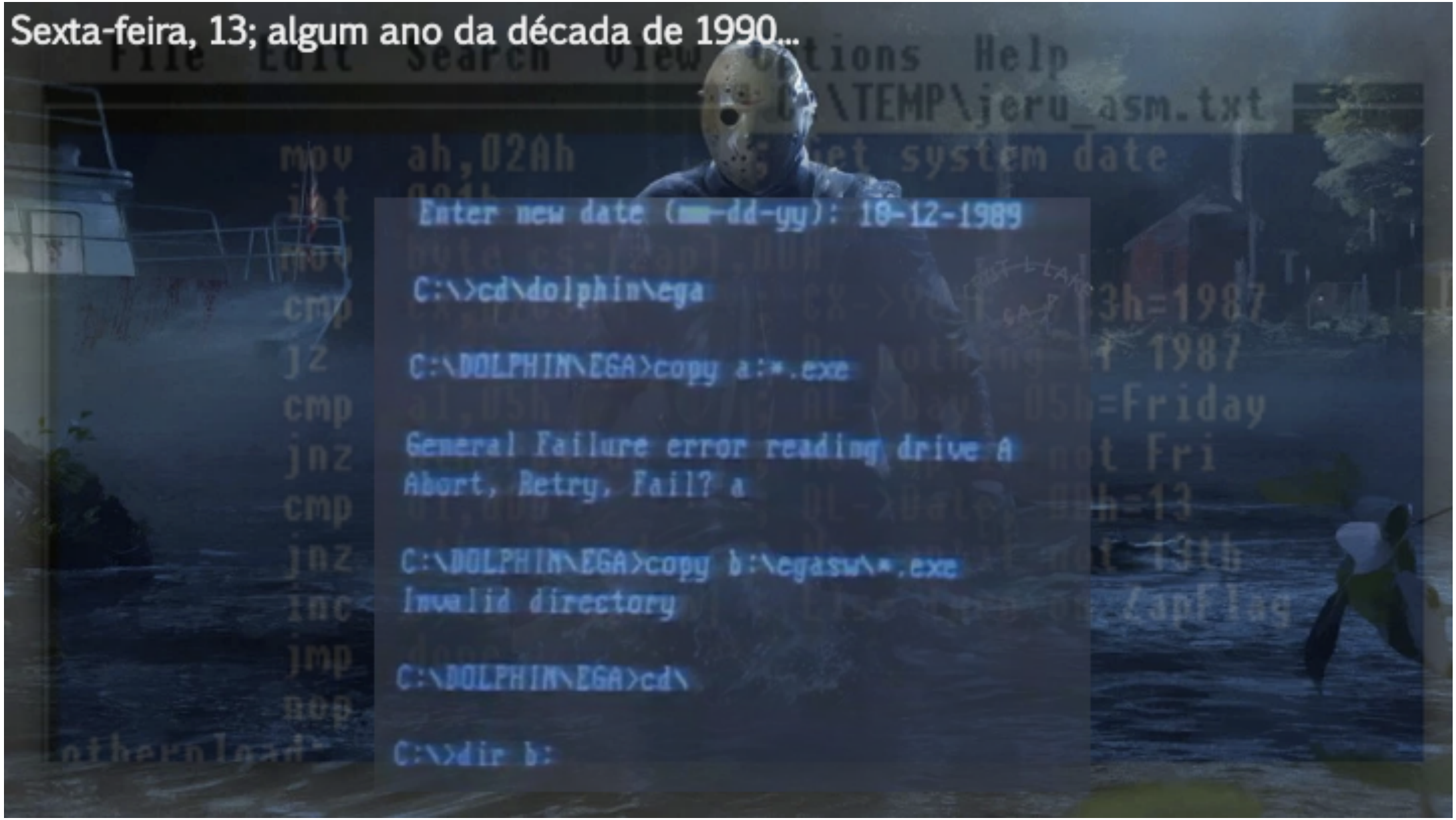
Malware

Software malicioso e indesejado

Sexta-feira, 13; algum ano da década de 1990...



Conceitos gerais

Malware

- Programas que apresentam comportamento "malicioso"
  - Malware = Malicious software
- Classificação quanto à "autonomia"
  - Códigos que necessitam de hospedeiro (parasitas)
    - Códigos "nativos": backdoor, timebomb
    - Códigos "invasores": vírus, códigos injetados
  - Códigos autônomos
    - Worms, bots,...
- Classificação quanto à capacidade de replicação

Alguns exemplos 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

Tipos de Malware: parasitas vs autônomos

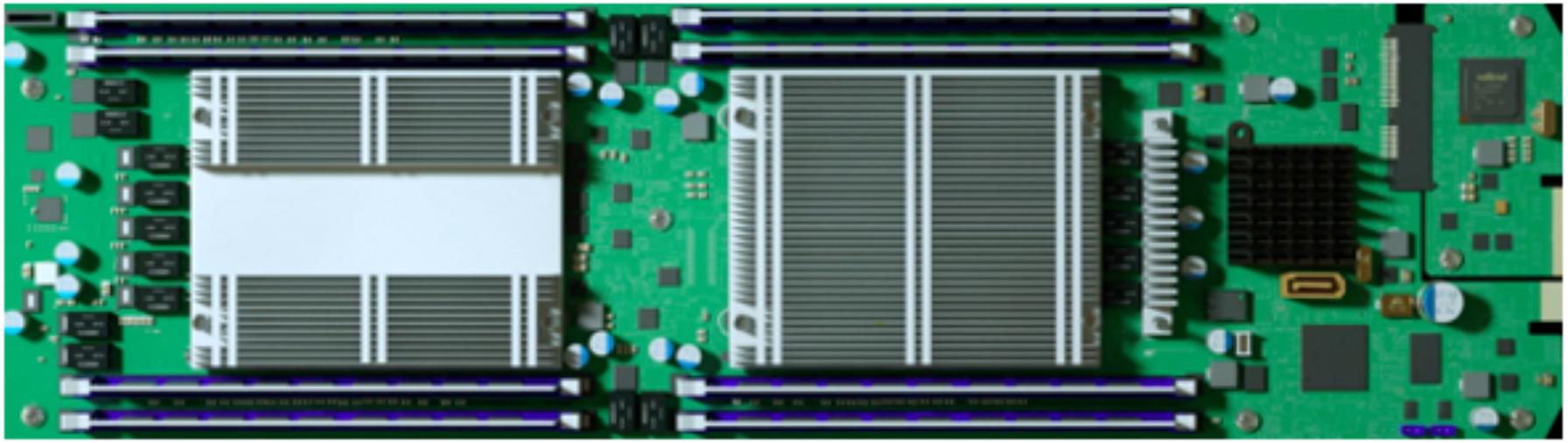
- Parasitas
  - Precisam de um hospedeiro para existir
  - Rotinas e fragmentos de programas que se anexam a aplicações maiores
  - Exemplos: vírus, backdoors, bombas lógicas

- Independentes/Autônomos
  - Existem por si mesmos
  - Programa completo com todas as funcionalidades necessárias para seus objetivos
  - Exemplos: worms e bots

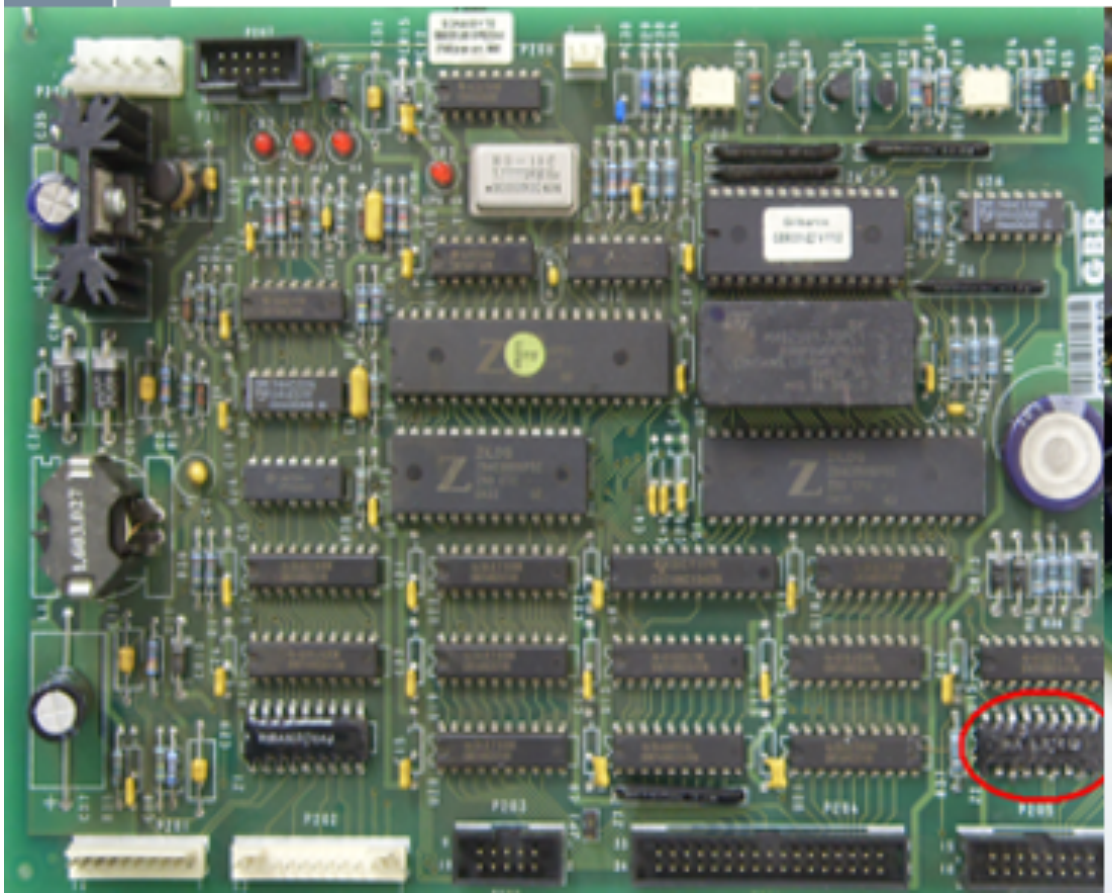
Tipos de Malware: capacidade de replicação

