ou responsável**: porta de rede desabilitada.

4.2.5. Recuperação

A fase de recuperação consiste em restaurar os sistemas afetados e retomar a operação normal do negócio. As seguintes ações de recuperação foram observadas:

DIA 5 em diante: (i) Foi estabelecido um fluxo padrão para autorização do desbloqueio de portas que exigia sempre autorização do grupo de resposta a incidentes; (ii) Redes de filiais foram reconectadas gradativamente, na medida em que seus administradores reportavam status seguro. Eventualmente, em casos onde não foi possível atuação, mas a reconexão se fazia necessária, para minimizar os riscos foram liberadas portas de maneira seletiva, apenas para garantir a operação dos serviços essenciais. Na medida em que foram religadas, as redes ganharam monitoração especial para identificação de possíveis riscos; (iii) No processo de avaliação das redes de filiais, foram detectados vários problemas de padronização e arquitetura. Este processo de avaliação deveria ocorrer frequentemente, independente do processo de resposta a incidentes.

4.2.6. Acompanhamento

O objetivo principal da fase de acompanhamento é estabelecer lições aprendidas, disseminá-las internamente na organização e, eventualmente, para agentes regulatórios externos. Relatórios técnicos e gerenciais textuais, com detalhes sobre o incidente, lições aprendidas e recomendações, foram gerados poucos dias após o ataque.

4.3. Oportunidades de melhoria e contribuições

Mesmo sendo considerado um processo de resposta bem sucedido, várias oportunidades de melhoria foram observadas.

Na fase de identificação, inicialmente, foi desafiador detectar os *hosts* suspeitos. Os critérios e regras de detecção, bem como as corretas configurações das ferramentas, aconteceram na medida em que o incidente era tratado. Embora a escolha correta de ferramentas e configuração de regras e correlações sejam pontos fundamentais para a detecção de eventos, que é o cerne da resposta a incidentes, é recorrente a dificuldade das organizações de operar e amadurecer este processo [Ab Rahman and Choo 2015]. Visibilidade do ambiente é de suma importância, portanto **há carência de um modelo que auxilie as organizações no processo de seleção, configuração e operação de ferramentas de monitoração, bem como metodologias de avaliação da sua eficiência e maturidade**.

Na fase de **contenção**, observou-se falta de colaboração e pesquisa com atores externos. Um analista dedicado à pesquisa sobre o *malware* ou informações assertivas dos fornecedores de soluções de segurança teriam permitido a implantação do *kill switch* com

maior antecedência, já que a informação estava disponível desde o **dia 2**. As distribuições de atualizações e pacotes de *software* foram lentas. É preciso investir em ferramentas e processos que tornem mais eficiente esta distribuição.

Na fase de **erradicação**, houve problemas com a correta identificação de responsáveis pelos servidores no Banco de Dados de Gestão de Configuração (BDGC), ou seja, uma não conformidade com políticas gerais e boas práticas de Segurança da Informação. A equipe também não possuía privilégios adequados em diversos *hosts* que precisavam de tratamento, outro problema que poderia ser resolvido com a utilização de ferramentas e processos adequados.

Na fase de **recuperação**, foram identificadas diversas vulnerabilidades e desvios de padrões durante o processo de reconexão das filiais, permitindo a sua documentação e indicação das correções. Este foi um saldo positivo desta fase, porém também é um indicativo de que o processo de revisão e auditoria das conexões deve ser implantado como uma rotina sistemática e periódica.

No contexto do **acompanhamento**, ao longo do tratamento, não havia uma pessoa dedicada à documentação dos processos, tampouco um modelo de dados ou sistema de apoio para o seu registro. De uma maneira geral, nota-se que há carência de um modelo estruturado para a documentação do incidente. Por esta razão, a criação dos relatórios técnicos e executivos foi um processo lento que exigiu a colaboração de todos os envolvidos e a consulta a informações de fontes diversas, como e-mails e rascunhos em papel. Incidentes menos relevantes provavelmente não serão documentados ou não terão o mesmo nível de detalhes e escrutínio. **Este é um campo com grande oportunidade de melhoria**, uma vez que a documentação sistemática dos incidentes permite: (i) ater-se a detalhes importantes; (ii) obter estatísticas e conhecimentos diversos da base de incidentes após a sua conclusão e (iii) possibilidade de compartilhamento de informações anonimizadas com órgãos de defesa e outros grupos de resposta a incidentes.

