Submetido em 09.06.2017. Aprovado em 10.11.2017

RANSOMWARE: ESTE PROBLEMA TAMBÉM PODE SER SEU

Cauê Zaghetto,
Luiz Henrique Morais Aguiar,
Bruno Souza Lobo
Almeida Gabriel Freitas dos Santos

Abstract

Due to the world increasingly connected through interconnection networks and the internet, ensuring the security of the computing elements that make up these networks has become a challenge. Among the various types of digital attacks that exist, we highlight malware. Malware is malicious code that exploits user vulnerabilities for the purpose of controlling and manipulating the attacked computer. Currently, a special type of malware, called ransomware, has been gaining notoriety. Ransomware is a malicious code that has the purpose of hijacking user data and then requesting a redemption value for that data. This article presents a detailed explanation of how the ransomware came to be and how it works, as well as a detailed study of how to protect against this type of attack, and finally, what measures to take in case of infection.

Key words: *ransomware*, *malware*, *security*.

Resumo

Com o mundo cada vez mais conectado através das redes de interconexão e da internet, garantir a segurança dos elementos computacionais que compõem essas redes vem se tornando um desafio. Dentre os diversos tipos de ataques digitais existentes, destacam- se os *malwares*. *Malwares* são códigos maliciosos que exploram vulnerabilidades dos usuários com a finalidade de controlar e manipular o computador atacado. Atualmente, um tipo especial de *malware*, o chamado *ransomware*, vem ganhando notoriedade. O *ransomware* é um código malicioso que tem a finalidade de sequestrar os dados do usuário e, posteriormente, solicitar um valor de resgate por esses dados. Esse artigo apresenta uma explicação detalhada de como surgiram e como agem os *ransomware* além de apresentar um estudo minucioso de como se proteger deste tipo de ataque e, finalmente, aborda medidas

Submetido em 09.06.2017. Aprovado em 10.11.2017

a serem tomadas em caso de ser infecção.

Palavras-chave: *ransomware*, *malware*, *segurança*.

1 Introdução

Imagine que ao chegar à porta de sua casa e tentar abri-la perceba que sua chave não encaixa na fechadura. Por incrível que pareça, o problema não é a chave, mas a fechadura. Ela foi trocada! Como arrombar a porta não parece uma boa solução, você precisa da nova chave e apenas uma pessoa a tem: aquele que trocou a fechadura.

O exemplo acima é uma analogia para que se possa entender melhor o conceito de *ransomware*, que é um termo geral usado para descrever uma classe de *malwares*[1] utilizados para extorquir digitalmente vítimas, obrigando-as a realizar o pagamento de taxas (LISKA; GALLO, 2016). Em outras palavras, podemos definir *ransomware* como um *malware* que sequestra os arquivos de um computador e cobra resgate para devolvê-los.

É importante que se tenha em mente que existem basicamente duas principais formas de extorsão digital. Essas duas formas de *ransomware* são: aquelas que criptografam e negam acesso a determinados arquivos ou conjunto de arquivos; e aquelas que restringem o acesso (bloqueiam) ao sistema operacional (SO) em si. Essas ameaças não estão limitadas à posição geográfica (todos países são alvos em potencial) ou a determinados sistemas operacionais (LISKA; GALLO, 2016). Em verdade, desde dispositivos móveis baseados em *Android* ou *iOS* a *desktops* baseados em *Windows*, *Linux* ou MAC OS, todos estão sujeitos a ameaças em potencial e correm risco de atentados do tipo *ransomware*. A Figura 1 apresenta a tela de um computador infectado por *ransomware*.

Figura 1 – Exemplo de atuação de *Ransomware* que aplicou o algoritmo de criptografia AES-256 nos arquivos de um computador (SECURITY, 2016).

Mas como isso acontece? Como nossos dados são sequestrados? Como podemos nos proteger? Esse artigo convida o leitor a descobrir as respostas para estas e outras perguntas.

1.1 HISTÓRIA DO *RANSOMWARE*

Por mais estranho que possa parecer o *ransomware* não é um problema que surgiu nos últimos 2 anos, ele apenas ganhou notoriedade neste período. O primeiro *malware* deste tipo foi escrito em 1989 e se chamava AIDS[2] *trojan* (GIRI; JYOTI; AVERT, 2006). Esse *malware* substituía o arquivo AUTOEXEC.BAT[3] por uma versão maliciosa de tal maneira que todos os arquivos e diretórios do computador desapareciam, ficavam escondidos. Apesar de se apresentar como um código malicioso que criptografava todos os arquivos do PC (*Personal Computer*), descobriu-se posteriormente que apenas o nome dos arquivos era alterado utilizando criptografia de chave simétrica simples (LISKA; GALLO, 2016; MAO, 2003). Em pouco tempo duas soluções definitivas chamadas AIDSOUT e CLEARAID foram desenvolvidas e o AIDS *trojan* foi superado. Detalhes acerca do AIDS *trojan* e das soluções encontradas podem ser encontrados na literatura (BATES, 1990).

---

1 Abreviatura utilizada como sinônimo de *malicious software*

2 Termo em alusão à Síndrome da Imunodeficiência Adquirida.

3 Abreviatura de *Automatic Execution*, arquivo que roda automaticamente ao se inicializar o SO.

Uma informação interessante, que dado o rápido desenvolvimento da tecnologia pode passar desapercebida pelo leitor, é a de que como à época não havia internet pública, o *malware* era espalhado via *Floppy Disc* e o pagamento era realizado via envio de dinheiro por correio para o Panamá.