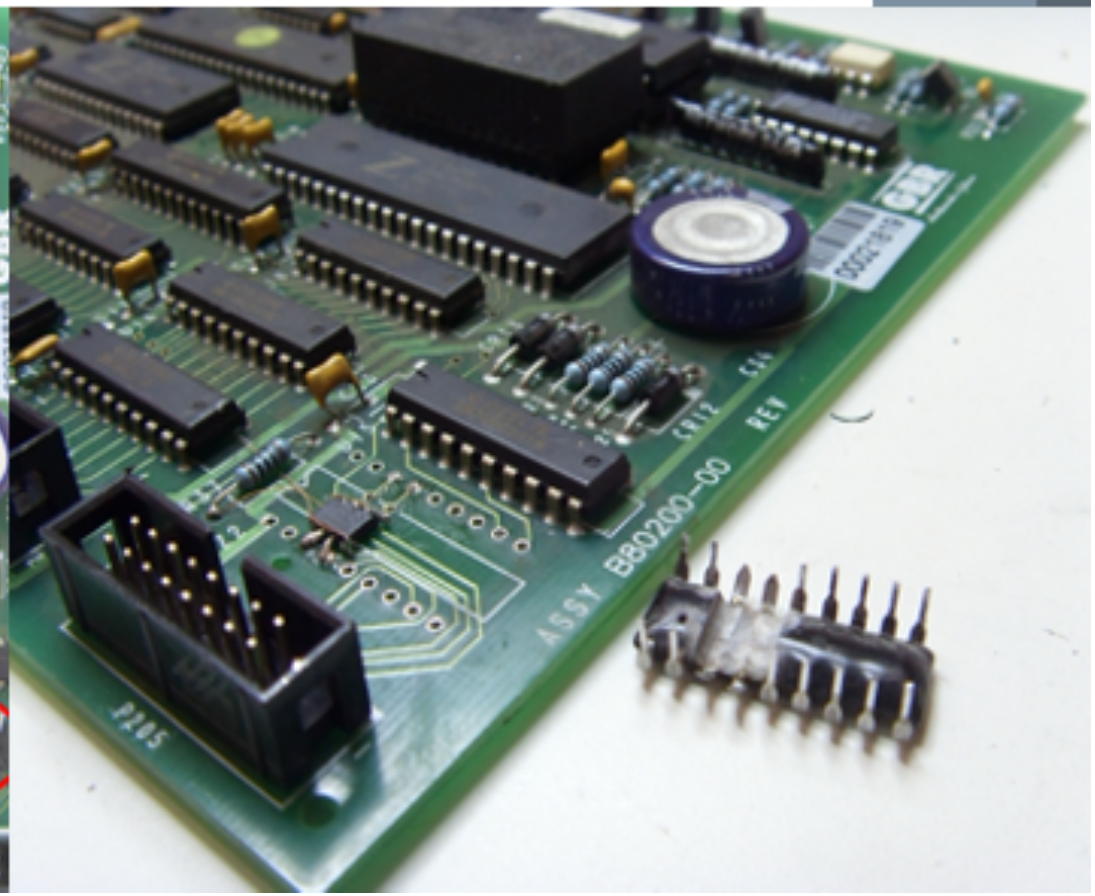
- Não replicáveis
  - Não possuem capacidade de infectar e propagar
  - Exemplos: backdoors e bombas lógicas
- Replicáveis
  - Produzem cópias de si mesmo para serem ativadas posteriormente
  - Vírus e worms

ChinaChips (mal-hard-ware)

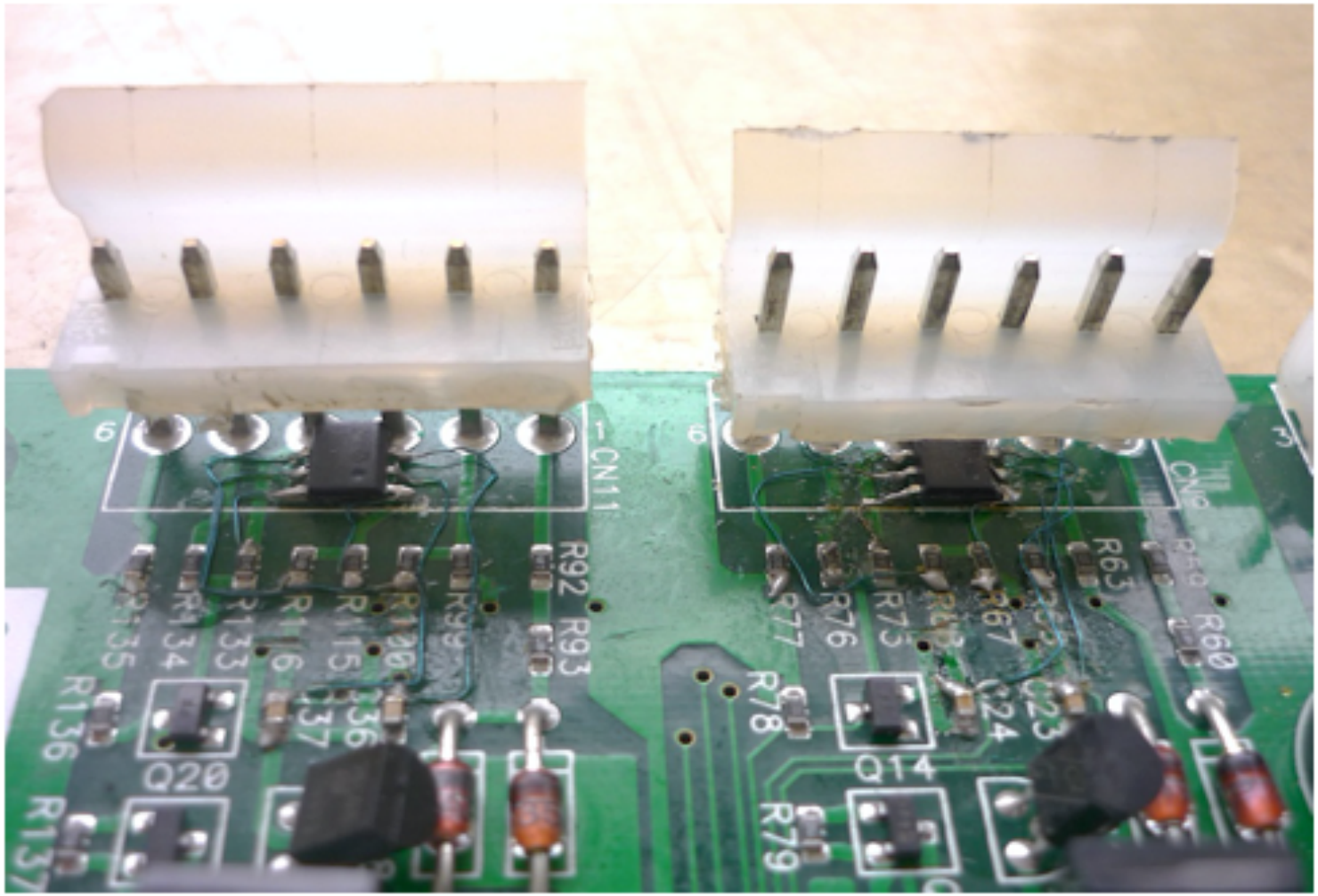


BrazilChips (mal-hard-ware)

