**RANSOMWARE: ENTENDA E PROTEJA-SE.**

Guilherme Ola Prestes; Heverson Dias de Moura

**Resumo:** Atualmente o uso da internet vem se tornando algo indispensável para pessoas e empresas, com esse aumento exponencial na utilização da internet a preocupação com a segurança da informação vêm sendo discutida. Principalmente depois de alguns ataques de ransomware, como o Wannacry e Petya, que geraram grandes percas por todo o mundo. Através deste artigo demonstraremos as melhores práticas atuais para defender-se desse cibercrime.

**Palavras-Chave:** Ransomware; malware; segurança da informação.

RANSOMWARE: UNDERSTAND AND PROTECT YOURSELF.

**Abstract:** Nowadays the use of the internet has become indispensable for people and companies, with this exponential increase in the use of the Internet, the concern with information security has been discussed. Especially after some ransomware attacks, like Wannacry and Petya, which have generated large losses worldwide. Through this article we will demonstrate current best practices to defend against cybercrime.

**Keywords:** Ransomware; malware; information security.

**Introdução**

Atualmente o uso da internet vem se tornando algo indispensável para as pessoas e empresas, e com esse aumento exponencial na utilização da internet a preocupação com dados pessoais e empresariais vêm sendo fortemente discutida.

Os cibercriminosos estão se aproveitando destas informações e utilizando alguns tipos de códigos maliciosos (malware) para capturar dados, onde o mais atual e conhecido é o ransomware.

**Segurança da Informação**

A segurança da informação é a arte e a ciência da proteção de dados valiosos em todas as várias formas de armazenamento.  Segundo o BusinessDictionary (2017), a segurança da informação protege de forma segura os dados de uma organização contra o acesso ou modificação não autorizados para garantir sua disponibilidade, confidencialidade e integridade.

Conforme Friedrich (2014), a disponibilidade é o fator que garante que pessoas autorizadas acessem as informações e possam fazê-lo sempre que necessário. A confidencialidade é o fator que garante que somente pessoas autorizadas terão acesso à informação, protegendo de acordo com o grau de sigilo, e a integridade é o fator que garante que a informação não seja alterada mesmo que de forma acidental ou intencional.

Entre esses fatores da segurança da informação, deve-se verificar com cuidado e analisar o que proteger. Ela nos encaminha a tratar de muitos pontos que podemos chamar de ameaças, sendo a maioria das vezes proporcionada por fatores humanos.

**Hackers**

Hackers são pessoas que tem uma grande facilidade na manipulação de computadores e rede de computadores, um hacker é capaz de modificar ou criar scripts que poderão possibilitar a criação de uma porta de entrada para computadores que supostamente estão protegidos.

Segundo Businessdictionary (2017) a definição para palavra hacker é um programador que manipula códigos e senhas, ou consegue acesso remoto de um computador protegido.

Embora o termo “hacker” refira-se essencialmente a uma pessoa que pode subverter a segurança do computador sem qualquer propósito malicioso, porém a maioria das pessoas referem-se a palavra como criminosos cibernéticos que com suas habilidades em computação invadem sistemas de computadores para fins maliciosos.

Os hackers têm uma forma de pensar normalmente muito semelhante uns com os outros, eles pensam que os acessos aos computadores deveriam ser totais e ilimitados, não ficando somente em computadores, mas também a qualquer coisa que possa ser usada para ensinar a alguém alguma coisa sobre como o mundo funciona. (LEVY, 2010, P.40).

Há diversos ideais que caracterizam grupos de hackers, os White Hat Hackers, Black Hat Hackers e os Hacktivists. Os White Hat são os chamados hackers éticos, que são especialistas em testes de vulnerabilidades e penetração, eles geralmente prestam serviços para empresas para identificar as falhas de segurança da mesma. Os Black Hat segundo Oliveira (2017), também conhecidos como cracker, são responsáveis por corromper sistemas, modificar, apagar ou roubar informações em busca de ganhos pessoais.

Os Hacktivists são conhecidos por suas ideologias políticas e religiosas, normalmente eles aproveitam-se das vulnerabilidades para revelar a todas as pessoas do mundo problemas nessas áreas, um dos mais conhecidos grupos de hackers, chamado Anonymous, encaixa-se nessa ideologia.

**Criptografia**

A palavra criptografia é uma derivação de duas palavras de origem gregas a kryptós (oculto) e gráphein (escrever), (CUNHA, 2008).

