



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER
V12 – EC-COUNCIL

Progresso do curso

Módulo 6. System Hacking

Módulo 7. Malware Threats

Módulo 8. Sniffing

Módulo 9. Social Engineering

Módulo 10. Denial-of-Service (DoS)

Conceitos de Malware:

Malware, abreviação de software mal-intencionado, é um software utilizado para interromper as operações do computador, recolher informações sensíveis, ter acesso aos sistemas privados, ou exibir publicidade indesejada. Um malware é definido pela sua intenção maliciosa, agindo contra as exigências do usuário do computador.

Um malware pode ser furtivo, destinado a roubar informações ou espionar os usuários do computador por um longo período sem o seu conhecimento ou pode ser projetado para causar danos, muitas vezes como sabotagem (por exemplo, o Stuxnet), ou para extorquir pagamento (CryptoLocker). "Malware" é um termo utilizado para se referir a uma variedade de formas de softwares hostis ou intrusivos, incluindo vírus, worms, cavalos de tróia, ransomware, spyware, adware, scareware e outros programas maliciosos.

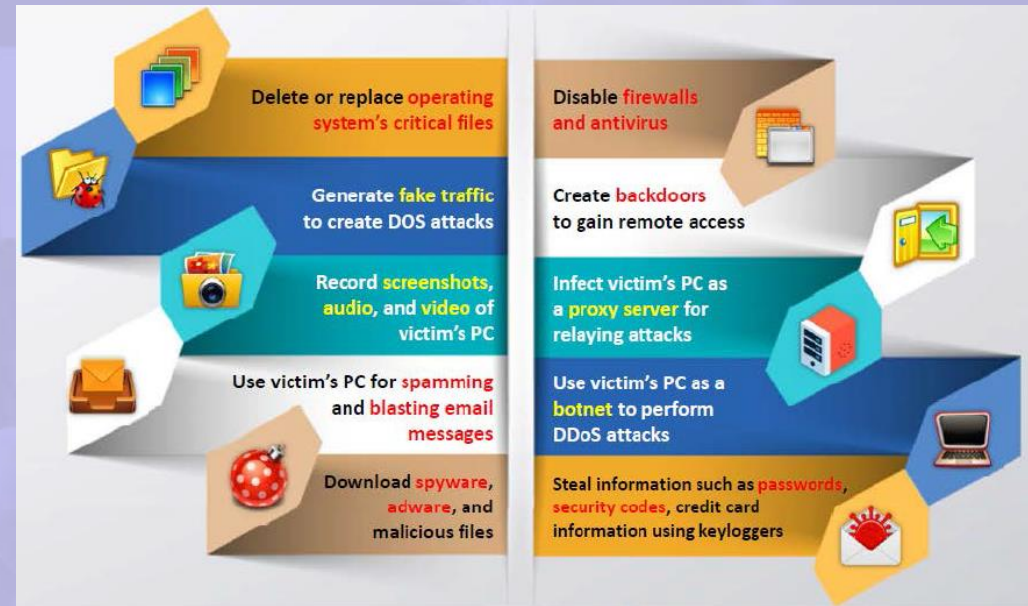
1	Instant Messenger applications	6	Browser and email software bugs
2	IRC (Internet Relay Chat)	7	NetBIOS (FileSharing)
3	Removable devices	8	Fake programs
4	Attachments	9	Untrusted sites and freeware software
5	Legitimate "shrink-wrapped" software packaged by a disgruntled employee	0	Downloading files, games, and screensavers from Internet sites

CEHv12 (ANSI)

07.Malware Threats

Trojan

- Um cavalo de Tróia de computador é usado para entrar no computador da vítima sem ser detectado, concedendo o atacante acesso irrestrito aos dados armazenados no computador e causando imensos danos à vítima.
- Por exemplo, um usuário baixa o que parece ser um filme ou um arquivo de música, mas quando ele executa o arquivo ele desencadeia um programa malicioso que pode apagar o disco do usuário desavisado e enviar o número de seu cartão de crédito e senhas para o atacante. Um cavalo de Tróia também pode ser envolvido em um programa legítimo, o que significa que este programa pode ter funcionalidades escondidas que o usuário desconhece.



	CD-ROM drawer opens and closes by itself		Abnormal activity by the modem, network adapter, or hard drive
	Computer browser is redirected to unknown pages		The account passwords are changed or unauthorized access
	Strange chat boxes appear on victim's computer		Strange purchase statements appear in the credit card bills
	Documents or messages are printed from the printer themselves		The ISP complains to the victim that his/her computer is IP scanning
	Functions of the right and left mouse buttons are reversed		People know too much personal information about a victim

Portas comuns utilizadas por Trojans

Portas comuns utilizadas por Trojans



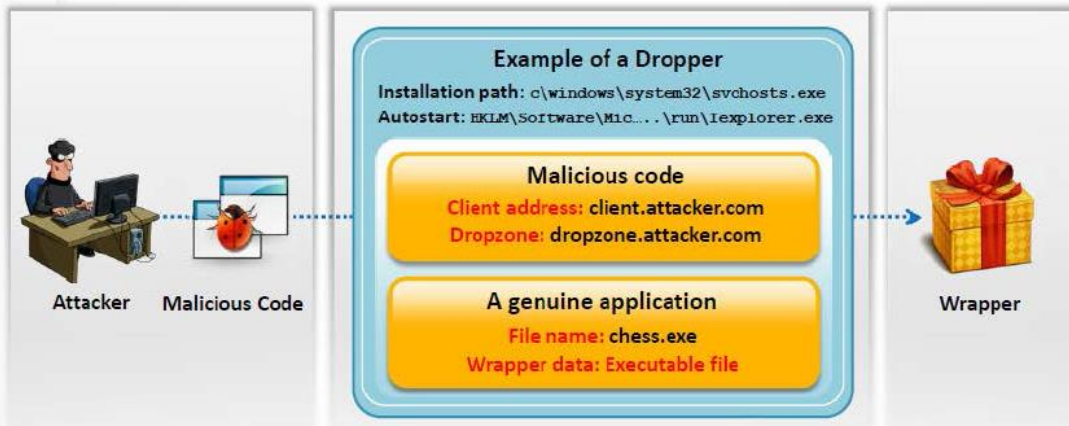
Indicadores de um ataque com trojan

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5589	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOffice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Como infectar um sistema com um Trojan