Em um estudo com outra empresa da Forbes 500, [Grispos 2016] identificou que pequenas melhorias na qualidade da documentação do incidente trouxe ganhos significativos para o processo de resposta a incidentes. Por esta razão, optou-se por contribuir na dissertação com um *framework* de resposta a incidentes que foque na melhoria sistemática da documentação e registro dos incidentes, baseado nos achados de [Grispos 2016] e na ontologia proposta por [VERIS 2017].

O trabalho de [Ab Rahman and Choo 2015] corrobora com as conclusões sobre as oportunidades no contexto do acompanhamento, pois conclui que "não há estudo abrangente sobre o tratamento de incidentes" na literatura.

5. Conclusões e próximos passos

Ainda que mudem as motivações e as técnicas, os sinais indicam que as ameaças cibernéticas continuarão avançando. Por mais que se invista em soluções e processos preventivos, incidentes serão inevitáveis e é preciso preparar-se para respondê-los de maneira eficiente e, por isso, a produção acadêmica neste campo é tão importante. Com esta breve análise podemos, confirmar a hipótese de que a crise poderia ter sido pior caso o *malware* tivesse uma ou mais das seguintes características: (i) uma vulnerabilidade de dia zero – aquela sem correção disponível pelo fabricante; (ii) não tivesse o recurso de *kill switch*;

(iii) adotasse comportamento discreto na fase de disseminação, com ativação futura programada (do módulo *ransomware* ou qualquer outro).

Este estudo de caso é parte de um trabalho maior, de dissertação de mestrado, onde pretende-se construir um *framework* de apoio para o desenvolvimento de processos e práticas relacionados à resposta a incidentes de Segurança da Informação.

Referências

Ab Rahman, N. H. and Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, 49:45–69.

AYRAPETOV, D. (2017). Practical defense for cyber attacks and lessons from 2017 sonicwall annual threat report. 29 ago. de 2017.

CERT.br (2017). Estatísticas dos incidentes reportados ao cert.br - 2017. 16 ago. de 2017.

Cobb, S. (2017). Rot: Ransomware of things. 29 ago. de 2017.

Economist.com (2017). Ransomware attacks were on the rise, even before the latest episode. 29 ago. de 2017.

Formby, D., Durbha, S., and Beyah, R. (2017). Out of control: Ransomware for industrial control systems. 29 ago. de 2017.

Franceschi-Bicchierai, L. (2016). Hackers make the first-ever ransomware for smart thermostats. 29 ago. de 2017.

Gibbs, S. (2016). Ransomware attack on San Francisco public transit gives everyone a free ride. 12 fev. de 2017.

Grispos, G. (2016). *On the enhancement of data quality in security incident response investigations*. PhD thesis, University of Glasgow.

Healey, J. (2016). Winning and losing in cyberspace. In *International Conference on Cyber Conflict (CyCon)*, pages 37–49. IEEE. 08 fev. de 2017.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E. (2015). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, volume 9148, pages 3–24. Springer International Publishing, Milan.

O Globo (2015). Investimento em segurança da informação cresce mais no país - 2015. 08 fev. de 2017.

Reuters (2017). Analysis: Wannacry attack shows trend toward 'economic' cyber threats, rising regulatory risk. 28 ago. de 2017.

Smith, M. (2016). Kansas Heart Hospital hit with ransomware; attackers demand two ransoms. 12 fev. de 2017.

Symantec (2017). Ransom.wannacry technical details. 31 ago. de 2017.

Trend Micro (2016). Trend micro's definition of ransomware. 12 fev. de 2017.

VERIS (2017). Vocabulary for event recording and incident sharing. 27 mar. de 2017.

Winton, R. (2016). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. 12 fev. de 2017.

Yin, R. K. (2015). *Estudo de Caso: Planejamento e Métodos*. Bookman editora.

