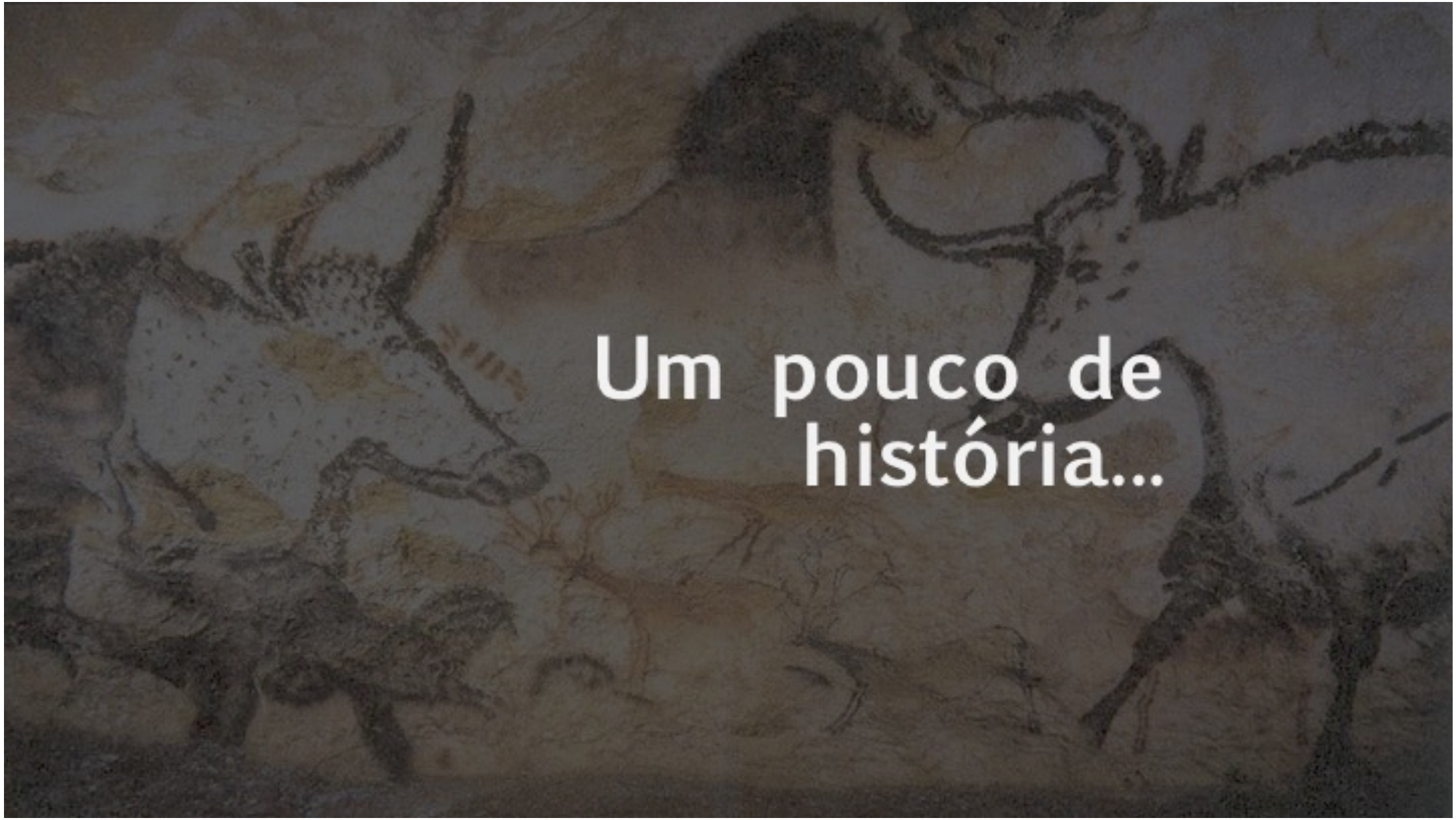
