Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciências da Computação

Uma Análise da Evolução dos Ransomwares e das Técnicas de Prevenção e Remediação

Trabalho de Graduação

Discente: Tomás Arruda de Almeida

Orientador: Ruy José Guerra Barretto de Queiroz

Recife, 2016

Tomás Arruda de Almeida

Uma Análise da Evolução dos Ransomwares e Técnicas de Prevenção e Remediação

Trabalho desenvolvido para conclusão do curso de Bacharelado em Ciência da Computação da Universidade Federal de Pernambuco, sob orientação do Professor Ruy José Guerra Barretto de Queiroz.

Recife, 2016

Agradecimentos

Meus agradecimentos vão primeiramente a minha família por todo o apoio dado durante toda a minha vida, principalmente pela preocupação e cuidado na minha educação, sempre se esforçando para promover as melhores oportunidades para que eu tivesse uma educação concreta e bem sucedida.

Agradeço também a todos os meus amigos e que, de fora e de dentro da minha graduação na UFPE que se mostraram sempre disponíveis pra me ajudar no que fosse necessário em todos os âmbitos da minha vida, pessoal e profissional. Agradeço também a todos os momentos de descontração que me ajudaram a seguir adiante com um sorriso no rosto e também pelos aprendizados que forma dados por eles e tanto me motivaram e me ajudaram.

Meus agradecimentos também vão para todos os professores do curso de Ciência da Computação da UFPE pela enorme quantidade de conteúdo passado para mim, principalmente ao professor Ruy de Queiroz pela atenção na orientação desse projeto, com o cuidado de me manter informado em relação a todos os acontecimentos na área de segurança da informação. Um agradecimento especial a todos aqueles responsáveis por proporcionar minha participação no programa Ciências sem Fronteiras na Universidade de Kent, me proporcionando um enorme crescimento pessoal e profissional acarretado por todos os professores que foram responsáveis pelo meu aprendizado e amigos que me enriqueceram pessoalmente e culturalmente.

Abstract

Ransomwares are malwares that, when infecting a computer, are capable of block the user's access to his compute or encrypt important data from him. When succeeded they ask for a ransom - mainly in bitcoins - to unlock these data. The ransomwares have became a enormous threat nowadays, attacking common users, small and medium businesses, police departments and even big hospitals networks. They have shown a tremendous capacity to evolve their technics to avoid defence strategies, increasing their success rate in extortions. This project aims to analyse the various types of ransomwares, as well as the attacks history, seeking to demonstrate their evolution and impact.

Keywords: ransomware, malware, security, cryptography, bitcoins.

Resumo

Os ransomwares são malwares que, ao infectar um computador, podem bloquear o acesso do usuário ou criptografar dados importantes dele. Uma vez bem sucedidos, cobram uma quantia – geralmente em bitcoins -, para desbloquear o acesso a essas informações. Eles têm se tornado uma ameaça cada vez mais presente em nosso dia a dia visto que seu alvo vai desde usuários comuns, pequenas e médias empresas, departamentos de polícia até grandes redes de hospitais. Possuem uma enorme capacidade evolutiva, no que concerne às técnicas de bloqueio de estratégias de defesa; aumentando assim, sua resistência e capacidade de obter sucesso na extorsão. Será analisado neste trabalho, os diversos tipos de ransomwares e os seus ataques ao longo do tempo, com o intento de demonstrar a sua evolução e impacto.

Palavras-chaves: ransomware, malware, segurança, criptografia, bitcoins.

Índice

1 Introdução 8
1.1 Contextualização e Motivação 9
1.1.1 Malware 9
1.1.2 Sistema de Bitcoins 11
1.1.3 Ransomware 12
1.2 Objetivo do trabalho 13
1.3 Metodologia 13
1.4 Estrutura do trabalho 14

3 Ransomwares 15
3.1 Pré-infecção 15
3.2 Infecção 16
3.2.1 Procura por Alvos 16
3.2.2 Apreensão de dados 17
3.2.3 Cobrança de Resgate 18
3.3 Histórico de Ransomwares 18
3.3.1 O Primeiro Ransomware: AIDS Trojan 19
3.3.2 CryptoLocker 19
3.3.3 CryptoWall 21
3.3.4 Locky 23
3.3.5 CTB-Locker 26
3.4 Mobile Ransomwares 28
3.4.1 Simplocker 29
3.4.2 Small 30
3.4.3 Fusob 31
3.5 Outros Ransomwares 32
3.5.1 KeRanger 32
3.5.2 Petya 32
3.5.3 KimcilWare 33
3.5.4 CryptXXX 34
3.5.5 Jigsaw 35
3.5.6 TeslaCrypt 35

4 Histórico de ataques 38
4.1 Ataques a Hospitais 38
4.2 Ataque a Sites: Malvertising 40
4.3 Ataques à Polícia 40

5 Evolução da Abordagem 42
5.1 Análise de técnicas de ataque 42
5.1.1 Exploit Kits 43
5.1.2 Ransomware as a Service 45
5.1.3 Ransomware Cross-platform 47
5.2 Análise de técnicas de defesa 48
5.2.1 Técnicas de prevenção 48
5.2.2 Criação de Ferramentas 50

5.2.3 Uso da blockchain contra os ransomwares 52
5.2.4 Outras técnicas de combate 53
5.3 Impacto dos ransomwares 54
5.4 Uma perspectiva futura 55

6 Conclusão 58
6.1 Limitações do Trabalho 59
6.2 Trabalhos Futuros 59

7 Bibliografia 60

1 Introdução

Os chamados vírus de computador tem atingido sistemas ao redor do mundo desde a década de 80, quando surgiu o primeiro vírus formalmente apresentado. A nomenclatura “vírus de computador” foi designada para apenas uma categoria dos chamados malwares. Ao longo do tempo, até os dias de hoje, outras categorias de malwares foram surgindo, e a quantidade de ataques aumentado. Um tipo em especial, conhecida como criptovírus, conhecidos dessa forma por utilizarem de criptografia em seus ataques, ganhou maior representatividade nos últimos anos, principalmente após a virada do século. A partir dele surgiu um outro conceito, mais específico, o de ransomware, que tem se mostrado ser uma das maiores ameaças digitais já conhecidas.

O ransomware é uma tipo de malware capaz de “sequestrar” informações das suas vítimas, impossibilitando seu acesso a elas, e em seguida cobrar um “resgate“, um valor em dinheiro, em troca da senha que permitirá a recuperação das informações. Os Ransomwares têm se tornado, cada vez mais, uma grande ameaça para a segurança digital, de acordo com MEHMOOD (2016). Desde 2015 houve um aumento de 35% dos Crypto-Ransomwares, conhecidos dessa forma por criptografar os dados de sua vítima. Também, segundo a KASPERSKY (2016a), houve um aumento de 30% dos ataques de ransomwares no primeiro trimestre de 2016 comparado ao mesmo período de 2015, o número de vítimas desse período em 2016 gira em torno de 345.900. Portanto, ao longo do tempo, o número de vítimas tem aumentado e diversos tipos de ransomwares tem surgido e se aperfeiçoado, sempre no intuito de driblar as estratégias de segurança existentes e ganhar mais dinheiro de suas vítimas. Com base nesse enorme crescimento e impacto dos ransomwares atualmente este trabalho tem o propósito de analisar esse fenômeno comparando os diversos tipos de ransomwares e examinando os grandes ataques envolvendo ransomwares, tudo isso com o

objetivo de mostrar a vertiginosa evolução em sua capacidade ofensiva, em comparação com as técnicas de defesa atualmente, alertando sobre o grande perigo representado por esse tipo de malware.

Este capitulo tem o papel de introduzir conceitos chaves que facilitarão o entendimento de conceitos futuros como os de ransomwares e suas implicações. Além de explanar a motivação de levar o assunto, que atualmente é muito explorado de diversas formas, a um nível que demande cada vez mais atenção, tanto do público em geral quanto das autoridades competentes.

1.1 Contextualização e Motivação

1.1.1 Malware

O malware, de acordo com a PCTool, pode ser definido como um software malicioso que foi desenvolvido com a finalidade de causar algum dano ao computador da vítima, sem que ela tenha conhecimento. A Microsoft, por sua vez, define como software que obteve acesso a um computador sem o informe ou consentimento do usuário. Mas como ele tem acesso a um computador? Muitas vezes ele consegue ingresso através de anexos em e-mails, download e instalação de softwares desconhecidos.

Existem vários subtipos de malwares. Os mais conhecidos são: o popular vírus de computador, o *worm* e o Cavalo de Troia (ou *Trojan Horse).* Mas o que são, afinal*?*

Vírus: o chamado vírus de computador, é um software malicioso que está sempre junto com algum outro software e só pode infectar um computador quando esse software é executado. O vírus pode causar diversos transtornos em um computador infectado como, por exemplo, apagar arquivos importantes. É importante observar que o vírus só pode infectar e ser espalhado com auxílio humano, anexando-o a outro programas e transferindo de computador para computador.(BAEL, 2015)

Worm: assim como um vírus, worm tem a mesma capacidade de causar dano. A diferença crucial entre os dois está em como o worm se

propaga para outros computadores: diferentemente do vírus, o worm não precisa de auxílio humano para se difundir.. Ele, por sua vez, tem a capacidade de se duplicar por conta própria e se espalhar através das redes de computadores e a internet de forma autônoma. (BAEL, 2015)

Cavalo de Troia: o chamado Cavalo de Troia, assim como o vírus, só pode infectar um computador caso seja instalado através da ação humana. Assim como sua referencia mitológica, o Cavalo de Troia chega em um computador disfarçado de um programa aparentemente benéfico para o usuário, contudo pode causar diversos malefícios ao computador (BAEL, 2015). É importante observar também que, segundo (BAEL 2015), o Cavalo de Troia pode criar vulnerabilidades no computador como um backdoor. Em outas palavras esse tipo de malware pode abrir espaço para entrada de outros malwares ou coleta de informações do usuário, como por exemplo spywares e keyloggers que, segundo Siciliano (2013), conseguem rastrear cada comando de um usuário, executado pelo computador, como clique do mouse e tecla pressionada. Portanto o Cavalo de Troia representa uma ameaça no sentido de descobrir informações bancárias e senhas de contas online do usuário.

Os malwares são muitas vezes associados à internet - em razão de ser, atualmente, o seu principal veículo de propagação -, mas é importante frisar que a sua existência antecede a popularização da rede mundial de computadores. Como especificado pela PRICEONOMIC (2015), um dos primeiros vírus, ao infectar um computador, conseguia infectar os outros computadores da rede interna, nunca se propagando além desse ponto, pois não existia a internet, as redes eram apenas locais. Criado em 1971, ssse vírus era chamado de CREEPER e apenas mostrava uma mensagem na tela do computador da vítima e nada mais. Ainda segundo a PRICEONOMIC (2015), os primeiros malwares que realmente se tornaram virais foram compartilhados por mãos humanas através de floppy disks.

Sabemos que a internet é um veículo realmente eficiente de propagação de todo tipo de dado; a sua popularização tornou possível as epidemias de malwares. De acordo com BARLOWE (2012), os primeiros malwares a obterem destaque foram o Melissa, em 1999, e o LoveLetter, em

2000, ambos se espalhavam por e-mail e modificavam arquivos no computador das vítimas.

1.1.2 Sistema de Bitcoins

Com o surgimento da internet, muitos serviços considerados importantes foram impulsionados ao crescimento; e com o advento deles, novas ameaças vieram. Segundo o Statista (2016), em 2016 o comércio eletrônico chegou a movimentar 1,92 trilhões de dólares, adquirindo uma importância significativa em relação às vendas em lojas físicas. É necessário compreender também que o comércio digital investiu no 'mercado dos malwares', principalmente ao incentivar a coleta de informações financeiras do usuário utilizando spywares, por exemplo.

Também impulsionado pelo crescimento do comércio virtual no mundo, NAKAMOTO (2008) desenvolveu uma moeda inteiramente eletrônica, o bitcoin. Segundo ele, os bitcoins foram criados, sobretudo, para facilitar a venda online de produtos e serviços, no intuito de proporcionar segurança nas transações e redução de custos proporcionados por serviços de terceirização de pagamento.

Em seu artigo, Satoshi Nakamoto define sua solução, grosso modo, como uma moeda eletrônica com assinatura criptográfica, de modo que a moeda possa ter apenas um dono. Ainda segundo ele, deve existir um histórico de transações de forma que evite a duplicação de gasto da mesma moeda.

Como explicado por KOSHY, KOSHY & MCDANIEL (2014), no sistema de bitcoin, cada usuário possui uma chave identificadora, conhecida como endereço de bitcoin; assim, a moeda é transferida de um usuário para outro através da assinatura, com o endereço do destinatário atestando a propriedade dela.

De acordo com REID & HARRIGAN (2012), uma criptomoeda é caracterizada por sua segurança e por seu (pseudo)anonimato. Como é possível notar na proposta de Nakamoto, cada usuário só precisa ser identificado pela sua chave, representada por uma cadeia de 26 a 35

caracteres alfanuméricos, escondendo, dessa forma, a real identidade do indivíduo. Contudo, como demonstrado por REID & HARRIGAN (2012), bitcoins não apresentam total privacidade visto que a real identidade dos usuários pode ser deduzida analisando o histórico de transações e o comportamento de usuários em redes. Esse histórico de transações é denominado BlockChain; e ele armazena todo o histórico de transações de bitcoins já feitas até hoje.

1.1.3 Ransomware

Nos últimos anos, houve um crescente número de ataques dos chamados *scareware* que, por sua vez, tiram vantagem do medo das suas vítimas de perderem informações importantes ou as terem expostas sem sua autorização. Um subtipo de *scareware* obteve bastante relevância nos últimos anos, o chamado ransomware (KHARRAZ, 2015).

A palavra “ransomware”, cunhado pela mídia, surgiu por volta de 2005 (GAZET, 2008). Segundo BHARWAJ (2015) o *ransomware* pode ser dividido em duas categorias, o *Crypto Ransomware* e o *Locker Ransomware*. A variante *Locker* bloqueia o acesso do usuário ao sistema, muitas vezes, substituindo a área de trabalho por alguma outra tela que bloqueia a manipulação do computador pelo usuário. Um computador infectado pela variação *Crypto* tem seus dados criptografados por fortes algoritmos de criptografia, impedindo, dessa forma, que o seu usuário tenha acesso a tais informações.

Deve-se notar que a característica que o define - segundo o próprio nome, *ransom*, que do inglês significa “dinheiro pago pelo resgate de algo“ -, é cobrar um valor de resgate por suas informações criptografadas ou a retomada do acesso a seu computador pelo usuário. Em outras palavras, um ransomware é um malware capaz de extorquir sua vítima.

1.2 Objetivo do trabalho

Este trabalho tem como objetivo principal apresentar um panorama geral do que vem a ser o fenômeno do ransomware, com destaque aos Crypto Ransomwares, e de analisar os diversos tipos de ransomwares que, ao longo dos últimos anos vem extorquindo massivamente milhares de vítimas. Esta análise possui um enfoque mais relacionado à evolução que os ransomwares tem sofrido, com o intento de driblar técnicas de prevenção e remediação. Além disso, é necessário analisar, também, o impacto dessa leva de malwares, que tem cada vez mais se destacado na segurança digital.

1.3 Metodologia

Para este trabalho foi realizada uma pesquisa exploratória em diversas fontes, principalmente em sites de notícias gerais e de tecnologia da informação, com enfoque em segurança sobre ransomwares, visto ser um tema em ebulição nos dias atuais. Além disso, foi realizado um estudo de casos de diversos ataques de ransomwares, no intuito de identificar diferentes técnicas e abordagens de ataque e defesa.

