Danielle Cristiny Gonçalves Pereira
Isabela de Almeida e Lima

# RANSOMWARE E SUAS RELAÇÕES COM A CRIPTOGRAFIA

Paracatu-MG
Agosto 2017

Danielle Cristiny Gonçalves Pereira
Isabela de Almeida e Lima

# RANSOMWARE E SUAS RELAÇÕES COM A CRIPTOGRAFIA

Instituto Federal Triângulo Mineiro

Orientador: Claiton Luis Soares

Paracatu-MG
Agosto 2017

# Sumário

# 1 Introdução

O primeiro *Ransomware* surgiu em 1989 por Joseph L. Popp. O trojan, era conhecido como AIDS, que enganava usuários e tentava extorquir dinheiro das vítimas. Ao criptografar o disco rígido criminosos pediam dinheiro para *descriptografar* os dados. Na década de 80 não havia nenhuma segurança computacional e a internet era utilizada por poucas pessoas como, por exemplo, especialistas em ciência e tecnologia, por isso, os ataques não eram tão bem- sucedidos como nos dias atuais. (AFRIKATEC, 2017a)

A tecnologia utilizada não era muito evoluída, apresentando falhas e, assim, facilitando alguns especialistas de analisar o código do *malware* e rastrear os *cibercriminosos*. A criptografia utilizada era simétrica que consiste em utilizar uma mesma chave para criptografar e *descriptografar* dados. Depois de alguns anos, o *Ransomware* passou a utilizar uma criptografia assimétrica que possui duas chaves diferentes, uma para criptografar e outra para *descriptografar* os arquivos, assim, dificultando rastrear os criminosos.(AFRIKATEC, 2017c)

O criador do *Ransomware* Joseph L. Popp, era um biólogo evolutivo com um doutorado em Harvard. Ele era bastante conhecido, pois, criou um observatório de borboletas epónimo junto a sua filha no estado de Nova York. Utilizava o recurso computacional, era um cientista e pesquisador. Dessa maneira, se interessou pela tecnologia e então criou o *Ransomware*, porém até nos dias de hoje não se sabe ao certo porque Popp liberou seu código malévolo.(SIMONE, 2017)

O primeiro estilo moderno de *Ransomware* surgiu por volta de 2005, conhecido como *Trojan Gpcoder*. Outro *malware* apareceu em 2011, o *Trojan Winlock*, ele era uma forma mais evoluída, pois, em vez de criptografar os arquivos exibia um aviso falso de ativação do produto Windows que só poderia ser removido caso o usuário digitasse uma chave de ativação, para conseguir essa chave a vítima deveria ligar para um número internacional. Também no ano de 2011, surgiu um novo *Ransomware*, conhecido como "O Police", ele bloqueava o acesso ao teclado e ao mouse e usava imagens que declarava que o usuário havia cometido um crime e deveria pagar uma multa para recuperar o acesso ao computador.

Com esses novos ataques que vinham se infiltrando constantemente em meio computacional como forma estratégica de obter dinheiro de uma forma rápida e pratica surgiram o termo *hacker* e *cracker*. O termo *hacker* foi criado, pois, representa uma pessoa que possui uma grande facilidade e capacidade em desenvolver quaisquer atividades em um computador. Dessa maneira, também surgiu o termo *crackers* que consiste em indivíduos que obtém conhecimento computacional e utiliza isso para obter vantagens. Assim, por trás de um ataque desse *malware* sempre há um *cracker*.(INACARATO, 2017)

O *Ransomware* é considerado um grande problema em relação a segurança da informática e nos últimos anos vem se manifestando em maior escala nas redes, pelo fato da tecnologia está avançando e consequentemente aumentando o número de usuários da internet e também utilizando o recurso computacional para arquivar documentos pessoais, tais como arquivos de fotos, vídeos, planilhas, texto e etc, a partir disso que os *crackers* se aproveitam para criptografar arquivos valiosos e pedirem algo em troca.