01 Create a new Trojan packet using a **Trojan Horse Construction Kit**

02 Create a **dropper**, which is a part in a trojanized packet that installs the **malicious code** on the target system



03 Create a wrapper using **wrapper tools** to install Trojan on the victim's computer






04 Propagate the Trojan

05 Execute the dropper

06 Execute the damage routine

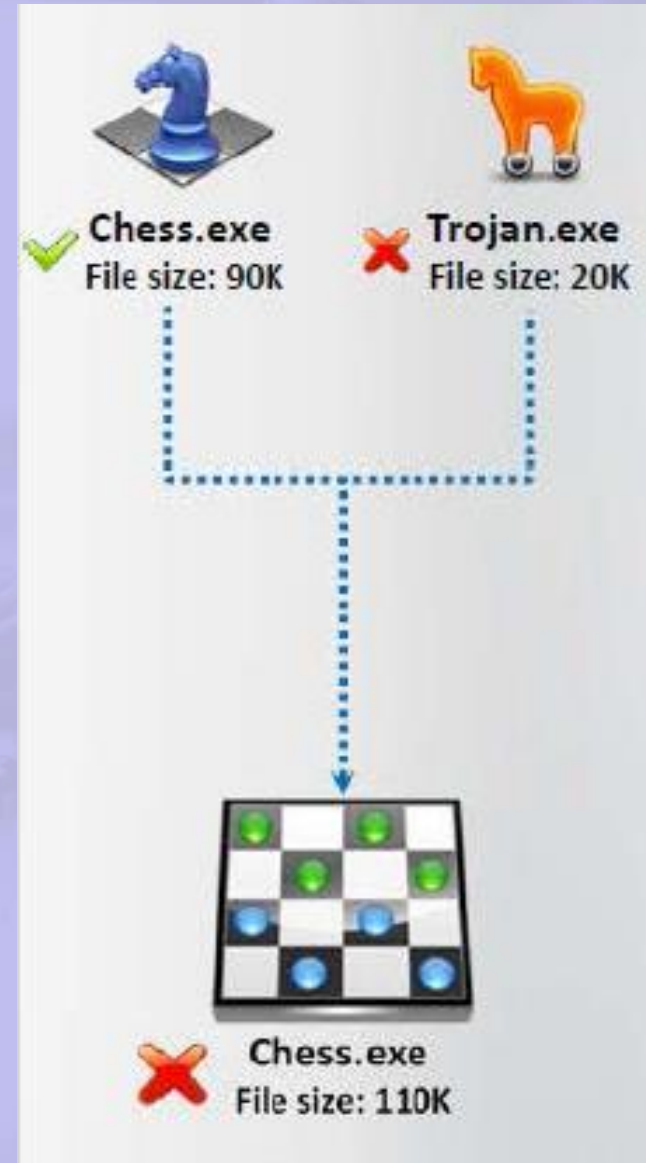


Técnicas de evasão de antivírus

01	Break the Trojan file into multiple pieces and zip them as single file	
02	ALWAYS write your own Trojan, and embed it into an application	
03	Change Trojan's syntax: <ul style="list-style-type: none">• Convert an EXE to VB script• Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)	
04	Change the content of the Trojan using hex editor and also change the checksum and encrypt the file	
05	Never use Trojans downloaded from the web (antivirus can detect these easily)	

Wrappers

- Wrappers são utilizados para vincular o executável Trojan com uma aplicação .exe genuína, como jogos ou aplicações de escritório. Quando o usuário executa o exe malicioso, ele primeiro instala o Trojan em segundo plano e em seguida, executa o aplicativo genuíno em primeiro plano.
- O atacante pode comprimir qualquer binário (DOS/WIN) com ferramentas como petite.exe. Esta ferramenta descompacta um arquivo exe em tempo de execução. Isso torna possível o Trojan entrar virtualmente sem ser detectado, uma vez que a maioria dos softwares antivírus não são capazes de detectar as assinaturas no arquivo.



Tipos de Trojan

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- GUI Trojan
- FTP Trojan
- E-mail Trojan
- Remote Access Trojan
- Proxy Server Trojan
- Botnet Trojan
- Covert Channel Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan

Command Shell

- O command shell trojan dá acesso remoto ao shell do host alvo. O server do Trojan é instalado na máquina da vítima, onde é aberta uma porta para o atacante se conectar. O client do trojan é instalado na máquina do atacante para ele se conectar na máquina da vítima.
- As ferramentas listadas abaixo são trojans do tipo command shell:
- Netcat
- MoSucker
- Jumper
- Biodox

- Command shell Trojan gives **remote control of a command shell** on a victim's machine
- Trojan server is installed on the victim's machine, which **opens a port for attacker** to connect. The client is **installed on the attacker's machine**, which is used to launch a command shell on the victim's machine

```
C:\>nc.exe -h
[vl.10 NT]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [options] [hostname] [port]
options:
-d          detach from console, stealth mode
-e prog     inbound program to exec [dangerous!!]
-g gateway  source-routing hop point[s], up to 8
-G num      source-routing pointer: 4, 8, 12, ...
-h          this craft
-i secs     delay interval for lines sent, ports scanned
-l          listen mode, for inbound connects
-L          listen harder, re-listen on socket close
-n          numeric-only IP addresses, no DNS
-o file     hex dump of traffic
```