Com base nisso a seguinte metodologia foi adotada:

- Pesquisa bibliográfica dando prioridade a artigos científicos;
- Seleção das fontes bibliográficas base do artigo;
- Análise da bibliografia básica;
- Construção das informações básicas e estrutura do projeto;
- Pesquisa exaustiva sobre informações atuais em relação ao tema;
- Remodelagem do conteúdo do artigo de acordo com as novas informações encontradas;

É importante ressaltar que foram poucos os artigos científicos encontrados que tocam o conteúdo que este projeto quer abranger. Certamente, muito se deve ao dinamismo e ineditismo apresentado pelo fenômeno do ransomware nos dias atuais.

1.4 Estrutura do trabalho

Este trabalho é dividido em 3 partes principais: na primeira parte será feita uma abordagem analítica dos ransomwares, conceituando-os e classificando-os de acordo com suas técnicas de ataque. Para ela, foram escolhidos ransomwares que tiveram destaque na mídia mundial principalmente devido a seu impacto e inovação na sua capacidade ofensiva como o CryptoLocker, Cryptowall, Locky, etc. Também será feita uma abordagem histórica sobre o primeiro ataque de ransomware demonstrando como a evolução tem ocorrido de forma drástica de acordo com tecnologias usadas atualmente.

Na segunda parte, serão analisados grandes ataques que obtiveram grande visibilidade na mídia mundial. Ataques esses, como, por exemplo, a hospitais nos Estados Unidos, ataque a sites (como New York Times). Essa parte do trabalho tem como objetivo demonstrar que, o destaque midiático dos ransomwares, é um reflexo direto da sua evolução e de seu potencial danoso, causando cada vez mais impacto em nossa sociedade.

Por fim, na terceira parte do projeto, será feita uma análise sobre técnicas de ataque utilizadas pelos ransomwares e técnicas de defesa na sociedade atual. Serão analisadas técnicas para aumentar a possibilidade de infecção como no caso dos Exploit Kits e técnicas e modalidades de ransomwares que podem expandir muito seu raio de influência. Também será feita uma projeção em relação aos ransomwares, destacando, caso os ataques continuem, novas técnicas extremamente danosas de infecção.

3 Ransomwares

Nos últimos meses os ataques de ransomwares tem aumentado de forma vertiginosa, indicando um estado de alerta para a segurança digital. De acordo com SOLOVE (2016) estatísticas apontam que no primeiro semestre de 2016, comparado ao mesmo período do ano anterior, os ataques experimentaram um crescimento de 300%. Estatísticas também indicam que em relação ao primeiro trimestre de 2016 os ataques aumentaram cerca de 30%.

A noção de malwares que utilizam criptografia em seus ataques e demandam uma quantia em dinheiro eletrônico foi inicialmente introduzida por YOUNG & YUNG (1996). O chamado ransomware se enquadra nessa noção estabelecida por YOUNG & YUNG (1996). Ele é um tipo de malware, muitas vezes sendo categorizado como Cavalo de Troia; ao infectar o computador da sua vítima, impede-a de acessar seus arquivos a menos que ela pague uma quantia requisitada, uma espécie de resgate pelo sequestro.

De acordo com DROZHZHIN (2016) primeiramente durante algum tempo as primeiras ondas de ataques pertenciam a variante Locker Ransomwar, ou Blocker. Porém, após a utilização de criptografia nesse tipo de malware, os ransomwares começaram a ganhar mais visibilidade nos últimos anos através da variante Crypto. Neste trabalho, eles serão tratados pela sua modalidade mais comum - os Crypto Ransomwares -, que utilizam de técnicas de criptografia para limitar o acesso de sua vítima a seus próprios arquivos. Pode-se distinguir o ataque de um ransomware em duas fases: a pré-infecção e a infecção propriamente dita. A primeira diz respeito a como o ransomware chega até suas vítimas enquanto que a segunda trata de como ele interage com elas.

3.1 Pré-infecção

Uma das razões pelas quais os ransomwares podem ser classificados como Cavalo de Troia se dá pelo fato deles não possuírem a capacidade de se multiplicar e espalhar de forma automática, pois depende de outras

técnicas para chegar até a sua vítima. A forma que os ransomwares usam para chegar até suas vítimas é majoritariamente através de engenharia social como e-mails falsos e maliciosos. Outra abordagem se dá através do dos Exploit Kits que, segundo CHEN & LI (2015) é uma aplicação web capaz de explorar as vulnerabilidades de um sistema, evitando que o malware seja detectado, para assim poder fazer o download do ransomware no computador da vítima.

MEHMOOD (2016), aponta duas estratégias de ataque para os ransomwares, a *War Driving, e a Targeted Attack.* Na estratégia *War Driving* o malware visa infectar a maior quantidade de usuários possíveis através de campanha de e-mails maliciosos ou infectando softwares aparentemente confiáveis, sendo baixado para o computador da vítima junto com ele. Por sua vez na estratégia *Targeted Attack* o malware procura infectar apenas um indivíduo ou um pequeno nicho de vítimas de forma pontual e direta utilizando de artifícios para enganar a vítima. Um exemplo de desse tipo de abordagem aconteceu em 2015 quando criminosos se fizeram passar por técnicos de suporta da McAfee conduzindo indivíduos para salas de chat com o intuito de fazer a vítima baixar softwares maliciosos.

3.2 Infecção

Após chegar até o computador da sua vítima o ransomware inicia o seu processo de infecção passando por algumas etapas necessárias até finalizar seu ataque. De acordo com GAZET (2008), pode-se distinguir 3 etapas pelas quais o *ransomware* passa após a infecção de um computador: procura por alvos, apreensão de dados, cobrança de resgate.

3.2.1 Procura por Alvos

A procura por arquivos a serem criptografados é algo que varia de acordo com o *ransomware*, contudo, eles procuram sempre criptografar arquivos que pareçam ser importantes para o usuário daquele computador. Em outras palavras, certas extensões de arquivos, como .dll, não são muito

visadas pelos *ransomwares*, uma vez que estes podem não apresentar algo de muito valor para o usuário, não tornando estritamente necessário para ele o pagamento do regate. Portanto extensões como .doc, .mp3, .png, etc, arquivos que possam ter algum valor, de certo modo, sentimental, para o usuário. Outra razão para selecionar bem os arquivos, como salientado por GAZET (2008), é evitar o alto custo computacional que seria criptografar muitos arquivos, muitos deles inúteis para o propósito do ataque. É importante destacar, como foi dito por GRIFFIN (2016), que *ransomwares* como o *Locky*, por exemplo, não criptografam arquivos do sistema para não prejudicar o uso do computador.

3.2.2 Apreensão de dados

A fase da extorsão se resume na preparação desses arquivos selecionados com o objetivo de conseguir meios para extorquir as suas vítimas. O mais comum, como nos casos dos ransomwares do tipo Crypto, é quando ele criptografa os arquivos para pedir um valor de resgate por eles. Para os ransomwares mais recentes é comum o uso de criptografia assimétrica (uso de chave pública e chave privada), como é o caso do Cryptolocker, como salientado por FLOOD (2013), onde os arquivos selecionados são criptografados por uma chave pública e só podem ser descriptografados pela chave privada. Como demonstrado por LIAO (2006), alguns ransomwares codificam os arquivos e os separam em uma pasta oculta, em seguida os arquivos originais são apagados, aumentando o efeito da extorsão sobre a sua vítima.

É importante observar que, para a obtenção das chaves de criptografia, os ransomwares podem apresentar duas abordagens. Uma mais simples é quando o próprio ransomware gera as chaves de criptografia simétrica ou assimétrica. Esse tipo de abordagem é muito frágil, pois a vítima consegue ter acesso as chaves localmente. A outra, mais complexa, é quando o ransomware entra em contato com um servidor externo para obtenção das dessas chaves, impossibilitando o acesso da vítima à chave de decodificação.

De acordo com MEHMOOD (2016), alguns ransomwares, como o CryptoLocker, utilizam um gerador de domínios para poder alcançar o servidor de controle, tentando se conectar com ele através de diversos domínios, até conseguir, evitando dessa forma que o firewall consiga barrar a tentativa de contato com o servidor de controle.

3.2.3 Cobrança de Resgate

A terceira e última fase, a da cobrança do valor de resgate, é o objetivo final atacantes que estão por trás dos *ransomwares*, quando espera-se que a vítima realize o devido pagamento. Primeiramente, de acordo com MEHMOOD (2016), o ransomware deve alertar ao usuário sobre a sua presença uma vez que todas as fases anteriores foram concluídas, informando ao usuário sobre o que foi feito com os arquivos e o que ele deve se feito para obter o acesso a eles novamente. Este alerta pode ser dado de diversas formas, desde um simples popup até arquivos de texto espalhados pelo computador ou alteração do papel de parede da área de trabalho. Essas mensagens geralmente dizem a quantia a ser paga pelo resgate dos arquivos e as formas de pagamento. É importante observar que *ransomwares* mais atuais, como o *CryptoLocker*, *CriptoWall* e o *Locky* usam como principal moeda de resgate o bitcoin, principalmente devido a seu caráter de proporcionar pseudo-anonimato aos envolvidos na transação. Os primeiros *ransomwares*, requisitavam envio de dinheiro em espécie para endereços predeterminados, como é o caso do *AIDS Trojan*.

3.3 Histórico de Ransomwares

Aqui serão analisados alguns ransomwares mais famosos que obtiveram papel de destaque nos últimos tempos, pela inovação nas técnicas de ataque e impacto. Essa análise também o papel de mostrar a evolução dos ransomwares ao longo do tempo, desde o primeiro ataque noticiado, até seus grandes representantes atualmente.

3.3.1 O Primeiro Ransomware: AIDS Trojan

O biólogo Joseph Popp, considerado pai dos ransomwares, segundo a KnowBe4, desenvolveu em 1989 o AIDS Trojan, o primeiro ransomware da variante crypto. Ele infectou aproximadamente 20.000 disquetes, titulado "AIDS Information Introductory Diskette", com o seu malware e os distribuiu na conferencia da World Health Organization's AIDS. De acordo com GAZET (2008), o AIDS Trojan foi o primeiro ransomware a infectar computadores. Ele começava a funcionar efetivamente após 90 reboots do sistema para então criptografar arquivos da vítima, ou seja, uma bomba lógica disfarçada de um software informativo sobre o vírus da AIDS.

Após criptografar as informações do usuário é mostrada uma mensagem ao usuário pedindo o pagamento de um resgate pelas informações codificadas:

"The price of 365 user applications is US$ 189. The price of a lease for the lifetime of your hard disk is US$ 378. You must enclose a bankers draft, cashier' s check or international money order payable to PC CYBORG CORPORATION for the full amount of 189 *or* 378 *with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama."*

É importante observar que o pagamento era feito através de cartas enviadas pelos correios. Com essa abordagem, as autoridades poderiam facilmente identificar seu destinatário através de um análise do endereço informado. Era uma técnica pouco eficiente, para o atacante, em comparação ao sistema de bitcoins utilizado atualmente. Além disso, segundo GEZET (2008) era utilizada um criptografia fraca baseada em substituição mono-alfabética.

3.3.2 CryptoLocker

Segundo dados da Symantec, o Cryptolocker surgiu pela primeira vez em meados de setembro do ano de 2013. É importante destacar que desde então ele passou a ser a ameaça número um dos meios digitais; atacando

computadores com o sistema operacional Windows. E, de acordo com a Zenzero, estima-se que foram infectados aproximadamente 250.000 computadores, a maioria de pequenas e médias empresas. Estas tinham seus arquivos importantes criptografados e então precisavam pagar a quantia pedida para evitar maiores perdas financeiras.

De acordo com BLUE (2013), logo após seu surgimento, o CryptoLocker cobrava de suas vítimas o valor de 2 bitcoins para ter seus dados resgatados. Contudo, devido ao aumento do valor do bitcoin essa quantia foi reduzida até chegar a 0,3 bitcoins. Com base nisso, pode-se concluir que as chances das vítimas pagarem os resgate da informação começou a diminuir pelo alto custo do bitcoin na época - que flutuava entre US$500 a pouco mais de US$1000 - forçando o valor, em bitcoins, a cair. JEFFERS (2013) afirma que, até dezembro de 2013, o CryptoLocker obteve aproximadamente 30 milhões de dólares de suas vítimas.

Figura 1 - Tela com instruções para as vítimas do CryptoLocker.

Fonte: http://www.zdnet.com/article/new-cryptolocker-ransomware-targets-gamers/

Com relação a sua criptografia, o CryptoLocker utilizava o esquema RSA de chave pública e privada, geradas em um servidor externo. Como explicado em ABRAMS (2013), o CriptoLocker era capaz de criptografar

dados do computador infectado e de todos os computadores mapeados na rede. Para criptografar os dados ele entrava em contato com um servidor que gerava as chaves públicas e privadas de 2048 bits. Apenas a chave pública era enviada, desta forma só após a confirmação do pagamento do resgate a chave privada era enviada para descriptografar os arquivos.

Deve-se notar que o CryptoLocker não apagava arquivos de backup do computador da vitimas, fazendo com que a restauração do sistema fosse uma forma eficiente de remediar o ataque. Contudo, segundo a KREBS (2013), caso os arquivos de backup estivessem conectados fisicamente ou através da rede ao computador infectado havia uma chance dos arquivos serem criptografados juntamente com todos os outros.

No dia 2 de junho de 2014 o FBI anunciou a desativação da rede do CryptoLocker. Segundo o FBI, ao desativar um outro malware, a botnet GameOver Zeus, a rede do CryptoLocker foi desativada também, responsabilizando o russo Evgeniy Bogachev, considerado líder do grupo, baseado na Rússia e na Ucrânia, responsável pelos ataques milionários envolvendo os 2 malwares.

É importante observar que embora a rede do CryptoLocker tenha sido desativada, uma nova variante foi descoberta recentemente. No ano de 2015 uma nova variante do CryptoLocker começou a atacar usuários de jogos online como World of Warcraft, Minecraft e usuários de Steam (OSBORNE 2015). Essa nova variante do malware procura arquivos de jogos online e do Steam para criptografar, atingindo um nicho específico de vítimas, de jovens adultos que, por sua vez, podem não possuir muitos arquivos importantes, como certas organizações, em suas máquinas, contudo, jogos, cujo arquivos ficam armazenados localmente, podem ser atingidos.

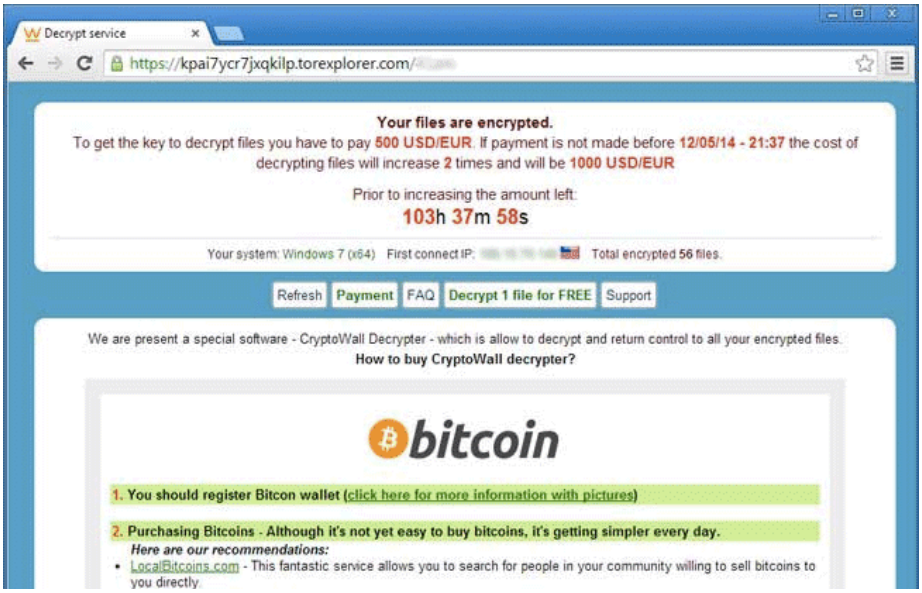
3.3.3 CryptoWall

Primeiramente, é importante ressaltar que o CryptoWall começou a ganhar notoriedade com a queda do CryptoLocker, no início de 2014, e conseguiu representar uma ameaça ainda maior do que seu antecessor. Segundo DUNN(2016) o CryptoWall chegou a possuir 4 versões ao longo do

tempo e em apenas 6 meses, a Dell Secure Works estimou que 625.000 computadores foram infectados e até outubro de 2014 mais de 1 milhão. DUNN (2016) também afirma que segundo a Cyber Threat Alliance, em novembro de 2015 o CyptoWall 3.0 tinha conseguido coletar aproximadamente 325 milhões de dólares de suas vítimas. O CryptoWall ainda encontra-se ativo atualmente em sua quarta versão.