Atualmente há dois tipos de *Ransomware* o *crypto* (codificador) e o *locker* (bloqueador) e dentre esses *Ransomwares* pode-se citar alguns ataques que estão ocorrendo diante a sociedade nos dias de hoje como, por exemplo, *WhannaCry*,*Petya* e *BadRabbit*.

## 1.1 Objetivos

### 1.1.1 Objetivo Geral

Informar o que é *Ransomware* e suas respectivas formas de ataques. mostrando a maneira abrangente que está vinculada na Web, e também diversas formas de proteções contra tais fatos.

### 1.1.2 Objetivos Específicos

Nesse trabalho espera-se alcançar os seguintes objetivos:

- Relatar o uso maléfico da criptografia;
- Apontar usuários mal-intencionados;
- Mostrar as vulnerabilidades da rede e exposição a ataques;
- Apresentar um exemplo de código de criptografia e descriptografia;
- Recomendar métodos de segurança;
- Informar sobre ataques com potências diversificados.

## 1.2 Justificativa

Nesse âmbito, ao pesquisar sobre *Ransomware*, pode-se observar que há uma necessidade de proteger arquivos por causa de grandes ataques em massa que estão ocorrendo no mundo. Algoritmos de alta qualidade estão cada vez mais dificeis de serem descodificados. Por esse fato o tema foi escolhido para descrever sobre o mesmo e alertar individuos a se protegerem .

## 1.3 Metodologia

Esse trabalho será realizado através de uma pesquisa exploratória para obter informações sobre os ataques *Ransomware* e causa danos na sociedade, exemplo disso seria, o *Wanna decryptor* ( *Ransomware* que explora a maioria das vezes, vulnerabilidades do sistema operacional Windows) . Por meio dessas informações obtidas nas pesquisar será mostrado as vulnerabilidades do Windows. Nesse trabalho também será apresentado um código de criptografia e descriptografia para mostrar o quanto é complexo e dimensão do problema, que esse ataque causa atualmente nas redes.

# 2 Desenvolvimento

## 2.1 CRIPTOGRAFIA E SUAS RELAÇÕES COM *RANSOMWARE*

Com o avanço tecnológico, a necessidade de proteger arquivos e dados tornou-se uma necessidade. Empresas que utilizam serviços onlines se preocuparam com esse fato, pois ao perder seus respectivos arquivos os danos e prejuízos seriam drásticos. Com isso, foi criado a criptografia que tem origem de uma palavra grega, cujo seu significado é "escrita escondida". A criptografia foi utilizada antigamente pelos egípcios, romanos e gregos para que suas mensagens não fossem invadidas e lidas por inimigos.

Atualmente, a criptografia é utilizada para ocultar informações transmitidas e que podem ser transformadas apenas com sua chave original. Caso outros usuários tenham acesso a essas mensagens, elas ficaram impossíveis de serem identificadas. Apenas quem obtém a chave do código que poderá ter acesso aos dados.

Ademais, existem dois tipos de criptografias: simétrica e assimétrica. Quando o emissor e receptor possuem acesso a mesma chave e traduz os arquivos ela se denomina simétrica como, por exemplo, envio de e-mails. Exemplo de criptografia Simétrica:

- DES (*Data Encryption Standard*): Criado em 1977 pela IBM, é considerado inseguro devido a suas chaves de 56-bits (permite até 72 quatrilhões de combinações). Foi quebrado utilizando o método de "força bruta" (tentativa e erro);(SCHUNCKE, 2012)

- RC (*Ron's Code ou Rivest Cipher*): Existem diferentes versões do algoritmo, como a RC4, RC5 e RC6, todas criadas por Ron Rivest na empresa RSA Data Security. Muito utilizado em e-mails, usa chaves de 8 a 1024 bits. (SCHUNCKE, 2012)

Já a assimétrica utiliza-se uma chave pública e outra privada. A chave privada é a única capaz de traduzir a informação, assim, o receptor pode traduzir o que qualquer um pode codificar. Um exemplo disso é o método que é utilizado às senhas de cartão de crédito.