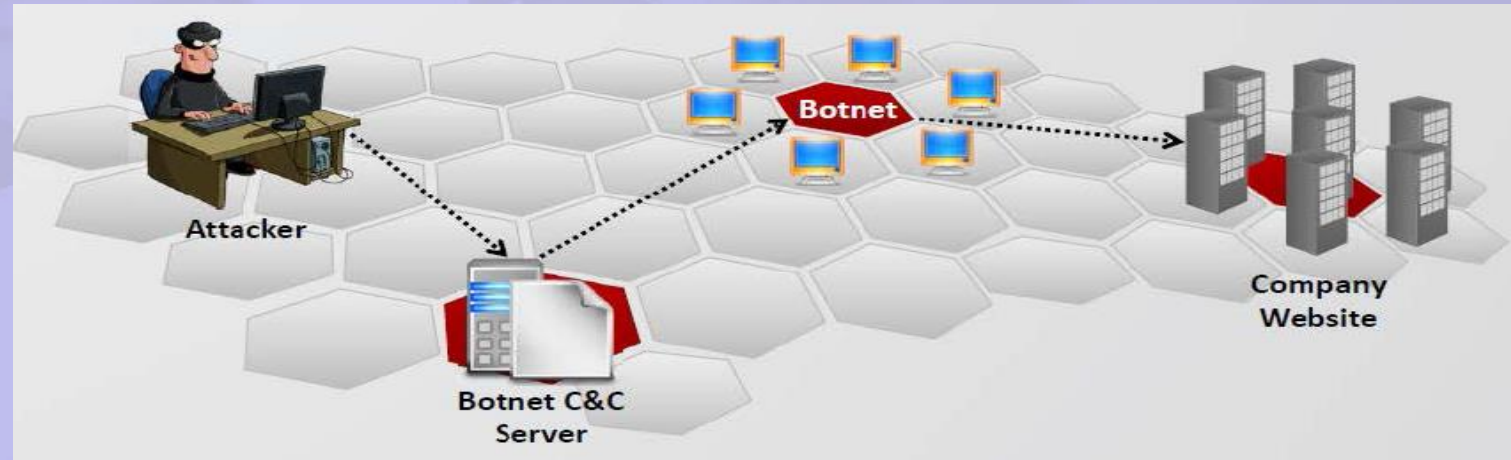
Defacement

- Os Trojans do tipo defacement, uma vez instalados no sistema podem destruir ou mudar o conteúdo inteiro das informações e/ou aplicações instaladas. Este tipo de trojan é mais perigoso quando os alvos são servidores web, eles mudam o conteúdo dos arquivos HTML o que resulta na alteração da página no site. Quando os alvos são sistemas e-business, os estragos são ainda maiores.
- Ele permite que visualize e edite quase todos os aspectos de um programa Windows compilado. Desde os menus até as caixas de diálogos. Recursos de edição permitem que você visualize, edite, extraia e substitua strings, bitmaps, logos e ícones de qualquer programa Windows.



Botnet

- Um trojan do tipo botnet é uma coleção de programas robôs que são executados automaticamente. Isso se refere a um conjunto de máquinas comprometidas rodando programas sobre o comando do mesmo servidor de comando e controle (C&C). O atacante pode controlar todas essas máquinas remotamente, essas máquinas infectadas por worms ou trojans podem enviar spam, vírus ou executar ataques de negação de serviço. Exemplos são: Illusion Bot e NetBot Attacker.



Proxy Server

- O trojan proxy server é um tipo de trojan que personaliza o sistema alvo para atuar como um servidor proxy. Quando esse trojan infecta o usuário ele inicia um serviço de proxy oculto na máquina do usuário. O atacante pode usar esse tipo de trojan para realizar outros ataques e ter a origem do ataque como o endereço do computador infectado.
- Exemplos são:
- W3bPrOxy
- Tr0j4nCr34t0r