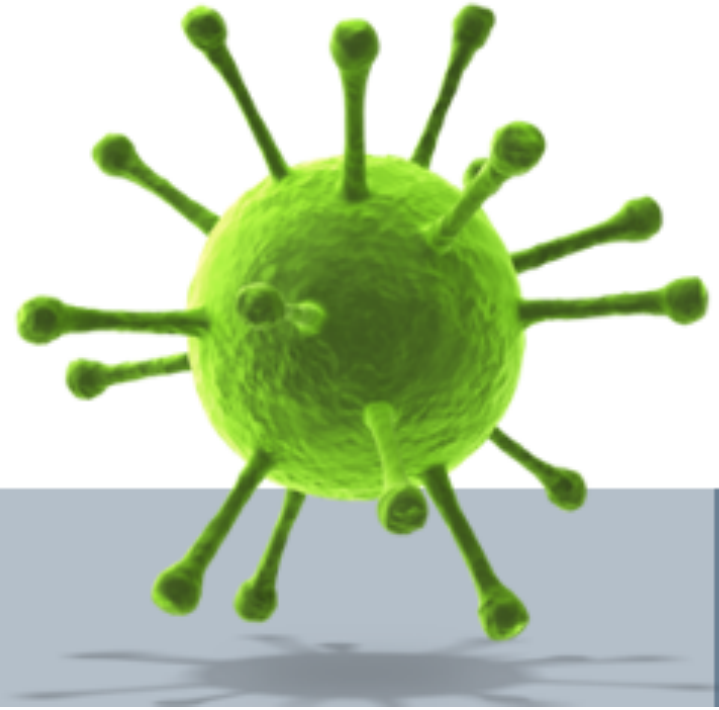




BrazilChips (mal-hard-ware)



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.
- Muitos conceitos de vírus aplicam-se também a outros tipos de malware
  - Estudaremos nos vírus, mas veremos as analogias posteriormente

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

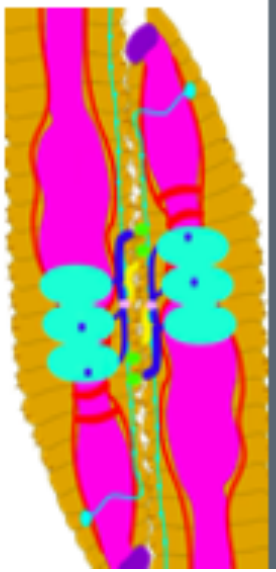
- Programa de replicação que se propaga sobre a rede
  - Usando e-mail, execução remota, login remoto
- Tem fases como um vírus:
  - Dormência, propagação, ativação, execução
  - Fase de propagação: busca outros sistemas, se conecta a eles, se copia e executa
- Pode disfarçar-se como um processo do sistema

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

Theory of self-reproducing automata (von Neumann)

Theory of

Self-Reproducing Automata

JOHN VON NEUMANN

edited and completed by **Arthur W. Burks**

University of Illinois Press
URBANA AND LONDON 1966

PREFACE

In the late 1940's John von Neumann began to develop a theory of automata. He envisaged a systematic theory which would be mathematical and logical in form and which would contribute in an essential way to our understanding of natural systems (natural automata) as well as to our understanding of both analog and digital computers (artificial automata).

To this end von Neumann produced five works, in the following order:

(1) "The General and Logical Theory of Automata." Read at the Hixon Symposium in September, 1948; published in 1951. *Collected Works* 5.288–328.[1]

(2) "Theory and Organization of Complicated Automata." Five lectures delivered at the University of Illinois in December, 1949. This is Part I of the present volume.

(3) "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components." Lectures given at the California Institute of Technology in January, 1952. *Collected Works* 5.329–378.

(4) "The Theory of Automata: Construction, Reproduction, Homogeneity." Von Neumann started this manuscript in the fall of 1952 and continued working on it for about a year. This is Part II of the present volume.

(5) *The Computer and the Brain*. Written during 1955 and 1956; published in 1958.

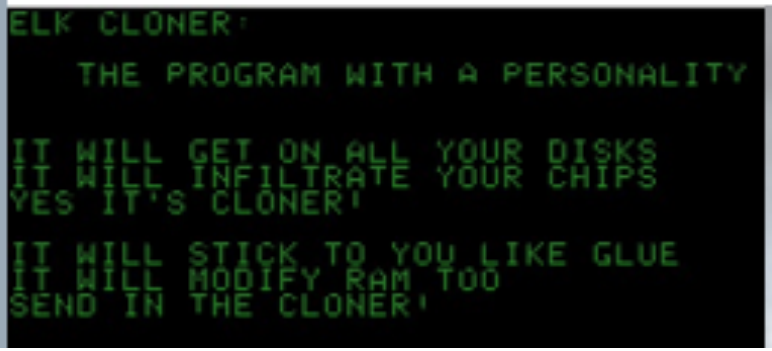
The second and fourth of these were left at his death in a manuscript form which required extensive editing. As edited they constitute the two parts of the present volume, which thus concludes von Neumann's work on the theory of automata.

Creeper, 1971

- Desenvolvido por Bob Thomas na empresa BBN
- Versão original do worm simplesmente se movia pela ARPANET entre computadores DEC PDP-10 (mainframes) rodando o sistema operacional TENEX
- Versão posterior, capaz de se "copiar", foi desenvolvida por Ray Tomlinson (BBN)
- Ray também desenvolveu o "Reaper", worm projetado encontrar e remover o Reaper
  - Considerado primeiro antivirus

Elk Cloner (1982)

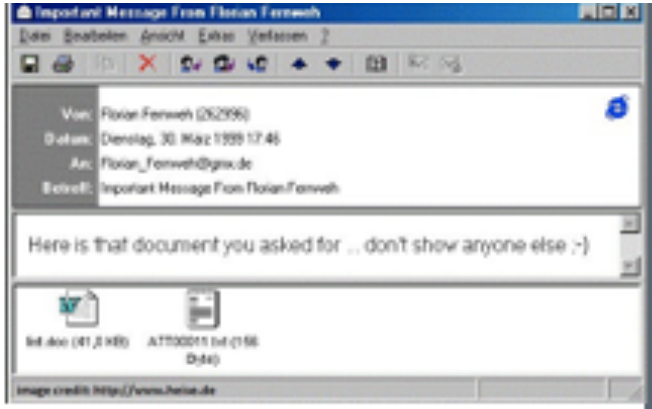
- Desenvolvido por Rich Skrenta, então com 15 anos
- Se anexava ao sistema operacional do Apple II e se propagava por disquete
  - Se um computador era bootado a partir de um disquete infectado, uma cópia do vírus era colocada em memória
  - Se outro disquete era inserido, uma cópia (infectada) do sistema operacional era feita



Morris worm (1988)

- Paradigma para o estudo de worms
- Lançado no MIT por Robert Morris (estudante de Cornell)
- 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

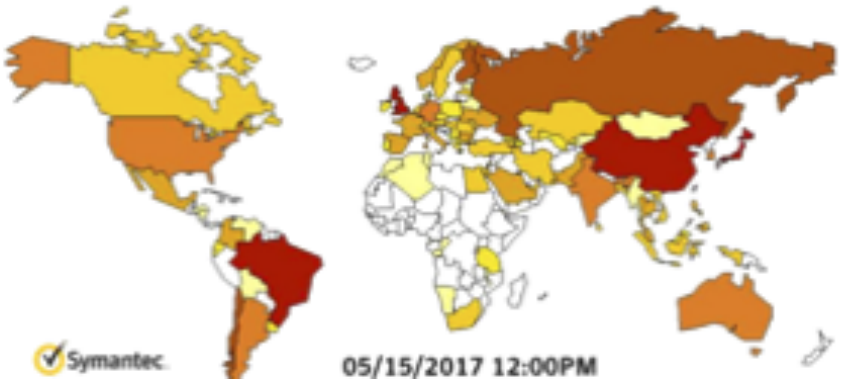
Melissa (1999)



- 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

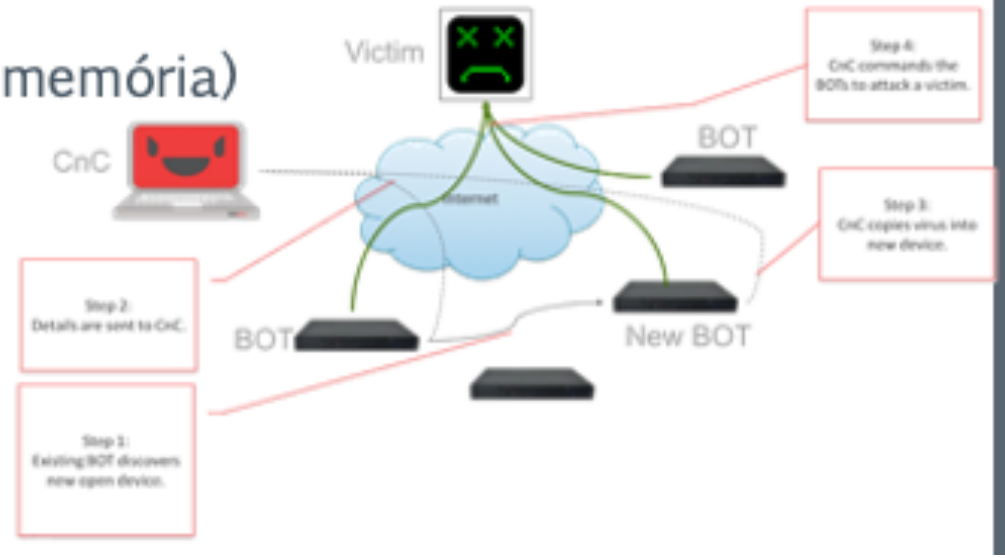
Wannacry (2017)

- 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

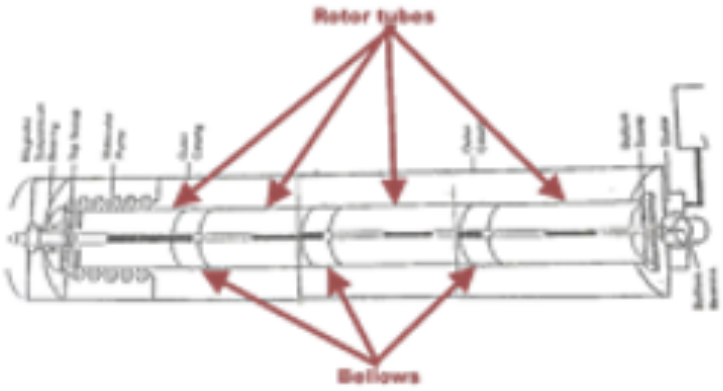


Mirai (2016)

- 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 funcio 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

Estudo de Caso: Mirai Dyn 2016

Ataque DDoS que mudou paradigmas...