- *El Gamal*: Criado pelo estudioso de criptografia egípcio Taher Elgamal em 1984. Utiliza o problema "logaritmo discreto" para segurança.(SCHUNCKE, 2012)

- RSA (*Rivest, Shamir and Adleman*): Criado por três professores do MIT, é um dos algoritmos mais usados e bem-sucedidos. Utiliza dois números primos multiplicados para se obter um terceiro valor. A chave privada são os números multiplicados e a chave pública é o valor obtido. Utilizada em sites de compra e em mensagens de e-mail. (SCHUNCKE, 2012)

Portanto há indivíduos que utilizam a criptografia para bloquear o acesso de usuários aos seus arquivos. Assim, houve a relação da criptografia com o *Ransomware* que é um software malicioso usado para criptografar arquivos e assim extorquir dinheiro das vítimas. Caso não haja o pagamento do resgate, os arquivos não serão descriptografados e mesmo que haja não é garantido que os arquivos sejam devolvidos. A forma mais eficaz de recuperar os arquivos é efetuando o pagamento ou, buscá-los em um *Backup* e certificar que o *Ransomware* foi removido do computador.

## 2.2 *RANSOMWARE*

O *Ransomware* é um *malware* que obtêm vários tipos de ataques com seus potenciais diversificados como, por exemplo, ataques de fraudes eletrônicas, roubo de dados de cartão de crédito, venda de dados pessoais, envio de *phishing* para e-mails corporativos, entre outros. Através desses ataques o *crypto-ransomware* solicita pagamento utilizando uma moeda virtual (*Bitcoin*) das vítimas em troca de seus dados criptografados. De acordo com Fernando Ulrich:

> "O *Bitcoin* é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro."(ULRICH, 1892)

Nos últimos tempos o *Ransomware* vem praticando diversos ataques, e um dos maiores que se já teve foi o ataque em escala global, atingindo cerca de 74 países. Entre eles, os que mais causaram impacto nas sociedades foram contra as empresas de telefonia nos países do Reino Unido, Espanha, Rússia e Taiwan.

O *Ransomware* que está causando essa polêmica no mundo todo é uma variação do *WannaCry*, também conhecido por *WCry* ou ainda *WannaCrypt0r Ransomware* .

A Microsoft confirmou que o *WannaCrypt* tem origem em armas cibernéticas da NSA (Agência de Segurança Nacional, dos Estados Unidos), que teriam sido roubadas por *hackers* no início deste ano. ( Alves, 2017)

A sua funcionalidade é a mesma dos outros: pedir o resgate dos arquivos encriptografados, porém, ele conseguiu esse alto nível de infecção de computadores por causa de sua forma de duplicação e propagação parecido com qualquer vírus to tipo "Worm". As extensões dos arquivos infectados são: doc,. dot, .tiff, .java,. psd, .docx, .xls, .pps, .txt, .mpeg, entre outros.

A maioria das vítimas dos ataques de *Ransomware* são usuários do *Windows*, pois existem muitas vulnerabilidades nesse sistema operacional. Os meios mais viáveis para se defender desse fato é ficar atento a e-mails de pessoas desconhecidas e passar a utilizar Linux por ser mais confiável. Segundo a Microsoft as versões mais afetadas são: Microsoft *Windows Vista* SP2, *Windows Server* 2008 SP2 and R2 SP1, *Windows* 7, *Windows* 8.1, *Windows* RT 8.1, *Windows Server* 20ww and R2, *Windows* 10, *Windows Server* 2016.

### 2.2.1 TIPOS DE *RANSOMWARE*

1. *Ransomware Reveton*

   Foi descoberto em 2012 quando começou a se espalhar. Um sistema operacional quando é infectado por esse vírus, aparece um aviso na tela mostrando que o computador está sendo utilizado para download de atividades ilegais, com a intenção de aparentar com a realidade, aprensenta o IP do computador e a imagem do webcan . E para obter os seus dados novamente é preciso pagar uma multa.

