Um dos maiores ataques de Ransomware da história está acontecendo, entenda como funciona e como se proteger

Que bela praga, não? Eu vou falar um pouco sobre o ataque de Ransomwares que está acontecendo em mais de 70 países, segundo a Kaspersky, e que aparentemente afetou máquinas aqui no Brasil também e para completar vou dar algumas dicas que podem ajudar você a se prevenir ou remediar.

Com informações da **Computeworld**, que fez um belo trabalho reunindo informações, eu vou tentar fazer um apanhado geral e simplificado para você entender o que está acontecendo. Um ataque de ransomware em escala global está atingindo algumas dezenas de países e sequestrando arquivos em computadores, especialmente de empresas de telefonia. Temos alguns casos mais impactantes noticiados em empresas do Reino Unido, Espanha, Rússia e Taiwan, entretanto, segundo levantamentos da empresa de segurança russa, Kaskersky, cerca de 74 países foram afetados, com mais de 45 mil ataques registrados.

O que é Ransonware?

De maneira simples, ransomware é um tipo de malware que infecta máquinas de sistemas operacionais variados e que criptografa arquivos do usuário, os ransomwares possuem variações, mas este é o tipo mais comum, uma vez criptografados, os ransomwares exibem mensagens de resgate dos arquivos mediante a pagamento de um acerta quantia, comumente em Bitcoins, mas podem ser utilizadas outras moedas digitais também.

Qual é o Ransomware?

O Ransomware que está causando todo este problema parece ser uma variação do "WannaCry", também conhecido por "WCry" ou ainda "WannaCrypt0r ransomware". Ele funciona como qualquer outro Ransonware, encriptando arquivos e pedindo resgate, mas o que garantiu que ele tivesse maior sucesso de infecção foi a sua forma de duplicação e propagação, um comportamento semelhante a qualquer outro vírus to tipo "Worm", pelas informações, ele afeta especificamento o protocolo SMB do Windows, especialmente versões mais antigas do sistema da Microsoft, uma vez que uma máquina em rede seja infectada, ele poderia se espalhar para as demais. Os tipos de arquivos que ele afeta são os com as extensões doc, .dot, .tiff, .java, .psd, .docx, .xls, .pps, .txt, .mpeg, entre outros.

De onde veio o Ransomware?

Não se sabe exatamente a origem dele, o "WCry" em si já existia há algum tempo na verdade, e as vulnerabilidades do Windows 10 que permitiam o ataque foram corrigidas ainda em Março pela Microsoft, contudo, o "WCry" parece ter sido "levemente" modificado graças ao vazamento de ferramentas de **hacking da NSA que aconteceu recentemente,** uma das ferramentas, chamada de "EternalBlue", parece conseguir explorar facilmente o protocolo SMB do Windows para invasão e aparentemente, segundos os laudos da Kaspersky, foi utilizada para incrementar o "WCry".

Como o Ransomware parece ter se propagado principalmente por e-mail e o país de maior detecção feita pela Kaspersky foi a Rússia, é possível que ele tenha se originado lá, entretanto, como a Kaspersky tem maior atuação lá, o fato deles terem detectado uma maior quantidade na Rússia pode se dever a isso, não sei, a empresa mesmo comentou que eles poderia ter uma "visão local do caso", que poderia ser muito mais grave do que as estimativas deles.

Quem é afetado por ele? Quem são as vítimas?

Resumidamente: Usuários de Windows. Mas vamos detalhar e especificar mais. Este ransomware afetou diversas empresas de Telefonia especialmente, como a Telefónica na Espanha, a Vivo, que pertence à empresa aqui no Brasil, não relatou até então nenhuma infecção, ainda que tenha declarado estar tomando providências para evitar o problema.

Os computadores afetados, segundo o site da Microsoft, são os que usam as seguintes versões do Windows:

- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016

Sendo que correção original para a primeira versão do WCry foi liberada pela empresa, mas muitos destes usuários, ou não usam o Windows 10, ou não atualizaram. A recomendação é instalar os seguintes patches de correção que deverão aparecer nas atualizações do sistema: 017-10, 017-12 e 017-15.

Usuários de Linux e macOS não precisam se preocupar desta vez, os sistemas estão seguros, contudo, fica o alerta, pois pode ser que este ataque não afete ambos, mais não seria a primeira vez que algo do tipo acontece, tanto com macOS, quanto com Linux, como eu disse, vale o alerta para o futuro.

O que você pode fazer para se defender?

Como este tipo de vírus não vem por "download espiritual", a dica principal é até óbvia, você deve ficar atento a e-mails que eventualmente receba de pessoas desconhecidas e que, neste caso, possuam um anexo malicioso ou algum tipo de link.

Utilizar Linux ou macOS pode ajudar também, pois o sistema normalmente visado é o Windows, e no caso do Linux, as atualizações rápidas do modelo open source de desenvolvimento devem ajudar também.

Independente do sistema que você utilize, mantenha-o sempre atualizado, especialmente programas que tem acesso direto à internet, como navegadores, em caso de você utilizar o Windows, utilize um bom antivírus também e quem sabe um Firewall, assim você diminui as chances de ter problemas do tipo.

Acima de tudo, o maior clichê do mundo da segurança doméstica, "o melhor antivírus é o usuário", continua válido, então fique ligado, ter sempre um backup dos seus arquivos é algo importantíssimo, aliás, ter mais de um, neste caso vale aquela máxima: "**Backup, quem tem dois, tem um, e quem tem um, não tem nenhum!".**

Caso você perceba que a infecção já está em ação, realmente, desligar o computador e passar um antivírus no disco rígido com o sistema desligado, ou com o Windows em modo de segurança pode ser a salvação, entretanto, arquivos que já foram criptografados são dificilmente recuperáveis em tempo hábil, alguns especialistas em segurança dizem que isso só é possível de se fazer quando o Ransomware possui algum erro de programação e a encriptação é falha, em outros casos é praticamente impossível.

Outra dica dada pelos especialistas de segurança é você nunca pagar o resgate pedido pelos criminosos, por dois motivos simples. Não incentivar a prática dos criminosos, obviamente, e porque nada garante que o criminoso te ajude a descriptografar os seus arquivos de fato, mesmo mediante a pagamento, estatisticamente, quando houve este pagamento, os criminosos simplesmente não respondem e você continua com os seus dados sequestrados e agora com uma conta bancária mais magra.

Fonte:

DioLinux - https://goo.gl/Njujyn