Tendo em vista o destaque do CryptoWall, é importante observar os meios pelos quais o malware foi amplamente distribuído. De acordo com CABAJ et al (2015), esse ransomware poderia ser contraído de duas maneiras: através de um e-mail fraudulento ou de um servidor de um exploit kit. CABAJ et al. (2015) também informa que, após entrar no computador da vítima, o malware entra em contato com diversos servidores para conseguir a chave pública RSA de 2048 bits para então criptografar as informações importantes da vítima e então gerar instruções de como pagar o resgate, com um endereço online para a página de pagamento. Além disso BISSON (2016a) afirma que além do método RSA de criptografia o CryptoWall também usa uma chave AES(Advanced Encryption Standard) para codificar todos os arquivos e então criptografar a chave AES e o arquivo codificados com a chave pública RSA. BISSON (2016a) também destaca que, no CryptoWall 4.0 apresenta uma nova funcionalidade: o nome dos arquivos também são criptografados juntamente com os arquivos. Essa funcionalidade pode alertar o usuário sobre o que está acontecendo, possibilitando que ele desligue o computador a tempo de contatar técnicos e tomar alguma medida emergencial. Após criptografar os arquivos, segundo SYMANTECH (2015), o CryptoWall cria um documento de texto ou página HTML com instruções para o resgate dos dados.

Figura 2 - Tela com instruções para as vítimas do CryptoWall.



Fonte : http://www.precisesecurity.com/rogue/remove-cryptowall

Segundo BISSON (2016a), o CryptoWall 4.0, antes de codificar as informações da vítima, desativa o sistema de restauração do Windows e deleta os últimos 1000 pontos de restauração. Com base nisso, em comparação com o seu antecessor, o CryptoLocker, o CryptoWall reduz ainda mais as formas de evitar o pagamento.

Em relação as formas de pagamento do CryptoWall; de acordo com DUNN (2016), para efetuar o pagamento do resgate, a vítima é direcionado para um site na DeepWeb, onde a quantia em bitcoins pedida podia variar por região geográfica. Essa abordagem era utilizada, possivelmente, para facilitar o pagamento de acordo com as condições econômicas do local, nos Estados Unidos o valor pedido era de US$700, variando entre 1 e 2 bitcoins ao longo do tempo.

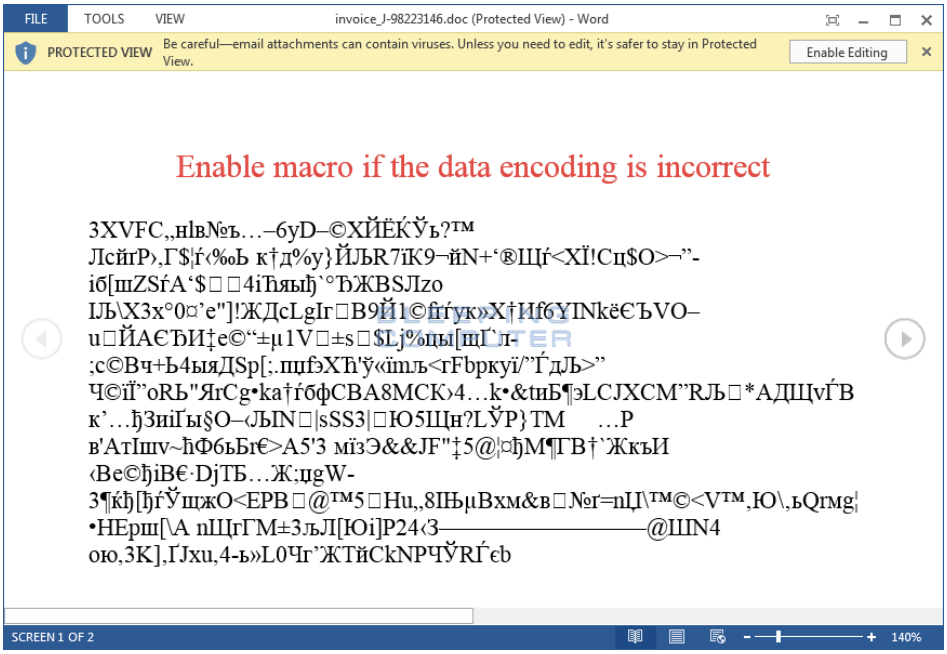
3.3.4 Locky

Locky, conforme reportado por BELCHER (2016), foi descoberto no dia 16 de Fevereiro de 2016 e foi logo demonstrando características que o colocaram numa posição de alerta para a segurança digital. O Locky, de acordo com GALLAGHER (2016b), tem como principal forma de contágio um

e-mail que diz estar entregando uma mensagem de *invoice*, com o assunto similar a "**ATTN: Invoice J-98223146**". Esse e-mail possui como anexo um documento de texto do Microsoft Word com o conteúdo aparentemente embaralhado, que requer que o usuário ative o macro para possibilitar a leitura. Uma vez ativado, o malware é automaticamente instalado no computador da vítima.

A ferramenta macro, por sua vez, fornecida desde a década de 90 pelo Microsoft Word, permite que o usuário programe tarefas a serem executadas pelo computador com o pretexto de automatizar tarefas na edição de textos. O macro também pode executar tarefas que influenciem diretamente o funcionamento do computador.

Figura 3 – Documento de texto pelo qual, ao habilitar o macro, o Locky infecta o computador da vítima.

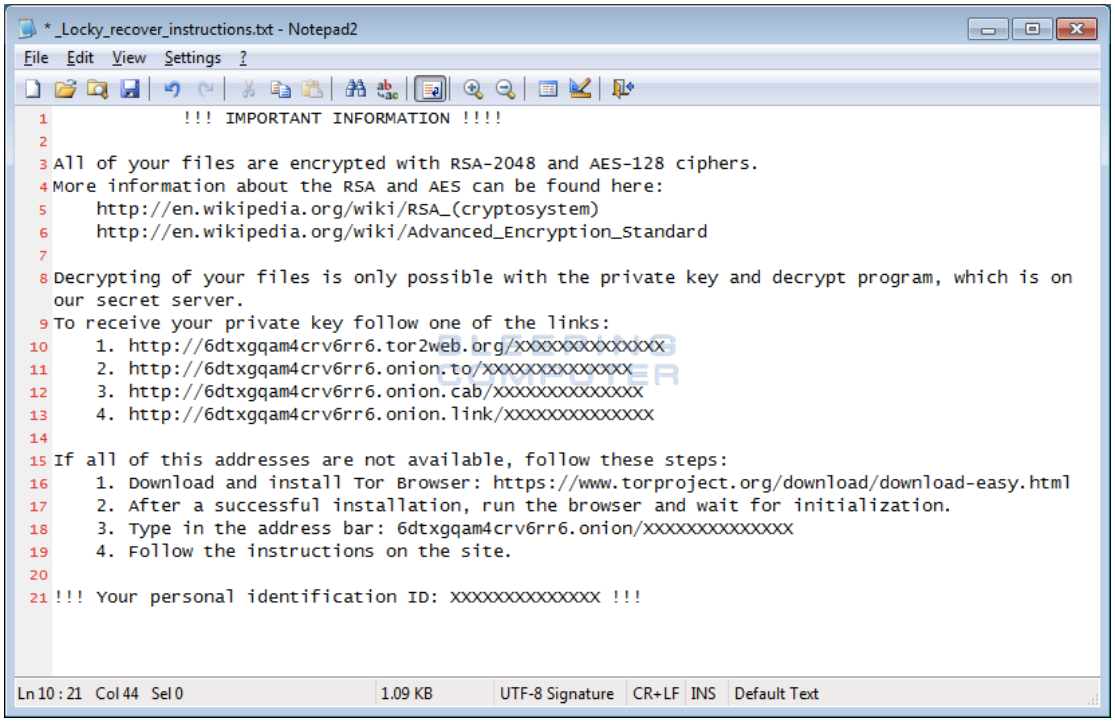


Fonte : http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

Com relação às técnicas de codificação do Locky, como apresentado por ABRAMS (2016a) em seu artigo, ele criptografa as informações utilizando AES-128 e RSA-2048. Primeiramente, antes de criptografar os dados da vítima, ele apaga todos os *Shadow Volume Copies* - arquivos usados para fazer a restauração do sistema caso algo aconteça - forçando o usuário a

guardar arquivos de backup externos. Outro ponto a ser destacado, relativo ao comportamento do malware, é que, além de criptografar arquivos locais, ele também criptografa arquivos compartilhados, mapeados e não mapeados, na rede. Similarmente ao CryptoWall, o Locky também modifica os nomes dos arquivos codificados; a nova forma do nome do arquivo seria **[unique_id][identifier].locky**.

Figura 4 – Documento de texto com as instruções para as vítimas do Locky.



Fonte : http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

Após “sequestrar“ os dados da vítima o Locky modifica o papel de parede do seu computador com o objetivo de alertá-la sobre o ataque e conduzi-la ao pagamento da quantia demandada. Além disso, na área de trabalho, e em cada pasta que possui um arquivo criptografado, o Locky deixa um arquivo, intitulado **_Locky_recover_instructions.txt**, com as instruções de pagamento. É relevante destacar que é cobrado às vítimas o valor de 0,5 bitcoins pelo resgate dos dados “sequestrados“. Esse valor é relativamente baixo comparado a seus antecessores, muito possivelmente

como uma forma de induzir mais pessoas a pagarem o valor pedido por considerá-lo demasiado baixo.

3.3.5 CTB-Locker

CTB-Locker, CTB significando "**Curve, Tor and Bitcoin**", também conhecido como Critroni foi, de acordo com ABRAMS (2016b), descoberto no verão de 2014, quando experimentou uma distribuição massiva, atacando sistemas Window. Atualmente, em 2016, o CTB-Locker se apresentou com uma segunda versão que, diferentemente da primeira versão, tem como alvo servidores web, "sequestrando" sites. Em adição, a primeira versão do ransomware voltou de forma atualizada, com melhorias, e experimentou novamente um acréscimo no número de vítimas.

Segundo ABRAMS (2014) o CTB-Locker para Windows, em sua primeira versão, quando infectava um computador, ele criava uma instancia dele mesmo para ser executada após o login do usuário. Após sua execução ele vasculhava por todos os drivers mapeados e criptografava os arquivos compatíveis - geralmente música, fotos e documentos - então criptografava os arquivos com um tipo de criptografia inédita até então para os ransomwares, o Elliptic Curve Cryptography (ECC). Por sua vez, como demonstrado por SULLIVAN (2013) , ECC é um tipo de criptografia de chaves pública e privada baseado em um problema matemático conhecido como logaritmo discreto sobre curvas elípticas. Essa abordagem faz com que a criptografia seja mais difícil de ser quebrada, em comparação a criptografia baseada em fatoração, como a RSA. ABRAMS (2014) também aponta outra característica incomum do CTB-Locker na época, o ransomware entrava em contato com o servidor de comando via TOR, dificultando o rastreio da comunicação.

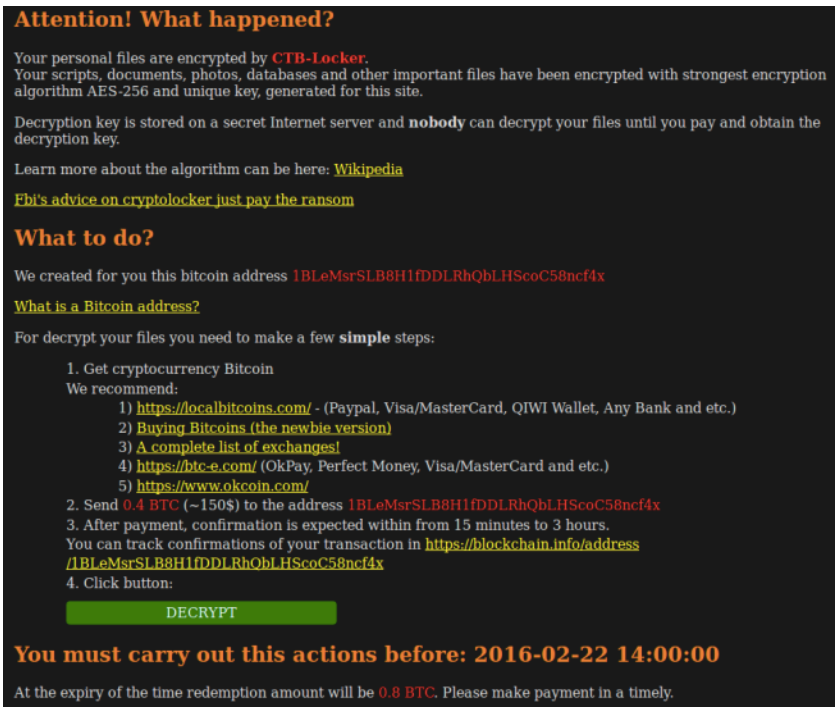
Um detalhe interessante, informado por ABRAMS (2014), é que o CTB-Locker permite que o usuário descriptografe 5 itens sem pagar o custo do resgate. Isso é permitido como uma prova da capacidade do ransomware de descriptografar todos os arquivos caso o regate seja pago. O valor

cobrado por ele era bem reduzido, na época, sendo 0,2 bitcoins, o que representava aproximadamente US$120.00

A nova versão do CTB-Locker para o Windows apresenta uma série de melhorias, uma delas, notificada por ABRAMS (2016b), é o uso de certificados roubados para assinar seu executável para adquirir a confiança do sistema.

Por sua vez, como citado anteriormente, existe uma nova versão do CTB-Locker, com o enfoque completamente diferente, que é o de criptografar web servers, procurando atacar websites e seus donos. Como especificado por ABRAMS(2016), quando esse ransomware invade um webserver ele vai renomear os arquivos index.php ou index.html para original_index.php ou original_index.html e copiar um novo index.php que fará a criptografia dos dados e mostrará na tela do site as informações para descriptografar os arquivos. É notável que o CTB-Locker para web utiliza uma criptografia AES-256 para os arquivos selecionados, gerando duas chaves: uma para criptografar 2 arquivos que podem ser descriptografados gratuitamente e outra para os demais; descriptografados apenas via pagamento.

Figura 5 – Tela com instruções para as vítimas do CTB-Locker.



Fonte : https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html

É notável, também, esse ransomware apresenta uma forma original de enviar as chaves AES-256 para a vítima: usando a BlockChain do sistema de bitcoins. Primeiramente, deve-se perceber que, somente a partir de 2014 o sistema de bitcoins passou a ter, em suas transações, que ficam armazenadas na BlockChain, um bloco arbitrário de texto denominado OP_RETURN, esse bloco é usado pelo CTB-Locker para enviar as chaves de criptografia para a vítima. Segundo SINEGUBKO (2016), ao enviar o valor de bitcoins pedido uma outra transação é criada, usando um script inválido, porém a transação fica registrada, sendo o conteúdo do OP_RETURN dessa segunda transação as duas chaves de resgate. É mister perceber que esse método dificulta muito o rastreio da origem do ransomware, ou seja, seu servidor de controle.