2. *Ransomware CryptoLocker*

   Esse *Ransomware* reapareceu em setembro de 2013, como um trojan chamado *CryptoLocker* e a mensagem avisava que caso não houvesse um pagamento dentro de 3 dias a chave privada seria excluída.

3. *Ransomware CryptoLocker.F e TorrentLocker*

   Esse *Ransomware* surgiu em 2014, seu ataque era feito por meio de e-mails fraudulentos com mensagens sobre falhas de encomenda. Os primeiros ataques que ocorrem foram nomeados de *CryptoWall* e *CryptoLocker*. Outro trojan também criado nessa época foi o *Ransomware torrente locker* que também

usava a mesma *keystrean* para os computadores infectados, assim tornando mais difícil da criptografia ser quebrada. Ao final do mesmo ano foram aproximadamente 9.000(nove mil) usuários foram vítimas desse golpe.

4. *Ransomware Cryptowall – Help Decrypt*

   Esse *Ransomware* também surgiu em 2014 e foi espalhando como parte de uma maliciosa campanha de publicidade, assim tendo vários sites como alvos, os anúncios que apareciam eram redirecionados para sites fraudulentos que usavam módulos de extensão para o navegador baixar dados. A versão mais recente que está em meio a rede é, o *CryptoWall* 4.0, ele reforçou seu código para evitar a detecção pelo antivírus e não criptografa mais só dados, mas também os nomes dos arquivos.

5. *Ransomware KeRanger*

   Em 2016 foi descoberto o *KeRanger* o primeiro *Ransomware* desenvolvido para afetar o sistema operacional da Apple, iOS. Para ser infectado há uma executável com a extensão .DMG que é disfarçado com arquivo Rich Text, o vírus fica parado sem se executar durante um tempo, mas depois começa a criptografas os arquivos.

6. *Ransomware Manamecrypt – CryptoHost*

   Esse vírus na realidade não criptografa arquivos e sim os copia para uma pasta no disco local (C:) que é protegida por senha utilizando arquivos.rar., o mesmo terá um nome de 41 caracteres e sem extensão.

## 2.3 PREFERÊNCIA A ARQUIVOS VALIOSOS

Os criminosos na maioria das vezes buscam atacar empresas e locais em que os arquivos têm extrema importância, assim, podendo pedir uma quantia bastante generosa, em vez de fazer ataques mais comuns e receber menores quantias em dinheiro.

Os cibercriminosos antes de realizarem seus ataques estudam os seus públicos alvos e procuraram as vulnerabilidades onde seus negócios poderiam dar certo, pode-se citar como, exemplo, disso o ataque *WannaCry*, os *Hackers* procuraram falhas em sistemas operacionais e quando encontraram uma falha no sistema Windows começaram a propagar os seus vírus em meio a rede. OS alvos mais procurados são:

- Domésticos: pelo fato de estarem mais expostos, por não conhecerem métodos de segurança; assim facilitando a infecção dos vírus e por terem muitos arquivos sem *backup* e por isso o valor para resgate é mais garantido.(AFRIKATEC, 2017b)

- Empresas: usualmente os servidores ligam-se aos outros computadores da rede para o bom funcionamento e rendimento, isso facilita para que somente um servidor seja infectado e assim comprometendo todo o andamento da mesma, com isso é preciso que faça o pagamento para que não haja muito prejuízo com a perda dos dados. As consequências causadas não se resumem apenas no valor a ser pago para resgatar arquivos e documentos criptografados. Não há garantias de recuperação dos arquivos mesmo efetuando o pagamento. Isso acarreta problemas nos estabelecimentos como, por exemplo, perda de informações importantes, paralisação da empresa, perda de credibilidade, prejuízos financeiros entre outros. Nesse caso a quantia exigida não é baixa quanto a dos usuários domésticos (US300), e sim um valor mais alto (dezenas de milhões de dólares) pelo fato de todo o rendimento da empresa depender dos arquivos criptografados.(AFRIKATEC, 2017b)