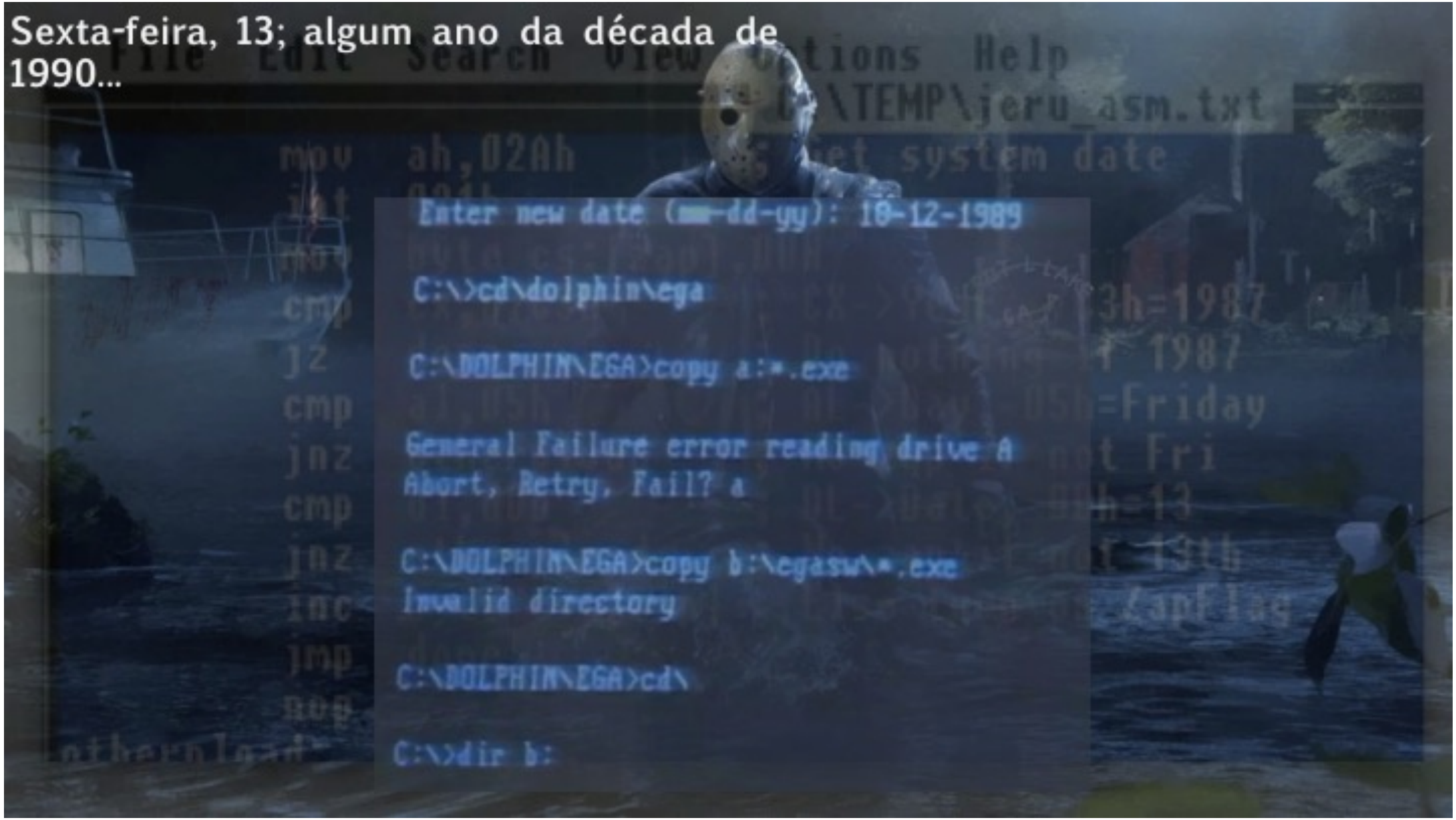
6. Malware