Segundo Singh (2008), criptografia é um estudo dedicado a escrever mensagem codificada. Ela utiliza cifras e códigos para substituir as letras ou palavras, em um processo conhecido como encriptação.

A criptografia é feita por computadores que manipulam apenas números binários, sequência de 0 e 1. Primeiramente deve-se transformar a mensagem em números desse tipo (CUNHA, 2008).

Existem tipos de chaves utilizadas para a criptografia que podem ser divididas em duas grandes categorias.

Criptografia de chave assimétricas: é uma chave do tipo pública, que pode ser livremente divulgada e uma privada que deverá ser mantida com seu criador. Quando um dado é criptografado com uma das chaves, somente a outra pode ser usada para descodificar (CARTILHA, 2017).

Criptografia de chave simétrica: é uma criptografia de chave única, esta utiliza-se de uma mesma chave para codificar dados e para descodificar, ela é utilizada para garantir a confidencialidade dos dados (CARTILHA, 2017).

Na grande maioria dos casos, a criptografia é utilizada para proteção dos dados sigilosos armazenados em seu computador, como os arquivos de senhas.

Porém, como trata-se de uma forma praticamente impossível de ser quebrada, a criptografia também está sendo utilizada por hackers para capturar dados com os ataques dos malwares o ransomware.

**Códigos maliciosos (Malware)**

Malware é um termo abreviado que significa "software malicioso". Este é um software que foi projetado especificamente para obter acesso ou danificar um computador sem o conhecimento do proprietário (CERT.BR, 2017). Existem vários tipos de malware, incluindo vírus, spyware, trojan, worms ou qualquer tipo de código malicioso que infiltra em um computador.

Segundo a cartilha de segurança para internet do Cert.br (2017), existem diferentes tipos de malware que possuem características únicas.

Vírus é o tipo de malware mais comum, e é definido como um programa malicioso que pode executar-se e espalhar-se infectando outros programas ou arquivos.

Worm é um tipo de malware que pode se auto-replicar sem um programa hospedeiro, costumam espalhar-se sem qualquer interação humana ou diretivas dos autores de malware.

Trojan é um programa malicioso que é projetado para aparecer como um programa legítimo, mas uma vez ativada após a instalação, os trojans podem executar suas funções mal-intencionadas.

[Spyware](http://searchsecurity.techtarget.com/definition/spyware) é um tipo de malware que é projetado para coletar informações e dados sobre usuários e observar sua atividade sem o conhecimento dos usuários.

Outros tipos de malware incluem funções ou recursos projetados para um propósito específico, por exemplo o Ransomware.

**Ransomware**

Segundo Melo (2016), ransomware é um código malicioso instalado em um recurso computacional sem o consentimento do usuário, o qual posteriormente criptografa todos os dados do computador ou o bloqueia completamente. Então exigem um resgate alegando que após a vítima efetuar o pagamento, ela receberá a chave de descriptografia para recuperar seus arquivos.

O Ransomware não é um vírus. Os vírus infectam seus arquivos ou software e têm a capacidade de replicar, já o Ransomware codifica seus arquivos para torná-los inutilizáveis. Eles podem ser removidos com um antivírus, mas se os arquivos estão criptografados, não há chances de recuperá-los.

Conforme a Kaspersky (2017), o ransomware tem evoluído muito e tem basicamente duas categorias, os cryptors e os blockers.

Os cryptors criptografam os arquivos valiosos, fotos, documentos, base de dados, entre outras. Uma vez que seus dados estão encriptados, os mesmos não podem ser acessados. Os blockers, restringem o acesso dos usuários aos dispositivos infectados, levando o bloqueio de todo o sistema ou máquina.

O Ransomware geralmente é instalado em seu computador através de um anexo mal-intencionado em seu e-mail ou através de algum website infectado que você esteja navegando (AVAST, 2017).

Ataques feitos por e-mail geralmente conhecidos como e-mail spoofing, consiste em alterar os campos de cabeçalho do e-mail, fazendo aparentar que foi enviado de uma determinada origem confiável, quando na verdade veio de outra. Esta técnica é possível devido ao protocolo SMTP (Simple Mail Transfer Protocol) que permite que sejam alterados os campos do cabeçalho.

Os ataques recentes demonstraram que os criminosos virtuais se esforçam para melhorar o seu código, adicionando recursos que tornam a detecção mais difícil e ajustando seus e-mails mal-intencionados para torná-los eficazes.