- Dispositivos móveis: nestes os números de ataques não são em grande massa, pois, a quantia pedida é um valor significantemente baixo. Dessa maneira, os criminosos estão tentando aprimorar as criptografias para fazerem ataques mais rigorosos. Dos poucos ataques efetuados em dispositivos móveis a grande maioria são voltados para o sistema operacional Android que corresponde à 80% dos mesmos, pelo fato da grande maioria da população utilizar esse modelo os restantes são voltados para os sistemas IOS e Windows phone.(AFRIKATEC, 2017b)

## 2.4 RECOMENDAÇÕES DE SEGURANÇA

Especialistas de Segurança da Informação estão recomendando no mercado, controles que contribuirão para prevenir, detectar os impactos no caso da concretização de um incidente de *Ransomware* nas empresas como, por exemplo, atualização de *Patches*, Ferramenta de *Antispam*, Cópias de Segurança (backups), Gestão do software de Antivírus, entre outros.

## 2.5 CASOS DE ATAQUES *RANSOMWARE*

### 2.5.1 ATAQUE EMPRESA AGROXVEN

Um fato que se mostra exemplo de ataque *Ransomware* é, conforme Morocho e Mosquera (2016), o da empresa chamada Agroxven, uma empresa que está relacionada seleção e exportação de produtos agrícolas. Em agosto de 2016 os funcionários da empresa tentaram acessar o servidor da empresa, e observaram que os mesmos estavam bloqueados, então deduziram que havia uma falha no sistema. No próximo dia de trabalho o mesmo problema estava acontecendo e resolveram comunicar com a Onsystec – empresa que fornece soluções para seus clientes, é um sistema de computador de negócios que gerencia funções de integração e gestão de negócios – após observar o que estava acontecendo, concluíram que todos os bancos de dados haviam sido presos. Os engenheiros de suportes viram que o caso da Agroxven apresentava um grau de complexidade, pois os vírus costumam criar arquivos não mais que 2K, porém os da empresa mantiveram seu peso original, mostrando que não foram criados por vírus para enganar usuários e sim um malware que tinha aplicando um algoritmo de criptografia para mudar os nomes e as extensões, mas mantendo seus reais conteúdos. O que realmente havia acontecido, era que o banco de dados do servidor com sistema operacional *Windows Server* tinha sido infectado por um *Ransomware*

### 2.5.2 *WANNA CRY*

Em 12 de maio de 2017 houve novamente outro ataque *Ransomware*em massa, onde atingiu mais de 70 países atacando várias empresas e instituições.

Segundo a *Kaspersky Lab*, foram registrados mais de 45 mil ataques em 74 países, incluindo o Brasil. (ALVES, 2017)

O *WannaCry* por sua vez é mais potente, além de infectar uma máquina e criptografar os arquivos ele também faz a distribuição do *malware* pela rede, assim, fazendo com que todos os computadores vulneráveis que esteja conectado a ela sejam infectados. *WannaCry* colocou boa parte do mundo em um enorme caos, ele afetou a Europa logo no começo do dia. Já no Brasil foi paralisado grandes órgãos como, por exemplo, o Ministério Público do Estado de São Paulo (MPSP), Instituto Nacional do Seguro Social (INSS), TJPS, entre outros.

Agentes do FBI se fizeram como vítimas do *Ransomware* para apenas pagar o resgate de seus arquivos e conseguir acesso aos criminosos. A criptografia usada por esses indivíduos são tão boas que esses agentes, aconselha em alguns casos que as vítimas paguem pelo resgate. O FBI alerta as pessoas a manter o antivírus sempre ativo e atualizado, fazer *backups* e manter um deles *offline*, ficar atentos a e-mails desconhecidos e corrigir falhas de segurança nos computadores, assim, prevenindo futuros ataques.

# 3 Conclusão

O uso maléfico da criptografia se tornou um tipo de negócio vantajoso para os *cibercriminosos*. Com o surgimento de algoritmos de criptografia de alta complexidade é praticamente impossível descriptografar e recuperar alguns arquivos. Por esse fato, empresas precisam estar preparadas para que não sejam vítimas desses ataques.