Software malicioso e indesejado


Um pouco de
história...


Sexta-feira, 13; algum ano da década de 1990...
Enter new date (mm-dd-yy): 10-12-1989
C:\>cd\dolphin\ega
C:\DOLPHIN\EGA>copy a:*.exe
General Failure error reading drive A
Abort, Retry, Fail? a
C:\DOLPHIN\EGA>copy b:\egasw*.exe
Invalid directory
C:\DOLPHIN\EGA>cd\
C:\>dir b:

Sibéria, 1982

Cyberwar

War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | From the print edition

AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."

Síria, 2007

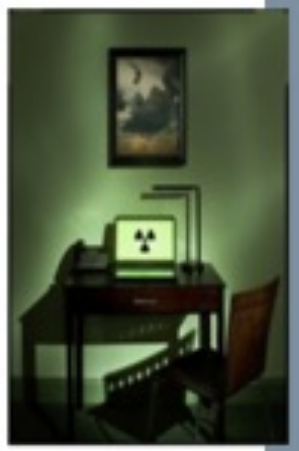
ANNALS OF WAR

SEPTEMBER 17, 2012 ISSUE

THE SILENT STRIKE

How Israel bombed a Syrian nuclear installation and kept it secret.

BY DAVID MAKOVSKY



The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.
PHOTOILLUSTRATION BY DAN WINTERS.

In the first days of March, 2007, agents from the Mossad, the Israeli intelligence agency, made a daring raid on the Vienna home of Ibrahim Othman, the head of the Syrian Atomic Energy Commission. Othman was in town attending a meeting of the International Atomic Energy Agency's board of governors, and had stepped out. In less than an hour, the Mossad operatives swept in, extracted top-secret information from Othman's computer, and left without a trace.

Irã, 2010


Image Credit: Digital Globe - ISIS
Image Date: 2 January 2006
Approximate location of underground cascade halls for the Fuel Enrichment Plant
Hidden entrance to underground facilities
Location of the Pilot Fuel Enrichment Plant
* = New construction

O que esses exemplos têm em comum?

Software... fazendo o que não deveria

Malicious Software

Malicious Software

Malware

Conceitos gerais

Malware

- Programas que exploram vulnerabilidades do sistema
- Conhecido como software malicioso ou *malware*
  - Fragmentos de programas que precisam de um programa host
    - ex. vírus, bombas lógicas, e backdoors
  - Programas autônomos independentes
    - ex. vermes, bots
  - Se replicam ou não
- Ameaças sofisticadas aos sistemas computacionais

Tipos de Malware: parasitas vs autônomos

- Parasitas
  - Precisam de um hospedeiro para existir
  - Rotinas e fragmentos de programas que se anexam a aplicações maiores
  - Exemplos: vírus, backdoors, bombas lógicas
- Independentes/Autônomos
  - Existem por si mesmos
  - Programa completo com todas as funcionalidades necessárias para seus objetivos
  - Exemplos: worms e bots

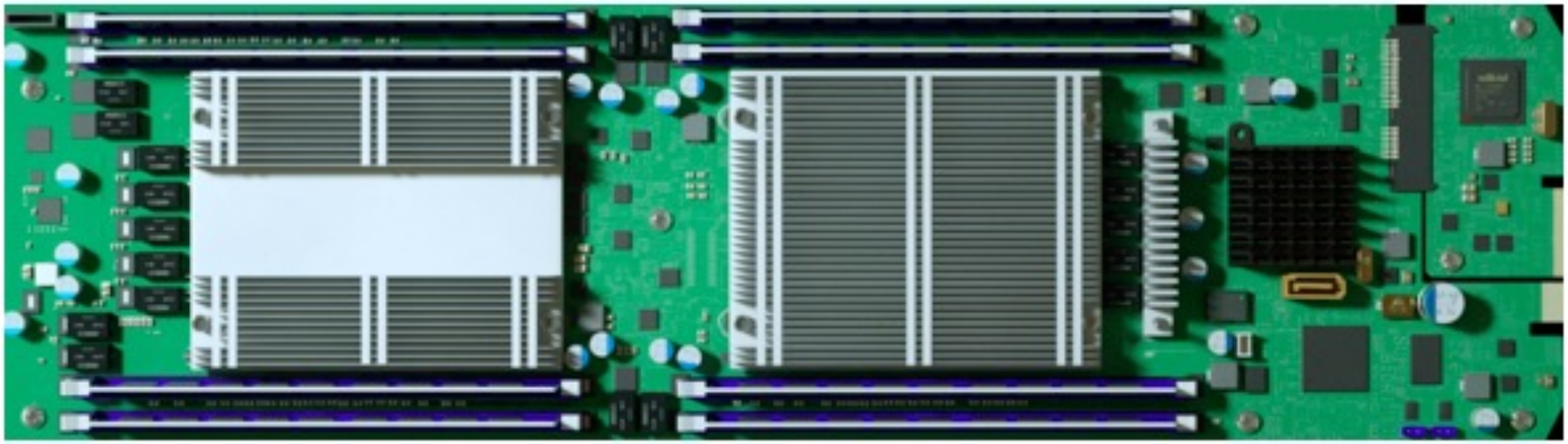
Tipos de Malware: capacidade de replicação