FTP

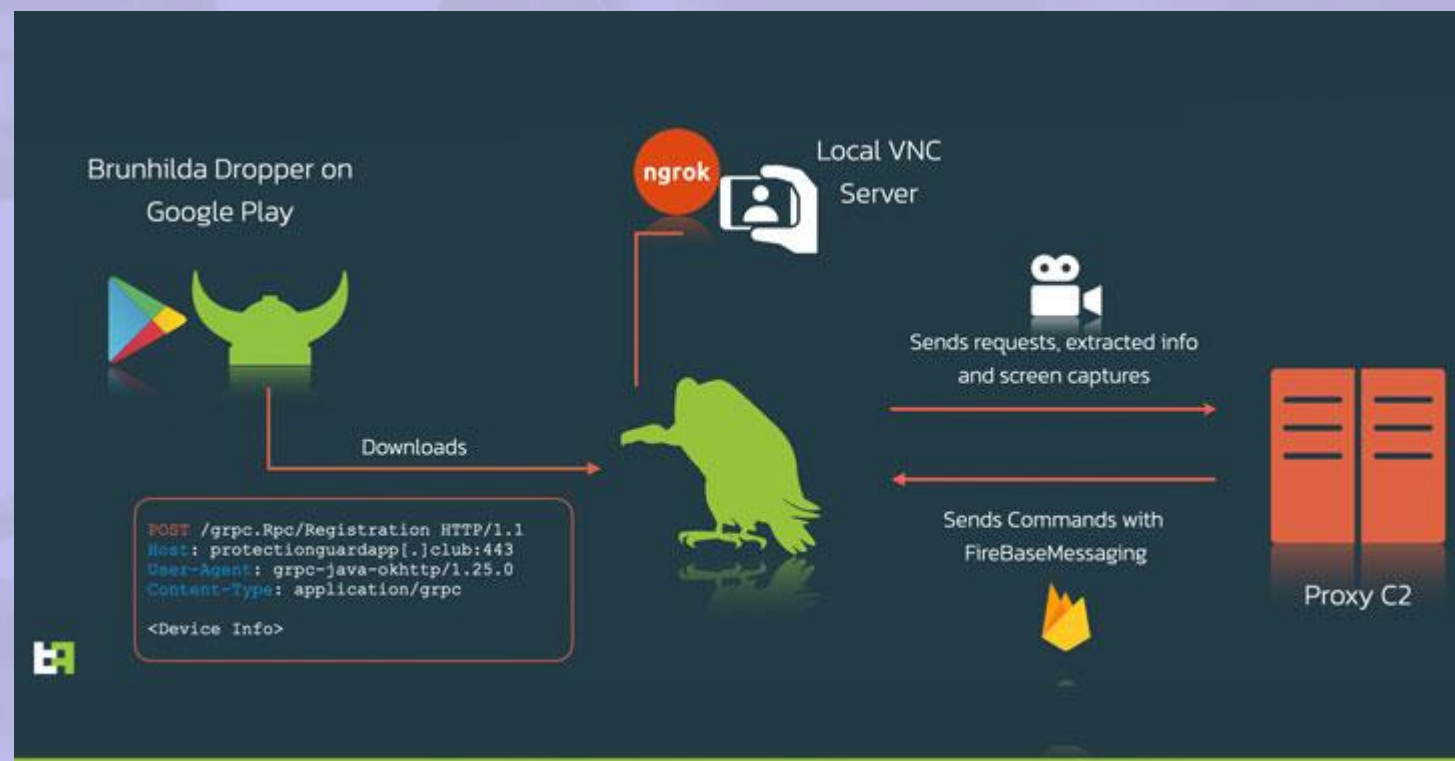
- O trojan FTP é designado para abrir a porta 21 na máquina do usuário e ter acesso ao sistema através do protocolo FTP. Ele instala um serviço FTP na máquina da vítima. Normalmente depois que o atacante tem esse nível de acesso ele instala malwares na máquina da vítima para expandir suas possibilidades dentro do sistema. Um exemplo desse tipo de trojan é o TinyFTP.



VNC

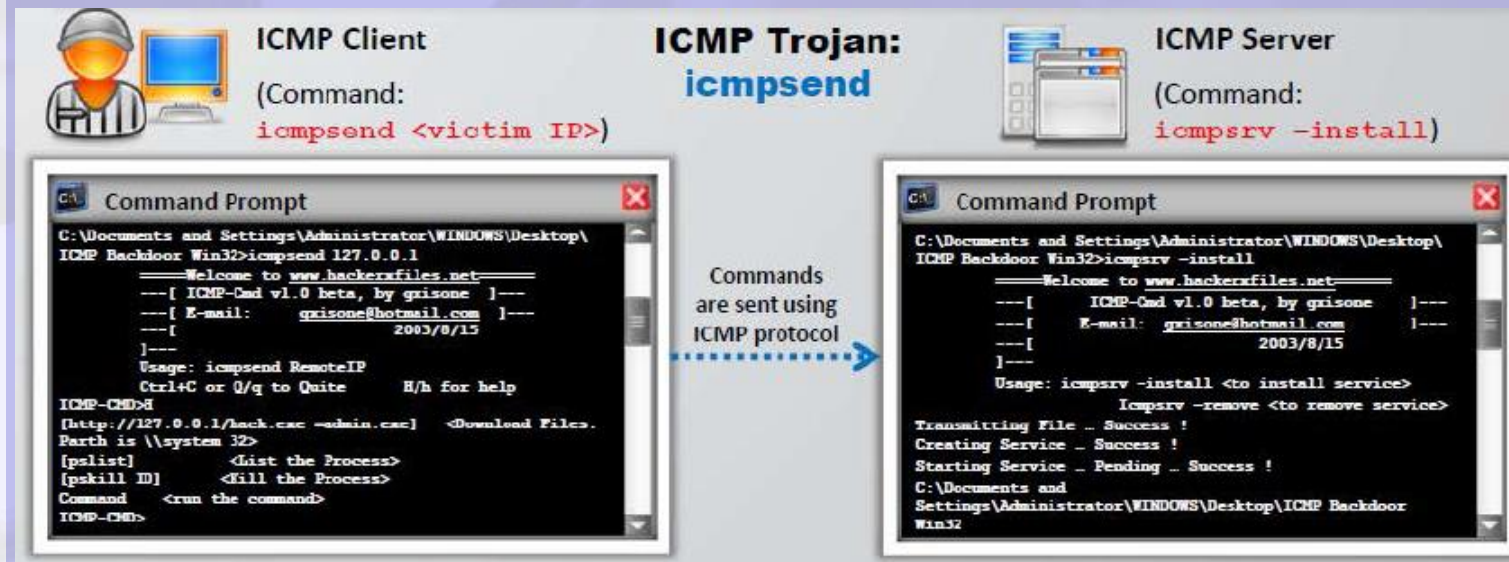
- Esse tipo de trojan permite que um atacante use o sistema alvo como um servidor VNC. Esse tipo de trojan não vai ser detectado por um antivírus depois que for executado porque o serviço VNC é considerado uma funcionalidade e não uma ameaça. O WinVNC e VNC Stealer, são exemplos desse tipo de trojan.

