A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Lições do WannaCry

Visão Geral

Recentemente você provavelmente assistiu uma grande cobertura na mídia sobre um novo ataque cibernético chamado “WannaCry”. O “WannaCry” infectou mais de 200.000 computadores impedindo uma variedade de organizações de acessarem seus dados, incluindo hospitais no Reino Unido. Foram várias as razões pelas quais este ataque ganhou muita atenção. Primeiro, ele se espalhou rapidamente de computador para computador, atacando uma vulnerabilidade conhecida em máquinas Windows. Segundo, o ataque foi através de um tipo de malware chamado “Ransomware”, ou vírus de resgate, ou seja, uma vez que infecta seu computador, ele encripta todos os seus arquivos, impedindo-o de acessar seus dados. As únicas formas de recuperar seus dados são através do seu backup ou pagando 300 dólares de resgate ao atacante para que ele decripte seus dados. Terceiro e mais importante, esse ataque nunca deveria ter sido capaz de acontecer. O “WannaCry” atacou computadores Windows expostos por uma vulnerabilidade para a qual a Microsoft havia emitido uma correção meses atrás. Mas muitas organizações falharam em instalá-la, ou ainda estavam utilizando sistemas operacionais como o Windows XP, que são tão antigos que não há mais correções disponíveis para eles. Aqui vão três passos simples que você pode seguir para certificar-se de que ataques como o “WannaCry” nunca irão lhe infectar.

Editor Convidado

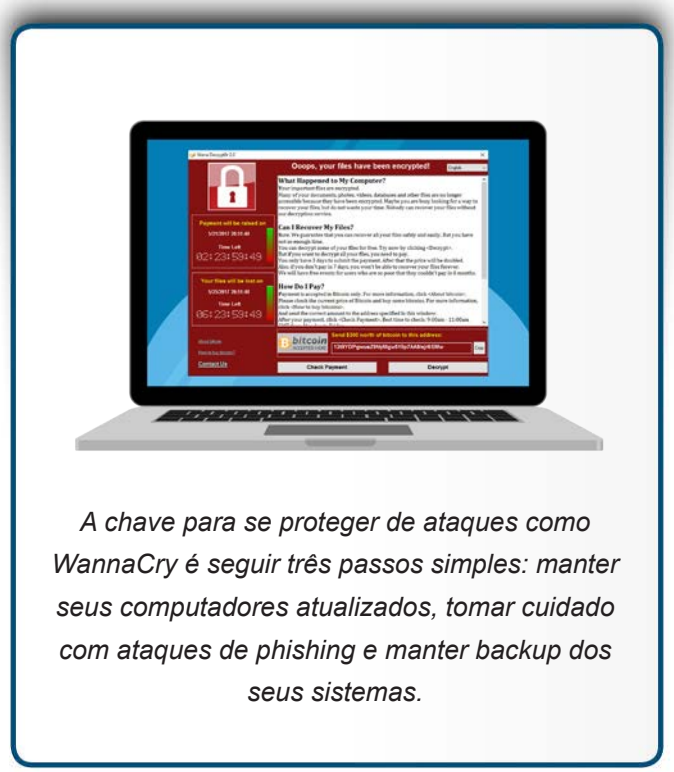
Dr. Johannes Ullrich é Decano de Pesquisa do Instituto de Tecnologia SANS e fundador do DShield.org. É responsável pelo **SANS Internet Storm Center** que monitora as ameaças de segurança atuais. E leciona Segurança de Aplicações Web (**DEV522**), Detecção de Intrusão (**SEC503**) e IPv6 (**SEC546**).

