SEMINÁRIO DE TECNOLOGIA, GESTÃO E EDUCAÇÃO
Período de 26 a 30 de outubro
Alcides Maya
FACULDADE E ESCOLA TÉCNICA

VULNERABILIDADES DE REDES: WANNACRY

Rodrigo Rodrigues Scotti[1]
Anderson santos da silva [2]
João Padilha Moreira [3]

RESUMO

Este artigo tem como objetivo abordar o vírus WannaCry (ou WannaCrypt), um malware do tipo ransomware que por dois dias conseguiu atacar mais de 230 mil computadores em 150 países. Neste artigo será abordado o que é o WannaCry, como é realizado o ataque, como este vírus conseguiu chegar a uma escala global e como se prevenir. Ao final é realizada uma breve conclusão sobre o assunto.

Palavras-chave: Ransomware, WannaCry, WannaCrypt, Windows.

ABSTRACT

This article aims to address the WannaCry virus (or WannaCrypt), a ransomware-type malware that for two days managed to attack more than 230,000 computers in 150 countries. In this article we will cover what WannaCry is, how the attack is carried out, how this virus managed to reach a global scale and how to prevent it. At the end, a brief conclusion is made on the subject.

Keywords: Ransomware, WannaCry, WannaCrypt, Windows.

[1]Acadêmico do Curso Superior em Tecnologia em Sistemas para Internet – Faculdade Alcides Maya. rodrigo.scotti@alcidesmaya.edu.br

[2]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br

[3]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. joao_moreira@alcidesmaya.edu.br

RANSOMWARE WANACRY

Também conhecido como WannaCrypt, WannaCry é um vírus ransomware que criptografa os arquivos e pastas do computador dando a possibilidade da devolução apenas com o pagamento por BitCoin. Na figura abaixo, podemos observar a mensagem de alerta do WannaCry:

O vírus exige o pagamento de U$ 300 BitCoins num prazo de até 3 dias, tendo o valor dobrado após o prazo. Caso o pagamento não seja realizado em até 7 dias, os hackers ameaçam apagar para sempre os arquivos criptografados. Nenhum especialista garante que com a realização do pagamento será liberado os arquivos (COSSETTI, 2017).

Em 2017 este vírus realizou um ataque mundial tendo início no dia 12 de maio de 2017 na Ásia por computadores Windows, infectando 10 mil máquinas a cada hora e sendo parado após 3 dias de ataque.

Ao total, o ransomware se espalhou por 150 países atacando mais de 230 mil computadores (LATTO, 2020). Segundo a página Proof, empresa de segurança de redes, (2020):

> Não se sabe ainda quem foi o paciente zero, mas o primeiro caso do WannaCry que ganhou repercussão na mídia foi quando alguns funcionários da Teléfonica comunicaram a infecção na empresa se comunicou oficialmente algum tempo depois. Seus executivos afirmaram que dentro da sua rede a infecção começou através de máquinas externas de funcionários, conectadas via VPN.

Os cibercriminosos fizeram proveito de uma brecha no sistema operacional Windows para realizar este ataque mundial. Segundo Kaspersky (2020), a empresa Microsoft lançou a correção de segurança que prevenia os sistemas Windows contra esse ransomware, porém muitas pessoas e organizações acabaram não atualizando seus sistemas operacionais, causando a exposição da vulnerabilidade. Um dos fatores que fez com que o vírus se espalhasse rapidamente é por razão que o código do WannaCrypt se espalha como um worm por redes, conexões muito comum em ambientes empresariais (COSSETTI, 2017).

Com a correção da brecha feita pela Microsoft, os computadores que se mantém atualizados possuem a prevenção ao ataque WannaCrypt. Ainda Cossetti (2017) relata que embora os sistemas operacionais sem suporte como Windows XP, Windows 8 e Windows Server 2003 receberam um patch de atualização pois são versões do sistema operacional Windows muito utilizado. por empresas e governos.

CONCLUSÃO

Como abordado neste artigo, podemos concluir a grande necessidade de manter um sistema operacional atualizado e da utilização de sistemas que ainda possuem suporte. Cada versão desatualizada podem conter brechas para que pessoas mal intencionadas consigam tirar proveito das falhas.

Na atual realidade que vivemos, é indispensável o cuidado com a segurança quando realizado o trabalho home office. Muitas vezes é necessário o acesso a VPN da empresa e deve ser realizado a navegação nos sites de forma cautelosa, não abrir e-mails de índole duvidosa. Pois caso seu computador seja atacado, o hacker terá acesso livre a todos os dados de sua empresa.

Vale ressaltar que mesmo sendo em 2017, este tipo de ataque ainda ocorre, mesmo sendo em menor escala. Precisamos tomar todos os cuidados que nos cabem.

REFERÊNCIAS

COSSETTI, Melissa. **WannaCry: tudo que você precisa saber sobre o ransomware.** 2017. Dispnível em <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml>. Acessado dia 23 Out. 2020.

KASPERSKY. 2020. **O que é o ransomware WannaCry?** Disponível em <https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry>. Acessado dia 23 Out. 2020.

LATTO, Nica. 2020. **O que é o WannaCry?** Disponível em <https://www.avast.com/pt-br/c-wannacry>. Acessado dia 23 Out. 2020.

PROOF. 2020. **WannaCry: o primeiro ransomworm na indústria de cibersegurança.** Disponível em <https://www.proof.com.br/blog/wannacry-ransomworm/>. Acessado dia 23 Out. 2020.