- Não replicáveis
  - Geralmente são acionados por "gatilhos" (triggers)
  - Exemplos: backdoors e bombas lógicas
- Replicáveis
  - Produzem cópias de si mesmo para serem ativadas posteriormente
  - Vírus e worms

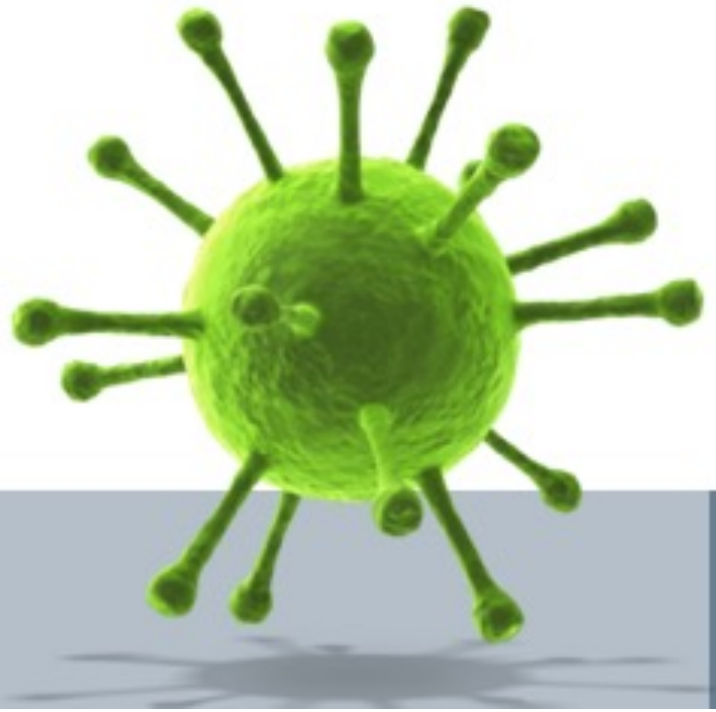
Algumas classes de malware

- Vírus: código de software que busca se replicar e se anexar a um executável (que passa a ser executado, também).
- Worm: programa de executa de forma independente e que se propaga para outros host na rede ou em outras redes
- Bomba lógica: código de software que permanece ”dormente” até que determinada condição lógica o ativa
- Cavalo de Troia: aplicação de software que esconde comportamento potencialmente malicioso.
- Backdoor: acesso indevido – não documentado – codificado em um software
- Flooder: programas que geram grande volume de tráfego, com objetivo de comprometer disponibilidade e desempenho
- Spyware: programa que coleta informações de um host ou rede e transmite a outro sistema

ChinaChips (mal-hard-ware)



Vírus



Definição de vírus

› Malware que, quando executado, tenta replicar-se em outro executável ou código de script da máquina; quando é bem-sucedido, o código ou script é dito estar infectado. Quando o código infectado é executado, o vírus também é executado.

Vírus

- Trecho de software que infecta programas
  - Modificam programas para incluir uma cópia do vírus
  - São executados secretamente junto com o programa hospedeiro
- Específico para sistema operacional e hardware
  - Se aproveitando de seus detalhes e fraquezas
- O vírus de computador carrega em seu código instruções para fazer cópias perfeitas de si mesmo
  - (Os vírus biológicos são pequenos fragmentos de código genético que podem assumir o controle de uma célula viva e para fazer milhares de réplicas suas.)