Mirai/Dyn IoT DDoS (out-2016)

Ataque Mirai/Dyn

- Série de ataques DDoS tendo como alvo o provedor Dyn de DNS (21-outo-2016)
  - Consultas a partir de dezenas de milhões de endereços de IP
  - Dispositivos conectados à Internet foram extensamente usados no ataque: impressoras, câmeras, controles de garagem, monitores de bebês,...
    - Tais dispositivos foram infectados com o malware Mirai
- Importantes plataformas de serviços ficaram indisponíveis para usuários da Europa e América do Norte
- O grupo Anonymous assumiu responsabilidade, mas pouca evidência foi, de fato apresentada.

Serviços Impactados

Airbnb[11]
Amazon.com[8]
Ancestry.com[12][13]
The A.V. Club[14]
BBC[13]
The Boston Globe[11]
Box[15]
Business Insider[13]
CNN[13]
Comcast[16]
CrunchBase[13]
DirecTV[13]
The Elder Scrolls Online[13][17]
Electronic Arts[16]
Etsy[11][18]
FiveThirtyEight[13]
Fox News[19]
The Guardian[19]
GitHub[11][16]
Grubhub[20]
HBO[13]
Heroku[21]
HostGator[13]
iHeartRadio[12][22]
Imgur[23]
Indiegogo[12]
Mashable[24]
National Hockey League[13]
Netflix[13][19]
The New York Times[11][16]
Overstock.com[13]
PayPal[18]
Pinterest[16][18]
Pixlr[13]
PlayStation Network[16]
Qualtrics[12]
Quora[13]
Reddit[12][16][18]
Roblox[25]
Ruby Lane[13]
RuneScape[12]
SaneBox[21]
Seamless[23]
Second Life[26]
Shopify[11]
Slack[23]
SoundCloud[11][18]
Squarespace[13]
Spotify[12][16][18]
Starbucks[12][22]
Storify[15]
Swedish Civil Contingencies Agency[
Swedish Government[27]
Tumblr[12][16]
Twilio[12][13]
Twitter[11][12][16][18]
Verizon Communications[16]
Visa[28]
Vox Media[29]
Walgreens[13]
The Wall Street Journal[19]
Wikia[12]
Wired[15]
Wix.com[30]
WWE Network[31]
Xbox Live[32]
Yammer[23]
Yelp[13]
Zillow[13]

Contexto histórico

› J. Assange asilado na embaixada do Equador (Londres)
  – Pressão dos EUA por restrição de acesso à Internet

State Department denies pressuring Ecuador to cut Assange's internet

By ERIC GELLER | 10/18/2016 12:26 PM EDT | Updated 10/18/2016 02:40 PM EDT

Share on Facebook Share on Twitter

The State Department today flatly denied a WikiLeaks allegation that it encouraged the Ecuadorian government to shut down Julian Assange's internet connection.

WikiLeaks, citing "multiple U.S. sources," said early today that Secretary of State John Kerry pressured Ecuador — which has hosted Assange in its London embassy since 2012 — to cut off Assange's internet before he could publish more hacked emails from Hillary Clinton campaign chairman John Podesta.

Contexto histórico

› Assange asilado na embaixada do Equador (Londres)
  – Pressão dos EUA por restrição de acesso à Internet

WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical

By **ERIC GELLER** and TONY ROMM | 10/21/2016 10:05 AM EDT | Updated 10/21/2016 08:05 PM EDT

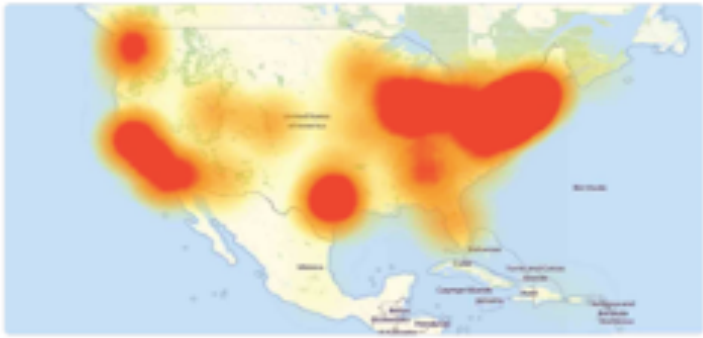
Share on Facebook Share on Twitter

A massive cyberattack Friday on a key internet routing company knocked offline major websites like Spotify, Twitter and The New York Times, as WikiLeaks supporters claimed credit.

But security researchers were quick to cast doubt on their boasts. The federal government has said it is investigating, declining to speculate on who is responsible.

WikiLeaks
@wikileaks
Follow

Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point.



2:09 PM - 21 Oct 2016

Investigação e responsabilidades

- Nenhum grupo de hackers reivindicou responsabilidade durante ou imediatamente após o ataque
  - O ataque foi uma botnet coordenada por um grande número de dispositivos habilitados para Internet das Coisas (IoT), incluindo câmeras, gateways residenciais e monitores de bebês, que haviam sido infectados com o malware Mirai.
  - O Mirai é projetado para forçar a segurança em um dispositivo IoT, permitindo que ele seja controlado remotamente.
  - O código-fonte do Mirai havia sido lançado na Internet de forma aberta algumas semanas antes, o que dificultaria a investigação do criminoso
- Em 25 de outubro de 2016, o presidente dos EUA, Obama, afirmou que os investigadores ainda não tinham ideia de quem realizou o ciberataque.
- Em 13 de dezembro de 2017, o Departamento de Justiça anunciou que três homens (Paras Jha, 21 anos, Josiah White, 20 e Dalton Norman, 21) haviam declarado sua culpa em casos de cibercrime relacionados aos botnets Mirai e clickfraud.

Estudo de Caso: Stuxnet

O malware “definitivo”

Sabotagem ao Programa Nuclear Iraniano (2010)

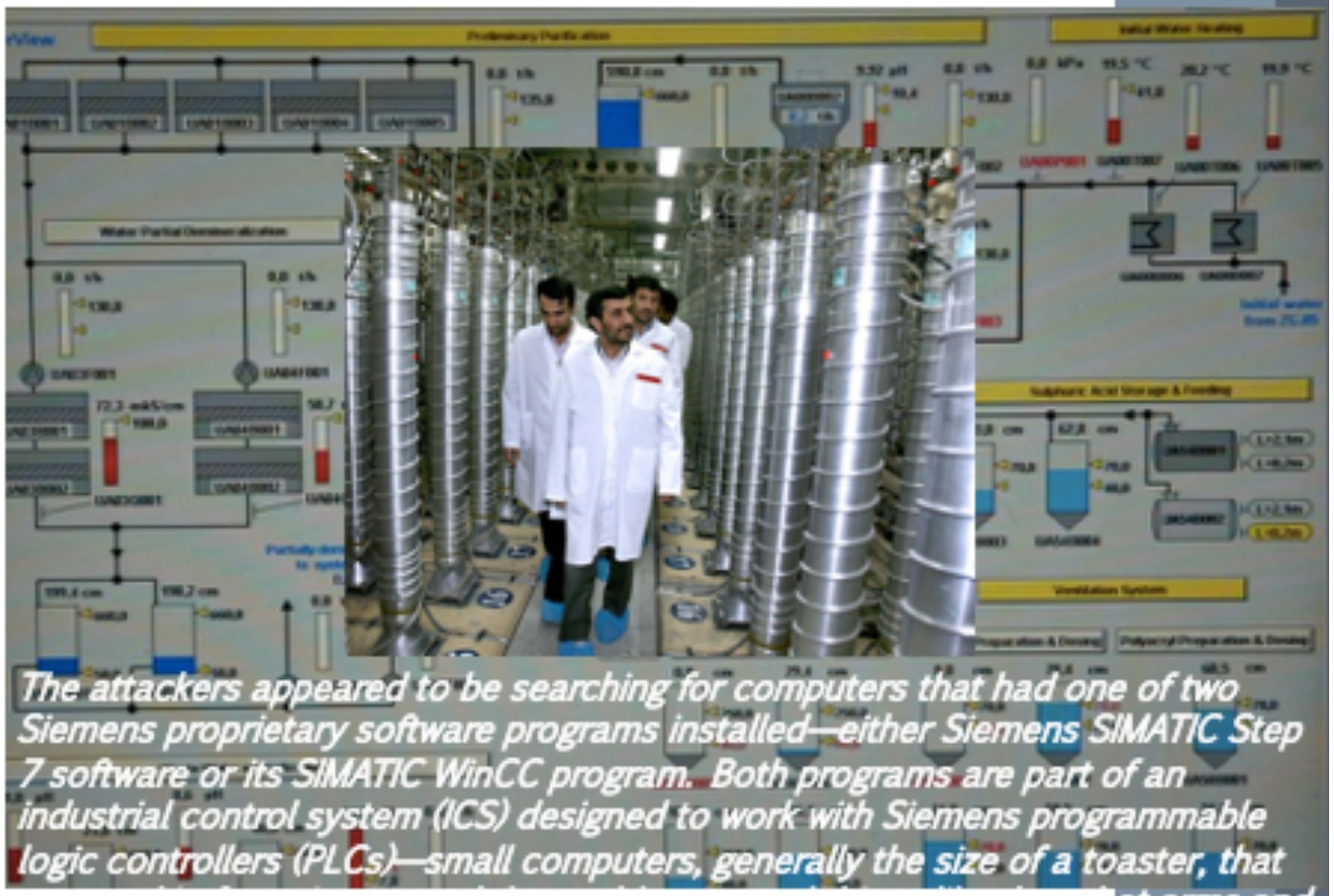
Cyberwar

The meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | From the print edition