Android Malware Uses VNC to Spy and Steal Passwords from Victims



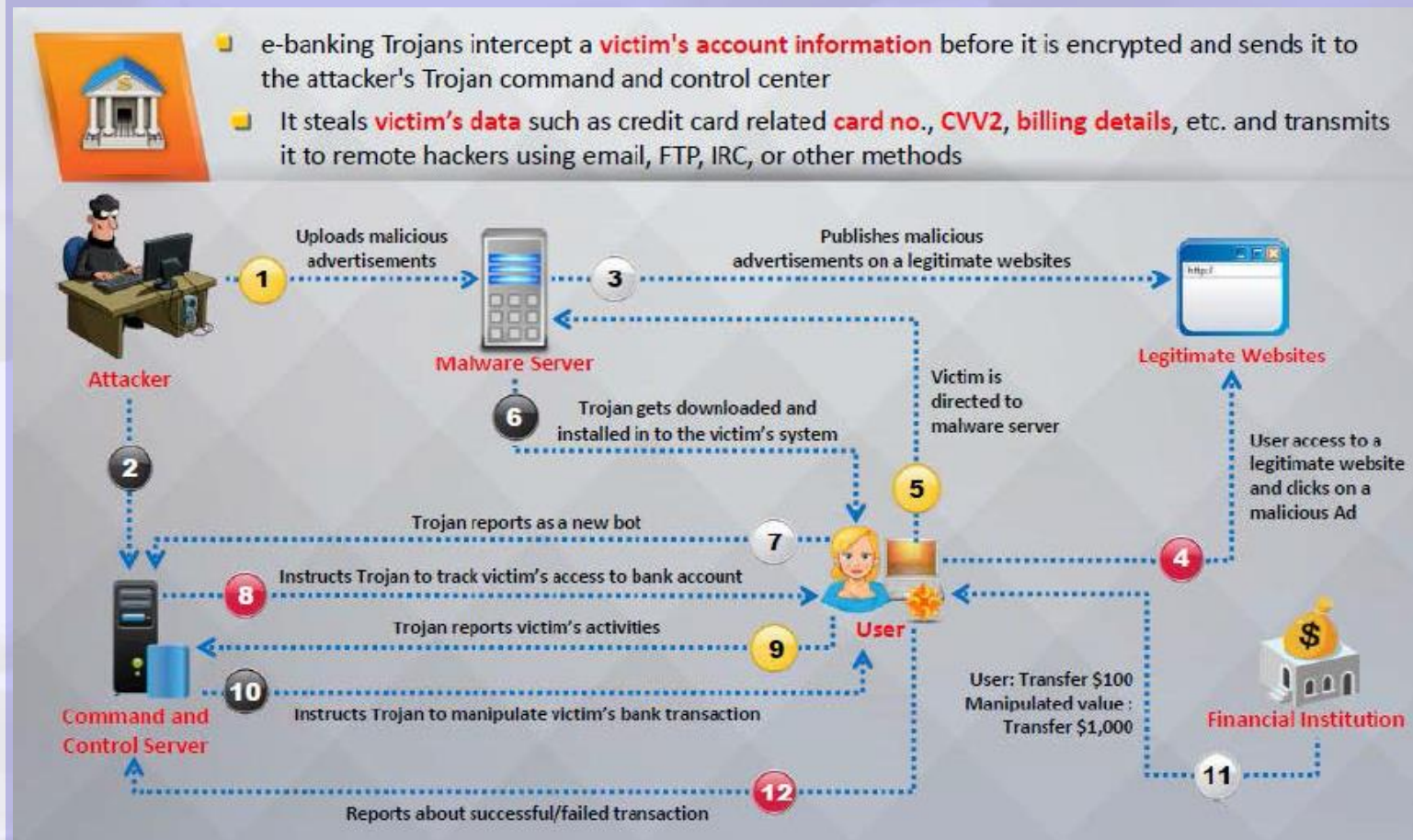
ICMP

- O conceito de tunelamento ICMP é simples, desde que o tunelamento de informações arbitrárias na parte de dados de pacotes ICMP_ECHO e ICMP_ECHO_REPLY seja possível. Dispositivos de rede não filtram o conteúdo do tráfego ICMP_ECHO, tornando o uso deste canal atraente para hackers.