Investir em Segurança é fundamental para que não ocorra invasões e perda de dados importantes. E um dos maiores problemas de invasões são por causa de sistemas operacionais vulneráveis. Devido a muitas invasões, a Microsoft desenvolveu o *Windows Defender* Antivírus para amenizar os ataques, assim, os usuários podem ter um acesso com mais segurança e evitar perda de dados.

Ademais, uma solução mais radical para tal problema seria optar pelo sistema operacional Linux, que obtém um nível de segurança computacional de excelência. Além de ser fácil de encontrar para download, e é gratuito. (BURNETT; PAINE, 2002)

# 4 Cronograma

Tabela 1 – Cronograma

| **ATIVIDADES** | **MAI** | **JUN** | **JUL** | **AGO** | **SET** | **OUT** | **NOV** |
|---|---|---|---|---|---|---|---|
| Períodos/Atividades | | | | | | | |
| Definição de Objetivos e Justificativa | | | | | | | |
| Levantamento Bibliográfico | | | | | | | |
| Apresentação e discussão de dados com orientador | | | | | | | |
| Definição da pré estrutura do trabalho | | | | | | | |
| Elaboração do relatório | | | | | | | |
| Apresentação do projeto para a banca | | | | | | | |
| Correção do relatório | | | | | | | |
| Procura de código na literatura de criptografia e descriptografia | | | | | | | |
| Procura de mais dados na literatura sobre ransomware | | | | | | | |
| Elaboração do trabalho | | | | | | | |
| Entrega do Trabalho | | | | | | | |

# Referências


AFRIKATEC. *Série – A Evolução do Ransomware – Parte 2 – A origem*. 2017. ⟨http://www.afrikatec.com.br/serie-a-evolucao-do-ransomware-parte-2-a-origem/⟩. [Online; acessado em: 14-nov-2017].

AFRIKATEC. *Série – A Evolução do Ransomware – Parte 3 – Os alvos*. 2017. ⟨http://www.afrikatec.com.br/serie-a-evolucao-do-ransomware-parte-3-os-alvos/⟩. [Online; acessado em: 15-nov-2017].

AFRIKATEC. *Série – A Evolução do Ransomware – Parte 9 – Conclusão*. 2017. ⟨http://www.afrikatec.com.br/serie-evolucao-do-ransomware-parte-9-conclusao/⟩. [Online; acessado em: 15-nov-2017].

ALVES, P. *Herói acidental? Quem 'parou' o ataque do ransomware WannaCrypt*. 2017. ⟨https://www.techtudo.com.br/noticias/2017/05/heroi-acidental-quem-parou-o-ataque-do-ransomware-wannacrypt.ghtml⟩. [Online; acessado em: 19-set-2017].

BURNETT, S.; PAINE, S. *Criptografia e segurança: o guia oficial RSA*. [S.l.]: Gulf Professional Publishing, 2002.

INACARATO. *Hackers, Crackers e nova modalidade de crime virtual – Ransomware, e a Responsabilidade nos Crimes Eletrônicos (Parte 3)*. 2017. ⟨http://inacarato.com.br/site/lang/en-us/hackers-crackers-e-nova-modalidade-de-crime-virtual-ransomware-e-a-responsabilidade-nos-crimes-eletronicos-parte-3/⟩. [Online; acessado em: 15-nov-2017].

MOROCHO, R. A. R.; MOSQUERA, E. G. Infección con ransomware en el servidor de base de datos del sistema onsystec erp. *3C Tecnologia*, 3ciencias, v. 5, n. 4, p. 56, 2016.

SCHUNCKE, A. *Quais os principais tipos de criptografia?* 2012. ⟨https://www.oficinadanet.com.br/post/9424-quais-os-principais-tipos-de-criptografia⟩. [Online; acessado em: 21-set-2017].

SIMONE, A. *The Strange History of Ransomware*. 2017. ⟨https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b⟩. [Online; acessado em: 15-nov-2017].

ULRICH, F. Bitcoin-a moeda na era digital. *Journal, volume*, v. 2, p. 239, 1892.