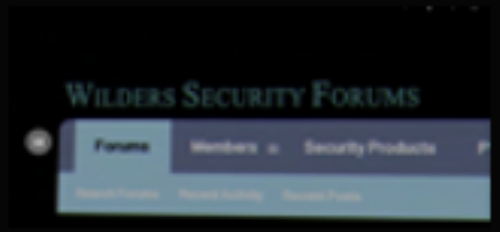
IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals (see article). It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

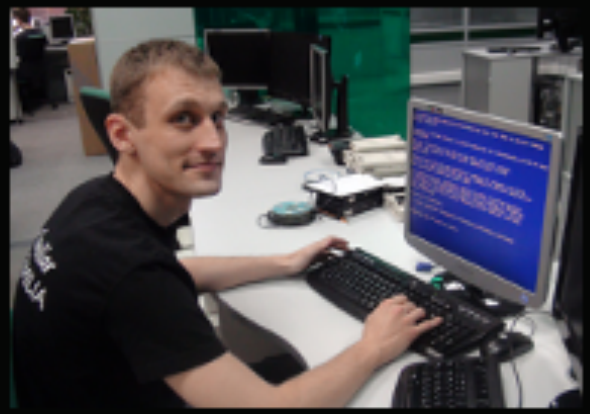


The attackers appeared to be searching for computers that had one of two Siemens proprietary software programs installed—either Siemens SIMATIC Step 7 software or its SIMATIC WinCC program. Both programs are part of an industrial control system (ICS) designed to work with Siemens programmable logic controllers (PLCs)—small computers, generally the size of a toaster, that

ot arms and

Descoberta





Malware Detected

Discussion started by sergey ulasen

ılware installs two drivers: mrxnet.sys and mrxcls.sys

us, **current malware should be added to very dangerous category**
ıses the risk of the virus epidemic
ıe current moment.

Modules of **current malware were first time detected** by "VirusB
specialists **on the 17th of June, 2010** and were added to the an