Contudo, como apresentado por SINEGUBKO (2016), a versão do CTB-Locker para web servers tem sido uma grande falha, pois os donos de sites não tem pago o resgate pelos seus sites, uma vez que serviços de hospedagem muito comumente também oferecem um serviço de backup para sites. Portanto, os donos de sites podem ter seus dados de volta sem pagar o resgate que, ao longo do tempo, reduziu de 0,4 para 0,15 bitcoins por causa disso.

3.4 Mobile Ransomwares

De acordo com KASPERSKY (2016b) sua solução de segurança para dispositivos Android, em 2015 registrou 35.413 ataques de ransomware, já esse número em 2016 praticamente quadruplicou com 136.532 casos, todos eles foram evitados. Além disso estatísticas também apontam que, entre 2014 e 2015, 2.04% dos ataques de malwares eram de ransomware, já entre 2016 e 2016 esse número dobrou, foi para 4,63%. Essas estatísticas apontam um enorme crescimento, entre 2015 e 2016 de ataques de ransomwares para dispositivos mobile.

Nos últimos anos foi possível observar uma competição entre dois grandes ransomwares para Android: o Small e o Fusob. O Small representou, entre 2014 e 2015, uma parcela de 69,11% dos araques. Enquanto o Fusob,

entre 2015 e 2016, conseguiu superar o Small e representar 56,25% dos ataques. Em seguida serão analisados esses 2 ransomwares para a plataforma mobile, contudo primeiramente, é importante destaca a importância do Simplocker, o primeiro ransomware da variante Crypto a atingir o sistema Android.

3.4.1 Simplocker

Simplocker foi considerado como o primeiro Ransomware do tipo Crypto a atingir o sistema operacional Android. Ele infecta o aparelho através do download de um aplicativo de pornografia infantil, o Sex Xonix, encontrado em um site falso imitando a Play Store (loja de aplicativos do Android). Segundo HAMADA (2014) esse aplicativo, quando baixado, executa o ransomware que, após criptografar os dados do usuário, mostra uma mensagem dizendo que o aparelho foi bloqueado por acesso a pornografia infantil, cobrando uma “multa“ para desbloquear o celular. Esse tipo de ataque de engenharia social tem sido muito comum, induzindo o pagamento por causa do medo de consequências legais para as vítimas.

Existem meios de prevenir e remediar os efeitos do Simplocker apresentados também por HAMADA (2014), em seu artigo. Primeiramente, é possível impedir que o malware comece a criptografar os dados da vítima: entrar rapidamente no modo de segurança do aparelho e desinstalar o malware. Caso os arquivos já tenham sido criptografados, é possível descriptografá-los, uma vez que o ransomware não entra em contato com um servidor de comando, a chave está armazenada localmente no aparelho, ou seja, é possível conseguir a chave sem pagar o valor cobrado.

Percebe-se, portanto, que o Simplocker é bastante rudimentar e facilmente contornável, contudo abriu espaço para a exploração do Android como alvo para novos ataque de crypto ransomwares. Felizmente, os ransomwares não podem ser encontrados na Play Store original pois todos os aplicativos, teoricamente, devem ser testados antes de serem disponibilizados para o usuário final, logo deve-se tomar cuidado ao baixar aplicativos não registrados na loja oficial do Android.

3.4.2 Small

Segunda KASPERSKY (2016b) o Small é o segundo ransomware mais popular a atacar aparelhos Android, representado por uma parcela de 12%. Praticamente todos os ataques envolvendo esse malware ocorreram em países do leste europeu, como a Rússia e Ucrânia, além do Cazaquistão, no Oriente Médio. Ele é majoritariamente contraído através de sites pornográficos e SMS maliciosos. Foi primeiramente notificado em Junho de 2014.

É importante observar que esse ransomware surgiu primeiramente como representante da variação Locker. Atingia majoritariamente países de língua russa e cobrava um valor entre 700 a 3.500 rublos. Aparelhos celulares infectados por ele eram impossibilitados de serem utilizados, pois o ransomware bloqueava suas funções, além disso ele requisitava direitos de administrador do aparelho, fazendo com que não pudesse ser desinstalado.

A sua segunda variação é um representante dos ransomwares do tipo Crypto. De acordo com KASPERSKY (2016b) seu funcionamento inicial era basicamente o mesmo da primeira variação do Small, contudo, após bloquear o acesso do usuário ao aparelho, ele criptografa os dados do usuário.

Já sua terceira variação apresenta um comportamento bastante singular, até então, para um ransomware. Primeiramente, como notificado por KASKERSPY (2016b) é importante observar que essa variação se enquadra melhor na classificação de Cavalo de Troia, pois ele apresenta múltiplas funcionalidades e uma delas é como ransomware. Ao infectar um aparelho o Small manda todas as informações do aparelho incluindo o número do telefone e manda esses dados para os seus servidores, em seguida a sua central de comando possui uma série de instruções a serem mandadas para esse malware, ditando seu comportamento. Essas instruções podem envolver o bloqueio do aparelho, a codificação dos dados, mandar SMS através do aparelho, fazer downloads, entre várias outras.

Esse tipo de ransomware tem se mostrado ser bastante danoso pois pode agir no celular de diversas formas, sem ser percebido, antes de criptografar os dados e pedir dinheiro pelo resgate.

3.4.3 Fusob

De acordo com KASKERSKY (2016b) o Fusob , ransomware da variação locker, é atualmente o mais popular para dispositivos Android, atacando mais de 100 países ao redor do mudo. Esse tipo de ransomware é comumente contraído através de sites e aplicativos pornográficos, como xxxPlayer, mais recentemente descobriu-se que ele também é distribuído através de Exploit kits. Foi primeiramente notificado em janeiro de 2015.

Ao iniciar sua execução, o Fusob faz uma checagem do pacote de língua instalado no aparelho e caso encontre algum pacote do leste europeu como Rússia, Geórgia, Hungria, ou alguns países do oriente médio como Cazaquistão e Azerbaijão, ele não conclui o ataque. Essa informação é importante para compreender contexto político e social envolvendo ataques de ransomwares, com o objetivo não apenas de arrecadar fundos, mas de danificar economicamente certos países e instituições. Enquanto o Small atacava principalmente países do leste europeu o Fusob os protegia de seus ataques.

Como Small, o Fusob pede direitos de administrador do aparelho para evitar ser removido, além disso o usuário fica sem ter acesso as propriedades do aparelho. Em seguida o ransomware envia para os seus servidores informações sobre o aparelho e o histórico de chamadas e informações de contatos, além da localização do aparelho. Assim como no caso do Small o servidor pode mandar uma série de comandos de controle para o ransomware, entre eles estão: bloquear o aparelho, instalar um APK e até mesmo capturar uma imagem utilizando a câmera do aparelho.

É Importante observar que o Fusob não utiliza bitcoins como forma de pagamento, ao invés disso ele demanda o pagamento através de códigos de cartões pré-pagos da iTunes Store.

3.5 Outros Ransomwares

3.5.1 KeRanger

Como afirmam XIAO e CHEN (2016), em 2014 foi descoberto pela Kaspersky um ransomware, chamado File Coder, que atacava o sistema operacional da Apple, o MacOS. Contudo esse ransomware se apresentava de forma incompleta. Então, foi descoberto, em 4 março de 2016, outro ransomware, o KeRanger, também tendo como alvo o MacOS. Porém, desta vez, o KeRanger se mostrou ser o primeiro ransomware inteiramente funcional a atingir o sistema operacional da Apple.

O KeRanger, como apresentado por XIAO e CHEN (2016), estava sendo distribuído através do download de uma versão do instalador do cliente BitTorrent para MacOS, o Transmission versão 2.90. Até o momento da sua descoberta a versão maliciosa ainda estava disponível para download, pouco tempo depois o link foi removido. Tudo aponta para um suposto ataque ao site de distribuição do software Transmission, recompilando uma versão maliciosa e disponibilizando para download. Pois, de acordo com FARIVAR (2016), a Transmission emitiu uma nota pedindo que os usuários atualizem para a versão 2.91 e apaguem a versão 2.90.

3.5.2 Petya

Identificado em 2016, o ransomware conhecido como Petya apresenta técnicas que o diferencia de muitos outros ransomwares, como o que ele faz e como ele infecta. Segundo BISSON (2016b), o Petya faz com que o sistema operacional não execute ao ligar o computador, executando seu próprio sistema. Isso é possível porque o Master Boot Record, o código que vai dizer como inicializar o sistema operacional, é substituído por um código desse ransomware. Uma vez reiniciado o computador e o sistema do Petya é executado, ele faz parecer que o sistema está fazendo uma checagem de disco, enquanto isso o ransomware está criptografando a Master File Table (MFT) do computador da vítima. No Windows, todos os arquivos e diretórios

são armazenados como metadados na MFT, portanto, com essa tabela criptografada, a vítima basicamente perde acesso ao seu disco rígido. Após esses passos o Petya mostra uma mensagem ao usuário exigindo o pagamento, de aproximadamente US$480, para devolver o acesso do computador a sua vítima.

Um outro diferencial do Petya em relação a outros ransomwares, como reportado por BISSON (2016b), é a forma inusitada de engenharia social usada para chegar até suas vítimas. Esse ransomware tem como objetivo atingir companhias alemães e para tal o atacante envia um e-mail simulando ser um candidato profissional enviando o currículo. Esse e-mail vem acompanhado com um link do dropbox (serviço de armazenamento na núvem), que também representa uma inovação, contendo uma imagem JPG do funcionário e um executável com o Petya.

3.5.3 KimcilWare

De acordo com ABRAMS (2016d) KimcilWare foi descoberto em 2016 e é uma variante de ransomwares que atacam websites utilizadores da plataforma Magento de e-commerce. Contudo não se tem muitas informações aprofundadas sobre o seu funcionamento. Sabe-se que o KimcilWare criptografa informações do site usando uma criptografia de bloco Rijndael e cobra das suas vítimas entre U$140 e U$415, aproximadamente.

Segundo ABRAMS (2016b), os websites atingidos apresentam em comum o uso de uma plataforma de e-commerce chamada Magento. Suspeita-se que os atacantes tenham invadido os servidores dessa plataforma e inserido scripts para criptografar informações dos servidores dos sites que utilizam seus serviços. Foram identificados dois scripts diferentes atingindo esses websites. Um deles, ao criptografar os arquivos, o ransomware atribui a extensão “.kimcilware” nos arquivos codificados e cria um arquivo index.html com as instruções de resgate, cobrando aproximadamente US$140. O outro atribui a extensão “.locked“ aos arquivos e, ao invés de criar um index.html, gera um documento de texto com as instruções, dessa vez cobrando aproximadamente US$415.

Embora ABRAMS (2016d), em seu artigo, diga que não existe forma de recuperar os dados sem recorrer ao pagamento, contudo é sim possível. Através de uma análise do código fonte e de conhecimento sobre a criptografia de bloco Rijndael, PHAN & PAZ (2016) demonstram que é possível descriptografar os arquivos. Pela criptografia usada ser simétrica, ou seja, a chave para criptografar é a mesma para descriptografar, e, a partir de informações do código fonte do KimcilWare, é possível obter essa chave e ter acesso aos arquivos novamente.

3.5.4 CryptXXX

Observado pela primeira vez em abril de 2016, o CryptXXX é responsável pelo início de uma grande evolução dos ransomwares. Ele, além de impedir o acesso da vítima as seus arquivos, é capaz de roubar informações dela. De acordo com a BISSON (2016c) o CryptXXX é distribuído para suas vítimas, majoritariamente, através de exploit kits e atua como um ransomware qualquer. Ao infectar o computador de sua vítima ele criptografa arquivos atribuindo uma extensão “.crypt” a eles e, em seguida, mostra a mensagem com instruções para a vítima pagar US$500 para descriptografar os dados. Contudo, uma vez estabelecido no computador da vítima o CryptXXX começa a roubar uma enorme quantidade de dados.

BISSON (2016c) aponta uma nota da empresa de segurança Proofpoint que diz que esse tipo de comportamento já era esperado desse ransomware por conta de um dos seus distribuidores; o Bedep. Ele é um malware que tem a capacidade de baixar outros malwares no computador de sua vítima. No contexto do CryptXXX, o Bedep é distribuído para o computador das suas vítimas através do Angler Exploit Kit, uma vez á ele pode baixar uma série de malwares, entre eles o CryptXXX. Era esperado que esse ransomware também roubasse informações porque Bedep possui um vasto histórico de distribuir malwares capazes de roubar informações de suas vítimas. Segundo GOODIN (2016b), após a liberação de uma solução da Kaspersky Lab para descriptografar o CryptXXX, uma nova variante do ransomware foi lançada, anulando a solução desenvolvida. Isso atesta a

capacidade adaptativa dos ransomwares, a evolução diante das técnicas de defesa.

3.5.5 Jigsaw

O Jigsaw é um tipo de ransomware, primeiramente notificado em abril de 2016, que apresenta uma forma inovadora de extorsão: ele ameaça vazar informações criptografadas. De acordo com GOODIN (2016c) esse novo ransomware criptografa informações do usuário assim como qualquer outro, contudo, além da apreensão dos dados da vítima ele ameaça publicar informações da sua vítima. Esse tipo de abordagem, impor medo, faz com que, mesmo que o usuário possua backup para recuperar os dados, ele sinta-se incentivado a pagar o sequestro pelas ameaças estabelecidas.

A mensagem gerada pelo Jigsaw apresenta um tom de ameaça:

"Very bad news! I am a so-called ransomware/locker with following advanced functions:
Encrypting all your data.
Collecting all logins, contacts, eMail, Passwords and Skype History .....Done!
Uploading all of it on a server .....Done!
Sending a copy of those Datas to ALL of your contacts.....Pending"

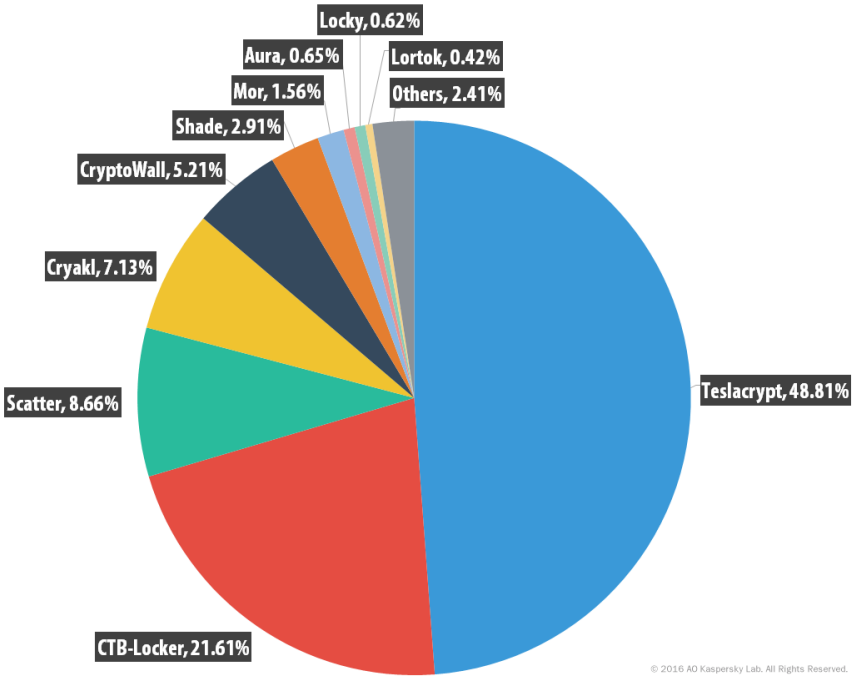
Além dessa tipo inovador de extorsão o Jigsaw também apresenta um serviço de suporte ao vivo para auxiliar a vítima a conseguir os bitcoins necessários para o pagamento do sequestro. O Jigsaw é um representante bastante perniciosa de uma nova leva de ransomwares que tem surgido em 2016, cada vez mais difíceis de serem contornados, apresentado várias manobras de ataque inovadoras evitando diversas técnicas de defesa.