Desde então, centenas de versões diferentes deste *malware* foram criadas (SE- CURITY, 2012), cada uma com a sua peculiaridade, mas todos com o mesmo objetivo, extorquir dinheiro do usuário. O problema é que com a difusão da internet e com a criação das chamadas moedas digitais, como por exemplo o Bitcoin (NAKAMOTO, 2008), os ataques cibernéticos começaram a tomar enormes proporções, pois agora o pagamento havia se tornado não-rastreável, criando assim uma onda de massificação do *ransomware* como mostra o infográfico histórico apresentado na Figura 2.

Submetido em 09.06.2017. Aprovado em 10.11.2017

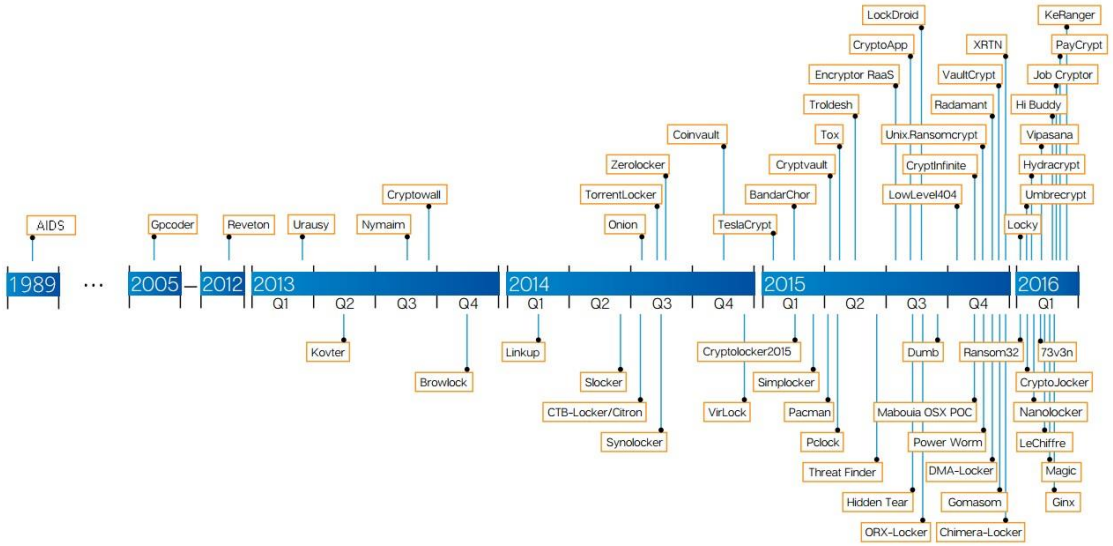

Figura 2 – Histórico do *Ransomware* (SECURITY, 2016).

Com essa criação e distribuição em massa de novos *ransomwares*, ficou evidente que os sistemas atuais estão altamente vulneráveis e, na maioria das vezes, isso ocorre ou pode ocorrer pela falta de conhecimento das pessoas/usuários que utilizam o "mundo digital".

Fazendo uma analogia rápida e simples, considere o fato de que hoje há no Brasil 56,9 milhões de veículos e 60,7 milhões de motoristas (GLOBO, 2014). Imagine agora que esses motorista não sabem muito bem diferenciar o acelerador do freio, ou que não sabem olhar o velocímetro e reconhecer a que velocidade o veículo se encontra. Sem dúvida, dada a enorme quantidade de veículos circulando, esse desconhecimento/inabilidade dos usuários (motoristas) iria gerar um **caos e uma série de riscos e acidentes**.

Neste sentido, não há dúvida de que é necessário preparar-se para dirigir um veículo. Já no que diz respeito a imersão digital, essa postura não é compartilhada. É comum usuários que conhecem apenas rasamente os softwares que estão usando, sentirem-se seguros e protegidos. Certamente isso gera, de maneira análoga, **"caos e uma série de riscos e acidentes"**. O grande problema é que, aproveitando-se dessa inabilidade e despreparo dos usuários, estelionatários digitais fazem uso de diversas ferramentas e métodos (*e.g.*: *ransomware*, *malware*, *vírus*) para extorquir as pessoas.

1.2 COMO FUNCIONA O SEQUESTRO DOS DADOS

Agora que os conceitos básicos acerca dos chamados *ransomwares* já foram apre- sentados e que as lições do passado foram aprendidas, é momento de explicar como os ataques são realizados. A Figura 3 apresenta a "anatomia" de um

ataque *ransomware*.