You should take into consideration that virus infects Operating

Chegando aos grandes vendors de AV


KASPERSKY lab


KASPERSKY


EUGENE KASPERSKY

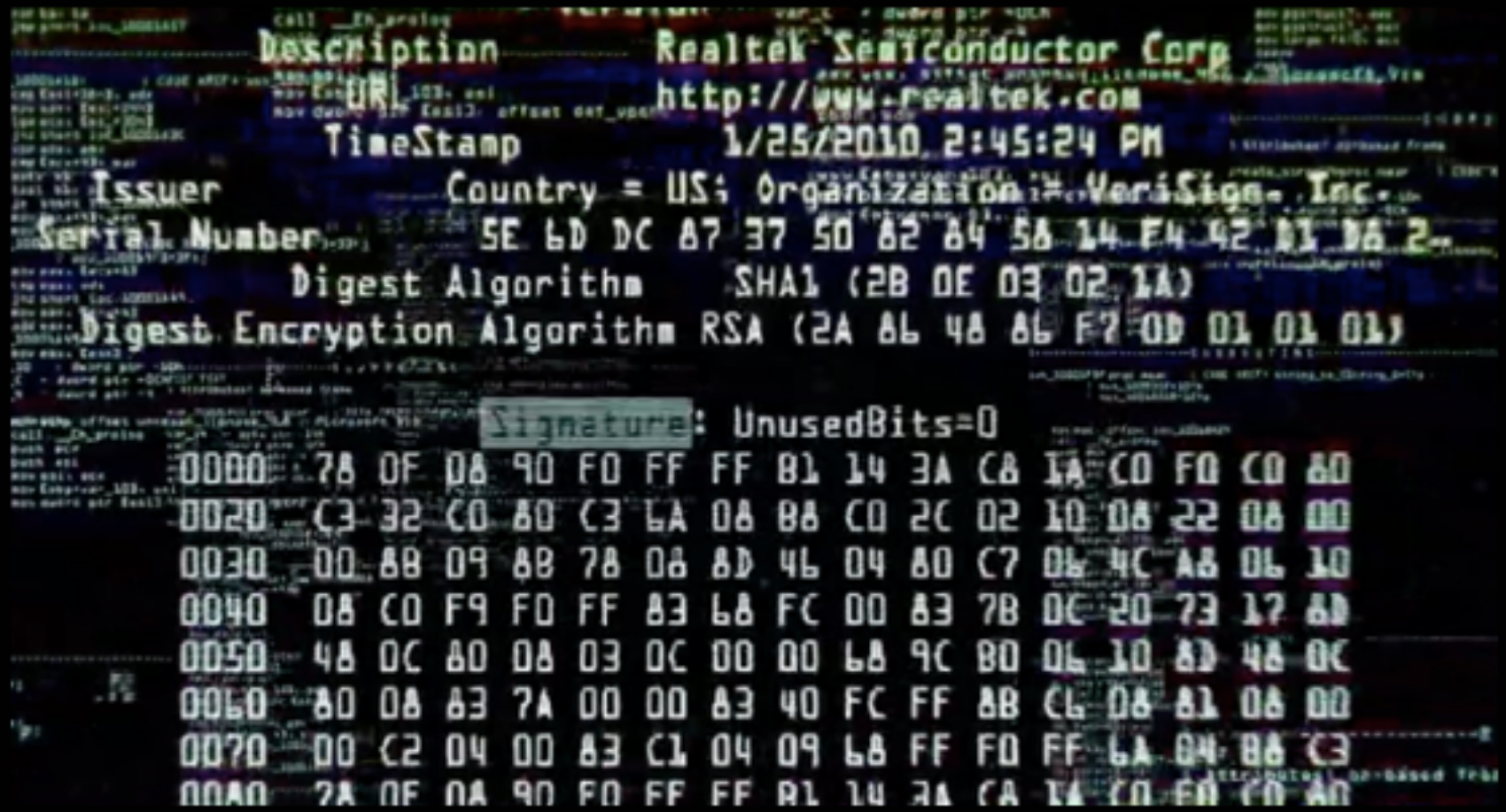

VITALY KAMLUK

Origem do nome Stuxnet

Deep analysis

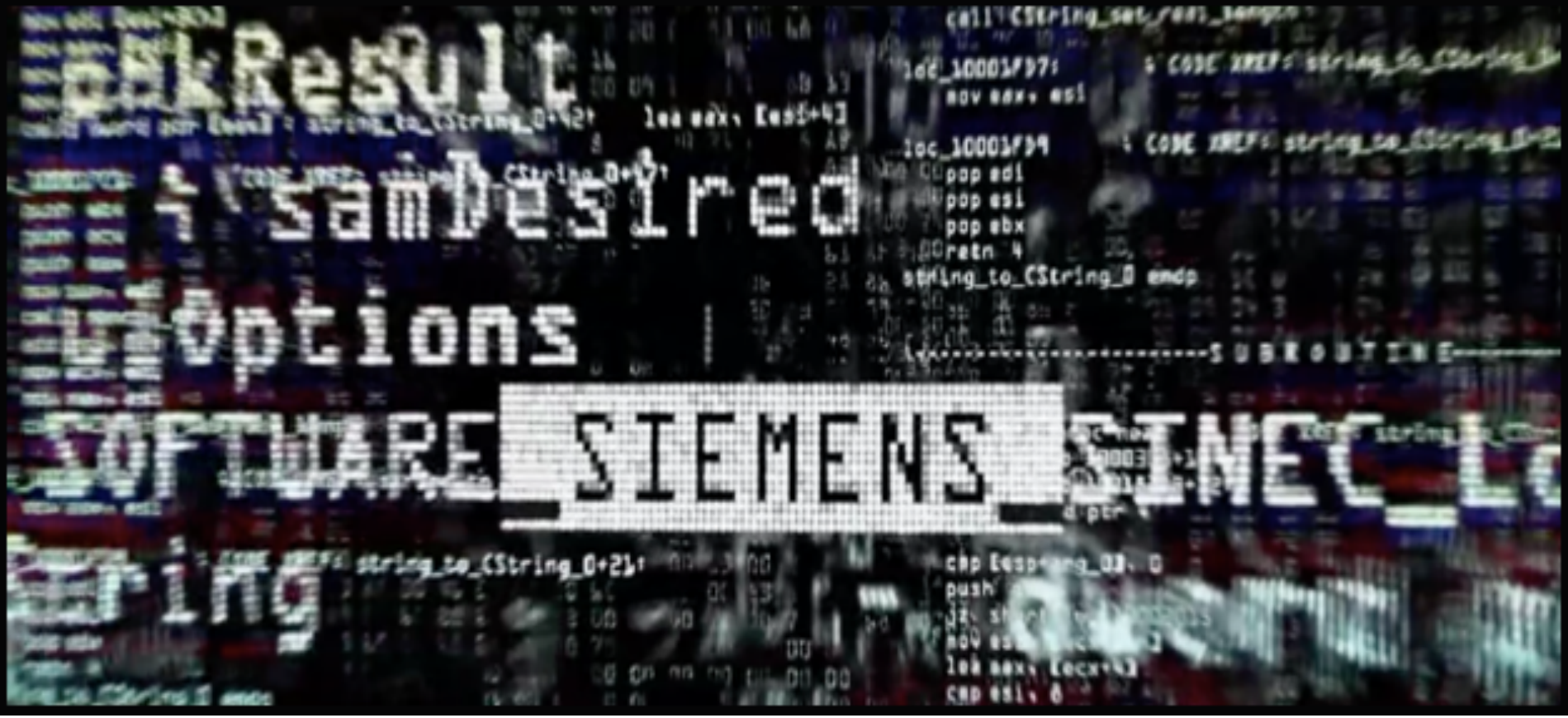
- Código cerca de 20 vezes maior que um malware típico
- Ausência de bugs (algo raro)
  - Código denso e correto
- Uso de quatro zero-days
  - Comparação: naquele ano, a Symantec registrou apenas outros 12 zero days
  - Um zero-day pode ser vendido por centenas de milhares de dólares no submundo
    - Mercado negro vs branco vs cinza
- Quem poderia estar envolvido
  - Provavelmente, um estado-nação

Uso de certificado digital Windows



Uso de certificado digital Windows

Uma pista sobre o alvo: Siemens



Programmable Logic Devices

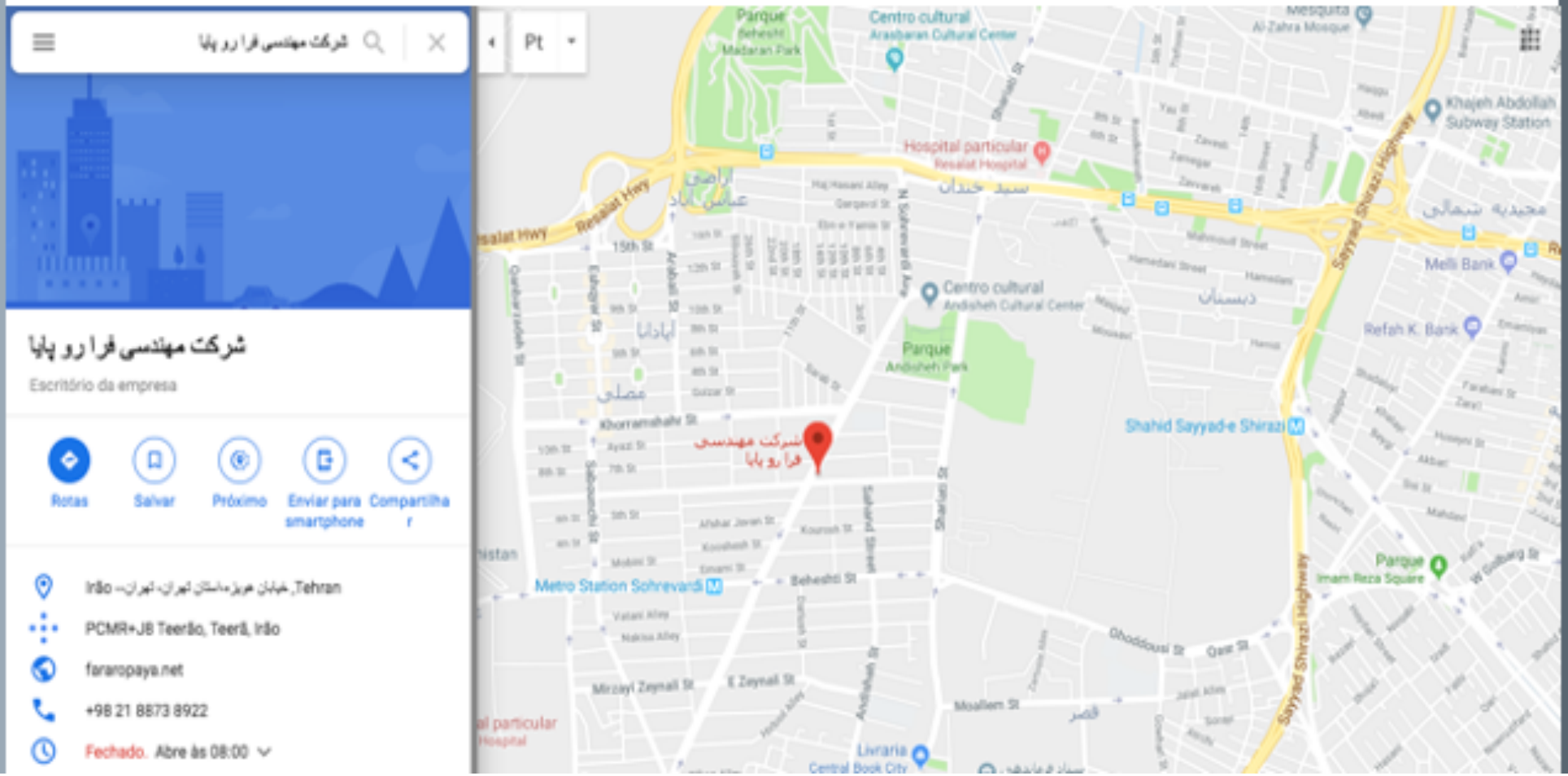
Infraestruturas críticas

Testes de Laboratório

- Seletividade: nos testes de laboratório, o malware realizava uma série de ”checks” e quando esses checks falhavam, o malware não fazia nada
- Furtividade: o malware se conportava de maneira bastante discreta, sem manipular controles de rede
- Parecia estar buscando um alvo muito específico
  - Tanto esforço para um alvo específico – deveria ser um alvo muito valioso

Modelo-alvo de PLC

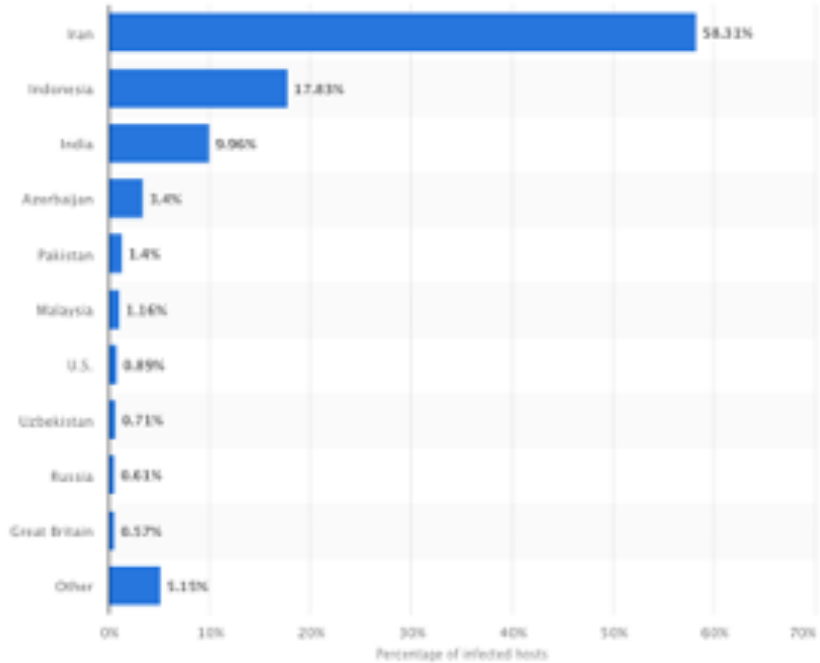
Fabricado pela Fararo Paya (Teerã/Irã)



Voltando ao mundo real

- Milhões de sistemas infectados em todo o mundo
- Refinando as estatísticas, foi possível observar origem das infecções
  - O país mais afetado, desde o princípio, era o Irã
  - Algo incomum em termos de malware
  - Observar o cenário geopolítico...

Percentage of Stuxnet infected hosts by country in 2010



Cenário Geopolítico no Irã

› Várias explosões de gasodutos

https://www.activistpost.com/2010/08/whos-blowing-up-irans-gas-pipelines.html

Who's blowing up Iran's gas pipelines?

TOPICS: Bomb Crime Iran Mahmoud Ahmadinejad

AUGUST 20, 2010

Con Coughlin
Telegraph

In the past few weeks Iran's gas infrastructure, which is central to the country's energy requirements, has been hit by a series of unexplained explosions.

