WannaCry
Um pouco sobre um dos maiores CyberAttacks do Mundo

Henrique Rosa[51923] — Diogo Matos[54466]

Universidade de Évora, Évora 7000-000, Portugal

Abstract. O ataque WannaCry foi um dos maiores e mais devastadores ciberataques de ransomware na história, afetando milhões de sistemas em mais de 150 países. Explorando uma vulnerabilidade no protocolo SMB do Windows, conhecida como EternalBlue, o ransomware encriptou dados de sistemas críticos e exigiu resgates em Bitcoin. Este artigo explora a natureza do ataque, a sua propagação, os setores mais afetados e as respostas globais que ajudaram a conter sua disseminação. Analisamos também as implicações econômicas e as lições aprendidas que sublinham a importância de manter sistemas atualizados e protegidos contra vulnerabilidades conhecidas.

Keywords: Ransomware · CyberAttack · Malware · Segurança · Virus · EternalBlue

1 O que foi o WannaCry?

Foi um vírus de computador que abalou o mundo, afetando milhões de pessoas e equipamentos. Mais especificamente, tratava-se de um ransomware que se espalhou globalmente através de PCs com o Sistema Operativo Windows, tirando partido de um exploit chamado EternalBlue.

O custo estimado dos danos causados pelo WannaCry for de cerca de 4 mil milhões de dólares, classificando-o assim como um dos maiores ciberataques do mundo.

Embora a identidade da pessoa/grupo por trás deste ataque seja até hoje desconhecida, o governo dos Estados Unidos atribuiu oficialmente a culpa à Koreia do Norte, mais especificamente o grupo Larazus.

1.1 Propagação

O vírus propagou-se através do vetor de ataque chamado "EternalBlue" - uma vulnerabilidade no protocolo SMB do Windows que permite que um invasor execute código remotamente num computador vulnerável sem a necessidade de credenciais de acesso. Isto significa que, se um sistema não estiver atualizado com

os patches de segurança necessários, um invasor pode explorar essa vulnerabilidade para infectar o computador com malware sem a necessidade de interação do utilizador.

paragraph EternalBlue foi desenvolvido pela National Security Agency (NSA) dos Estados Unidos para sistemas Windows. Este exploit foi roubado e exposto por um grupo chamado The Shadow Brokers um mês antes do ataque. Embora a Microsoft tenha lançado patches para fechar esta vulnerabilidade, muitos dos sistemas afetados pelo WannaCry não tinham aplicado estas atualizações, ou estavam a usar versões desatualizadas do Windows que já não recebiam suporte.

Uma vez infetado, o computador envia pacotes maliciosos para todos os dispositivos conectados na mesma rede. Esses pacotes contêm dados que o sistema interpreta como instruções de código a serem executadas, permitindo que o malware se propague de forma autónoma e exponencial. Considerando que muitos utilizadores do Windows em todo o mundo não tinham atualizado o seu software ou estavam a usar versões desatualizadas do sistema operativo, esta falha permitiu que o WannaCry se espalhasse rapidamente, infetando centenas de milhares de computadores em mais de 150 países em questão de dias.

A rápida disseminação do WannaCry evidenciou a importância de manter os sistemas operativos atualizados com os patches de segurança mais recentes. A vulnerabilidade explorada pelo EternalBlue já havia sido corrigida pela Microsoft meses antes do ataque, mas a falha na aplicação dessas atualizações permitiu que o ransomware causasse danos em larga escala.

O ataque começou às 07:44 UTC de 12 de maio de 2017 e foi interrompido algumas horas depois, às 15:03 UTC, pela ativação de um kill switch descoberto por Marcus Hutchins. Este kill switch impediu que computadores já infetados fossem encriptados ou continuassem a espalhar o WannaCry.

1.2 Mas afinal o que faz o vírus WannaCry?

Fig. 1. Interface WannaCry

Uma vez infectado, o WannaCry encripta os arquivos do sistema, tornando-os inacessíveis para o utilizador, exibindo uma ‘’nota de resgate” que exige que o utilizador pague uma quantia em Bitcoin para desencriptar os arquivos num tempo de até 6 dias, após os quais os arquivos seriam apagados. O valor inicialmente pedido seria de 300 dólares, sendo esse valor dobrado se o utilizador demorasse muito a pagar. A Figura 1 mostra um pouco do que era a interface mostrada a quem era infetado.

O WannaCry utiliza o exploit EternalBlue para ganhar acesso ao sistema e o DoublePulsar para instalar e executar uma cópia de si mesmo. Quando executado, o malware primeiro verifica um domínio kill switch; se não o encontrar, encripta os dados do computador e tenta explorar a vulnerabilidade SMB para se espalhar para outros computadores na Internet e lateralmente na mesma rede. O malware esconde a pasta extraída, modifica os dados de segurança, cria uma chave de encriptação e elimina cópias dos ficheiros.