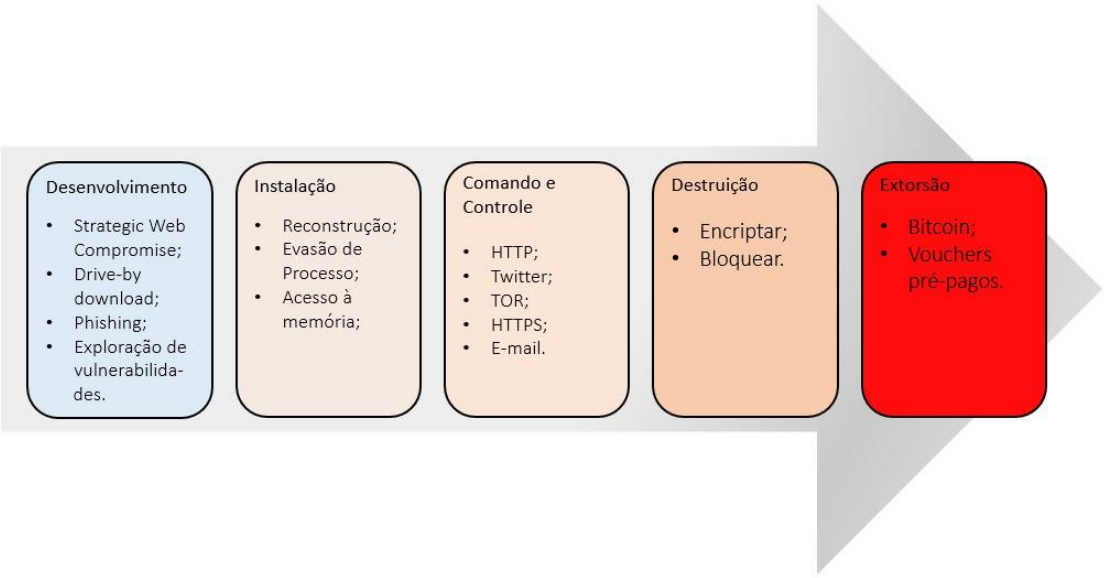

Figura 3 – Anatomia, passo a passo, de um ataque de *ransomware* (LISKA; GALLO, 2016).

Como já mencionado, uma vez instalado o *malware*, este poderá criptografar (ou encriptar) os arquivos mais importantes como, por exemplo, documentos PDF ou documentos de escritório como do Word e Excel ou até mesmo todo o sistema operacional.

Para efeito de esclarecimento e entendimento, vale destacar que criptografar ou encriptar é o processo de codificar mensagens ou informação de tal forma que apenas pessoas "autorizadas" tenham acesso (DIFFIE; HELLMAN, 1979). Neste processo uma "chave" é gerada de tal maneira que apenas aqueles que conhecem essa chave podem decodificar a informação previamente criptografada.

O processo de criptografar uma informação é relativamente antigo. Uma das formas de criptografia mais conhecidas da antiguidade é a cifra de César[4], que consistia em criar uma tabela de conversão de caracteres na qual está definido, por exemplo, que toda vez que a letra "a" for utilizada essa deve ser substituída pela letra "b" e assim por diante. Desta forma, a seguinte frase: "Este é um exemplo simples de mensagem" seria escrita como: "Ftuf f vn fyfnqmp tjnqmft ef nfotbhfn". Fica aqui uma pequena tarefa para o leitor: seguindo a mesma lógica, o que significa "QBSBCFOT WPDF BDFSUPV"?

A criptografia é usada para esconder[5] o conteúdo de uma mensagem e é comumente usada em nosso cotidiano. Hoje existem técnicas extremamente modernas e algumas delas são, até o momento, impossíveis de se quebrar (ASSOCIATIONS, 2000). No caso dos *ransomwares*, a chave necessária para decodificar os documentos cifrados fica em posse do criminoso e o valor pago pelo

resgate é para que se tenha acesso a ela e, dessa maneira, “recupere-se as informações”.

Voltando à Figura 3, é possível perceber que o ataque ocorre em cinco fases: desenvolvimento, instalação, comando e controle, destruição e extorsão. A seguir, cada uma dessas fases é explicada brevemente.

1.2.1 Desenvolvimento

Esta é a primeira fase do ataque *ransomware*. Aqui os alvos são escolhidos a partir de alguns métodos e técnicas que exploram, em geral, vulnerabilidades dos sistemas e inabilidades/fragilidades dos usuários. As quatro principais formas de ataque são:

---

4 Júlio César, foi um patrício, líder militar, político e ditador.

5 É importante tomar cuidado com esse termo. Na maior parte das vezes usa-se criptografia para proteger a informação e, por isso, o ato de esconder é benéfico.

1. ***Strategic web compromise*** - Apesar de não possuir uma tradução adequada para português, ocorre quando usuários entram em *sites* "contaminados" que fazem constantemente um levantamento de usuários e suas fragilidades a fim de escolher os alvos em potencial. Em geral, usuários que, realizam transações de pagamento de maneira desprotegida, não atualizam frequentemente o sistema operacional e não possuem antivírus adequado/atualizado, são mapeadas por estes sites como alvos;
2. ***Drive-by Download*** - Ocorre quando o sistema faz automaticamente *download* de pedaços de códigos maliciosos ou spywares[6] sem que o usuário tome conhecimento;
3. ***Phishing emails*** - São usados para capturar informações dos usuários, direcioná-los para sites maliciosos ou injetar *malwares* em suas máquinas. Podem ser de distribuição em massa ou especialmente desenvolvidos para uma certa empresa ou indivíduo.
4. ***Exploração de Vulnerabilidades*** - Os ataques exploram vulnerabilidades internas da rede de computadores com intuito de atacar uma determinada empresa.

Para cada um dos tipos de ataques descritos acima existem formas de se defender. Vale ressaltar que, de maneira geral, os três primeiros tipos (mais usados) exploram fragilidades do usuário final, pois notoriamente requerem algum tipo de interação com o mesmo, mas o último é um ataque contra uma certa organização ou empresa e para defender-se faz-se necessário o uso de métodos institucionais.