3.5.6 TeslaCrypt

O TeslaCrypt foi primeiramente descoberto em fevereiro de 2015 apresentando um nicho diferente de vítimas para seus ataques: "gamers". Como relatado por ABRAMS (2015), além de também criptografar – usando

criptografia simétrica AES - arquivos como outros ransomwares do deu tipo, ele foi o primeiro ransomware a codificar arquivos de jogos digitais. Com isso, se apresentou com uma abordagem de apelo emocional a , principalmente, jovens adultos impedindo-os de jogar e os fazendo perder o progresso conquistado durante o jogo. Não se sabe ao certo se esta característica aumenta o impacto desse ransomware, contudo é provável que não aumente de forma significativa pois muitos jogos possuem sistema de salvamento na cloud, ou seja, cópias do status do progresso em servidores externos.

Figura 6 – gráfico com parcela de ataques de ransomwares em 2016.



Fonte - http://kasperskylab.livejournal.com/74966.html

De acordo com a figura 6 em 2016 o TeslaCrypt apresentou a maior parcela dos ataques envolvendo ransomware, provavelmente por causa de uma campanha extremamente agressiva através, principalmente do uso de exploit kits.

Apesar de tudo, segundo ABRAMS (2015) o TeslaCrypt teve sua criptografia quebrada e uma ferramenta chamada TeslaDecoder criada para decodificar os dados sequestrados da vítima. Porém, como reportado por SINITSYN (2015), no segundo trimestre de 2015 foi encontrado uma outra versão desse ransomware, o TeslaCrypt 2.0 que, por sua vez, apresenta uma

criptografia bem mais forte. Esta variante ainda sem nenhuma forma de ser decodificada.

4 Histórico de ataques

Nos últimos meses a mídia tem documentado inúmeros ataques de ransomwares a sistemas ao redor do mundo, principalmente nos Estados Unidos. É importante notar que na maioria dos ataques noticiados não fica claro qual ransomware foi utilizado. Outro ponto a ser destacado é que no que é notificado pode ser observado alguns dados conflitantes como no caso do ataque um Hospital na Califórnia que, como reportado adiante, apresenta dúvidas em relação ao valor pago pela vítima. Questões também podem e devem ser levantadas em relação ao papel da mídia na notificação do público em geral sobre ataque de ransomwares. Por se apresentar como uma faca de dois gumes, a mídia, ao passo que alerta a população sobre os perigos dos ataques e vulnerabilidades dos sistemas atuais, ela também pode servir como um veiculo incentivador da continuidade dos ataques de ransomwares. Isso ocorre pois ela atesta a grande eficácia dos ransomwares em causar pânico e levar ao pagamento de valores absurdos para os atacantes. O FBI, por um lado, tem agido no sentido de aconselhar as vítimas a não pagarem os valores requisitados, a menos que seja a última alternativa, ou seja, quando não existem arquivos de backup a serem restaurados.

4.1 Ataques a Hospitais

No dia 5 de Fevereiro de 2016, a rede de computadores do Hospital Hollywood Presbyterian Medical Center foi infectado por um ransomware, ainda desconhecido, causando inúmeros prejuízos tanto sociais quanto financeiros. Como reportado por BELCHER (2016) o hospital passou 10 dias sem conseguir usar o seu sistema, pois informações críticas foram criptografadas e inutilizadas até que o hospital pagasse a quantia demandada pelos atacantes.

De acordo com CROUCH (2016) o hospital passou esse tempo utilizando papeis para guardar as informações dos pacientes. Informações anteriores, assim como histórico de pacientes e resultados de exames, ficaram retidos nos computadores. Além disso 911 pacientes precisaram ser

transferidos para outros hospitais devido a problemas de acesso a serviços digitais vitais para o funcionamento do hospital.

Finalmente, no final dos 10 dias, o hospital afirma ter pagado uma quantia de US$17.000 para ter seus dados de volta (RAGAN 2016). Contudo, existe uma confusão relativa ao valor pago pelo hospital, pois, como explicitado por RAGAN (2016), indícios apontam que a quantia pedida pelo ransomware era de 9000 bitcoins, o que, segundo o valor do bitcoin no período, representava uma quantia de 3,4 milhões de dólares. Com base nesses dados é possível levantar dúvidas em relação á veracidade da quantia que foi paga, principalmente quando existe um alerta geral, por parte do FBI, de que não se deve pagar a quantia ao atacante, pois isso incentivaria a propagação de mais ransomwares. Tendo isso em vista, fica claro, portanto, que publicar que um ransomware rendeu valores tão altos quanto 9000 bitcoins seria um enorme incentivo ao aperfeiçoamento e expansão do uso de ransomwares por parte de organizações criminosas.

Outros hospitais, como reportado por GALLAGHER (2016a), também foram vítimas de ransomwares nos Estados Unidos no ano de 2016. Dados de uma rede de hospitais da MedStar foram criptografados por um ransomware chamado Samsam, também conhecido como Samas ou MSIL. O epicentro do ataque foi um hospital da rede chamado Baltimore's Union Memorial Hospital em Maryland. Autoridades afirmam que a quantia pedida no ataque foi de 45 bitcoins, totalizando, à época aproximadamente, US$18.900.

GALLAGHER (2016a) também explica que a origem do ataque a rede StarMed tem relação com falhas na segurança de aplicações baseadas em Java e principalmente no JBoss Application Server. Eram expostas vulnerabilidades no servidor JBoss através da ferramenta JexBoss, em seguida, após alguns passos, eram utilizadas ferramentas para roubar credenciais do sistema. Em seguida a rede era analisada com o objetivo de procurar computadores Windows que poderiam ser invadidos usando as credenciais roubadas e poder inocular o Samsam.

4.2 Ataque a Sites: Malvertising

Recentemente, no mês de março de 2016, como mostrado por HERN (2016), grandes sites foram alvos de ataques maliciosos, como o New York Times, a BBC e AOL, no sentido de servirem como plataforma de distribuição de ransomwares através de suas propagandas. Primeiramente, deve-se ressaltar que existem inúmeras propagandas maliciosas em sites com pouca credibilidade pela internet que, ao serem acessadas, podem contaminar sua vítima com os mais diversos tipos de malware. Contudo, o diferencial nesse tipo de ataque é a exploração de vulnerabilidades em sites de alta credibilidade para usar suas propagandas como veiculo de transmissão de ransomwares.

HERN (2016), em seu artigo no The Guardian, denomina o ataque como Malvertising, *malware* + *advertising* (propaganda), e explica que ao clicar na propaganda infectada, o usuário é redirecionado para um servidor do Angler Exploit Kit. Por sua vez um exploit kit explora as vulnerabilidades do computador da vítima e faz como que ele baixe malwares e o instale. HERN (2016) também informa que o Angler Exploit Kit conseguiu infectar as propagandas desses sites explorando uma vulnerabilidade que surgiu após uma atualização do Microsoft Silverlight, usado nessas propagandas.

4.3 Ataques à Polícia

Foram reportados que, no final de 2014 e início de 2015, alguns departamentos de polícia dos Estados Unidos foram vítimas de ataques de ransomwares desde quando os ataques começaram a se tornar algo mais massivo, a partir de 2013 com o surgimento do CryptoLocker.

Como reportado por MILLER (2015), em dezembro de 2014 o departamento de polícia de Tewksbury sofreu um ataque do ransomware CryptoLocker, deixando o departamento sem acesso a seus dados por aproximadamente 5 dias. Nesse período, com a ajuda do FBI, Homeland Security e o Massachusetts State Police, foram feitas tentativas de quebrar a criptografia. Sem sucesso, foi necessário pagar o valor de US$500 para ter

novamente acesso aos dados. Foi declarado, também, que, nesse caso, o backup mais recente, não corrompido, datava de 18 meses antes do ataque, inviabilizando a restauração do sistema para essa data.

De acordo com PRATT (2015) novamente outro ataque aconteceu em janeiro de 2015, dessa vez no departamento de polícia de Midlothia. É dito que a infecção foi efetuada através de um e-mail contendo o ransomware e que apenas um único computador foi infectado, não o sistema inteiro. Como, nesse caso, os arquivos de backup existentes foram todos corrompidos, foi decidido pagar a quantia pedida pelo atacante. O valor não foi informado.

MILLER (2015) também destaca a ocorrência de outro ataque em Novembro de 2013: o departamento de polícia de Swansea também foi atacado e teve que pagar um valor de US$750 para reaver seu dados.

Com base em tudo demonstrado até então fica claro que ataques de ransomware não fazem distinção de vítimas, simplesmente infectam o sistema da pessoa ou organização que não tomaram as devidas precauções para evitar ser infectado. Além disso, evidências apontam para a importância da manutenção de arquivos de backup para evitar o pagamento do “resgate“ aos criminosos, principalmente backups externos à rede.

5 Evolução da Abordagem

A abordagem escolhida pelos diversos ransomwares para atacar suas vítimas tem variado ao longo do tempo. Esse ponto pode ser demonstrado através de análise do comportamento dos ransomwares em destaque e dos grandes ataques nos últimos tempos, tanto em termos de tecnologia utilizada na infecção como em termos de vítimas escolhidas e engenharia social. É notório que ela tem evoluído para amplificar a quantidade de vítimas, principalmente com o objetivo de fazer, a qualquer custo, com que elas paguem o valor do resgate. É possível observar também que esforços tem sido feitos no sentido de aumentar a defesa contra os ransomwares, tanto para neutralizá-los, uma vez que eles já efetuaram ataques, quanto para evitar novos ataques.

Nesta sessão será apresentada a evolução das técnicas e abordagens de ataque e devesa, que atualmente tem sido usadas respectivamente por ransomwares e órgão de defesa. Em seguida, será feita uma breve análise do impacto dos ransomwares e diversos setores sociais e econômicos, ao longo do tempo. Então, por fim será feito um panorama das técnicas de ataque que futuramente podem ter um enorme impacto nos meios digitais.

5.1 Análise de técnicas de ataque

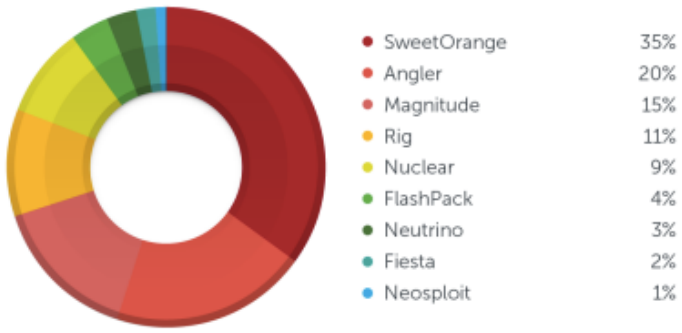
Neste trabalho foram abordados diversos tipos de ransomwares e os principais ataques a eles atribuídos. A partir disso é possível observar que os ransomwares tem evoluído e muitas vezes utilizando abordagens diferentes para, cada vez mais, expandir seu raio de influência. Nessa sessão serão abordados alguns métodos de ataque adotados pelos ransomwares no intuito de evitar procedimentos de defesa já consolidados.

5.1.1 Exploit Kits

Vários métodos são utilizados por malwares para chegarem até suas vítimas, atualmente houve um aumento do uso dos chamados Exploit Kits para esse fim. KOTOV e MASSACCI (2013) definem Exploit Kit, de forma simples: um software comercializado no mercado negro digital que pode ser usado para executar ataques a computadores. De forma mais detalhada o Exploit Kit é uma aplicação do lado servidor HTTP que, ao ser acessada, através do redirecionamento em uma página comprometida, explora as vulnerabilidades do browser utilizado. Essas vulnerabilidades são usadas para executar instruções no computador da vítima para baixar e instalar softwares maliciosos. Segundo CHEN e LI (2015) o primeiro Exploit Kit a ser reportado foi o WebAttacker Kit, em 2006, e atualmente são conhecidos 70 outros em atividade.

De forma sucinta, como explicado por CHEN e LI (2015), os Exploit Kits possuem 4 etapas em seu fluxo de trabalho: contato, redirecionamento, exploração e infecção. A etapa de contato é como o usuário chega até o Exploit Kit. Essa aproximação pode ser através de link em e-mails maliciosos ou redirecionamento de sites invadidos. A etapa de redirecionamento ocorre quando, ao acessar um site, teoricamente seguro, porém invadido, o usuário é redirecionado através de controle de tráfego, muitas vezes realizados por terceiros através de provedores de tráfego que vendem serviços no mercado negro. Ao chegar na landing page do Exploit Kit a fase de exploração é iniciada e então é analisado o ambiente do usuário e softwares vulneráveis são identificados, sejam eles browsers, flash, adobe, java, etc. Uma vez encontrado o ponto de vulnerabilidade do usuário é iniciada a fase de infecção. Nela o servidor utiliza a falha de segurança identificada para iniciar o download do malware diretamente no computador da vítima, concluindo, dessa forma, o ataque.

Figura 7 – Gráfico indicando a taxa de envolvimento de casa um dos Exploit Kits mais importantes na totalidade dos ataques envolvendo os mesmos (dados de 2014).



Fonte : https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

Um Exploit Kit muito usado na distribuição de ransomwares ao redor do mundo é o Angler. Várias fontes apontam o Angler como responsável pela distribuição de diversos tipos de ransomwares como, por exemplo, segundo CABAj et al (2015), o CryptoWall, segundo a SYMANTECH, o CryptoLocker e, segundo GOODIN (2016a) um ransomware chamado TeslaCrypt.

O Magnitude Exploit Kit, também em ascendência, representa uma parcela elevada dos ataques e, como apresentado por RAGAN (2016), foi responsável por um ataque nos servidores da PHP.net, onde quem acessava era redirecionado e tinha o computador infectado. Ele também é responsável por disseminar ransomwares como CryptoLocker e o CryptoDefence.

Um outro Exploit Kit, o Nuclear, tem causado muito impacto devido a seu uso na distribuição do ransomware Locky. De acordo com GALLAGHER(2016c) o Nuclear foi responsável pela infecção de aproximadamente 144.000 computadores em 200 países, por conta disso o mesmo se tornou um pivô na campanha de infecção do Locky.

Por sua vez, como observado na **figura 6,** o SweetOrange representava mais de um terço dos ataques envolvendo Exploit Kits em 2014, e, de acordo com CHEN e LI (2015), o mesmo distribui ransomwares em seus ataques. Como pôde ser observado, outros Exploit Kits como Angler, Magnitude e Nuclear também tem um importante papel na distribuição de ransomwares. Conclui-se, portanto, que, com base na **figura 6,** uma parcela

muito grande dos ataques de Exploit Kits podem envolver diversos tipos de ransomwares.

É importante constatar que, com o surgimento dos Exploit Kits, a origem de uma infecção por malware foi levada a um outro patamar. Enquanto essas infecções aconteciam de forma ativa, ou seja, intencionalmente baixando algum arquivo que poderia conter ou ser o malware, após o surgimento dos Exploit Kits, muitos ataques passaram a acontecer de forma passiva. Essa infecção passiva ocorre quando o download do malware é feito sem que o usuário tome conhecimento do que está acontecendo. Enfraquecendo, portanto, um dos principais meios de defesa contra ransomwares, que são algumas boas práticas de interação com o mundo digital, ou seja, principalmente, tomar cuidado com o que é baixado e instalado no computador.

5.1.2 Ransomware as a Service

Os uso dos Exploit Kits não foi o único método utilizado para expandir a influência dos ransomwares, outra forma foi facilitar o acesso a ransomware para atacantes que não possuem conhecimento técnico para criar um. Para tal finalidade organizações criaram um serviço denominado de Ransomware as a Service (RaaS). O RaaS, como definido por BHARWAJ et Al (2015), é um meio de comercializar serviços de ransomware onde o contratante pode pagar para que o contratado execute um ataque ou então adquirir o ransomware por uma certa quantia. Em outras palavras, uma pessoa ou organização que não possui conhecimento técnico para desenvolver um ransomware pode adquirir facilmente os serviços de um. Com base nisso, torna-se evidente que isso pode proporcionar um aumento significativo no número de ataques, pois o acesso ao malware é facilitado.