Correções

Primeiro e mais importante, certifique-se de que seus computadores, dispositivos móveis, aplicativos e qualquer outra coisa conectada na Internet esteja atualizada. Criminosos cibernéticos estão constantemente buscando novas vulnerabilidades no software utilizado pelos seus aparelhos. Quando eles descobrem, utilizam programas especiais para hackear seus aparelhos. Enquanto isso, as empresas fabricantes dos softwares utilizados nos seus aparelhos trabalham duro para corrigir as vulnerabilidades emitindo correções para esses softwares. Ao assegurar que seus computadores e dispositivos móveis instalem essas atualizações, você torna muito mais difícil a tarefa de hackeá-lo. É isso que é tão frustrante sobre a propagação do WannaCry. As atualizações para corrigir e parar este ataque foram divulgadas quase dois meses antes pela Microsoft. Se as empresas tivessem mantido seus computadores atualizados, esse ataque nunca teria funcionado. Para garantir que seus dispositivos estejam atualizados, habilite a atualização automática sempre que possível. Essa regra se aplica a quase qualquer tecnologia conectada a uma rede, não apenas a computadores e dispositivos móveis, mas também

Lições do WannaCry

TV's conectadas à Internet, roteadores domésticos, consoles de jogos e algum dia até seu carro. Se os seus Sistemas Operacionais ou dispositivos forem tão antigos ao ponto de não serem mais suportados com atualizações de segurança, como o Windows XP, substituam-nos com novas alternativas que tenham suporte.



A chave para se proteger de ataques como WannaCry é seguir três passos simples: manter seus computadores atualizados, tomar cuidado com ataques de phishing e manter backup dos seus sistemas.

Backups

Em alguns casos, ataques cibernéticos como vírus de resgate podem infectar até mesmo sistemas atualizados. Uma segunda forma de se proteger é fazer backup dos seus dados. Backups são cópias das suas informações armazenadas em algum lugar diferente do seu computador ou dispositivos móveis. Quando você perde seus dados valiosos, você pode recuperá-los dos backups. Infelizmente muitas pessoas falham em fazer backups regulares, mesmo que sejam simples e baratos. Há duas formas de fazer backup dos seus dados: em mídia física ou em armazenamento na nuvem. Cada abordagem tem suas vantagens e desvantagens. Você pode usar ambos, de forma conjunta, se estiver inseguro sobre qual método utilizar.

Mídias físicas são dispositivos que você controla como drives USB externos ou drives conectados em rede na sua casa ou no escritório. A vantagem de utilizar sua própria mídia física é que ela permite copiar e recuperar grandes quantidades de dados rapidamente. A desvantagem desta abordagem é que se você for infectado com um malware, como um Ransomware, é possível que esta infecção se espalhe até os seus backups. Se você estiver utilizando mídias físicas para seus backups, você deve armazenar cópias dos seus backups em um endereço diferente e seguro, daquele onde está seu computador. Certifique-se de que qualquer backup que você armazene esteja apropriadamente etiquetado. Soluções baseadas em nuvem são serviços online que fazem backup e armazenamento dos seus arquivos na Internet. Tipicamente, você instala um programa no seu computador que toma conta de tudo. A vantagem de soluções em nuvem é a simplicidade. Adicionalmente, se você for infectado com um Ransomware, a infecção geralmente não consegue acessar seus backups baseados em nuvem. As desvantagens são que o tempo para a cópia ou recuperação de quantidades muito grandes de dados pode ser muito grande. Certifique-se de investigar sobre a privacidade e segurança dos backups em nuvem. O serviço de backup dispões de forte segurança como criptografia ou autenticação forte?

Phishing

Finalmente, os atacantes estão constantemente atualizando e mudando seus métodos de ataque. Os criminosos

Lições do WannaCry

cibernéticos frequentemente utilizam um outro método chamado Phishing para atacar e infectar suas vítimas. Phishing é um ataque onde o criminoso cibernético envia um email tentando induzi-lo a abrir um anexo infectado ou visitar um site de internet malicioso. Se fizer um dos dois, seu computador será infectado. Embora o "WannaCry" não tenha utilizado esse método, ele é comumente utilizado por muitos tipos de ataques, incluindo muitos tipos de Ransomware. Adicionalmente, os criminosos cibernéticos que desenvolveram o "WannaCry" vão indubitavelmente atualizar seus métodos de ataque nos próximos meses e utilizar técnicas como o phishing para infectar ainda mais computadores. A chave para se proteger contra esse tipo de ataque baseado em email é o bom senso. Se um email ou mensagem parece estranha, suspeita ou muito boa para ser verdade, provavelmente ela é um ataque.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop

Marta Visser – Tradutora autônoma

Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

O que é um Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Usando a nuvem com segurança:	https://securingthehuman.sans.org/ouch/2016#november2016

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser