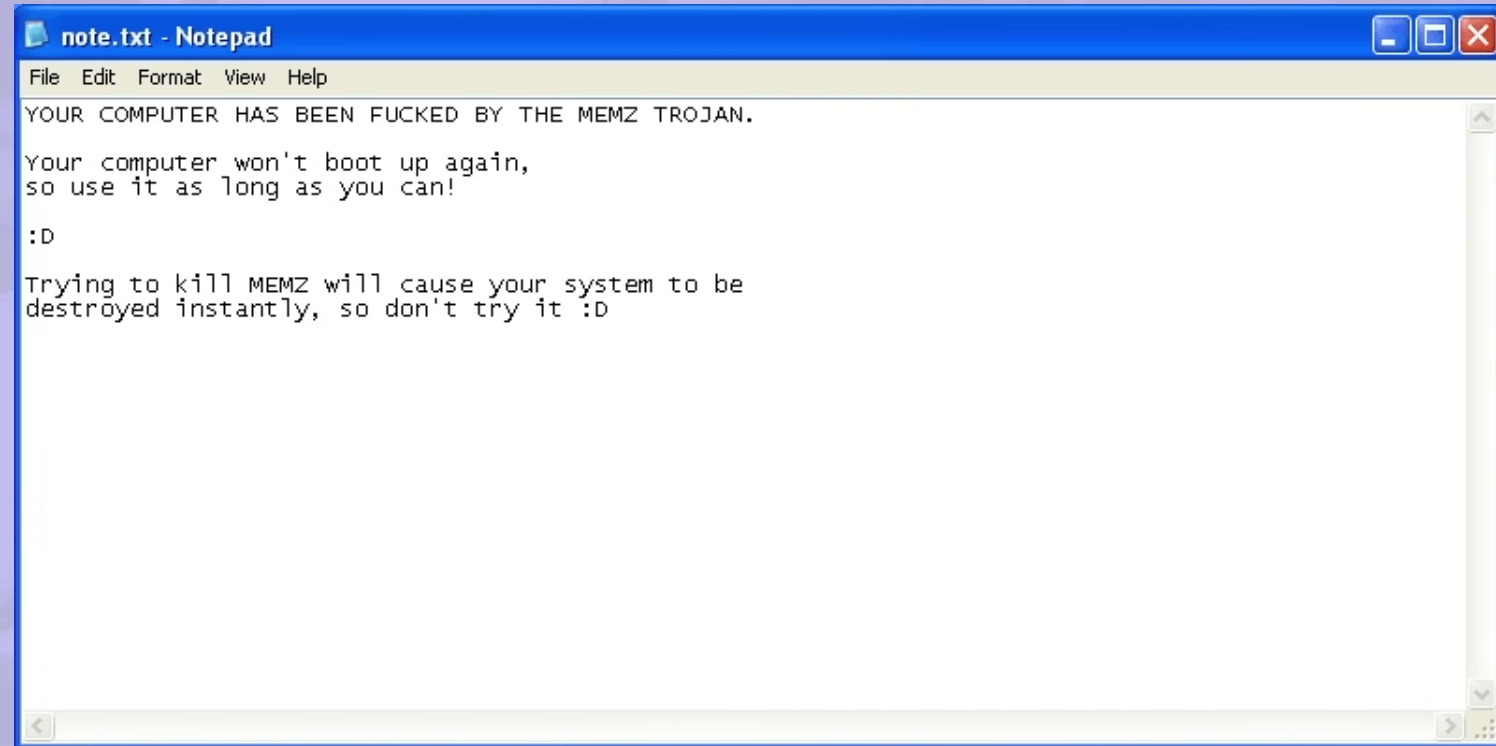
E-banking

- Trojans E-banking são muito perigosos e tornaram-se uma grande ameaça para as transações bancárias realizadas online. Este Trojan é instalado no computador da vítima, quando ele clica no anexo de e-mail ou clica em algum anúncio. O cavalo de Tróia é pré-programado com um intervalo mínimo e máximo para roubar. Por isso, não retira todo o dinheiro do banco.
- Em seguida, o Trojan cria screenshots do extrato da conta bancária; as vítimas não estão cientes deste tipo de fraude e pensam que não há variação no seu saldo bancário, a menos que verifique o saldo de outro sistema ou a partir de máquinas ATM.



Destrutivo

- O Trojan M4sT3r é projetado exclusivamente para destruir ou apagar arquivos do computador da vítima. Os arquivos são automaticamente eliminados pelos trojans, que podem ser controlados pelo atacante ou pode ser pré-programados como uma bomba para executar uma tarefa específica em uma determinada data e hora. Quando executado, este Trojan destrói o sistema operacional. Este Trojan formata todas as unidades locais e de rede.



Data Hiding

- Trojans criptográficos criptografam os dados presentes no computador da vítima e os torna em dados completamente inutilizáveis.
- Os atacantes exigem um resgate ou forçam as vítimas a fazer compras a partir de suas lojas on-line em troca da senha para desbloquear os arquivos.



Vírus

Os vírus de computador têm o potencial de causar estragos nos negócios e em computadores pessoais. Em todo o mundo, a maioria das empresas foi infectada em algum momento. Um vírus é um programa auto replicante que produz o seu próprio código, anexando cópias dele em outros códigos executáveis.

Este vírus opera sem o conhecimento ou o desejo do usuário. Como um vírus real, um vírus de computador é contagioso e pode contaminar outros arquivos. No entanto, os vírus podem infectar máquinas fora apenas com a ajuda de usuários. Alguns vírus afetam computadores logo que o seu código é executado; outros vírus permanecer latente até que uma circunstância lógica pré-determinada seja atendida. Existem três categorias de programas mal-intencionados:

- Trojans e rootkits
- Vírus
- Worms

Funcionamento dos Vírus

- Os vírus atacam o sistema do host de destino usando vários métodos. Eles se ligam aos programas e se transmitem para outros programas, fazendo uso de determinados eventos. Os vírus precisam de tais eventos para se instalar uma vez que não podem:
- Iniciar automaticamente
- Infectar outro hardware
- Causar dano físico a um computador
- Se transmitir utilizando arquivos não executáveis.