Várias organizações, incluindo Microsoft, Cisco, Malwarebytes, Symantec e McAfee, publicaram análises técnicas detalhadas do malware.

2 Setores Afetados

O ataque WannaCry teve um impacto significativo em diversos setores ao redor do mundo, afetando operações críticas e causando disrupções em várias indústrias. Abaixo, descrevemos alguns dos setores mais afetados e os impactos específicos que sofreram:

2.1 Assistência Médica

Um dos setores mais gravemente afetados foi o da assistência médica, com destaque para o Serviço Nacional de Saúde (NHS) do Reino Unido. Em Inglaterra e Escócia, até 70.000 dispositivos, incluindo computadores, scanners de ressonância magnética, frigoríficos de armazenamento de sangue e equipamentos de teatro, foram potencialmente comprometidos pelo ransomware. No dia 12 de maio de 2017, alguns serviços do NHS tiveram de recusar emergências não críticas e algumas ambulâncias foram desviadas para outros hospitais. Em 2016, foi reportado que milhares de computadores em 42 do NHS em Inglaterra ainda utilizavam o Windows XP. Em 2018, um relatório de membros do Parlamento concluiu que todos os 200 hospitais ou outras organizações do NHS verificadas após o ataque ainda não cumpriam os padrões de cibersegurança. Curiosamente, os hospitais do NHS em Gales e Irlanda do Norte não foram afetados pelo ataque.

2.2 Emergência e Segurança

Além do impacto direto nos hospitais, outros serviços de emergência também foram afetados, embora em menor escala. A capacidade de resposta a emergências foi comprometida, com desvio de ambulâncias e atrasos nos atendimentos devido à falha nos sistemas de IT.

2.3 Logística e Transporte

O setor de logística e transporte também sofreu com o ataque. Empresas como a FedEx e a Deutsche Bahn foram atingidas, causando disrupções nas operações de transporte e entrega. Em Espanha, a Telefónica também foi uma das empresas afetadas. A Nissan Motor Manufacturing UK, localizada em Tyne and Wear, Inglaterra, teve que interromper a produção após o ransomware infetar alguns dos seus sistemas. De forma semelhante, a Renault suspendeu a produção em vários locais para tentar conter a propagação do ransomware.

2.4 Telecomunicações

Empresas de telecomunicações foram igualmente afetadas. A Telefónica, uma das maiores operadoras de telecomunicações da Espanha, sofreu com a infeção, resultando em paralisações e disrupções nos serviços.

2.5 Indústria Automóvel

A indústria automóvel também não foi poupada. Além da Nissan e da Renault, outras empresas do setor enfrentaram dificuldades devido ao ataque, com paragens de produção e perda de dados importantes.

2.6 Educação

O setor da educação também viu interrupções, com várias instituições a enfrentar problemas nos seus sistemas informáticos, afetando a administração e a capacidade de ensino.

2.7 Outros Setores Afetados

Outros setores impactados pelo ataque incluíram o gás, a gasolina e os anúncios. Empresas nesses setores enfrentaram perdas significativas devido à interrupção dos seus sistemas informáticos e operações comerciais.

2.8 Impacto Económico

Segundo a empresa de modelagem de risco cibernético Cyence, as perdas económicas decorrentes do ataque cibernético poderiam chegar até 4 mil milhões de dólares, com outras estimativas situando as perdas na casa das centenas de milhões. O impacto do ataque foi considerado relativamente baixo em comparação com outros potenciais ataques do mesmo tipo e poderia ter sido muito pior se não fosse pela descoberta do kill switch por Marcus Hutchins ou se tivesse sido direcionado especificamente para infraestruturas altamente críticas, como centrais nucleares, barragens ou sistemas ferroviários.

O ataque WannaCry destacou a vulnerabilidade de várias indústrias a ataques cibernéticos e sublinhou a importância de manter sistemas de TI atualizados e protegidos contra exploits conhecidos.

3 Resposta ao Ataque

Depois de se espalhar rapidamente por todo o mundo, o especialista em segurança informática Marcus Hutchins descobriu um kill switch que diminuiu significativamente a propagação do ataque. Esse kill switch consistia num URL específico que o malware tentava acessar antes de se infiltrar nos sistemas infectados. Hutchins notou que o malware verificava a disponibilidade desse URL antes de prosseguir com o ataque. Ele então registrou esse domínio não utilizado, o que essencialmente ativou o kill switch. Quando o WannaCry tentava conectar-se a esse URL, se a conexão fosse bem-sucedida, o malware não continuava a sua atividade maliciosa, interrompendo efetivamente a propagação em muitos sistemas ao redor do mundo.

