UNIVERSIDADE DE COIMBRA

FACULDADE DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

O VÍRUS WANNACRY

ELTON DA SILVA CHELQUE

LUCAS DE SOUZA SANTOS

LUIZ HENRIQUE ARÊAS PERES

Coimbra, 2017

UNIVERSIDADE DE COIMBRA

FACULDADE DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

O VÍRUS WANNACRY

ELTON DA SILVA CHELQUE

LUCAS DE SOUZA SANTOS

LUIZ HENRIQUE ARÊAS PERES

Trabalho apresentado na disciplina de Meios Computacionais no Ensino da Matemática, ministrada pelo Prof. Drº Jaime Maria Monteiro de Carvalho e Silva.

Coimbra, 2017

O VÍRUS WANNACRY

WannaCry (ou WannaCrypt) é um vírus de criptografia (nomeadamente, *Ransom.CryptXXX*) que vem se espalhando por computadores com sistema operacional Windows, da Microsoft, desde o dia 12 de maio por todo o mundo e que já infectou mais de 300 mil computadores em 150 países.

O vírus é do tipo *Ransomware*, que se espalha através de links ou e-mails. Após indentificarem uma vulnerabilidade no sistema, os responsáveis pelo WannaCry criaram um software, que, ao entrar em contato com o computador, o bloqueia, codifica tudo que nele há e pede como resgate para a decodificação a quantia de 300 dólares em *bitcoins* (moedas). Segundo o programa Avast, o vírus consegue atingir 178 tipos de extensões de arquivos.

O *Ransomware* é um tipo de vírus bastante conhecido, porém, WannaCry tomou uma proporção assustadoramente grande num tempo muito pequeno, o que preocupa os especialistas.

Nesse tipo de ataque cibernético, é preferível a utilização da moeda *bitcoin* por se tratar de uma moeda virtual criptografada não envolvendo instituições financeiras para um indivíduo adquirir esse dinheiro. A cotação dessa moeda varia muito e, no dia 23 de maio, 1 *bitcoin* variou, em minutos, de 2236.91 a 1724.11 dólares.

Antes da criação do vírus, a agência de segurança americana NSA vinha utilizando ferramentas para acessar os computadores de pessoas que estavam sendo investigadas. Foi então que o grupo de hackers “Shadow Brokers”, ao encontrar essas ferramentas, descobriu e divulgou no site wikileaks.org a vulnerabilidade do sistema Windows, utilizada pela NSA para a sua ação.

A vulnerabilidade no sistema já havia sido detectada e a empresa montou uma atualização de correção, porém essa atualização era paga e nem todos os clientes a adquiriram, além de nem todas as versões do sistema serem contemplada, por já serem descontinuadas.

As especulações iniciais para a origem do vírus foram o Brasil e a Coreia do Norte. Esta última apontada como responsável pelo ataque depois que um integrante da Google encontrou semelhanças entre o WannaCry e outro vírus feito por hackers norte coreanos, que atacaram a empresa Sony, por seu filme “A Entrevista”, que tem uma apresentação de Kim Jong-Um, líder do país, que não os agradou.

Depois do grande alcanço do vírus, um britânico de 22 anos e responsável pelo site MalwareTech, chamado Marcus Hutchins, conseguiu frear a ação do vírus depois que registrou

o domínio com um endereço eletrônico encontrado no código do vírus. Segundo Hutchins, o malware se conecta a um domínio sem registro, mas ele estava programado para, caso identificasse um registro neste domínio, parar de se espalhar, como se fosse um dispositivo de segurança.

Esse registro lhe custou apenas 10,69 dólares e fez com que o vírus parasse de se espalhar. O feito acidental foi reconhecido pelo grupo de hackers HackersOne, que tem o hábito de recompensar pessoas que trabalham para encontrar problemas como esse. A quantia dada foi de 10 mil dólares, dinheiro que Marcus resolveu doar para instituições de caridade.

Porém, ainda não foi descoberta uma forma de destruiur o vírus. Um dos poucos avanços que se obteve foi o divulgado sexta-feira, dia 19, por pesquisadores franceses, que encontraram uma forma de salvar os computadores infectados.

A solução, de acordo com os pesquisadores, só funciona em algumas condições: se os computadores ainda não foram reiniciados depois da infecção e se for utilizada antes do vírus realmente bloquear o computador.

Três dos integrantes do grupo que conseguiu encontrar essa solução são Adrien Guinet, um especialista de segurança, Matthieu Suiche, um hacker conhecido internacionalmente, e Benjamin Delpy, que trabalha no Banque de France. Um resumo do que foi feito pelo grupo foi colocado em um blog criado por Suiche, que conta melhor como a ferramenta nomeada por eles de Wannakey foi criada.