Os maiores ataques de ransomware em 2017, foram [WannaCry](https://www.avg.com/en/signal/wannacry-ransomware-what-you-need-to-know)e Petya.

Em maio de 2017, um enorme cyberattack de ransomware chamado WannaCry se espalhou pela web, criptografando arquivos e dados de vítimas em mais de 150 países. O malware de extorsão atingiu milhares de indivíduos e instituições imensas em todo o mundo como a FedEx, Serviços Nacionais de Saúde da Grã-Bretanha, a Telefônica espanhola e a Renault da França (AVAST, 2017).

Os criadores do WannaCry aproveitaram-se do recurso do Windows chamado EternalBlue, que depende de uma vulnerabilidade do sistema que a Microsoft [corrigiu na atualização de MS17-010](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx), datada em 14 de março de 2017. Ao usar a exploração, os hackers podem obter acesso a computadores e fazer a instalação do encriptador.

Depois de invadir um computador com sucesso, o malware espalha-se pela rede local e para as outras máquinas. O código malicioso verifica outras máquinas com a mesma vulnerabilidade, e quando o EternalBlue encontra um computador vulnerável, ele infecta a máquina e criptografa os arquivos.

Portanto, ao ser instalado em um computador, o WannaCry pode infectar toda uma rede de área local e criptografar todos os dispositivos conectados na rede. É por isso que as grandes empresas sofreram com o ataque, quanto mais computadores na rede, maior o dano.

Segundo Kaspersky (2017), o WannaCry normalmente trabalha em duas partes, onde uma é a exploração que tem como propósito a infecção e a propagação. A segunda é a encriptação que é feita depois do usuário ter feito um download infectado com o malware.

O WannaCry, encripta vários tipos arquivos, incluindo documentos de escritório, fotos, vídeos e arquivos que potencialmente contêm dados críticos do usuário ou empresa.  Os arquivos criptografados são renomeados, e os mesmos ficam inacessíveis. Depois disso, altera o wallpaper do desktop para uma imagem que contém informações sobre a infecção e as ações que o usuário supostamente deve realizar para recuperar seus dados. O malware espalha notificações como documentos de texto com as mesmas informações em pastas do computador para garantir que o usuário receba a mensagem.

A principal diferença entre o WannaCry e os outros encriptadores é que um encriptador comum depende do erro do usuário, por exemplo clicar em um link malicioso permitindo que o anexo mal-intencionado seja executado. Já o WannaCry pode ser executado sem que o usuário faça nada, utilizando vulnerabilidades de rede.

Petya é um outro tipo de ransomware que está ativo desde pelo menos março de 2016. No seu núcleo, Petya atua como o resto de seus segmentos de malware de sequestro de dados. Ao invés de criptografar seus arquivos, um por um, como a maioria dos outros tipos de ransomware, ele impede você de ter acesso a todo o disco rígido criptografando a tabela de arquivos mestre, de modo que o sistema de arquivos se torne ilegível e o Sistema Operacional não consiga ser inicializado.

Segundo Avast (2017) Petya está por trás do enorme ataque ransomware que afetou organizações em todo o mundo em junho de 2017. A ucrânia foi o país mais afetado, com o Banco Nacional da Ucrânia, metrô de Kiev e vários aeroportos. Mas a escala do ataque é verdadeiramente global. Muitas empresas multinacionais também relataram ser afetadas.

Petya ataca normalmente um departamento de RH de uma agência pública ou empresa privada. Que recebe um pedido de emprego de e-mail falso com um link de download, alegando conter currículo de alguém. Este link baixa um executável que passa a criptografar o acesso ao computador da vítima (AVAST, 2017).

Se o código malicioso for executado em uma máquina, a primeira pista de que algo não está certo virá na forma de uma tela azul do Windows “da morte”. Isso significa que o Petya começou a criptografar o arquivo da tabela principal e irá mostrar uma tela de aviso, muitas vezes um crânio projetado em um fundo colorido e uma mensagem dizendo que você deve efetuar o pagamento. Normalmente em bitcoins, em troca do acesso aos arquivos do computador. O bitcoin é utilizado como forma de pagamento por se tratar de uma moeda virtual irrastreável facilitando que a identidade do hacker permaneça escondida.

Até este momento, ninguém realmente sabe com certeza. Empresas e instituições de todo o mundo como Rússia, Reino Unido e Índia foram afetadas, e não é possível identificar a origem geográfica exata do Petya.