Vírus

- Um vírus de computador tem três componentes:
  - **Mecanismo de infecção**: meio pelo qual um vírus se espalha ou se propaga, permitindo sua replicação.
  - **Carga útil**: atividade do vírus. Pode envolver danos ou pode envolver atividade benigna.
  - **Mecanismo de ativação**: evento ou condição que determina quando a carga útil é ativada ou entregue.
- Muitos tipos contemporâneos de malware também incluem uma ou mais variantes de cada um desses componentes

”Fases da vida” de um vírus

- **Dormência** - o vírus está ocioso.
  - Ativado por algum evento, como uma data, a presença de outro programa ou arquivo, ou a capacidade do disco excedendo algum limite. Nem todos os vírus têm esse estágio.
- **Propagação** - o vírus coloca uma cópia de si mesmo em outros programas ou em determinadas áreas do sistema no disco.
  - Geralmente se transformam para evadir a detecção. Programas infectados conterão clones do vírus.
- **Ativação (ou desencadeamento)** - vírus ativado para executar sua função
  - Pode ser causada por uma variedade de eventos do sistema, incluindo uma contagem do número de vezes que essa cópia do vírus fez cópias.
- **Execução** - a função é executada.
  - Pode ser inofensiva, como uma mensagem na tela, ou prejudicial, como a destruição de programas e arquivos de dados.

Possíveis "alvos" de um vírus

- Vírus de boot
  - Infecta MBR (master boot record) e se espalha quando um sistema é iniciado a partir do disco que contém o vírus.
  - Exemplo: Ping-Pong
- Vírus file-infecting
  - Infecta arquivos executáveis (exemplo: arquivos .exe e .com)
  - Exemplo: Jerusalem
- Vírus de macro
  - Infecta macros, que são instruções que incrementam os recursos de programas como processadores de texto.
  - Exemplo: Melissa
- Vírus "multipartido
  - Várias estratégias
  - Exemplo: Ghostball

Estratégias de evasão/ocultação

- Vírus criptografado
  - Criptografa todo o conteúdo do vírus, deixando em claro apenas a "crypto-engine" e a chave
- Vírus polimórfico
  - Vírus sofre mutação a cada infecção – e.g. criptografa com chave distinta (ou outra forma de codificação)
- Vírus metamórfico
  - Vírus sofre mutação a cada infecção – muda o código mantendo funcionalidade (técnicas similares à ofuscação)
- Obs.: vírus camuflado – virus busca passar despercebido – nomenclatura não consensual

Worms

Definição de worm

› Um programa de computador que pode ser executado de forma independente e pode propagar uma versão de trabalho completa de si mesmo em outros hosts em uma rede, geralmente explorando vulnerabilidades de software no sistema de destino.

Características de worms

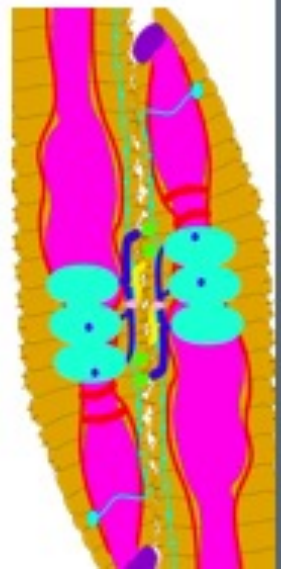
- Programa de replicação que se propaga sobre a rede
  - Usando e-mail, execução remota, login remoto
- Tem fases como um vírus:
  - Dormência, propagação, ativação, execução
  - Fase de propagação: busca outros sistemas, se conecta a eles, se copia e executa
- Pode disfarçar-se como um processo do sistema

Replicação de Worms – sondagem

- Busca por sistemas a serem infectados
  - Uma vez infectado um novo sistema, o processo se repete
- Estratégias de sondagem
  - Aleatório
  - Lista de execução
  - Topológico
  - Sub-rede local

Replicação de Worms – canais/meios

› Meios para se replicar e acessar sistemas remotos:
  - Correio eletrônico ou mensagens instantâneas
  - Compartilhamento de arquivos
  - Capacidade de execução remota
  - Acesso remoto ao arquivo ou capacidade de transferência
  - Capacidade de login remoto
  - Exploração de vulnerabilidades



Tecnologias de Worm

- Multiplataforma
- Multiexploração
- Disseminação ultrarrápida
- Polimórfico
- Metamórfico
- Múltiplos veículos de transporte
- Zero-days