1.2.2 Instalação

Uma vez que um código malicioso foi "entregue" ao sistema da vítima, inicia-se a infecção, e isso independe do sistema operacional específico que está sofrendo o ataque. Normalmente, num primeiro momento, um pequeno código é injetado no SO a fim de evitar detecção. Esse código passa a se comunicar com os chamados Canais de Controle e Comando (*command-and-control channels*) do extorsionista (LISKA; GALLO, 2016). A partir desse momento, com o auxílio deste pequeno código malicioso, o criminoso realiza a chamada **Reconstrução**, que se baseia em, de maneira imperceptível, inserir completamente o *ransomware* no sistema já comprometido. A partir deste momento o invasor começa a tomar o controle do sistema.

Para dificultar o contra-ataque, o *ransomware* se divide em uma grande quantidade de *scripts* processos, *batch files* e outras ferramentas, evitando a detecção por parte do SO e dos antivírus (LISKA; GALLO, 2016). Essa técnica é conhecida como **Evasão de Processo** (*Evasion Process*).

Uma vez que o *ransomware* está devidamente instalado e distribuído no SO, inicia-se o primeiro estágio que trata de avaliar se vale a pena infectar

definitivamente o computador.

Em caso afirmativo, o criminoso normalmente gera um código de *hash MD5* (RIVEST, 1992) tomando como base o *MAC address* ou o nome da máquina, com intuito de possuir um identificar único para aquele computador. Dessa maneira, o extorsionista sempre sabe qual máquina está vulnerável e pode sofrer ataques.

Finalmente, o *ransomware* se estabelece como um processo legítimo (idêntico à um processo não-malicioso) dentro do SO, toma conta da memória (**Acesso à Memória**) e do escalonamento de processos[7] e a fase de *command-and-control* se inicia.

1.2.3 Comando e Controle

A todo momento se faz necessária uma forma de controlar e dar comandos ao computador infectado. Para que o *ransomware* funcione da maneira prevista é necessário

---

6 Spyware consiste em um programa automático de computador que recolhe informações sobre o usuário.

que se estabeleça um canal de comunicação com o extorsionista de tal forma que este possa, quando julgar oportuno, enviar comandos para o computador vulnerável. Em verdade, é possível que neste momento seu computador tenha um pedaço de código malicioso "adormecido" apenas aguardando o comando de seu "senhor". Aqui devemos destacar que boa parte dessa comunicação se dá através de ***TOR - hidden service***[8], protocolos **HTTP** e **HTTPS**, **Twitter** e afins, e **e-mail**.

Uma vez que o *malware* se instala em um computador, este passa a buscar cons- tantemente maneiras de se comunicar com o extorsionista, procurando por instruções de como proceder. Essas instruções podem conter ordens para identificar arquivos que devem ser criptografados, indicar quando a operação de criptografia deve começar, enviar para o agressor o código IP da máquina infectada, enviar o *MAC address*, identificar a versão do SO, verificar quais navegadores (*browsers*) estão instalados, identificar quais ferramentas de antivírus estão presentes e outros. Isso feito, o extorsionista possui todo o conhecimento que precisa para orquestrar o ataque *ransomware*, e o impressionante é que toda essa parte de **Comando e Controle** é "silenciosa" e eficiente. Quando o usuário se der conta, a fase de **Destruição** já se iniciou!

1.2.4 Destruição

Neste ponto, a chave que será usada para processar os arquivos no sistema bloqueado ou criptografado é ativada e, a partir daí, o dispositivo-vítima ou parte

dele está inacessível (**encriptação**). Todos os arquivos que foram identificados pelo processo de **Comando e Controle** começarão a ser criptografados pelo *malware*. Isso pode incluir qualquer tipo de documentos do Microsoft Office à JPGs ou GIFs em qualquer quantidade. Algumas variantes não apenas criptografam os arquivos, mas também os nomes de arquivos, tornando ainda mais difícil para que você saiba até que ponto os atacantes chegaram e quais arquivos você perdeu. Uma variante, como já mencionado, pode *bloquear* completamente o SO de maneira que a vítima não consegue sequer manipular o sistema.

Neste momento você está pronto para ser extorquido. Seus dados foram sequestrados. Você deve pagar o resgate? A orientação é **NUNCA PAGAR**, mas infelizmente o trabalho de sua vida pode estar comprometido e, neste caso, você está na mão do criminoso.

1.2.5 Extorsão

Esse é o estágio final! Certamente ninguém quer chegar a esse ponto. Agora que os dados estão criptografados e bloqueados, normalmente uma tela como a apresentada na Figura 1 aparece para a vítima e o extorsionista exige pagamento do resgate.

Para convencer a vítima a realizar o pagamento é comum que se forneça uma “amostra grátis” que desbloqueia alguns arquivos e prova a eficiência do *ransomware*. Também é comum que haja pagamentos/desbloqueios escalonáveis de tal maneira que se pague mais ou menos para desbloquear mais ou menos arquivos. Pagamentos típicos são estabelecidos na ordem de $300,00 a $500,00 dólares quando o *ransomware* é aplicado a usuários comuns, mas quando aplicados à empresas chegam à ordem de dezenas de milhares de dólares (LISKA; GALLO, 2016).