The series of mysterious explosions began at the end of July when the state-owned Tehran Times reported that a pipeline carrying gas from Iran to Turkey had exploded near the eastern Turkish town of Dogubayazit. Iranian officials **blamed the blast** on Kurdish rebels.

This was followed earlier this month by reports in the Iranian press of an explosion in a gas pipeline on the outskirts of Tabriz. A few days later there was a more serious incident on August 4 when five people were killed when **another gas pipeline exploded** on the outskirts of the Pardis petrochemical plant. The explosion took place just a week after Iranian President Mahmoud Ahmadinejad had made an official visit to the complex. Finally, on August 10, a pipeline exploded in the city of Masjed Sleiman.

Cenário Geopolítico no Irã

› Atentados contra cientistas nucleares

Breve histórico do programa nuclear Iraniano

- Americanos apoiam programa nuclear iraniano durante administração Nixon
- Revolução derruba o Xá em 1979 – Irã passa a ser problema
- Transferência de tecnologia entre Paquistão e Irã a partir de meados de 1980
- Meados de 1990: maior financiamento; decisão de construir armas nucleares.
  - Possível motivação: facilidade com que americanos derrotaram Iraque
    - havia uma guerra de 8 anos entre Irã e Iraque...
- Outubro 2003: Irã resolve cooperar com IAEA
- Fevereiro 2006: Irã termina acordo e volta a enriquecer urânio em Natanz
  - EUA atolados no Afeganistão e no Iraque...

Dia nacional nuclear do Irã...

https://www.dw.com/coda/en/iran-celebrates-national-nuclear-day-with-two-new-projects/a-16730190

Iran celebrates national nuclear day with two new projects

Iranian President Mahmoud Ahmadinejad has launched two new nuclear projects that will allow the country to enrich uranium. The move came just days after nuclear talks with international leaders made little progress.

New facilities for mining and processing uranium opened in central Iran on Tuesday, coinciding with the country's National Day of Nuclear Technology.

Related Subjects International Atomic Energy Agency (IAEA), Iran, Hezbollah

Keywords iran, nuclear program, mahmoud ahmadinejad, national day of nuclear technology

Send us your feedback

Print Print this page

Permalink https://p.dw.com/p/18Chm

NEWS BULLETIN

Top stories in 90 seconds

DW News presents the most important news — in brief, quickly and up-to-date.

NEWS

Sri Lanka bombings: Death toll rises to 290 1H AGO

Morocco: Thousands call for release of jailed activists 1H AGO

Israel e EUA

- Ataque israelense ao Irã forçaria EUA a entrar em guerra contra IRÃ
- Medo de Israel que Irã desenvolvesse armas nucleares
- Preocupação dos EUA que Israel atacasse – e forçasse entrada dos EUA numa guerra
- Cooperação entre as inteligências
  - Proposta israelense pelo stuxnet

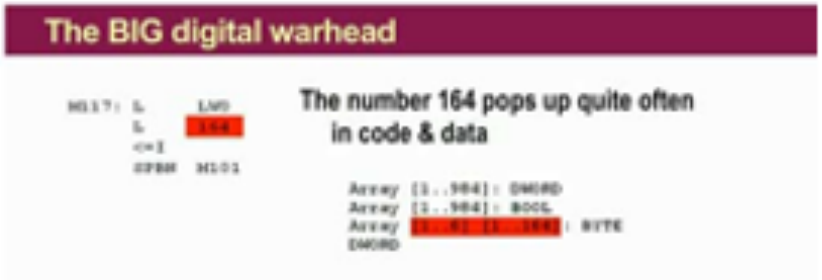
Tour de 2008 em Natanz

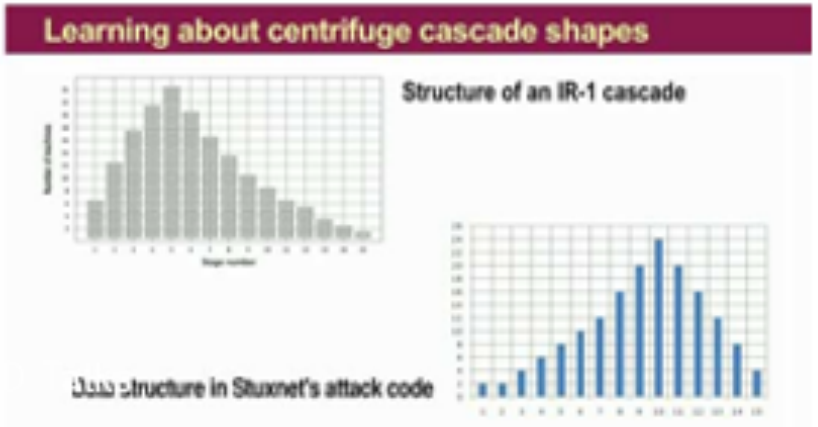
Configuração das centrífugas

(Supostos) Locais de testes do Stuxnet

Desvendando o alvo:

Natanz FEP





Fonte: Langner, TED Talks

Resultados dos testes; decisão sobre ataque

- Centrífugas destruídas
  - Exibição na situation room
- Descisão sobre "ataque"
  - O que temos capacidade de fazer
  - O que é legalmente aceitável
  - O que deveríamos fazer (política, diplomacia etc.)
- Data-limite: típico de governos

Resultados dos testes; decisão sobre ataque

- Centrífugas destruídas
  - Exibição na situation room
- Descisão sobre "ataque"
  - O que temos capacidade de fazer
  - O que é legalmente aceitável
  - O que deveríamos fazer (política, diplomacia etc.)
- Data-limite: típico de governos

Air gap

- Stuxnetfoi revulucionário no sentido de não precisar de contato com uma central de comando e controle
  - CCC diz o que o malware deve fazer
- Stuxnet não poderia ter CCC
- Natanz era isolada por air gap
- Não existe "verdadeiro" air gap
  - necessário atualizar equipamentos
  - necessário baixar logs
  - ...
- Ilusão de que uma planta industrial não pode ser atacada porque não está conectada à Internet...

Malware autônomo

- Propagação autônoma
- Identificação do alvo
- Uma vez no alvo, liberar o ataque
  - Ataque não poderia ser cancelado – uma vez liberado, o malware faria seu serviço
- Grande "certeza" por parte de quem lançou o ataque – ataque não poderia ser cancelado

Zero Day exploit

- Atacam falhas de segurança não exploradas/não documentadas, contra a qual não existe correção conhecida (*patches*) uma vez que o próprio desenvolvedor da solução – a priori – não conhece a falha;
  - Antivírus não possuem as assinaturas para detectar;
  - Objeto de desejo de agentes mal intencionados → **valiosos**!
  - Existe mercado para isso!

Onde vender um Zero Day...

Mercado Branco

- Programas de recompensa de *bugs*
- Fabricantes de softwares
- Donos de websites
- Empresas de segurança

Mercado Cinza

- Governos
- Agências de Inteligência
- Agências de Segurança
- Comerciantes de armas digitais
- Presumidamente agindo no interesse da segurança pública

Mercado Negro

- Usuários maliciosos
- Criminosos
- Espiões corporativos
- Furtar dados bancários
- Furtar segredos empresariais
- Recrutar uma *botnet*

Stuxnet – Dados e Fatos

- *Zero Day exploit*
  - A venda de *exploits* é legal e em grande parte não regulamentada.
  - O preço dos *Zero Days* varia muito, dependendo:

1) da raridade da vulnerabilidade

2) do tempo e dificuldade para encontrar uma brecha e desenvolver um *exploit* para ela

3) da quão difundido é o software em que a brecha é encontrada; e

4) da exclusividade da venda.

Stuxnet – Dados e Fatos

- *Zero Day exploit*

Sistema	Valor (US$)
Adobe Reader	5.000,00 a 30.000,00
Mac OS	50.000,00
Flash	100.000,00+
Windows	100.000,00+
iOS da Apple	100.000,00
Firefox	60.000,00 até 200.000,00+
Internet Explorer	60.000,00 até 200.000,00+
Chrome	60.000,00 até 200.000,00+

Stuxnet: 4 Zero Days!

Dependendo das habilidades em contornar as proteções de segurança que os fabricantes tenham colocado no software.