Outro grande ataque de ransomware foi o Locky. Visto pela primeira vez em fevereiro de 2016, segundo a Symantec (2016), Locky foi enviado para milhões de usuários em todo o mundo em sua primeira aparição. Em uma invasão de e-mail que afirmou ser uma fatura ou um recibo de pedido. Os e-mails continham um documento do Word ilegível, pediam aos usuários que habilitassem os macros para visualizar seu conteúdo e, em seguida, fazia o download do malware.

Como os hackers continuam melhorando seu código, qualquer uma dessas variantes pode reaparecer em qualquer ponto, então é importante saber que eles estão lá mesmo quando você não lê sobre isso nas notícias.

Quando se trata de Ransomware, qualquer um pode ser um alvo. Por exemplo, a WannaCry aproveitou uma vulnerabilidade do Windows para espalhar e infectar mais de 230.000 pessoas, empresas, autoridades públicas e organizações em todo o mundo (AVAST, 2017).

Qualquer pessoa que não instalou o patch de segurança Microsoft [lançado em março](http://www.csoonline.com/article/3180616/security/microsoft-released-18-security-bulletins-9-rated-critical-many-bugs-disclosedexploited.html) ficou vulnerável. Os usuários do Windows XP foram atingidos sem dificuldade. A Microsoft terminou o suporte para essa versão do Windows 3 anos atrás, e só foi estimulada a liberar um patch para essa versão bem depois do ataque ter se tornado severo.

Enquanto um patch ou atualização para corrigir esses problemas são em sua maioria rápidos e fáceis para usuários regulares, empresas e organizações são muito mais vulneráveis. Eles muitas vezes executam softwares personalizados que romperão com as atualizações e precisarão implementar as correções em um grande número de dispositivos, o que os desacelera. Algumas organizações não têm fundos suficientes para atualizações. Espera-se que os orçamentos de hospitais salvem vidas, não computadores.

Cibercrime é a maior preocupação para as organizações que trabalham com dados confidenciais, mas isso não significa que os usuários regulares de computadores estejam seguros, suas fotos ou arquivos pessoais também podem ser alvos para os hackers.

**Como remover Ransomware**

A exclusão do ransomware é bastante fácil. Na verdade, é o mesmo que remover um vírus ou qualquer outro tipo comum de malware. Utiliza-se a ferramenta de remoção de ransomware do antivírus (AVAST, 2017).

**Como se proteger**

A melhor proteção contra essa ameaça, é ser proativo em sua própria defesa cibernética. Uma vez que este malware em particular é tão complicado em sua natureza, recomenda-se que utilize várias camadas de proteção contra essa ameaça.

Fazer backup de dados importantes, é a maneira mais eficaz de combater a infecção pelo ransomware. Os atacantes têm influência sobre suas vítimas, criptografando arquivos valiosos e deixando-os inacessíveis. Se a vítima tiver cópias de backup, eles podem restaurar os arquivos uma vez que a infecção foi limpa. Pois o pagamento do resgate não garante que conseguirá o acesso aos arquivos. (CERT.BR, 2017; KASPERSKY, 2017).

Novas variantes de ransomware aparecem regularmente. Manter sempre o software de segurança atualizado para ajudar a proteger-se contra eles. (AVAST, 2017).

Mantenha o sistema operacional e outros softwares atualizados. As atualizações de software incluirão frequentemente patches para vulnerabilidades de segurança recém-descobertas que poderiam ser exploradas por invasores de ransomware. (CERT.BR, 2017)

Instale um bom software antivírus. Execute uma ferramenta de correção anti-malware em tempo real e configure uma proteção de firewall forte. (KASPERSKY, 2017).

O e-mail é um dos principais métodos de infecção. Desconfie de e-mails inesperados, especialmente se contiverem links e / ou anexos. (KASPERSKY, 2017).

**Considerações finais**

Se tudo isso parece-lhe um drama de suspense ruim, você não está sozinho. Milhares de pessoas foram vitimadas pelo ransomware, porém, a maioria dessas ameaças teriam sido evitadas se os usuários tivessem feito um passo muito simples: backup de suas informações.

O ransomware é um ataque agressivo e intrusivo em seu dispositivo pessoal, é uma ameaça que obtém seu poder da noção predominante de que a maioria dos usuários não faz backup regular de seus dados. A razão pela qual os usuários estão dispostos a pagar por seus dados pessoais é porque a única cópia da informação está no dispositivo que está sendo bloqueado. Se você tem várias cópias de seus dados pessoais, não há motivo para temer a perda dos dados.