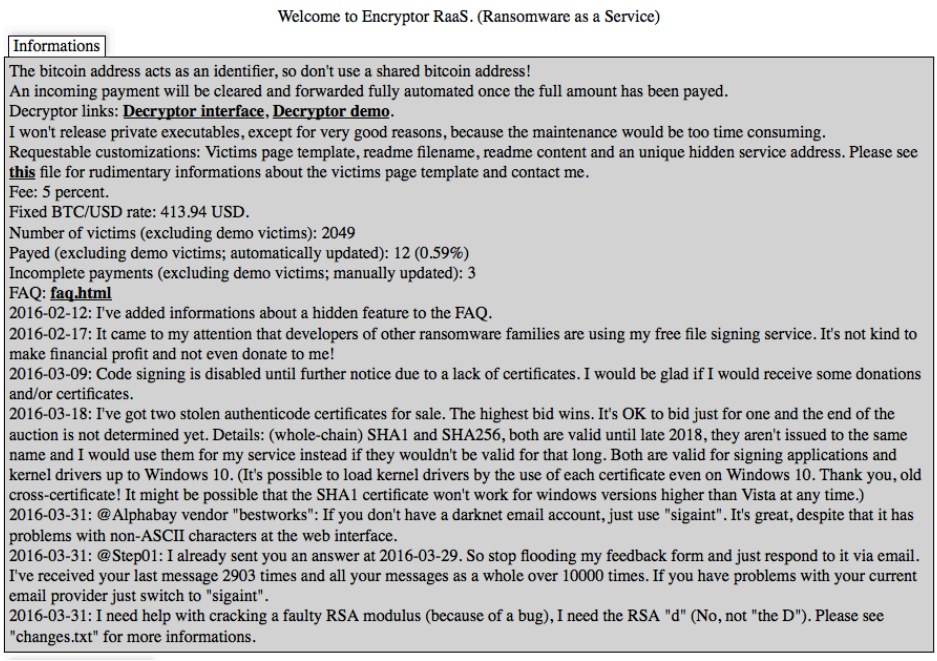
Em 2015 a McAfee Lab descobriu uma espécie de RaaS chamado Tox. Segundo MacAfee Lab (2015), kits para leigos poderem montar seus próprios malwares, em geral, tem se tornado algo comum. Contudo, apenas agora, com o Tox, se tornou possível fornecer esse mesmo tipo de serviço para os ransomwares. O Tox é uma ferramenta gratuita que funciona na

DarkWeb, ou seja, um conjunto de páginas não mapeadas por alguns engenhos de busca, que necessitam de navegadores específicos para serem acessadas, como o TOR. Segundo a MacAfee Lab (2015) são necessários apenas 3 passos para criar o ransomware: dar um nome, dizer qual o valor a ser pago pela vítima e preencher um Captcha. Após isso o consumidor recebe um executável para ser distribuído como bem entender. O Tox lucra requisitando 20% do valor arrecadado com o malware.

Para analisar melhor esse modelo de negócio envolvendo ransomwares, foi feita uma pesquisa na DarkWeb. O acesso foi feito utilizando o navegador TOR, capaz de esconder o IP de quem acessa as páginas, como uma medida de segurança, devido ao alto índice de atividades ilegais acontecendo da DarkWeb.

Mediante essa pesquisa foi encontrado um site (http://encryptor3awk6px.onion/Encryptor RaaS) que fornece os serviços do Encryptor RaaS.

Figura 8 – Página de início do site de que fornece o serviço de ransomware.

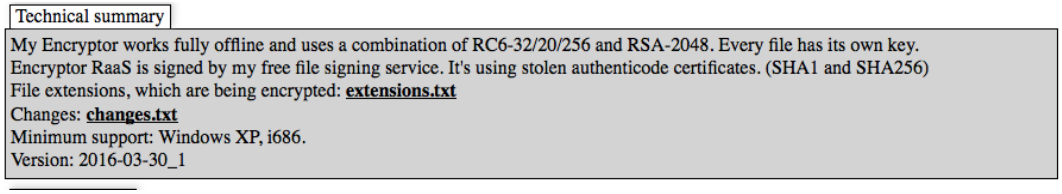


Fonte : http://encryptor3awk6px.onion/Encryptor RaaS

Nesse caso o malware é fornecido de forma gratuita aos clientes que querem usufruir desse serviço, tudo que o distribuidor pede é uma parcela de

5% do valor pago pelas vítimas. O site também fornece detalhes técnicos sobre o ransomware, além de um suporte por e-mail e uma sessão de perguntas frequentes.

Figura 9 – Sumário de detalhamento técnico fornecido pelo site que fornece o serviço de ransomware.



Fonte : http://encryptor3awk6px.onion/Encryptor RaaS

Pode ser constatado, através disso, que não só os ransomwares estão ficando mais especializados, se tornando mais difíceis de serem combatidos, mas novas abordagens tem surgido no intuito de facilitar o acesso de leigos a procedimentos de defesa e/ou prevenção. Essa abordagem fornece “poder de fogo“, de forma fácil, a quem estiver interessado, ampliando, possivelmente, a quantidade de vítimas dos ransomwares.

5.1.3 Ransomware Cross-platform

Uma das grandes limitações dos ransomwares até então é o sistema operacional do computador da sua vítima. Muitos ransomwares são desenvolvidos para afetar apenas um sistema operacional. Com base nisso surgiu um novo gênero de malware, o Cross-Platform Malwares, que é capaz de infectar computadores que possuam sistemas operacionais diferentes.

De acordo com PAGANINI (2016) pesquisadores do Kaspersky Lab descobriram um gênero de malware que se apresenta no formato de um executável Java (.jar), representando um risco para os sistemas Windows, Linux, Mac OS, e até mesmo Android, devido a portabilidades das aplicações java nos diversos sistemas. Para rodar uma aplicação java é necessário apenas que o Java Runtime Enviroment (JRE) esteja instalado no computador, o que ocorre em 70%-80% dos casos. Deve-se observar, também, que foi constatado que os grandes pioneiros dos Cross-Platform

Malwares são representantes de diversos grupos do submundo criminal brasileiro, como reportado por PAGANINI (2016).

É importante observar que o mercado de ransomware, em 2016, como apresentado por LEOB (2016), já possui um exemplar de Cross-Platform Ransomware, o Ransom32. Desenvolvido em NW.js, basicamente JavaScript, é baseado no WebKit, utilizado por diversos browsers. Enquanto os browsers limitam o que o JavaScript pode fazer, NW.js pode interagir com o sistema operacional. Aplicações desenvolvidas com ele podem ser executadas em diversos sistemas operacionais, inclusive sem precisar de um framework específico para ser executado, pois esses programas possuem a capacidade de se comprimir em um executável compatível.

Closs-Platform Ransomwares, tem como principal objetivo aumentar de forma devastadora a área de impacto dos ransomwares. Enquanto um único ransomware só poderia infectar computadores com o sistema operacional Windows, por exemplo, agora ele poderia também infectar computadores que utilizam Mac OS ou Linux, o que segundo a NETMARKETSHARE (2016), representaria um aumento de pouco mais de 13% nos computadores impactados pelo malware.

5.2 Análise de técnicas de defesa

Em termos de técnicas de defesa contra ataques de ransomwares pode-se observar um grande esforço por parte de organizações para reduzir o impacto desse tipo de malware. Primeiramente, é importante observar que existem vários meios de combater esse tipo de ameaça, seja através de técnicas de prevenção, criação de ferramentas de apoio ou derrubada de servidores.

5.2.1 Técnicas de prevenção

É importante observar que as técnicas de prevenção tem se mostrado uma das formas mais eficientes de combate a ransomwares, principalmente a manutenção de backups. GHEORGHE (2015) enumera 8 medidas, todas de

caráter preventivo, que devem ser tomadas para aumentar a defesa do computador contra ataques de ransomwares:

- **Educação do usuário** para evitar ataques de engenharia social através de e-mails ou sites suspeitos.
- **Utilizar Soluções de segurança atualizadas** para a detecção e eliminação do malwares antes que ele comece a funcionar.
- **Limitar aplicações que possam rodar** para impedir um ataque passivo de um ransomware.
- **Usar firewall** evitando dessa forma o a conexão com servidores de sites suspeitos.
- **Aumentar o nível de privilégios necessários para rodar um programa.**
- **Habilitar o serviço de restauração do sistema** para poder recuperar dados perdidos através da restauração do sistema para um ponto anterior a infecção.
- **Criar Backup** para a recuperação de dados perdidos.
- **Atualizar todos os programas** principalmente antivírus para ele saber lidar com novas ameaças existentes.

É importante salientar que, mesmo com todas essas medidas, como já foi demonstrado anteriormente, ransomwares tem evoluído sempre com o objetivo de contorná-las e efetivar a infecção. Portanto, essas medidas podem ser utilizadas apenas como meio de reduzir as chances de infecção ou até mesmo o impacto dela. Importante ter em vista que ransomwares como o CryptoWall apagam arquivos de restauração do sistema, e outros ransomwares ainda apagam arquivos de backup encontrados, outros ainda podem criptografá-los. Todavia uma solução ainda bastante efetiva contra ransomwares é a manutenção de arquivos de backup remotos, que não estão conectados ao computador infectado nem à rede a que ele pertence, assim o ransomware não poderia atingi-los.

5.2.2 Criação de Ferramentas

É notório que existem meios para eliminar a ameaça dos ransomwares uma vez que eles tenham infectado o computador da vítima, seja através de tutoriais ou através de ferramentas especializadas. Pode-se observar que pela internet existe diversos sites ensinando meios de se livrar de ransomwares utilizando serviços de restauração do Windows e uso do backup, que são bastante efetivos em certos casos. Contudo, é importante relembrar que muitos ransomwares já tem evoluído no sentido de evitar que o serviço de restauração do Windows seja utilizado como no caso do CryptoWall.

As ferramentas desenvolvidas sempre tem caráter de quebrar a criptografia de um ransomware específico. Organizações de segurança criam esses softwares através de análise do código e da criptografia utilizada por ransomwares. Outros softwares surgem após um servidor de ransomware ter sido derrubado, conseguindo informações importantes para quebrar seu esquema criptográfico, como tabela de chaves ou código gerador de chaves. De acordo com HIGGINS (2015), a empresa Cisco elaborou uma ferramenta capaz de descriptografar os arquivos criptografados pelo ransomware TeslaCrypt. Havia sido dito que o TeslaCrypt apresentava uma criptografia assimétrica RSA-2048, porém, através de engenharia reversa foi constatado que ela é simétrica, portanto a ferramenta desenvolvida pode descriptografar os arquivos do usuário contanto que a chave criptográfica ainda esteja no sistema. Segundo HIGGINS (2015), também foi aplicada a mesma técnica para criar um “remédio“ contra ataque do CryptoWall mas a criptografia assimétrica tornava extremamente difícil a criação dessa proteção.

De acordo com a ABRAMS (2016c) o ransomware Petya também teve sua criptografia quebrada e ferramentas desenvolvida para descriptografar os arquivos criptografados. Outro ransomware que teve sua criptografia, teoricamente, quebrada foi o KimcilWare. A forma de descriptografar os arquivos foi proposta por PHAN & PAZ (2016), através de análise do código fonte. Porém ainda não se sabe de um software capaz de fazer isso automaticamente.

O caso do CryptXXX, que teve sua criptografia quebrada pela Kaspersky lab, segundo ILYIN (2016), representa uma evolução das técnicas de defesa em comparação com as de ataque de ransomwares. Após o surgimento do CryptXXX logo foi desenvolvida uma solução pela Kaspersky Lab, o RannohDecryptor. Era necessário que o usuário fornecesse o backup de pelo menos um arquivo criptografado para conseguir descriptografar todos os outros arquivos. Pouco tempo depois, após o surgimento de uma segunda versão do ransomware, logo foi lançada uma atualização do RannohDecrypto que não requisitava mais um arquivo de backup para descriptografar todos os arquivos.

Alguns ransomwares também podem ter seus servidores derrubados, expondo seu código fonte e tabelas de chaves, possibilitando o desenvolvimento dessas ferramentas de combate. O FBI, assim como outras organizações, tem juntado esforços para combater os ransomwares, não só no intuito de prevenir e corrigir infecções, mas também derrubando seus servidores. Vários ransomwares tem sido desativados como foi o caso, já citado, do CryptoLocker que foi desativado juntamente com a botnet GameOrverZeus em 2014. Desativar um ransomwares pode abrir portas para o desenvolvimento de soluções para descriptografar dados criptografados dos computadores das vítimas. Isso se dá pois, muitas vezes, obtêm-se acesso a algoritmos de geração de chaves de criptografia ou banco de dados relacionando chaves publicas e privadas.

Conforme dito por KHANDELWAL (2014), após a queda dos servidores do CryptoLocker, desativado pelo FBI, as empresas Fireeye e Fox-it, desenvolveram uma ferramenta gratuita, baseado no banco de dados de chaves privadas nos servidores do CryptoLocker, para descriptografar arquivos em computadores infectados pelo ransomware.

Ainda assim, deve-se ter em mente que essas medidas para corrigir os problemas da infecção são escassas e apenas tem capacidade de combater alguns tipos de ransomwares mais vulneráveis. Dessa forma, é importante destacar que a melhor medida de combate a ransomwares atualmente é através da prevenção.

5.2.3 Uso da blockchain contra os ransomwares

A blockchain, como já foi dito, é um framework utilizado em várias aplicações, uma delas é a rede de bitcoins. Ela uma rede de blocos gerados através de processos criptográficos e cada bloco possui registros de transações de bitcoins, a blockchain inteira guarda todo o histórico de transação. Existem várias interfaces que podem ser usadas para visualizar todas essas transações, uma delas é o site “blockchain.info”.

Não apenas os ransomwares mas várias organizações criminosas utilizam do distema de bitcoins para manter seus negócios. Um exemplo desse tipo de organização é a SilkRoad, uma interface de compra e vinda que funciona da darkweb e é utilizada por muitos como meio de tráfico de drogas. O caráter de pseudo-anonimato do sistema de bitcoins protege a identidade real das pessoas envolvidas nesse tipo de negócio. Como funciona esse pseudo-anonimato? Cada usuário do sistema de bitcoins pode possuir 1 ou mais endereços, esses endereços podem guardar bitcoins e participar de transações, enviando ou recebendo bitcoins de outros endereços. Cada endereço é uma sequencia de 26 a 35 caracteres alfanuméricos, tornando impossível de identificar o proprietário de cada endereço olhando apenas para eles.

O pseudo-anonimado surge quando passaram a existir algoritmos que, a partir de estudos da blockchain, seus endereços e as relações entre eles, conseguem fazer estimativas sobre quem é o proprietário de cada endereço. SPAGNUOLO (2013) mostra um framework, o BitIodine, capaz de fazer uma análise forense na blockchain gerando clusters de endereços que possam pertencer a uma mesma pessoa ou organização, ele foi inclusive usado para analisar o endereços relacionados ao ransomware CryptoLocker. Alguns endereços de bitcoins já são associados a alguma organização quando ela publica um endereço para poder fazer transações (exemplo endereço de doação), com esse framework seria capaz de organizar os endereços pertencentes aquela organização em um grupo. Protanto, com um endereço de um grupo identificado, todos os outros seriam identificados também.

Esse tipo de abordagem podem auxiliar a descoberta organizações ou pessoas que possam estar por trás das fraudes relativas a ransomwares.

Essa abordagem cria um combate direto contra os ransomwares, descobrindo os culpados e desligando os servidores. São técnicas de ataque dentre as de defesa.