Uma pesquisa conduzida pela *Osterman* e patrocinada pela *Malwarebytes* revelou que 54% das empresas pesquisadas haviam sido vítimas de *ransomwares* nos últimos 12 meses (BLOG, 2016). Dentre as 540 empresas envolvidas na pesquisa notou-se que os alvos mais comuns eram empresas da área da saúde e do setor financeiro.

---

7 Processo pelo qual o SO escolhe quais programas serão executados.

8 Conjunto de softwares e redes de computadores capazes de evitar análise de tráfego de dados na internet. São usados pela chamada Deep Web, comumente utilizada para realizar ações escondidas, ilegais e fomentar o mercado negro (POLADIAN; STONE, 2014; CHACOS, 2013).

Resta ainda uma pergunta: como se realiza o pagamento do resgate? Basicamente existem duas maneiras clássicas de pagamento, ***Bitcoin*** e ***Vouchers Pré-pagos***.

1. ***Bitcoin*** - É uma forma de dinheiro, assim como o real, o dólar ou outro. A diferença é que essa moeda é puramente digital e não pode ser emitida por nenhum governo, banco ou país (INFOMONEY, 2014). Seu valor é livremente determinado pelos usuários e pelo mercado digital. O *bitcoin* vem sendo cada vez mais utilizado para realizar transações *online*, que são rápidas e não-rastreáveis. É por isso, exatamente, que os extorsionistas utilizam essa forma de pagamento para os *ransomwares*;
2. ***Vouchers Pré-pagos*** - De forma semelhante ao *Bitcoin* os *Vouchers Pré-pagos* ou *e-Vouchers* são uma maneira de transformar dinheiro real em dinheiro "virtual". A ideia é comprar alguns títulos ou cartões (semelhante àqueles cartões comprados em livrarias, cartões presente e outros) que podem ser convertidos em dinheiro ou mercadoria a qualquer momento. Esse método de compra/venda, assim como *Bitcoin*, é de difícil rastreamento e, por isso, preferido pelos criminosos.

1.3 COMO FUNCIONA O RESGATE DAS INFORMAÇÕES

Conforme mostrado, o que se resgata de verdade é a chave para decifrar os documentos, e não os arquivos em si. Neste sentido, pode-se dizer que os dados não foram sequestrados, mas sim a chave. Uma vez inserida a chave no sistema, os arquivos serão decifrados e recuperados, mas nada garante que o programa não deixará algum outro *malware* adormecido para atacar novamente depois de um tempo pré-determinado.

O interessante é que quando uma empresa é atacada por um *ransomware* é muito comum que contrate profissionais especializados para realizar o pagamento do resgate, uma vez que estes não são feitos por maneiras convencionais, utilizando dinheiro comum. Muitas vezes, por desconhecimento, a empresa ainda perde uma boa quantidade de dinheiro pagando profissionais que auxiliem no resgate.

1.4 Como sou infectado: em poucas palavras

Um computador pode ser infectado de diversas formas, as mais comuns são através de arquivos de escritório com macros ativadas, através de arquivos que enganam o usuário aparentando ser outra forma de arquivo (*e.g.*: imagens, PDFs e outros) normalmente recebidos por *e-mail (spam ou phishing)* e por introjeção de códigos maliciosos ao navegar em sites infectadores.

1.4.1 OFFICE MACRO

Quem está acostumado a trabalhar com as soluções de escritório, principalmente com o *Microsoft Office*, estão acostumados com as macros. Macros são formas de facilitar a utilização da ferramenta criando uma sequência de comandos otimizando, assim, o dia-a-dia. Contudo, pessoas com conhecimento de computação conseguem se utilizar destas macros para criar um conjunto de código arbitrário com intuito de infectar o computador de uma vítima, instalando algum tipo de vírus ou *trojan*.

1.4.2 FORMATO DO ARQUIVO

Boa parte dos arquivos de computador possuem uma extensão (tipo) como, por exemplo, .xls (EXCEL), .doc (Word), .pdf (Adobe), e assim por diante. É possível que alguns arquivos “disfarcem” suas extensões e, dessa forma, possam se apresentar como um de outro tipo, induzindo o usuário a instalar um *malware* acreditando que está, por exemplo, simplesmente abrindo uma fotografia.

1.4.3 *PHISHING* E SPAM

Com o intuito de enganar as vítimas, criminosos enviam *e-mails* falsos (SPAMs) para roubar informações ou para induzir o usuário a instalar um vírus. Essa tática de ataque é chamada de *phishing*. Por mais que este tipo de ataque pareça não ser relevante, apenas no primeiro trimestre de 2016 houve um crescimento de mais de 60% da quantidade de casos de *phishing* no mundo.

1.4.4 SITES MALICIOSOS

Ao navegar na internet o usuário nunca sabe ao certo se está acessando um site seguro. É muito comum que sites maliciosos, em tempo de navegação, recolham informações sobre seus usuários com intuito de eleger vítimas em potencial. Esses sites analisam vulnerabilidades dos usuários para que extorsionistas realizem ataques futuros. Essa técnica de levantamento de vítimas, como já mencionado, normalmente é chamada de *Strategic Web Compromise*.