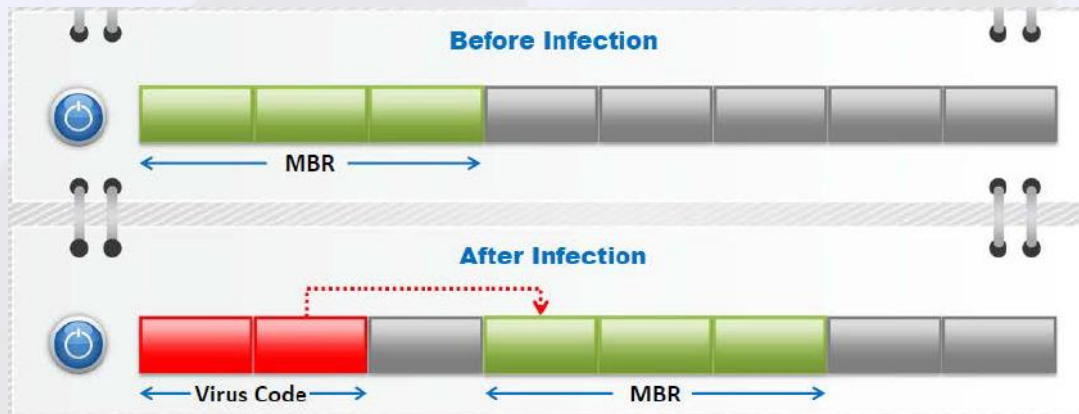
Tipos de vírus



Vírus

Vírus de Boot Sector

Os alvos mais comuns de um vírus são os setores do sistema, que não são nada, mas o Master Boot Record e os setores DOS Boot Record são setores fundamentais para o sistema. Estas são as áreas do disco que são executadas quando o PC é inicializado. O Disk Killer e o Stone Virus são exemplos desse tipo de vírus.



Vírus de arquivos

Arquivos executáveis são infectados por vírus de arquivo, uma vez que eles inserem seu código dentro de um arquivo original e são executados. Vírus de arquivos são maiores em número, mas eles não são os mais encontrados. Eles infectam os arquivos de diversas formas e podem ser encontrados em um grande número de tipos de arquivos.



Vírus

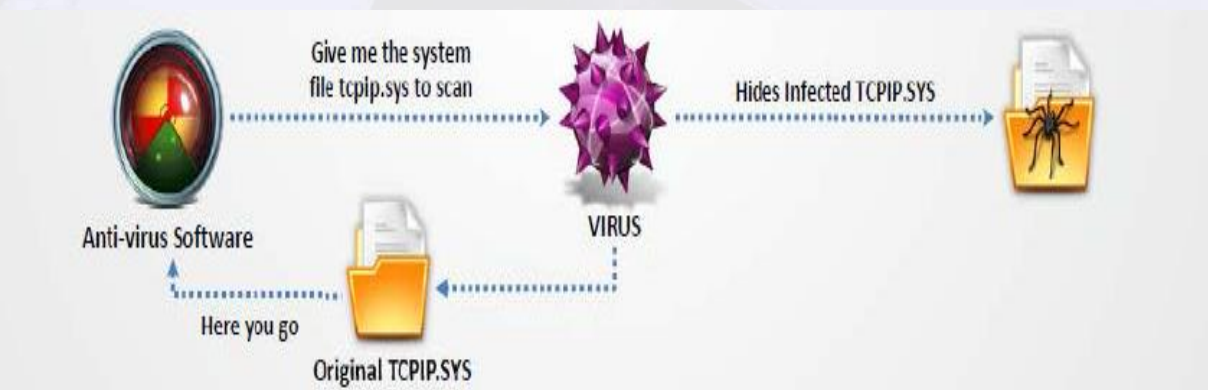
Vírus de Macro

O programa Microsoft Word ou um aplicativo similar pode ser infectado por um vírus de computador chamado vírus de macro, que executa automaticamente uma sequência de ações quando o aplicativo é acionado. Os vírus de macro são um pouco menos prejudicial do que outros tipos. Eles geralmente se espalham através de e-mails.



Vírus Stealth/Tunneling

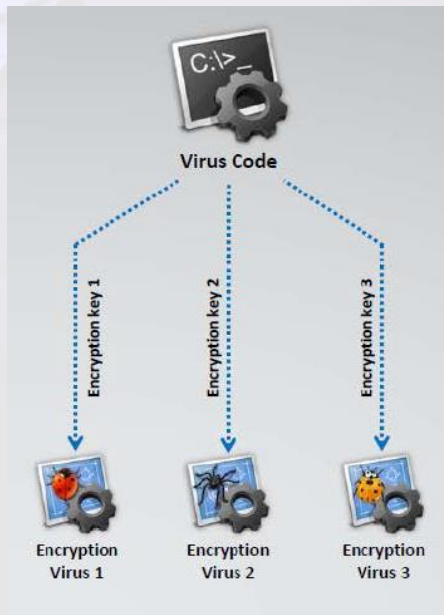
Estes vírus tentam se esconder dos programas antivírus alterando de forma ativa e corrompendo as interrupções das chamadas de serviço quando eles estão sendo executados. Os pedidos para executar operações no que diz respeito a estas interrupções de chamadas de serviço são substituídas por código do vírus. Estes vírus declaram informações falsas para ocultar sua presença dos programas antivírus.



Vírus

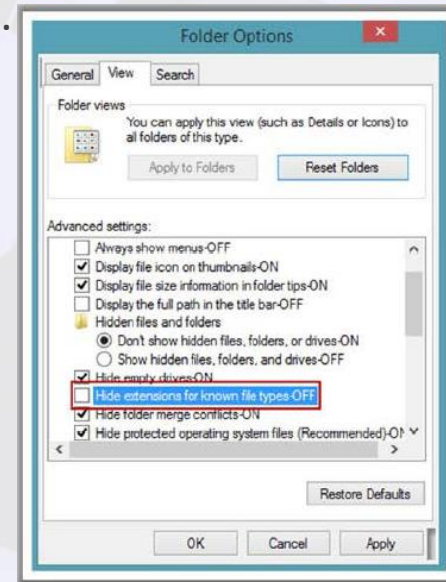
Vírus Criptográficos

Este tipo de vírus é constituído por uma cópia criptografada do vírus e um módulo de decodificação. O módulo de descryptografia permanece constante, ao passo que as diferentes teclas são utilizadas para criptografar.



