Vírus e Malwares

Ryan Karling[1]

[1] Instituto Federal Catarinense (IFC)

[2]Ciência da Computação - Segurança de Sistemas
Instituto Federal Catarinense (IFC) – Videira, SC – Brazil

karlingryan@gmail.com

Resumo. *A criação e expansão da rede mundial de computadores, conhecida como internet, foi possível conectar pessoas a milhares de km de distância, facilidade de acesso à informação e serviços essenciais sem sair de casa, entretanto como tudo no mundo tem uma parte que pode ser explorada, criminosos, que no mundo on-line são chamados de cibercriminosos se aproveitam da rede para infectar e roubar usuários. Estes criam malwares, ferramentas de invasão e roubo de dados para dispositivos conectados na internet.*

Computadores e dispositivos que estão na rede sempre estão vulneráveis a ataques, podendo ser infectados por vírus e Malwares, de início, podem parecer a mesma coisa, mas há diferenças. Pode-se dizer que vírus é um tipo de malware.
Malwares são softwares maliciosos que atacam computadores e redes, como worms, ransomware, spyware, trojans e vírus.
Vírus são malwares que infectam arquivos de sistema e de usuários, se propagam e replicam em arquivos, e em outros dispositivos da rede. Podendo ser realizada uma analogia a um vírus da gripe, que infecta as pessoas e se propaga pelo contato infectando outras pessoas.
A infecção desses programas maliciosos ocorre principalmente de duas formas, e-mails de phishing, e download de programas não oficiais, como torrentes de programas *crackeados*. As infecções também podem ocorrer por sites maliciosos e vulnerabilidades em softwares ou sistemas operacionais.
Todo Malware tem como objetivo danificar a máquina hospedeira, roubar seus dados, e até mesmo interromper serviços, isto depende do tipo de malware que infectou o hospedeiro. Vale ressaltar que cada tipo de software mal intencionado pode causar certo tipo de dano, ou certo tipo de roubo de informações. Sendo alguns deles:

- Vírus: programa que se replica e se espalha por meio da infecção de outros arquivos do sistema.
- Trojans: programa que se disfarça como um software legítimo para enganar o usuário e infectar o sistema.
- Worms: programa que se propaga por meio da rede sem a necessidade de interação do usuário.
- Ransomware: programa que criptografa os dados do sistema e exige um resgate para liberá-los.
- Spyware: programa que monitora as atividades do usuário sem o seu conhecimento ou consentimento.

- Adware: programa que exibe anúncios indesejados para o usuário.
- Rootkits: programa que se esconde no sistema para evitar a detecção de outras ameaças.

Para adicionar camadas de segurança e se manter mais protegido, deve-se manter o sistema operacional, e seus softwares sempre atualizados. Utilizar um bom software de antivírus, de preferência de código livre. Baixar programas e aplicativos somente de fontes confiáveis, como portal do desenvolvedor, ou loja oficial do sistema. Realize backups remotos regularmente, e sempre use boas práticas de senhas.
Vale lembrar que manter-se atualizado sobre novos ataques e como ocorrem, não clicar em links suspeitos, principalmente e-mails, são práticas que reforçam o cuidado do usuário. A conscientização pode parecer banal, mas ajuda o usuário que está na ponta, não estar vulnerável a ataques que entram por meio de engenharia social, como um e-mail de phishing por exemplo.
Em maio de 2017, devido a uma vulnerabilidade no protocolo SMB *(Server Message Block)* do Windows, milhões de máquinas ao redor do mundo foram infectadas e propagaram o ransomware *Wannacry*, que além de criptografar todas elas e cobrar resgate em *bitcoins* para a chave de descriptografia, parou vários serviços ao redor do planeta. O ataque também causou um tremendo prejuízo financeiro, não apenas pelo resgate, mas pela interrupção de serviços e organizações.