2 POR QUE ESTAMOS TÃO SUSCETÍVEIS A VÍRUS?

É muito comum, no dia a dia, tomar medidas de proteção e cuidados simples que minimizem a chance de ser roubado ou assaltado. Entre eles estão, colocar fechadura nas portas, dinheiro no banco, película nos vidros dos carros, cortina nas casas, sistema de monitoramento/alarme, etc. No entanto, o comportamento das pessoas no ambiente virtual é bastante diverso deste do mundo real. Some-se a isso o fato da internet estar cada vez mais presente na vida das pessoas e um cenário promissor para criminosos digitais está formado. Com a possibilidade de se navegar na internet através dos "smartphones" a quantidade de pessoas conectadas à rede deu um salto. O resultado final é preocupante.

A internet, além de vantagem óbvias, trouxe consigo os grandes problemas do mundo real, tais como: extorsão, estelionato, sequestro e outros. O problema é

que na mesma medida em que houve um massivo acesso à grande rede também esses golpes/crimes cibernéticos escalaram de forma considerável. Tem-se a crença de que sistemas extremamente complexos de segurança da informação conseguem tratar grande parte desses problemas e riscos digitais. Isso é apenas parcialmente verdade, uma vez que o **maior risco digital é o usuário despreparado**.

Os sistemas complexos de segurança da informação são de grande importância, mas apenas como analogia, de nada adianta termos a casa mais protegida do mundo se convidarmos espontaneamente o inimigo para entrar. Diante deste fato, podemos dizer que a forma mais efetiva de garantir que o usuário esteja protegido da maioria dos tipos de ataques é através da disseminação do conhecimento. Em outras palavras, é preciso treinar usuários a utilizarem a internet e dispositivos digitais de forma mais consciente e segura.

Entender como reagir a uma infeção e como se proteger dela, são conhecimentos essenciais para toda e qualquer pessoa do mundo atual imerso na tecnologia.

3 RESPOSTA AO INCIDENTE

Fui infectado por um *ransomware*, e agora?

Antes de continuar a discussão, cabe fazermos duas perguntas importantes:

1. Por que *ransomwares* atacam usuários domésticos (SECURITY, 2016)?

- Porque eles não têm *backup*;
- Porque eles têm pouca ou nenhuma educação em segurança digital;
- Porque a falta de consciência acerca dos perigos de estar *online* os torna alvos fáceis para serem manipulados;
- Porque não mantêm seus softwares *up-to-date* (atualizados);
- Porque acreditam que investimento em segurança digital é desperdício;
- Porque ao instalarem um antivírus qualquer, acreditam estar protegidos;
- Porque há uma enorme quantidade de usuários desse tipo, o que torna o “mercado” interessante para os criminosos digitais.

2. Por que *ransomwares* atacam corporações e empresas (SECURITY, 2016)?

- Porque é onde está o dinheiro;
- Porque o estrago é maior e, assim, aumentam a chance de receberem o resgate;
- Porque apesar das empresas investirem em tecnologia de segurança, a falibilidade humana ainda é uma enorme vulnerabilidade;
- Porque podem atacar não apenas computadores isolados, mas servidores, computadores em rede, repositórios *online* e outros;
- Porque o corpo de funcionários normalmente não tem habilidade de prevenção;
- Porque, quando se trata de empresas públicas (*e.g.: NASA*, Pentágono, Receita Federal e outros), um ataque bem-sucedido alimenta o ego dos criminosos.

Submetido em 09.06.2017. Aprovado em 10.11.2017

Agora que os cenários e as causas dos ataques estão compreendidos, retomemos à pergunta: **FUI ATACADO, O QUE FAZER?**

- Existe *backup* das informações?
- Quantas máquinas foram afetadas pelo vírus?
- Quais arquivos ou máquinas não estavam protegidos por *backups*?
- Onde está a nossa falha de segurança que permitiu a instalação do vírus?

A opção de formatar o computador (reinstalar completamente o SO sem manter nenhum arquivo ou registro antigo) é, do ponto de vista da segurança, sempre a melhor opção. No entanto, considerando a situação em que isso não seja possível, deve-se proceder com muita cautela, pois mesmo que um determinado antivírus remova (aparentemente) o *ransomware*, é possível que um *backdoor*[9] ou um vírus de difícil detecção estejam instalados de forma oculta no computador. Neste caso, mesmo que o usuário ou empresa decidam pagar o resgate, eles podem voltar a ser alvos do "mesmo" *ransomware*.

Caso se opte pela remoção do vírus, sugere-se a instalação de um novo antivírus. Indica-se instalar os antivírus das empresas *Malwarebytes* ou *TrendMicro*, pois são os que melhor detectam *ransomware* (BRINKMANN, 2016). Como neste momento deseja-se utilizar a ferramenta com a finalidade de remoção e não como prevenção, a versão gratuita atende perfeitamente as necessidades.

Caso não seja possível recuperar as informações e/ou não exista *backup* ou plano de contingência para casos extremos, a última alternativa é pagar o resgate. Como já foi dito, desejar-se-ia dizer ao leitor: **NÃO PAGUE**. No entanto, em alguns casos essa pode ser a única alternativa, mas lembre-se: é preciso evitá-la de todas as formas possíveis considerando-a a última-das-últimas opção.

Na eventualidade de haver um plano de contingência, execute-o. Se não for possível recuperar as informações e existir *backup*, formate as máquinas infectadas. Posteriormente melhore as ferramentas de proteção e treine a equipe para dirimir a chance de ocorrer este problema novamente. Em seguida aplique o backup para recuperar as informações.