Além disso, a moeda *bitcoin* é tida como irrastreável, contudo, é possível monitorar as movimentações realizadas, utilizando, por exemplo, o site https://blockchain.info/, o que pode ajudar a levar aos criadores do vírus e a recuperar o dinheiro dos resgates.

Porém, o vírus continua vivo e se espalhando facilmente pelos computadores do sistema Windows. Segundo especialista, a melhor forma de se proteger é manter o Windows e o Antivírus sempre atualizados, bem como ter cuidado com e-mails estranhos e sites que utilizem pop-up.

Em relação aos números obtidos dos computadores infectados, houve uma surpresa: esperava-se que as versões do Windows mais atingidas fossem a XP e a Vista, que são versões mais antigas, que a Microsoft não atualiza mais. Porém, o maior alvo do Wannacry foi a versão Windows 7, correspondendo a 98.35% do ataque (60.35%, na versão 7 x64 Edition; 31.72% na versão 7; 3.67%, na versão 7 Home x64 Edition e 2.61%, na versão 7 Home). Isso mostra que o ataque foi direcionado às máquinas que ainda não possuíam o patch de atualização com as correções disponibilizado pela empresa e não nas versões mais antigas, como se esperava.

Mesmo após a compra do domínio feita por Marcus, os hackers responsáveis pelo vírus, querendo derrubar o mecanismo de defesa, tentaram sobrecarregar o site, para seu domínio cair. Para isso, realizaram mais de 2.3 milhões de acessos ao site em apenas seis horas com uma rede de *botnets*. Para detê-los, Marcus recorreu a uma versão em cachê da página, o que permite que ele retome o site a um ponto antes dos acessos feitos.

Para além disso, não se tem previsão para se chegar a uma solução mais concreta.

REFERÊNCIAS BIBLIOGRÁFICAS

O QUE É O VÍRUS WANNACRY, COMO COMEÇOU E COMO ESTÁ A SER COMBATIDO?. Disponível em: <http://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/o-que-e-o-virus-wannacry-como-comecou-e-como-esta-a-ser-combatido>
Acesso: 20 de maio de 2017.

PESQUISADOR IMPEDE ACIDENTALMENTE A PROPAGAÇÃO DE WANNACRY, MAS DIZ QUE É TEMPORÁRIO. Disponível em: <https://jovemnerd.com.br/nerdnews/pesquisador-impede-propagacao-de-wannacrypt-mas-garante-que-isso-e-temporario/>
Acesso em: 20 de maio de 2017.

PESQUISADORES DESCOBREM COMO DESBLOQUEAR ARQUIVOS ATINGIDOS POR VÍRUS WANNACRY. Disponível em: <http://g1.globo.com/tecnologia/noticia/pesquisadores-descobrem-como-desbloquear-arquivos-atingidos-por-virus-wannacry.ghtml>
Acesso em: 20 de maio de 2017.

RESPONSÁVEL POR TRAVAR O VÍRUS WANNACRY VAI DOAR 10 MIL DÓLARES À CARIDADE. Disponível em: <http://observador.pt/2017/05/17/responsavel-por-travar-o-virus-wannacry-vai-doar-10-mil-dolares-a-caridade/>
Acesso em: 20 de maio de 2017.

BITCOIN. Disponível em: < http://www.dicionarioinformal.com.br/bitcoin/>
Acesso em: 22 de maio de 2017.

WINDOWS 7 FOI O MAIS AFETADO PELO RANSOMWARE WANNACRY. Disponível em:
<https://pplware.sapo.pt/microsoft/windows/windows-7-afetado-wannacry/>
Acesso em: 23 de maio de 2017.

WANNACRY: HACKERS QUE CRIARAM RANSOMWARE TENTAM REVIVER ATAQUE. Disponível em:
<http://www.techtudo.com.br/noticias/2017/05/wannacry-hackers-que-criaram-ransomware-tentam-reviver-ataque.ghtml>
Acesso em: 23 de maio de 2017.

O QUE VOCÊ PRECISA SABER SOBRE O RANSOMWARE WANNACRYPT. Disponível em:
<http://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml>
Acesso em: 23 de maio de 2017.

WANNACRY – COMO OS HACKERS IRÃO RESGATAR OS BITCOINS. Disponível em:
<http://multiversogeekacre.blogspot.pt/2017/05/wanna-cry-como-o-hackers-irao-resgatar.html>
Acesso em: 23 de maio de 2017.