5.2.4 Outras técnicas de combate

O FBI tem feito uma campanha definida por uma estratégia de eliminação dos ransomwares a longo prazo, que seria aconselhar todos os indivíduos e organizações infectadas a não pagar o valor cobrado pelos atacantes. A efetivação dessa estratégia reduziria drasticamente o lucro das organizações criminosas sobre os ransomwares, eliminando a ameaça. Todavia, essa situação é muito difícil de ser controlada, uma vez que na maioria das vezes não é possível recuperar as informações sem recorrer ao pagamento, fazendo com que o dano material de uma organização vítima seja maior caso ela não possua os arquivos importantes de volta.

Além disso, boa parte dessas boas práticas para prevenção dos ransomwares são substancialmente ineficientes no combate efetivo dos ransomwares pois, de acordo com a organização KASPERSKY (2016a), 43% de uma amostra de entrevistados nos Estados Unidos e canada nunca ouviram falar dos ransomwares. Portanto, com base nisso, a ameaça proporcionada pelos ransomwares ainda são desconhecidas por uma parcela muito grande da população, logo muitas pessoas não tomam as devidas precauções para evitá-los.

Também podem ser observados esforços em termos de criação de técnicas de defesa automatizada contra os ransomwares. YANG et al (2015), em seu artigo, propõe um modelo conceitual para análise dinâmica de softwares com o propósito de detectar malwares, em especial ransomwares, em aparelhos Android. A maioria dos Antivírus analisam o software de forma estática que, além de já possuírem uma lista definida de malwares a serem combatidos, descompilam a APK, detectam e comparam os componentes e analisam o código de reempacotamento, que pode injetar código malicioso no sistema. A solução propõe que, além disso, exista uma análise dinâmica das

aplicações que basicamente consiste numa simulação controlada da aplicação, com o objetivo de analisar seu comportamento no dispositivo.

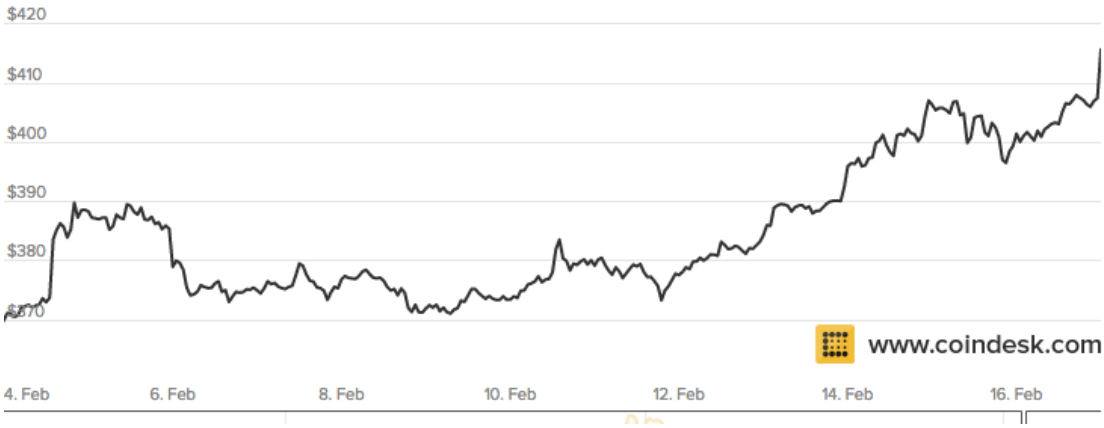
Em suma, pode-se observar que existe um grande esforço para se controlar o impacto dos ransomwares. Fica claro que os principais meios de combate a ransomwares estão nas técnicas de prevenção, boas práticas e manutenção de backup. As ferramentas disponibilizadas para remediar o ataque existem porem são poucas e limitadas, possibilitando a remoção dos efeitos de alguns ransomwares. Porém, fica claro que, através do que foi exposto, os avanços nas técnicas de ataque dos ransomwares tem conseguido contornar várias estratégias de defesa, fazendo com que, atualmente, a única estratégia realmente efetiva contra os ransomwares seja a manutenção de arquivos de backup externos.

5.3 Impacto dos ransomwares

Pelo caráter reversível dos danos que os ransomwares podem causar, fica claro que o maior impacto, direto, dos ransomwares na sociedade é econômico, outros tipos de consequências podem surgir caso a quantia não seja paga. De acordo com KASPERSKY (2016a) o FBI possui mais de 4.200 casos de reclamações em relação a ransomwares e estima-se que, pelo número de vítimas, 47 milhões de dólares foram transferidos para os atacantes. Sabe-se que, segundo FITZPATRICK (2016), apenas nos primeiros 3 meses de 2016 os ransomwares foram capazes de coletar 209 milhões de dólares em resgate, mostrando que, permanecendo nesse ritmo, só em 2016, ransomwares podem ser responsáveis por um rombo de 1 bilhão de dólares.

É notável que os ataques de ransomwares também impactaram flutuações cambiais no valor do bitcoin, que por si só podem causar mudanças na economia.

Figura 9 – Gráfico da flutuação do valor do bitcoin entre os dias 4 e 17 de fevereiro.



Fonte : http://www.coindesk.com/price/

Estima-se que a campanha do ransomware Locky tenha se dado início por volta de fevereiro de 2016 e justamente nesse período, como observado no gráfico da figura 9, houve um grande crescimento no valor do bitcoin entre os dias 12 e 17 de fevereiro, evidenciando um aumento na compra de bitcoins nesse período, possivelmente acarretado pelos gastos em bitcoins necessários para reverter os efeitos do Locky.

Curiosamente, ainda com base na figura 9, o gráfico de flutuação cambial de bitcoins pode, por sua vez, mostrar indícios de próximos ataques, pois, no dia 5 de fevereiro, quando ocorria um máximo local do valor do bitcoin em relação ao dólar americano, ocorreu o ataque ao Hospital Hollywood Presbyterian Medical Center. Ou seja, mesmo sendo uma possibilidade, o momento oportuno em que aconteceu o ataque ao hospital pode apontar para uma possibilidade de previsão de futuros grandes ataques de acordo com o valor do bitcoin, mostrando, portanto, que economia e ransomwares podem possuir uma correlação.

5.4 Uma perspectiva futura

Com base em tudo que foi observado, os ransomwares tem evoluído, tanto em infecção quanto em comportamento. Portanto, alguns especialistas

fazem projeções sobre o futuro dos ataques de ransomwares, ou seja, como eles se apresentariam e se comportariam em um futuro próximo.

Pesquisadores da TALOS (2016) afirmam que ransomwares tendem a imitar malwares clássicos, no seu estilo de propagação em massa, os chamados worms, como por exemplo, ameaças como Conficker e o SQL Slammer, worms que se destacaram pelo seu impacto e grande capacidade de se multiplicar. A TALOS (2016) exemplifica essa tendência com o caso do ransomware SamSam, que é capaz de se propagar na rede de computadores interna da vítima. Esse tipo de comportamento pode se tornar uma tendência e ser aperfeiçoada até o surgimento do chamado Cryptoworm, ou seja, ransomwares com capacidade de se propagarem para diversos computadores e sistemas de forma automática transformando, dessa forma, as infecções de ransomwares numa pandemia generalizada e extremamente perigosa.

Além disso TALOS (2016) sugere um modelo de framework de criação manutenção de ransomwares. Esse framework modularizaria os ransomwares e daria suporte a diferentes módulos, sendo esses módulos responsáveis pelo comportamento do ransomwares, que hipoteticamente teriam a capacidade de serem alterados para contornar estratégias de defesa e adaptar estratégias de ataque. Um exemplo é a escolha entre uma infecção mais agressiva ou uma mais cuidadosa, controlado por módulos que vão limitar o processamento do ransomware para ele passe despercebido sem sobrecarregar o processador. Outro exemplo seria um módulo permitira que o ransomware se copiasse em executáveis não protegidos pelo sistema na expectativa desses executáveis fossem propagados ou reexecutados para o ataque ser retomado. Essa enorme adaptabilidade dos ransomwares proporcionariam ataques mais específicos a organizações especificas compreendendo objetivos e vulnerabilidades, torando os ataques mais eficientes.

Com base em uma tendência atual de modernizar os carros imbuindo eles com um sistemas computadorizados e automatizados digitalmente, como computadores de bordo, carros autoguiados e ignição computadorizada, BOOTH (2016) chama atenção para uma nova modalidade de “roubo“ de carros seguindo a tendência dos ransomwares. Ele alerta que,

ransomwares desenvolvidos para infectar sistemas operacionais de carros podem, futuramente, impedir o carro de funcionar apenas bloqueando acesso do sistema a vários arquivos, forçando o dono do carro a pagar o valor do resgate para ter seu carro de volta. Outro risco, ainda mais sério, levantado por BOOTH (2016) é o caso de uma epidemia generalizada em carros de uma determinada empresa forçando esse fabricante a pagar o resgate para desbloquear todos os carros e não ter que reembolsar consumidores insatisfeitos.

Com essas perspectivas é notório que os ransomwares possuem um enorme potencial de evoluírem ainda mais se tornando cada vez mais perigosos e difíceis de controlar. Essas possibilidades futuras vem se tornando cada vez mais reais uma vez que o mercado de ransomwares tem se mostrado extremamente lucrativo para as organizações criminosas. Para isso os ransomwares tem se tornado cada vez mais perniciosos e difíceis de serem evitados e controlados. Consequentemente as tentativas de dissuadir as vítimas a pagarem pelo resgate tem falhado uma vez que pagar os valores, relativamente pequenos, do resgate tem sido menos danoso do que a perda dos dados.

6 Conclusão

Neste trabalho foi apresentado o conceito de ransomware e como essa nova ameaça tem crescido em impacto ao longo dos últimos anos, justificado pela sua vertiginosa evolução em estratégias ofensivas.

Primeiramente foram relatados diversos tipos de ransomwares que obtiveram um grande impacto em seus ataques e que apresentavam características inusitadas. Como é o caso do CryptoLocker, cujo impacto alertou as autoridades sobre o dano que esse tipo de malware pode causar. Ransomwares como CTB-Locker e o Locky também apresentaram métodos inovadores de ataques. O primeiro atacando, além de sistemas Windows, websites e o segundo através do uso de macro do Microsoft Word.

Em seguida foram apresentados diversos ataques de ransomwares ao longo do tempo, tendo em foco o dano causado por esse tipo de malware na sociedade. Esses ataques tiveram como principal representante o ataque a redes de hospitais na California, não deixando alternativas a não ser o pagamento da quantia requisitada. Esse ataque serviu de exemplo mostrando que ransomwares podem afetar setores da sociedade que impactam diretamente na vida das pessoas como, por exemplo, impedindo o acesso a sistemas de saúde.

Após essa explicação mais ampla sobre o fenômeno dos ransomwares foram analisadas mais a fundo a evolução das estratégias de ataque dos ransomwares. Foram expostas técnicas como o uso de Exploit Kits, os ransomwares cross-platform e os Ransomwares as a Service. Além disso foram também analisadas métodos de defesa contra os ransomwares. Essas técnicas tem se mostrado eficazes no combate a esse tipo de ameaça, porém ainda está longe de conseguir erradicar completamente os ransomwares.

Em suma, esse trabalho pôde mostrar a evolução dos ransomwares em comparação a evolução das defesas contra eles. Pode ser concluido que os ransomwares tem conseguido evitar os estorços despendidos contra eles. Inclusive, estimativas apontam para que, futuramente, eles apresentem ainda maior impacto com novas soluções como o Cryptoworm.

6.1 Limitações do Trabalho

As limitações encontradas na composição desse trabalho dizem respeito a falta de informações de cunho científico a respeito do tema. Foi necessário recorrer a artigos de fontes não científicas, principalmente em sites de notícias, e relatórios de organizações de segurança e tecnologia da informação. Muitas vezes foi preciso comprar fontes de forma a obter um maior grau de certeza sobre o que estava sendo dito em relação as notícias e aos detalhes técnicos dos ransomwares estudados.

6.2 Trabalhos Futuros

Como trabalho futuro seria útil fazer um estudo referente a utilização de ransomwares por organizações criminosas para atingir determinados fins de cunho político. Ransomwares, como visto nesse trabalho, tem uma enorme capacidade de danificar setores importantes da sociedade como hospitais, departamentos de polícias e organizações, além de coletar fundos através disso. Esse estudo analisaria através, principalmente, da deepweb e darkweb sobre organizações harcktivistas utilizando ransomwares ataques a organizações políticas. Esses ataques poderiam ter o propósito de arrecadar fundos para financiar campanhas, ao mesmo tempo, causando danos aos alvos especificados.

7 Bibliografia

ABRAMS, Lawrence (2013). **CryptoLocker Ransomware Information Guide and FAQ**. Bleeping Computer. 2013. Disponível em: <http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information> Acesso em: 11 Abril 2016.

ABRAMS, Lawrence (2014). **CTB Locker and Critroni Ransomware Information Guide and FAQ**. Bleeping Computer. 2014. Disponível em: <http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information#ctb_locker> Acesso em: 25 Abril 2016.

ABRAMS, Lawrence (2015). **TeslaCrypt and Alpha Crypt Ransomware Information Guide and FAQ**. Bleeping Computer. 2015. Disponível em: < http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#decrypt> Acesso em: 05 Julho 2016.

ABRAMS, Lawrence (2016a). **The Locky Ransomware Encrypts Local Files and Unmapped Network Shares**. Bleeping Computer. 2016a. Disponível em: <http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/> Acesso em: 18 Abril 2016.

ABRAMS, Lawrence (2016b). **CTB-Locker for Websites: Reinventing an old Ransomware**. Bleeping Computer. 2016b. Disponível em: <http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/> Acesso em: 20 Abril 2016.

ABRAMS, Lawrence (2016c). **Petya Ransomware's Encryption Defeated and Password Generator Released**. Bleeping Computer. 2016c. Disponível em: <http://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/> Acesso em: 09 Junho 2016.

ABRAMS, Lawrence (2016d). **The KimcilWare Ransomware targets web sites running the Magento Platform**. Bleeping Computer. 2016d. Disponível em: < http://www.bleepingcomputer.com/news/security/the-kimcilware-ransomware-targets-web-sites-running-the-magento-platform/> Acesso em: 09 Junho 2016.

BAEL, Vangie (2015). **The Difference Between a Computer Virus, Worm and Trojan Horse**. Webopedia. 2015. Disponível em: <http://www.webopedia.com/DidYouKnow/Internet/virus.asp>. Acesso em: 15 Março 2016.

BARLOWE, Bill et al (2012). **The evolution of malware and the threat landscape – a 10-year review**. Microsoft Security Intelligence Report: Special Edition, fevereiro, 2012.

BELCHER, Pat (2016). **The Rise of Locky: Dridex Crew Bets on Ransomware**. Invincea. 2016. Disponível em: < https://www.invincea.com/2016/02/dridex-crew-bets-on-ransomware/> Acesso em: 14 Abril 2016.

BHARWAJ, Akashdeep et al (2015). **Ransomware: A Rising Threat of new age Digital Extortion** . 2015. Disponível em: <https://xxx.arxiv.org/pdf/1512.01980v1.pdf >. Acesso em: 31 Março 2016.

BISSON, David (2016a). **Under the Hood of Cryptowall 4.0**. Tripwire. 2016a. Disponível em: <http://www.tripwire.com/state-of-security/security-awareness/under-the-hood-of-cryptowall-4-0/> Acesso em: 13 Abril 2016.

BISSON, David (2016b). **Petya ransomware goes for broke and encrypts hard drive Master File Table**. Graham Cluley. 2016b. Disponível em: < https://www.grahamcluley.com/2016/03/petya-ransomware/> Acesso em: 9 Junho 2016.