De maneira detalhada, o Fluxograma 4 indica o comportamento adequado que se deve ter no "mundo digital" e as ações que se deve ter em caso de infecção por *ransomware*.

---

9 *Backdoor* é um recurso utilizado por *malwares* para garantir acesso remoto ao sistema ou infectado.

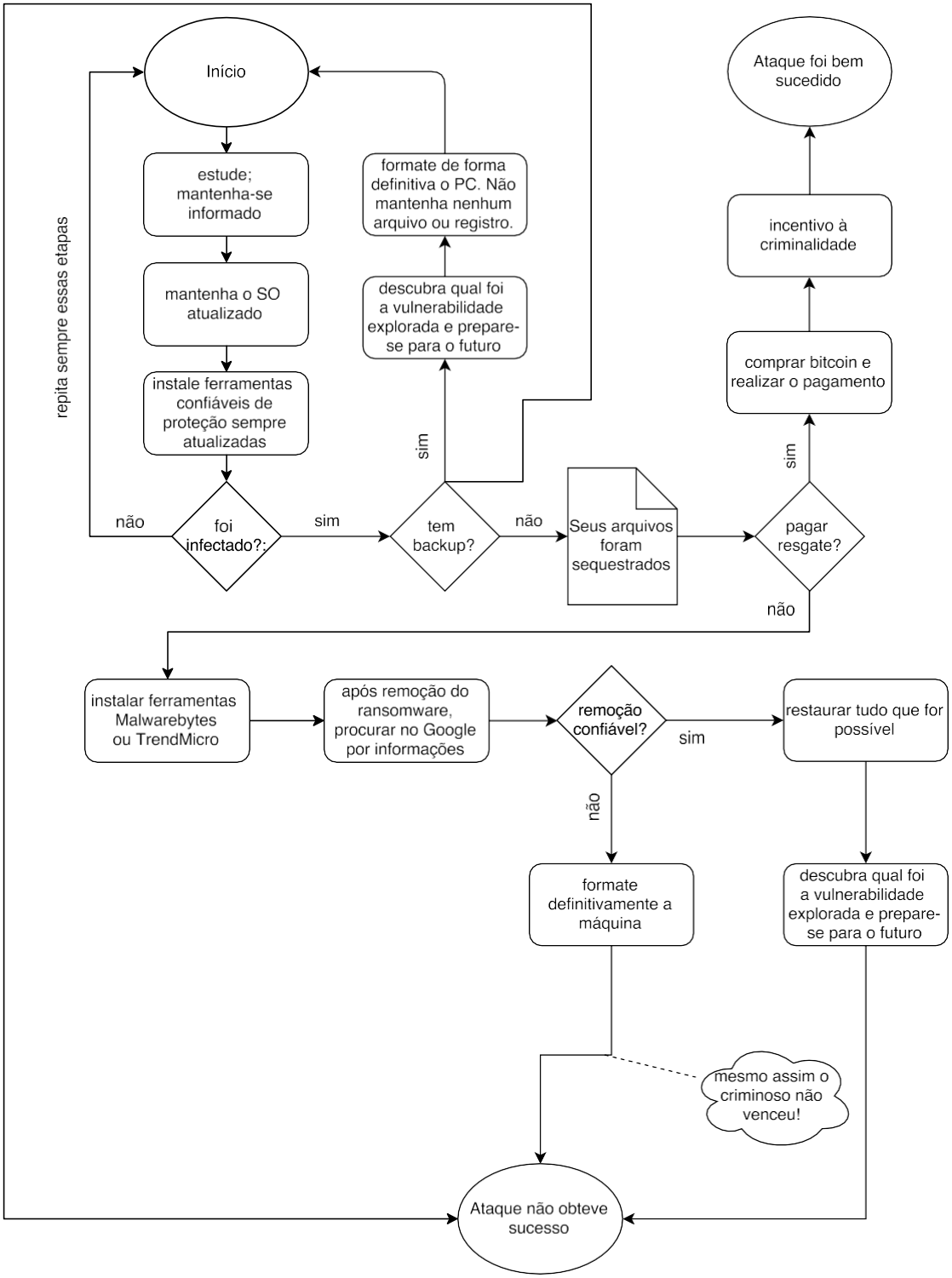

Figura 4 – Fluxograma de ações preventivas e/ou reativas a serem adotadas.

4 BACKUP

Backup é a chave para se ver livre do *ransomware*. Tendo-se cópias de segurança, o sequestro dos dados gerará somente incômodo. Será necessário "apenas" formatar as máquinas atingidas, restaurar os *backups*, rever políticas de segurança e treinar equipe. Para entender melhor como realizar boas rotinas de

backup, primeiro é necessário entender quais os tipos e para que servem.

4.1 ONLINE

Este tipo de *backup* é o feito na internet, ou seja, é utilizada alguma solução *online*. Atualmente, serviços de *backup online* famigerados vêm sendo muito utilizados. Na prática, para garantir que o usuário comum entenda como funciona esse serviço, podemos simplesmente dizer que os arquivos estão sendo depositados em um computador especial e seguro chamado de **servidor**. Este encontra-se em algum lugar do planeta sem que isso interfira ou gere qualquer incômodo para o cliente (KONRAD; SIPPLE, 1995).