Vírus de Extensão de Arquivos

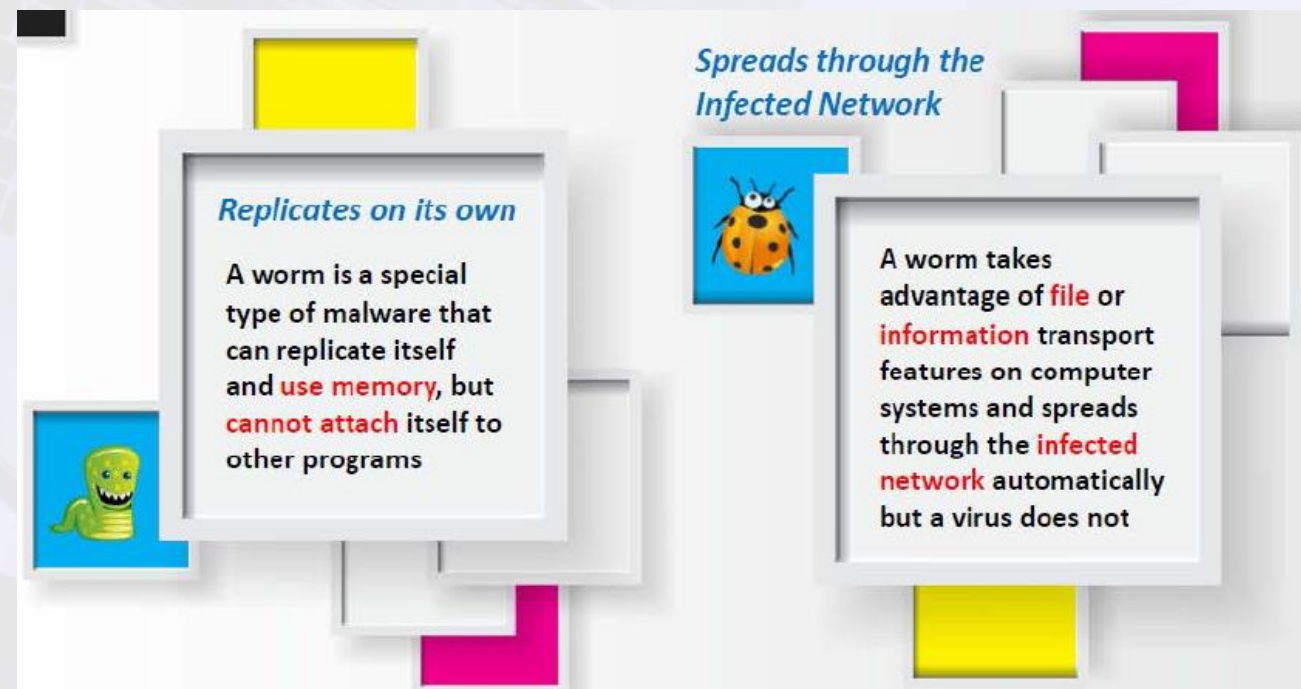
Vírus de extensão de arquivos alteram as extensões dos arquivos. Arquivos TXT são seguros, pois indicam um arquivo de texto puro. Se as extensões dos arquivos do seu computador forem apagadas e alguém lhe enviar um arquivo chamado BAD.TXT.VBS, você verá apenas BAD.TXT.



Worm

Worms de computador são programas maliciosos que se replicam, executam e se espalham por conexões de rede independente da interação humana. A maioria dos worms são criados apenas para replicar e se espalhar através de uma rede, consumindo recursos de computação disponíveis; no entanto, alguns worms transportar um payload para danificar o sistema do host.

Um worm não requer um hospedeiro para se replicar, embora em alguns casos pode-se argumentar que o hospedeiro de um worm é a máquina que tenha infectado. Os Worms são um subtipo de vírus. Worms foram considerados principalmente um problema de mainframe, mas depois que a maioria dos sistemas do mundo foram interligados, worms foram direcionados contra o sistema operacional Windows, e foram enviados por e-mail, IRC, e outras funções de rede.



Engenharia Reversa de Malware

Sheep dip refere-se à análise de arquivos suspeitos e mensagens recebidas por malware. Este computador sheep dipped é isolado de outros computadores na rede para bloquear quaisquer vírus de entrar no sistema. Antes de este procedimento ser realizado, todos os programas baixados são salvos em mídia externa, como CD-ROMs ou disquetes.

Um computador sheep dip é instalado com monitores de porta, monitores de arquivos, monitores de rede e software antivírus e se conecta a uma rede somente sob condições estritamente controladas.

Passo 1: Realizar análise estática quando o malware está inativo

Passo 2: Coletar informações sobre:

Valores de cadeia encontrados no binário com a ajuda de ferramentas de extração de strings tais como BinText

A técnica de compressão e empacotamento usadas com a ajuda de ferramentas de compressão e descompressão, tais como UPX

Passo 3: Configurar a conexão de rede e verificar se ela não está dando quaisquer erros

Passo 4: Execute o vírus e monitore as ações de processo e informações do sistema com a ajuda de ferramentas de monitoramento de processo como o Process Monitor e Process Explorer

Passo 5: Registrar informações de tráfego de rede usando ferramentas de armazenamento de pacotes monitoramento de conteúdo tais como NetResident e TCPView

Passo 6: Determinar os arquivos adicionados, processos gerados e alterações no registro com a ajuda de ferramentas de monitoramento do registro, como o Regshot

Passo 7: Coletar as seguintes informações utilizando ferramentas de depuração como OllyDbg e ProcDump:

- As solicitações de serviço
- As tentativas de conexões de entrada e de saída
- Informações das tabelas do DNS



Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.