Vírus versus Worms

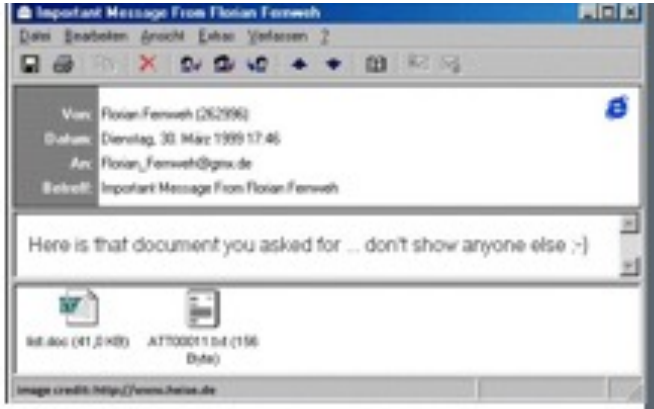
Kaspersky: "*An important distinction between computer viruses and worms is that viruses require an* ***active host program*** *or an already-infected and active operating system in order for viruses to run, cause damage and infect other executable files or documents, while worms are stand-alone malicious programs that can self-replicate and* ***propagate via computer networks****, without human help.*"

Virus e Worms notórios

Morris worm

- Paradigma para o estudo de worms
- Lançado por Robert Morris (1988)
- Vários ataques em sistemas UNIX
  - arquivo de senha prováveis
  - Exploração de bugs no sendmail, finger, e rsh/rexec
- Quando bem sucedido obtinha acesso remoto ao shell
  - enviava programa de bootstrap para copiar o verme

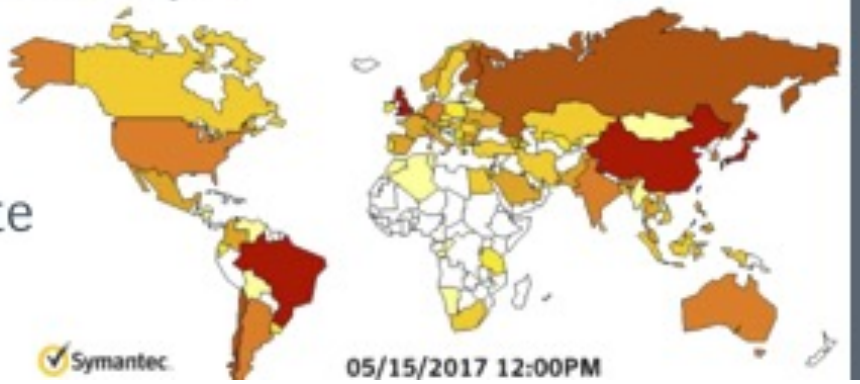
Melissa (1999)



- Mecanismo de propagação
  - Vírus de Macro – propagado por email
  - Email para 50 pessoas da lista de endereços
- Gatilho
  - Ao ser clicado (abrindo arquivo anexo)
- Furtividade
  - Nenhum mecanismo
- Payload
  - Substitui trechos de arquivo word por falas dos Simpsons
  - Envia arquivos Word para sua lista de contatos

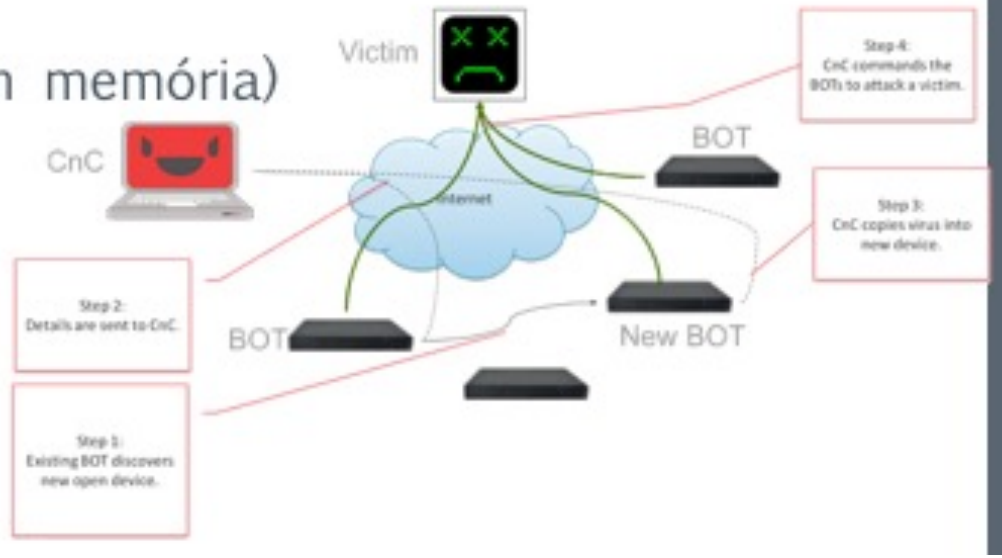
Wannacry (2017)