Ao ficar proativo sobre a segurança online e fazer backup dos dados pessoais, ter um bom antivírus, tomar cuidado ao abrir os e-mails, e manter o dispositivo atualizado, reduz significativamente as ameaças online causadas pelo Ransomware.

**Referências bibliográficas**

AVAST. **Ransomware**. Disponível em: <https://www.avast.com/pt-br/c-ransomware>. Acesso em: 29 out. 2017.

\_\_\_\_\_\_\_\_\_\_. **WannaCry**. Disponível em: < Https://www.avast.com/pt-br/c-wannacry>. Acesso em: 29. Out. 2017

\_\_\_\_\_\_\_\_\_\_. **Petya.** Disponível em: <https://www.avast.com/pt-br/c-petya>. Acesso em: 29. Out. 2017

BUSINESSDICTIONARY. **Information Security.** Disponível em: <http://www.businessdictionary.com/definition/information-security.html>. Acesso em: 19. Nov. 2017.

\_\_\_\_\_\_\_\_\_\_\_. **Hacker.** Disponível em: <http://www.businessdictionary.com/definition/hacker.html>. Acesso em: 20. Nov. 2017.

CERT.BR. **Cartilha de segurança para Internet**: códigos maliciosos (malware). Disponível em: <https://cartilha.cert.br/malware>. Acesso em: 20. Nov. 2017.

\_\_\_\_\_\_\_\_\_\_. **Cartilha de segurança para Internet**: ataques na internet**.** Disponível em: <<https://cartilha.cert.br/ataques/#3.1>>. Acesso em: 29.out.2017.

\_\_\_\_\_\_\_\_\_\_\_. Cartilha de Segurança para Internet: Criptografia. Disponível em: < https://cartilha.cert.br/criptografia/>. Acesso em: 20. Nov. 2017.

CUNHA, M. O. **Números primos e criptografia.** Disponível em: <http://nilsonjosemachado.net/sema20081104.pdf>. Acesso em: 20. Nov. 2017.

ENIGMA SOFTWARE. **Locky File Extension Ransomware.** Disponível em: <https://www.enigmasoftware.com/lockyfileextensionransomware-removal>. Acesso em: 29. Out. 2017.

FRIEDRICH, L.D.P.M. **Um sistema web para análise de gestão da segurança da informação segundo a norma ABNT NBR ISSO IEC 27002**. Santa Maria, RS. 2014. Disponível em: <http://www.redes.ufsm.br/docs/tccs/Lucimara\_Friedrich.pdf>. Acesso em: 19. Nov. 2017.

KASPERSKY. **WannaCry: Are you safe?** Disponível em: <https://www.kaspersky.com/blog/wannacry-ransomware> Acesso em: 29. Out. 2017

\_\_\_\_\_\_\_\_\_\_. **O que você precisa saber sobre ransomware**. Disponível em: <https://www.kaspersky.com.br/blog/ransomware-for-dummies/6790/>. Acesso em: 29.out. 2017.

LEVY, S. **Hackers:** heroes of the computer revolution. Gravenstein Highway North: O’Reilly, 2010.

MELO, V.A. Ransomware: o uso maléfico da criptografia. **Escola paulista de direito**, São Paulo, 2016. Disponível em: <<https://www.researchgate.net/publication/304540432_Ransomware_-_o_uso_malefico_da_criptografia>>. Acesso em: 29.out.2017.

MICROSOFT. **O que é ransomware?** Disponível em: <https://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx>. Acesso em: 29 out. 2017.

\_\_\_\_\_\_\_\_\_\_. **O que é malware.** Disponível em: < https://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx>. Acesso em: 29 out. 2017.

OLIVEIRA, P. R. **Oportunidades e ameaças na rede.** Disponível em: <https://www.riuni.unisul.br/bitstream/handle/12345/3155/Oportunidades%20e%20amea%C3%A7as%20na%20rede.pdf?sequence=1&isAllowed=y> Acesso em: 20. Nov. 2017.

SINGH, S. **O Livro dos Códigos: A ciência do sigilo – do antigo Egito à criptografia quântica.** 7. ed. Rio de Janeiro: Record, 2008.

SYMANTEC. **Locky ransomware on aggressive hunt for victims**. Disponível em: <https://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims>. Acesso em 29. Out. 2017.