UNIVERSIDADE DO VALE DO TAQUARI
CURSO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

CAVALO DE TROIA

Alessandra Elisa Santana

Lajeado, 08 de setembro de 2022

Cavalo de Troia (Trojan Horse ou Trojan)

Cavalo de Troia é um malware (programa malicioso) disfarçado de software legítimo, que finge ser inofensivo para que as pessoas baixem. Ele oculta o malware em algum arquivo que pode ser baixado, podendo ser qualquer coisa, desde um anexo recebido por e-mail até um jogo, música ou filme. Uma vez feito o download, o Trojan estará no sistema e poderá realizar as funções pelas quais foi programado, como espionagem, exclusão, cópia ou modificação de dados.

Existem diversos tipos desse malware e cada um deles possui um objetivo específico, além disso, podem estar em computadores ou dispositivos móveis. Um detalhe importante é que o cavalo de Troia não é como um vírus comum que se auto replica, como os worms, por exemplo. É preciso que ele seja baixado e instalado no sistema. Não criam réplicas de si mesmos (motivo pelo qual não são considerados vírus). Alguns cavalos de Troia são programados para se autodestruir após um certo período de tempo.

Origem do nome

O nome do malware cavalo de Troia faz referência a guerra de Troia, quando os gregos, simulando uma redenção, ofereceram como presente aos rivais troianos um grande cavalo de madeira. Achando que os gregos haviam desistido da guerra, os troianos decidiram levar o grande cavalo para dentro da cidade, quebrando parte da muralha para conseguir realizar o feito. Uma vez introduzidos, os soldados gregos saíram de dentro do cavalo e abriram os portões da fortaleza, permitindo que mais soldados entrassem e então destruíssem a cidade.

O que os cavalos de Troia fazem?

Os cavalos de Troia precisam ser baixados no sistema, e podem possuir diversas funções diferentes, dependendo para o que foram criados.

- **Criação de backdoors:** Fazem alterações no sistema de segurança, para que outros malwares ou cibercriminosos possam invadi-lo.
- **Espionagem:** Aguardam até o usuário utilizar senhas online ou inserir dados de cartões, para posteriormente enviar esses dados ao seu controlador.
- **Tomar conta do computador:** Muitas vezes os cibercriminosos não estão interessados em saber os dados do usuário, mas sim utilizar o computador como escravo em uma rede que está sob o seu controle.
- **Envio de SMS pagas:** No caso de estar no dispositivo móvel, é capaz de fazer seu celular enviar mensagens pagas para determinados números.

Formas de se proteger de um cavalo de Troia

- Uso de antivírus confiável;
- Manter o Sistema Operacional atualizado;
- Ter cuidado ao navegar na internet e acessar sites desconhecidos;
- Ter senhas únicas e complexas para as contas;
- Fazer backups frequentes dos seus dados;
- Avaliar o desempenho da máquina;
- Evitar downloads de arquivos piratas;
- Verificar os programas instalados na máquina;
- Escanear o dispositivo/sistema com frequência atrás de malwares;
- Não clicar em links suspeitos.

Mokotio: trojan bancário brasileiro

Reportagem retirada do site:
https://olhardigital.com.br/2021/11/03/seguranca/mekotio-trojan-bancario-brasileiro-faz-estrago-no-resto-do-mundo/

Na segunda metade de 2021 houveram cerca de 100 ataques cibernéticos utilizando uma nova versão do trojan Mokotio, responsável por uma série de fraudes digitais

bancárias em 2015. Pesquisadores descobriram o golpe distribuído em campanhas de phishing, com emails maliciosos.

Aparentemente a versão do Mokotio estava em operação desde junho de 2021, quando as forças de segurança da Espanha prenderam 16 criminosos realizando lavagem de dinheiro adquiridos pelo trojan. Em uma investigação inicial, a Guarda Civil Espanhola estimou um roubo de 3,5 bilhões de euros usando o programa malicioso.

Uma análise da Kaspersky aponta que o Mekotio faz parte da Tetrade — um dos quatro maiores famílias de trojans bancários “made in Brazil” que atingiram popularidade no exterior. A complexidade destes programas fez com que o nosso país entrasse na rota de exportação de malwares para o exterior.

As quatro famílias — Guildma, Javali, Melcoz (da qual o Mekotio faz parte) and Grandoreiro — são todas conhecidas por serem altamente complexas e burlarem sistemas de segurança com táticas de ofuscação. A natureza modular dos malwares também permitia que sua ação fosse reprogramada para agir diretamente em bancos de nacionalidades específicas.

Referências

Cavalo de troia (computação)

https://pt.wikipedia.org/wiki/Cavalo_de_troia_(computa%C3%A7%C3%A3o). Acesso em: 08 set. 2022.

O Que são os Vírus Cavalo de Troia e Como se Proteger Deles

https://www.hostinger.com.br/tutoriais/cavalo-de-troia-virus. Acesso em: 08 set. 2022.

O que é um Cavalo de Troia? É malware ou vírus?

https://www.avg.com/pt/signal/what-is-a-trojan. Acesso em: 08 set. 2022.