- Mecanismo de propagação
  - Exploit desenvolvido por NSA (?)
- Gatilho
  - Autônomo: uma vez obtido acesso, criptografa os dados e exibe mensagem
- Furtividade
  - Não é necessária – apenas uma execução
- Payload
  - Criptografia de chave pública
  - Sistema de pagamento de resgate

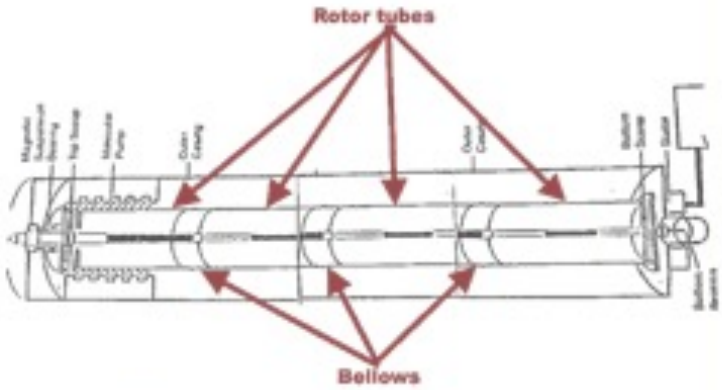


Mirai (2016)

- Mecanismo de propagação
  - Login de força bruta em dispositivos IoT
- Gatilho
  - Uso de Comando&Controle – contrução de botnet
- Furtividade
  - Fileless attack (residente em memória)
- Payload
  - Construção de botnet
  - Ataques UDP/TCP/HTTP



Stuxnet (2010)



- ”Paradigma” em vários aspectos
- Mecanismo de propagação
  - 4 zero-days (um zero-day pode chegar a 1US$mi no mercado negro)
  - 2 certificados digitais roubados (para assinar driver)
- Gatilho
  - Alto conhecimento sobre o alvo (modelo Siemens, cascata de centrífugas)
- Furtividade
  - Vírus criptografado
  - Atuação por 15min e 50min por mês
  - Retorno de informações falsas ao controlador
- Payload
  - Conhecimento profundo do sistema físico atacado

Propagação por engenharia social

Spam e Trojan

SPAM: e-mail indesejado

- Responsável por 45% a 90% do tráfego total de e-mail
- Parte significativa é propaganda
- Outra parte é fraudulenta ou compõe campanhas de phishing
- Grande parte é portadora de malware

Trojan

- Trojan (cavalo de Tróia) é uma ferramenta ou aplicativo aparentemente útil, mas que carrega funcionalidade oculta indesejada ou maliciosa
- São usados com diversos objetivos
  - monitorar comportamento
  - violar privacidade
  - permitir acesso a recursos
- Tipos de Trojan
  - Mantém funcionalidade e comportamento malicioso (paralelos)
  - Modifica o comportamento de uma aplicação (exemplo: programa de listagem de processo que omite processo malicioso)
  - Executa apenas função maliciosa

Payload

Objetivo e ações do malware

Possíveis objetivos de um malware

- Simples propagação
- Destruição de dados
- "Sequestro" de dados
- Espionagem/roubo de dados
- Danos físicos
- Construção de botnet para sobrecarga de serviço
- Acesso remoto e rootkit

Malware voltado à propagação

- Motivos: ”recreação”, ”pesquisa” ou ”liberação precoce” do malware
- Pode ter efeitos de indisponibilidade de redes e sistemas
- Exemplo: worm de Morris
  - Finalidade de pesquisa
  - Apenas se propagava
  - Causou degradação e indisponibilidade de serviços