BISSON, David (2016cs). **CryptXXX ransomware steals bitcoin and data from infected PCs**. Graham Cluley. 2016c. Disponível em: <https://www.grahamcluley.com/2016/04/cryptxxx-ransomware-steals-bitcoins-data-infected-pcs/>Acesso em: 9 Junho 2016.

BLUE, Violet (2013). **Cryptolocker's crimewave: A trail of millions in laundered Bitcoin**. ZDNet archive. 2013. Disponível em: <http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/>Acesso em: 31 Março 2016.

BOOTH, David (2016). **Motor Mouth: Ransomware is the future of car theft**. Driving. 2016. Disponível em: <http://driving.ca/auto-news/news/ransomware-is-the-future-of-car-theft> Acesso em: 11 Maio 2016.

CABAJ, Krzysztof et al (2015). **Network activity analysis of CryptoWall ransomware**. Przeglad Elektrotechniczny. Warsaw University of Technology. 2015.

CHEN, Joewph C. e LI, Brooks (2015). **Evolution of Exploit Kits: Exploring Past Trends and Current Improvements**. Trendmicro. 2015. Disponível em: < https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf> Acesso em: 12 Abril 2016.

CROUCH, Angie (2016). **FBI, LAPD Investigating Hollywood Hospital Cyber Attack**. NBCLosAngeles. 2016. Disponível em: <http://www.nbclosangeles.com/news/local/FBI-

LAPD-Investigating-Hollywood-Hospital-Cyber-Attack-368703121.html> Acesso em: 14 Abril 2016.

DROZHZHIN, alex (2016). **Ransomware's history and evolution in facts and figures**. Kaspersky Lab. 2016. Disponível em: < https://blog.kaspersky.com/ransomware-blocker-to-cryptor/12435/> Acesso em: 28 Junho 2016.

DUNN, John E. (2016). **CryptoWall 3.0 – the most succcessful malware in history is not unstoppable**. Computer World UK. 2016. Disponível em: <http://www.computerworlduk.com/security/cryptowall-30-most-succcessful-malware-in-history-is-not-unstoppable-3634801/> Acesso em: 13 Abril 2016.

FARIVAR, Cyrus (2016). **First Mac-targeting ransomware hits Transmission users, researchers say**. Arstechnica. 2016. Disponível em: <http://arstechnica.com/security/2016/03/first-mac-targeting-ransomware-hits-transmission-users-researchers-say/> Acesso em: 21 Abril 2016.

FBI (2014). **GameOver Zeus Botnet Disrupted Collaborative Effort Among International Partners**. FBI. 2014 Disponível em: <https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted>Acesso em: 05 Março 2016.

FITZPATRICK, David (2016). **Cyber-extortion losses skyrocket, says FBI**. CNN. 2016. Disponível em: <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology> Acesso em: 02 Junho 2016.

FLOOD, Raymond (2013). **Public Key Cryptography: Secrecy in Public**. Gresham College. 2013.

GALLAGHER, Sean (2016a). **Maryland hospital group hit by ransomware launched from within [Updated]**. Arstechnica. 2016a. Disponível em: < http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/> Acesso em: 14 Abril 2016.

GALLAGHER, Sean (2016b). **"Locky" crypto-ransomware rides in on malicious Word document macro**. Arstechnica. 2016b. Disponível em: <http://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/> Acesso em: 18 Abril 2016.

GALLAGHER, Sean (2016c). **"Nuclear" exploit kit service cashes in on demand from ransomware rings**. Arstechnica. 2016c. Disponível em: < http://arstechnica.co.uk/security/2016/04/nuclear-ransomware-exploit-kit-details/> Acesso em: 03 Maio 2016.

GAZET, Alexandre (2008). **Comparative Analysis of Various Ransomware virii**. In: EICAR 2008 EXTENDED. Journal in Computer Virology, Volume 6, Issue 1. pp. 77-90.

GHEORGHE, Alexandra (2015). **How to Strengthen Enterprise Defenses against Ransomware**. DarkReading. 2015. Disponível em: <http://www.darkreading.com/partner-perspectives/bitdefender/how-to-strengthen-enterprise-defenses-against-ransomware/a/d-id/1319245> Acesso em: 03 Maio 2016.

GOODIN, Dan (2016a). **Certified Ethical Hacker website caught spreading crypto ransomware**. Arstechnica . 2016. Disponível em: <http://arstechnica.com/security/2016/03/certified-ethical-hacker-website-caught-spreading-crypto-ransomware/> Acesso em: 03 Maio 2016.

GOODIN, Dan (2016b). **New and improved CryptXXX ransomware rakes in $45,000 in 3 weeks**. Arstechnica . 2016. Disponível em: < http://arstechnica.com/security/2016/06/new-and-improved-cryptxxx-ransomware-rakes-in-45000-in-3-weeks/> Acesso em: 27 Junho 2016.

GOODIN, Dan (2016c). **Meet Jigsaw, the ransomware that taunts victims and offers live support**. Arstechnica . 2016. Disponível em: <http://arstechnica.com/security/2016/06/meet-jigsaw-the-ransomware-that-taunts-victims-and-offers-live-support/> Acesso em: 06 Junlho 2016.

GRIFFIN, Nicholas (2016). **Locky Ransomware - Encrypt Documents, Database, Code, Bitcoin Wallets and More...** . Forepoint. 2016. Disponível em: < https://blogs.forcepoint.com/security-labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more >. Acesso em: 25 Março 2016.

HAMADA, Joji (2014). **Simplocker: First Confirmed File-Encrypting Ransomware for Android**. Symatec. 2014. Disponível em: <http://www.symantec.com/connect/blogs/simplocker-first-confirmed-file-encrypting-ransomware-android> Acesso em: 26 Abril 2016.

HERN, Alex (2016). **Major sites including New York Times and BBC hit by 'ransomware' malvertising**. The Guardian. 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising> Acesso em: 27 Abril 2016.

HIGGINS, Kelly Jackson (2015). **Cisco Offers Free Decryption Tool For Ransomware Victims**. DarkReading. 2015. Disponível em: <http://www.darkreading.com/cloud/cisco-offers-free-decryption-tool-for-ransomware-victims/d/d-id/1320188> Acesso em: 03 Maio 2016.

ILYIN, Yuri (2016). **How to beat CryptXXX again: an update**. Kaspersky Lab. 2016. Disponível em: < https://business.kaspersky.com/de-cryptxxx-2/5572/> Acesso em: 09 Junho 2016.

JEFFERS, Dave (2013). **Crime pays very well: Cryptolocker grosses up to $30 million in ransom**. PCWorld. 2013. Disponível em: <http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html>Acesso em: 31 Março 2016.

KASPERSKY (2016a). **Ransom-What? A study on consumers' awareness of ransomware**. Kaspersky Lab. 2016. Disponível em: < https://usblog.kaspersky.com/usa/files/2016/05/Ransomware-Report-Final.pdf> Acesso em: 02 Junho 2016.

KASPERSKY (2016b). **KSN Report: Mobile ransomware in 2014-2016**. Kaspersky Lab. 2016. Disponível em: <https://securelist.com/analysis/publications/75183/ksn-report-mobile-ransomware-in-2014-2016/> Acesso em: 06 Julho 2016.

KHANDELWAL, Swati (2014). Free CryptoLocker Ransomware Decryption Tool Released. The Hacker News. 2014. Disponível em: <http://thehackernews.com/2014/08/CryptoLocker-Decryption-Keys-Tool.html> Acesso em: 03 Maio 2016.

KHARRAZ, Amin et al (2015). **Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks**. In: ALMGREN, Magnus. Detection of Intrusions and Malware, and Vulnerability Assessment: 12th Edition, 2015. pp. 3-24.

KNOWBE4 (2016). **AIDS Trojan or PC Cyborg Ransomware**. KnowBe4. Disponível em: < https://www.knowbe4.com/aids-trojan>. Acesso em: 29 Março 2016.

KOSHY, Phillip; KOSHY, Diana e MCDANIEL, Patrick (2014). **An Analysis of Anonymity in Bitcoin Using P2P Network Traffic**. Pennsylvania State University, University Park, PA 16802, USA, 2014.

KOTOV, Vadim e MASSACCI, Fabio (2013). Anatomy of Exploit KitsPreliminary Analysis of Exploit Kits as Software Artefacts. In: **Engineering Secure Software and Systems**, pp 181-196, Paris, França 2013.

KREBS (2013). **How to Avoid Cryptolocker Ransonware**. Krebs on Security. 2013. Disponível em: <http://krebsonsecurity.com/2013/11/how-to-avoid-cryptolocker-ransomware/>Acesso em: 05 Março 2016.

LEOB, Larry (2016). **Cross-Platform Cryptoware Is Here**. Security Intelligence. 2016. Disponível em: <https://securityintelligence.com/news/cross-platform-cryptoware-is-here/> Acesso em: 03 maio 2016.

LIAO, Qinyu (2006). **RANSOMWARE: A GROWING THREAT TO SMES**. The University of Texas at Brownsville and Texas Southmost College, Brownsville. 2006.

MACAFEE LAB (2015). **Meet 'Tox': Ransomware for the Rest of Us**. McAfee Lab. 2015. Disponível em: < https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/> Acesso em: 02 maio 2016.

MEHMOOD, Shafqat (2016). Enterprise Survival Guide for Ransomware Attacks. **Global Information Assurance Certification Paper**. 2016. Disponível em: <https://www.giac.org/paper/gcih/24353/enterprise-survival-guide-ransomware-attacks/141997> Acesso em: 31 Maio 2016.

MICROSOFT (s. d.). **O que é malware?**. Microsoft. Disponível em: <https://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx>. Acesso em: 15 Março 2016.

MILLER, Jayne W. (2015). **Police pay ransom after cyberterror attack on network**. HomeNewsHere. 2015. Disponível em: <http://homenewshere.com/tewksbury_town_crier/news/article_8f8ce2ba-da0d-11e4-a127-578b97102bf0.html> Acesso em: 27 Abril 2016.

NAKAMOTO, Satoshi (2008). **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: < https://bitcoin.org/bitcoin.pdf >. Acesso em: 15 Março 2016.

NETMARKETSHARE (2016). **Desktop Operating System Market Share**. Netmarketshare. 2016. Disponível em: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0> Acesso em: 03 maio 2016.

OSBORNE, Charlie (2015). **New CryptoLocker ransomware targets gamers**. ZDNet archive. 2015. Disponível em: < http://www.zdnet.com/article/new-cryptolocker-ransomware-targets-gamers/>Acesso em: 05 Abril 2016.

PAGANINI, Pierluigi (2016). **Coder in the Brazilian Cyber Criminal underground are Pioneering Cross-platform malware relying on Java archive (JAR) Files**. Security Affairs. 2016. Disponível em: < http://securityaffairs.co/wordpress/45143/malware/cross-platform-malware.html > Acesso em: 02 maio 2016.

PCTOOL (s. d.). **What is malware and how can we prevent it?**. PCTool. Disponível em: <http://www.pctools.com/security-news/what-is-malware/>. Acesso em: 15 Março 2016.

PETERS, Sarah (2016). **Police Pay Off Ransomware Operators, Again**. DarkReading. 2016. Disponível em: <http://www.darkreading.com/attacks-breaches/police-pay-off-ransomware-operators-again/d/d-id/1319918> Acesso em: 27 Abril 2016.

PHAN, Tien e PAZ, Roland Dela (2016). **KimcilWare Ransomware: How to Decrypt Encrypted Files and who is Behind It**. Fortinet. 2016. Disponível em: <https://blog.fortinet.com/2016/04/01/kimcilware-ransomware-how-to-decrypt-encrypted-files-and-who-is-behind-it> Acesso em: 09 Junho 2016.

PRATT, Gregory (2015). **Midlothian cops pay ransom to retrieve data from hacker**. Chicago Tribune. 2015. Disponível em: < http://www.chicagotribune.com/news/local/breaking/ct-midlothian-hacker-ransom-met-20150220-story.html> Acesso em: 27 Abril 2016.

PRICEONOMICS (2015). **Who Invented the Computer Virus?**. Priceonomics. 2015. Disponível em: <http://priceonomics.com/who-invented-the-computer-virus/>. Acesso em: 15 Março 2016.

RAGAN, Steve (2014). **Exposed: An inside look at the Magnitude Exploit Kit**. CSO. 2014. Disponível em: < http://www.csoonline.com/article/2459925/malware-cybercrime/exposed-an-inside-look-at-the-magnitude-exploit-kit.html> Acesso em: 03 Maio 2016.

RAGAN, Steve (2016). **Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers**. CSO. 2016. Disponível em: <http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html> Acesso em: 14 Abril 2016.

REID, Fergal e HARRIGAN, Martin (2012). **An Analysis of Anonymity in the Bitcoin System**. Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Irlanda, 2012.

SICILIANO, Robert (2013). **What is a Keylogger?**. McAfee. 2013. Disponível em: <https://blogs.mcafee.com/consumer/what-is-a-keylogger/>. Acesso em: 15 Março 2016.

SINEGUBKO, Denis (2016). **Website Ransomware – CTB-Locker Goes Blockchain**. Sucuri blog. 2016. Disponível em: <https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html> Acesso em: 25 Abril 2016.

SINITSYN, Fedor (2015). **TeslaCrypt 2.0 disguised as CryptoWall. Securelist**. Disponível em: <https://securelist.com/blog/research/71371/teslacrypt-2-0-disguised-as-cryptowall/> Acesso em: 05 Julho 2016.

SOLOVE, Daniel (2016). **Ransomware Growing Out of Control. Tach Privacy**. 2016. Disponível em: < https://www.teachprivacy.com/ransomware-out-of-control/> Acesso em: 27 Junho 2016.

SPAGNUOLO, Michele (2013). **Bitlodine: Extracting Intelligence from the Bitcoin Network**. 2013. Politecnico di Milano. Disponível em: < https://miki.it/pdf/thesis.pdf> Acesso em: 02 Julho 2016.

STATISTA (2016). **B2C e-commerce sales worldwide from 2012 to 2018 (in billion U.S. dollars).** Statista. 2016. Disponível em: < http://www.statista.com/statistics/261245/b2c-e-commerce-sales-worldwide/ >. Acesso em: 15 Março 2016.

SULLIVAN, Nick (2013). **A (relatively easy to understand) primer on elliptic curve cryptography**. Arstechnica. 2013. Disponível em: <http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/> Acesso em: 25 Abril 2016.

SYMANTEC (s. d.). **Cryptolocker Q&A: Menace of the Year**. Symantec. Disponível em: <http://www.symantec.com/connect/blogs/cryptolocker-qa-menace-year>. Acesso em: 31 Março 2016.

SYMANTEC (2015). **Trojan.Cryptowall**. Symatex. 2015. Disponível em: <https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99> Acesso em: 05 Março 2016.

SYMANTECH (s. d.). **Web Attack: Angler Exploit Kit Website 15**. Symantech. Disponível em: <https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=28005> Acesso em: 03 maio 2016.

TALOS (2016). **RANSOMWARE: PAST, PRESENT, AND FUTURE**. Talos. 2016. Disponível em: <http://blog.talosintel.com/2016/04/ransomware.html#toc> Acesso em: 11 Maio 2016.

XIAO, Claud e CHEN, Jin (2016). **New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer**. Paloalto Network. 2016. Disponível em: <http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/> Acesso em: 21 Abril 2016.

YANG, Tianda et al (2015). Automated Detection and Analysis for Android Ransomware. **2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS),** e **2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS),** Agosto, 2015. pp. 1338 – 1343.

YOUNG, A.; M. YUNG (1996). Cryptovirology: extortion-based security threats and countermeasures. **IEEE Symposium on Security and Privacy. pp. 129–140. doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2**.

ZENZERO (s. d.). **Cryptolocker (Ransomware) – What is it? What are the risks? What can I do?**. Zenzero. Disponível em: <http://www.zenzero.co.uk/cryptolocker-ransomware/>. Acesso em: 31 Março 2016.