Esse princípio é chamado de transparência (COULOURIS; DOLLIMORE; KINDBERG, 2005) e unido às práticas de segurança adotadas pelas empresas que fornecem esse tipo de serviço, compõem características fundamentais do *backup online*.

- Vantagens:
  - Armazenamento mais seguro;
  - Soluções com configurações avançadas;
  - Acessível a partir de qualquer terminal com internet;
  - Grátis para pequenas quantidades de arquivos (5,0 GB);
  - Preço acessível (R$ 300,00 por ano) para quantidades maiores de espaço (1 TB).
- Desvantagens:
  - Não se pode controlar diretamente;
  - Dependente de conexão com internet;
  - É necessário aguardar envios e descargas para novos terminais através de um processo chamado sincronização.

4.2 OFFLINE

Este tipo de *backup* é o realizado em HDs (*Hard Disks*) externos ou em fita magnética na própria empresa, ou seja, é utilizada alguma solução caseira para realizar o *backup* dos dados.

- Vantagens:
  - *Backups* e restaurações rápidos;
  - Fácil acesso, sem necessidade de internet.
- Desvantagens:
  - Pode ser danificado, destruído ou roubado;
  - Não possui redundância por padrão.

Além de utilizar mídias físicas para fazer cópias dos arquivos, é possível fazer uso de algumas técnicas de restauração como forma de proteção. O sistema operacional *Windows*, por exemplo, fornece a criação de **pontos de restauração** e ***shadow copies***, que apesar de não protegerem o usuário dos ataques de

ransomware, podem ajudar na prevenção.

5. Conclusão

Os *malwares* estão cada vez mais eficientes e perigosos. Os ataques criminosos mais comuns e frequentes. Novos tempos exigem novas atitudes. É por isso que devemos, em qualquer dispositivo (*desktops*, celulares, *laptops* e outros), utilizar a internet de forma consciente e segura. Para tanto, o primeiro passo é conscientizar-se, o segundo instruir-se, o terceiro preparar-se e isso foi feito pelo leitor atento que aqui chegou. Não devemos contar com a sorte, ter sempre um *backup* recente dos arquivos importantes e ter em mente que a decisão de pagar resgates deve ser evitada a todo custo pois incentiva à criminalidade.

Submetido em 09.06.2017. Aprovado em 10.11.2017

Referências

ASSOCIATIONS, N. *An Introduction to Cryptography*. [S.l.]: Network Associations, 2000. Citado na página 4.

BATES, J. Trojan horse: Aids information introductory diskette version 2.0. *Virus Bulletin*, p. 3–6, 1990. Citado na página 2.

BLOG, B. *Ransomware*. 2016. <https://www.bitco/intoyou.com/blog/ransomware-bancos-compram-bitcoin/>. Citado na página 6.

BRINKMANN, M. *Anti-Ransomware Software Overview*. 2016. <http://www.ghacks.net/2016/03/30/anti-ransomware-overview/>. Citado na página 9.

CHACOS, B. *Meet Darknet, the hidden, anonymous underbelly of the searchable Web*. 2013. <http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html>. Citado na página 6.

COULOURIS, G. F.; DOLLIMORE, J.; KINDBERG, T. *Distributed systems: concepts and design*. [S.l.]: Pearson Education, 2005. Citado na página 11.

DIFFIE, W.; HELLMAN, M. E. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, IEEE, v. 67, n. 3, p. 397–427, 1979. Citado na página 4.

GIRI, B. N.; JYOTI, N.; AVERT, M. The emergence of ransomware. Citeseer. 2006. Citado na página 2.

GLOBO, P. G. *Com aumento da frota, pais tem 1 automovel para cada 4 habitantes*. 2014.

<http://g1.globo.com/brasil/noticia/2014/03/com-aumento-da-frota-pais-tem-1-automovel-para-cada-4-habitantes.html>. Citado na página 3.

INFOMONEY. *Dez formas de explicar o que e Bitcoin*. 2014. <http://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3160782/dez-formas-explicar-que-bitcoin>. Citado na página 7.

KONRAD, D. R.; SIPPLE, R. E. *Data base backup and recovery system and method*. [S.l.]: Google Patents, 1995. US Patent 5,404,508. Citado na página 11.

LISKA, A.; GALLO, T. *Ransomware: Defending Against Digital Extortion*. [S.l.]: O'Reilly, 2016. Citado 4 vezes nas páginas 2, 4, 5 e 6.

MAO, W. *Modern cryptography: theory and practice*. [S.l.]: Prentice Hall Professional Technical Reference, 2003. Citado na página 2.

NAKAMOTO, S. *Bitcoin: A peer-to-peer electronic cash system*. 2008. Citado

na página 3.

POLADIAN, C.; STONE, J. *Tour The Deep Web: Illegal Marketplaces, Book Clubs And Everything In Between*. 2014. <http://www.ibtimes.com/pulse/tour-deep-web-illegal-marketplaces-book-clubs-everything-between-1729404>. Citado na página 6.

RIVEST, R. The md5 message-digest algorithm. 1992. Citado na página 5.

SECURITY, H. *What is Ransomware and 15 Easy Steps To Keep Your System Protected*. 2016. <https://heimdalsecurity.com/blog/what-is-ransomware-protection/>. Citado 4 vezes nas páginas 2, 3, 8 e 9.