Malware voltado à destruição de dados

- Motivos: ”recreação” ou ”sabotagem”
- Exemplos: boa parte dos vírus clássicos
  - Chernobyl 1998
  - Kletz 2001

Malware voltado ao sequestro de dados

- Criptografa dados e pede "resgate" para descriptografar
- Exemplos: vários ransomware estudados

Malware voltado a espionagem/roubo de dados (spyware)

- Keylogger - contra-ataque em relação à criprografia
  - Objetivo típico: credenciais de acesso
- Spyware mais "gerais" monitoram vários aspectos do sistema – resposta a applets gráficos etc.
  - imagens, histórico de atividades, formulários web,...
- Phishing e spear phishing

Malware voltado a danos físicos

- Busca causar impacto direto em hardware e equipamentos
- Exemplos:
  - Stuxnet
  - Chernobyl

Malware voltado à construção de botnet

- Infecta máquinas para usar os recursos computacionais com finalidades maliciosas
  - Máquinas infectadas são denominadas "bots" ou "zumbis"
  - Rede de bots é denominada "botnet"
  - Botnet chega a ter de centenas de milhares a milhões de máquinas infectadas
- Controle remoto (C&C)
  - Bot é controlado a partir de uma central de comando e controle
    - Grande diferença em relação a worms
  - Geralmente, protocolos de aplicação como IRC (mais antigos) e HTTP (mais recentes)
  - Sofisticação do C&C definirá a flexibilidade da botnet

Uso de botnets

- Ataques de negação de serviço distribuídos (DDoS)
- Spamming
- Coleta de informações: captura de tráfego, keylogger
- Difusão de malware
- Propaganda
- Manipulação de votações e jogos online
- Botnets "do bem": SETI@home, GIMPS, Genome@home

Algumas botnets notórias

- EarthLink Spammer - 2000
- Storm – 2007
- Cutwail – 2007
- Grum – 2008
- Kraken - 2008
- Mariposa – 2008
- Conficker – 2008
- Necurs – 2012 até o presente
- Gamut – 2013 até o presente
- Methbot – 2016
- Mirai – 2016
- 3ve - 2018

Malware voltado ao acesso remoto e rootkit

- Backdoor: acesso secreto a um sistema
  - Backdoor "legítimo": porta de manutenção (bacalhau)
  - Backdoor malicioso: inserido sem autorização
- Exemplos: conta "especial", funcionalidade não-documentada, serviço em porta escondida,...
- Rootkit: programas "camulflados" que permitem acesso em nível admin a sistema
  - Espécie de backdoor
  - Modifica/subverte o sistema para dificultar detecção

Ativação do payload

- Bomba temporal (bomba lógica)
  - Payload é ativado quando determinadas condições temporais são atingidas
  - Ex.: Gasoduto trans-siberiano, Sexta-feira 13, Tim Lloyd
- Análise do ambiente (bomba lógica)
  - Payload é ativado quando determinadas condições lógicas ou do ambiente infectado são atingidas
  - Ex.: Stuxnet
- Comando&Controle
  - Ativação do payload é feita remotamente
  - Ex.: botnets

Contramedidas

Prevenção e resposta contra malware

Contramedidas

- Antivírus -> Antimalware
- Prevenção: política, pessoal, mitigação de vulnerabilidades e de ameaças
  - Aplicação de "patches" (mitigação de vulns)
  - "Hardening" do sistema
  - treinamento/conscientização
  - Política de segurança: procedimentos
- Resposta
  - Detecção
  - Identificação
  - Remoção

Sobre scanners...*

› Host-based versus scanner de perímetro

› Assinatura versus comportamento

MALWARE CONFERENCE (MALCON)

KNOW YOUR ENEMY

Research Track ■ Practical Solutions (Industry Track) ■ The Law

13th IEEE International Conference on Malicious and Unwanted Software "MALCON 2018"

Software ”indesejado”

Software ”indesejado”

- Malware é um conceito bem definido: pedaço de (soft/hard)ware com comportamento malicioso
- Mas nem todo software indesejado é deliberadamente malicioso...
  - ... os já mencionados ”bacalhaus”
  - ... funcionalidades legítimas mas não-conformes
- Software legítimo/indesejado/não-conforme é um dos maiores desafios da área de segurança