Paralelamente, especialistas rapidamente aconselharam os usuários afetados a não pagar o resgate, devido à falta de relatos de pessoas que recuperaram seus dados após o pagamento, além de que altos lucros incentivariam mais campanhas desse tipo. Até 14 de junho de 2017, após o ataque ter diminuído, um total de 327 pagamentos, totalizando US$130,634.77 (51.62396539 BTC), havia sido transferido.

No dia seguinte ao ataque inicial em maio, a Microsoft lançou atualizações de segurança fora do ciclo normal para produtos descontinuados, como o Windows XP, Windows Server 2003 e Windows 8; essas correções tinham sido criadas em fevereiro, mas estavam disponíveis apenas para aqueles que pagavam por um plano de suporte personalizado. As organizações foram aconselhadas a atualizar o Windows e corrigir a vulnerabilidade para se protegerem contra o ataque cibernético. Adrienne Hall, chefe do Centro de Operações de Defesa Cibernética da Microsoft, declarou que "Devido ao risco elevado de ataques cibernéticos destrutivos neste momento, decidimos tomar esta ação porque aplicar essas atualizações oferece maior proteção contra possíveis ataques com características semelhantes ao WannaCrypt [nome alternativo para WannaCry]".

Hutchins registrou um domínio nomeado em um DNS sinkhole que parou a propagação do ataque como um worm, porque o ransomware apenas encriptava os arquivos do computador se não conseguisse conectar-se a esse domínio. Embora isso não ajudasse os sistemas já infectados, diminuiu significativamente a propagação da infecção inicial e deu tempo para que medidas defensivas fossem implementadas em todo o mundo, especialmente na América do Norte e Ásia, que não haviam sido atacadas na mesma medida que outras regiões.

Em 14 de maio, uma primeira variante do WannaCry apareceu com um novo e segundo kill switch registado por Matt Suiche no mesmo dia. Isso foi seguido por uma segunda variante com o terceiro e último kill switch em 15 de maio, registado por analistas de inteligência de ameaças da Check Point. Poucos dias depois, uma nova versão do WannaCry foi detectada sem nenhum kill switch.

Em 19 de maio, foi relatado que hackers estavam tentando usar uma variante do botnet Mirai para realizar um ataque de negação de serviço distribuído (DDoS) no domínio do kill switch do WannaCry com a intenção de tirá-lo do ar. Em 22 de maio, Hutchins protegeu o domínio ao mudar para uma versão em cache do site, capaz de lidar com cargas de tráfego muito mais altas do que o site ao vivo.

Separadamente, pesquisadores da University College London e da Boston University relataram que seu sistema PayBreak poderia derrotar o WannaCry e várias outras famílias de ransomware ao recuperar as chaves usadas para criptografar os dados do usuário.

Descobriu-se que as APIs de criptografia do Windows usadas pelo WannaCry podem não limpar completamente os números primos usados para gerar as chaves privadas da carga útil da memória, tornando potencialmente possível recuperar a chave necessária se ainda não tivesse sido sobrescrita ou limpa da memória residente. Esse comportamento foi utilizado por um pesquisador francês para desenvolver uma ferramenta conhecida como WannaKey, que automatiza esse processo em sistemas Windows XP. Essa abordagem foi iterada por uma segunda ferramenta conhecida como Wanakiwi, que foi testada para funcionar no Windows 7 e Server 2008 R2 também.

Dentro de quatro dias do ataque inicial, novas infecções diminuíram drasticamente devido a essas respostas, demonstrando a eficácia das medidas de contenção e mitigação implementadas globalmente.

Conclusão

O ataque WannaCry serviu como um alerta global sobre a vulnerabilidade dos sistemas informáticos a ciberataques de grande escala. A exploração da vulnerabilidade EternalBlue pela NSA, a sua subsequente divulgação pelo grupo Shadow Brokers e a falha em atualizar os sistemas Windows expostos foram fatores cruciais que permitiram a rápida disseminação do ransomware. Os impactos económicos, operacionais e sociais foram significativos, afetando setores críticos como saúde, transporte e telecomunicações.

A resposta ao ataque, liderada por especialistas em segurança informática, governos e a própria Microsoft, destacou a importância da colaboração internacional e da prontidão tecnológica na mitigação de ciberameaças. A descoberta do kill switch por Marcus Hutchins e a rápida disseminação de patches de segurança foram essenciais para conter o ataque e evitar danos ainda maiores.

Este evento sublinha a necessidade imperiosa de práticas de segurança robustas, incluindo a aplicação regular de atualizações de software e a educação contínua sobre cibersegurança. O WannaCry tornou-se um marco na história da segurança informática, lembrando-nos da importância de estar sempre um passo à frente das potenciais ameaças.

References

1. How the North Korean hackers behind WannaCry got away with a stunning crypto-heist, https://www.technologyreview.com/2020/01/24/276082/lazarus-group-dragonex-chainalysis/
2. WannaCry ransomware attack, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack/
3. What was WannaCry?, https://www.malwarebytes.com/wannacry