Os ataques e a furtividade

- Ataques baseados na modificação dos parâmetros de operação das centrífugas
  - Padrão 1000Hz
  - Alterado para 1400Hz e para 2Hz
- Stuxnet permanecia inerte por treze dias
  - Sinais eram gravado e reenviados durante o ataque
- Num ciber-ataque ideal, a vítima não percebe que está sob ataque
  - Duvida de sua própria capacidade

Mudanças no código em 2010

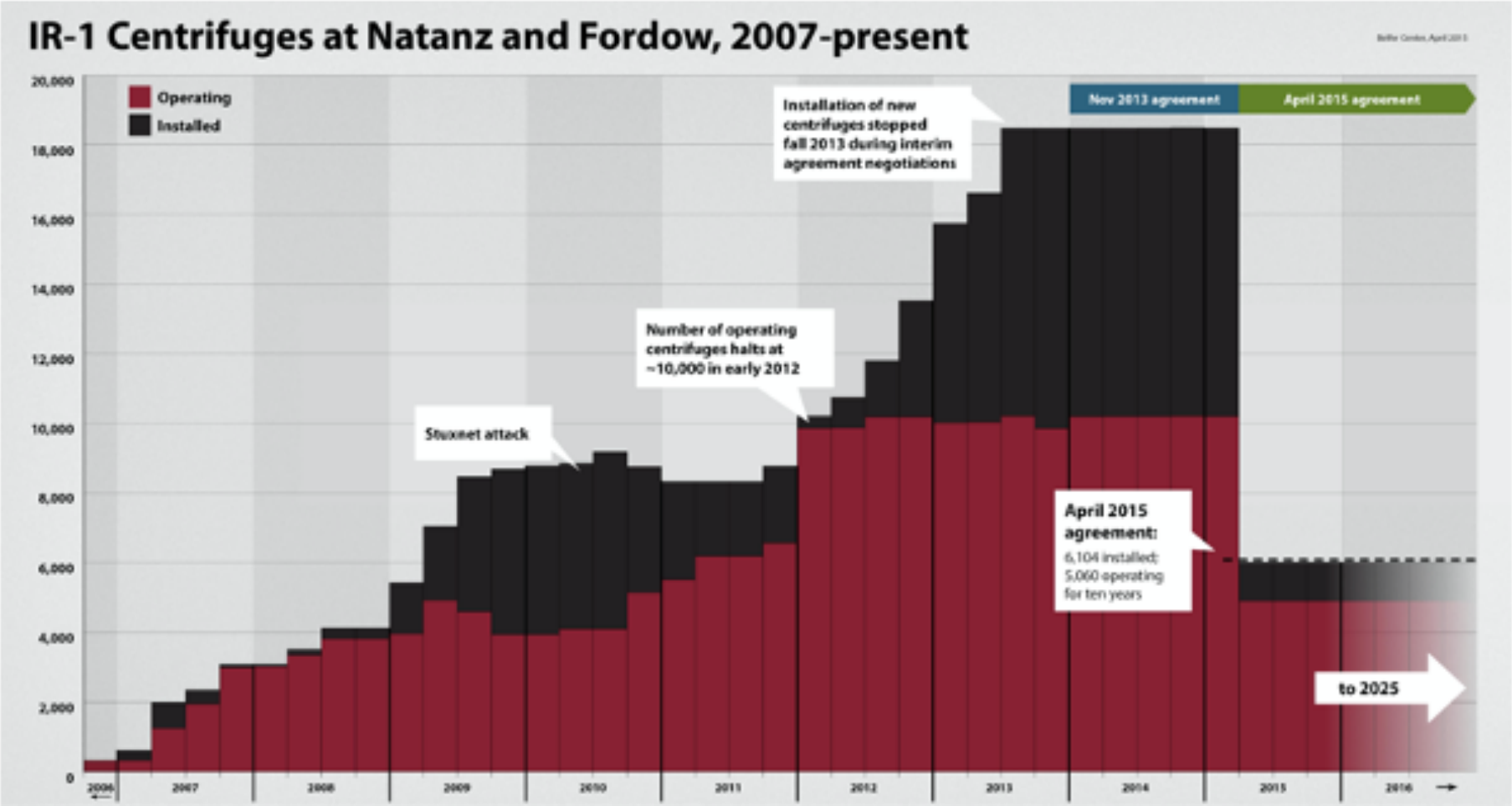
- Dificuldade em levar código até a usina
  - Versão 1.1
  - Versões anteriores eram menos "agressivas" – precisavam de algum "duplo-clique" pelos usuários.
- A versão 1.1 era tão "barulhenta" que chamou atenção da comunidade
  - Suposta ação dos israelenses (unidade 8200)
- Primeiras cinco infecções em fabricantes de sistemas industriais no Irã – fornecedores de Natanz
  - Ideia: funcionários levariam em seus pendrives e propagariam involuntariamente o malware em Natanz

Efeitos do Ataque (1)

- Atraso (um ano?) no programa nuclear iraniano
- Disseminação sem controle do malware
  - Obtido por nações "não-amigas"
- Possível caracterização como "ato de guerra"
- Efeitos "internos" – ação "defensiva" do DHS

- >>Não se assumiu autoria do ataque

Efeitos do Ataque (2)



Status sobre uso de armas cibernéticas

› Armas cibernéticas vs armas nucleares

Status sobre uso de armas cibernéticas

- Armas cibernéticas vs armas nucleares
  - PRESIDENTIAL POLICY DIRECTIVE/PPD-20

Status sobre uso de armas cibernéticas

› Armas cibernéticas vs armas nucleares
  – PRESIDENTIAL POLICY DIRECTIVE/PPD-20

TOP SECRET/NOFORN

PRESIDENTIAL POLICY DIRECTIVE/PPD-20

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
DIRECTOR OF NATIONAL INTELLIGENCE
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND COUNTERTERRORISM
DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: U.S. Cyber Operations Policy (U)

Status sobre uso de armas cibernéticas

› Armas cibernéticas vs armas nucleares
  – PRESIDENTIAL POLICY DIRECTIVE/PPD-20

IV. Cyber Operations with Significant Consequences (U)

Specific Presidential approval is required for any cyber operations - including cyber collection, DCEO, and OCEO - determined by the head of a department or agency to conduct the operation to be reasonably likely to result in "significant consequences" as defined in this directive. This requirement applies to cyber operations generally, except for those already approved by the President, even if this directive otherwise does not pertain to such operations as provided in the "Purpose and Scope" section of this directive. (S/NF)

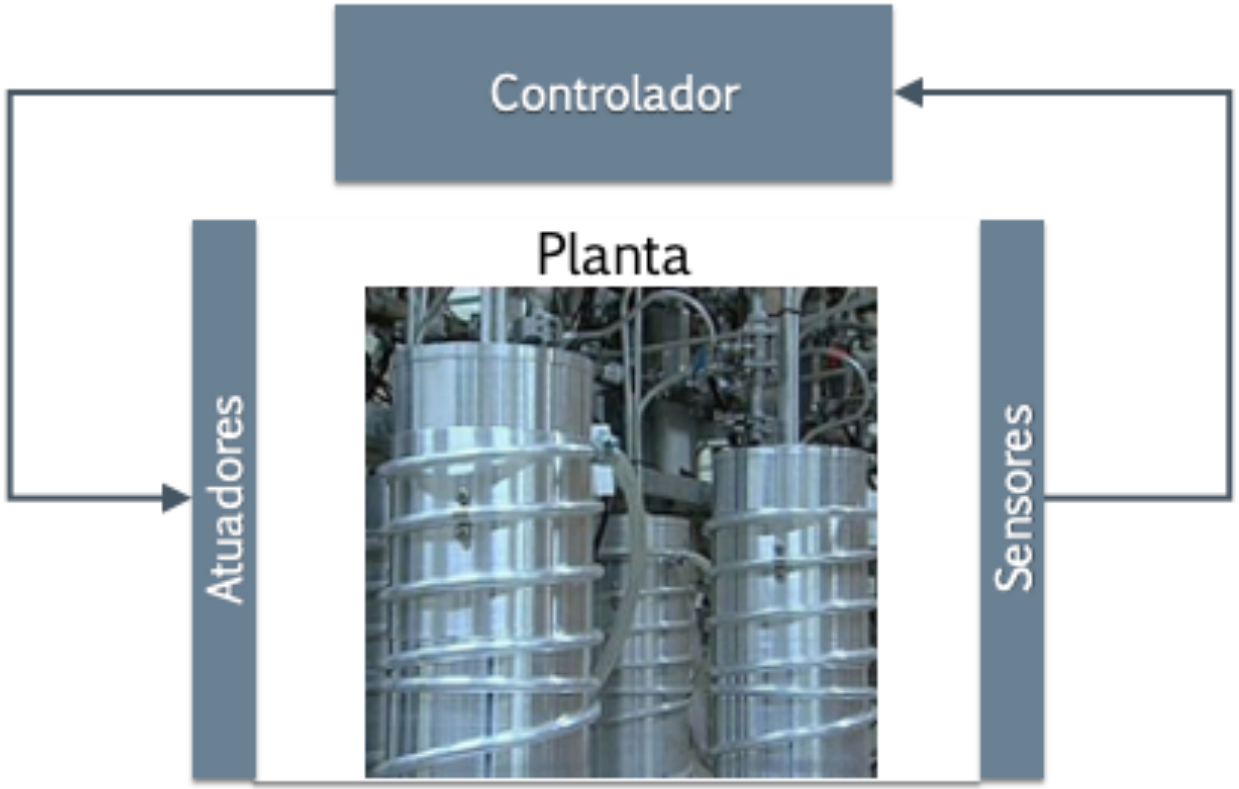
Status sobre uso de armas cibernéticas

- Armas cibernéticas vs armas nucleares
  - PRESIDENTIAL POLICY DIRECTIVE/PPD-20
  - Impacto potencial
  - Necessidade de "discussão"
    - Doutrina nuclear surgiu de mais de 20 anos de discussões
- Assunto ainda "superclassificado"
  - Armas cibernéticas surgem da comunidade de inteligência
- Dificuldades
  - Atribuição de responsabilidade
  - Inspeção

Mais sobre Stuxnet

Questões técnicas

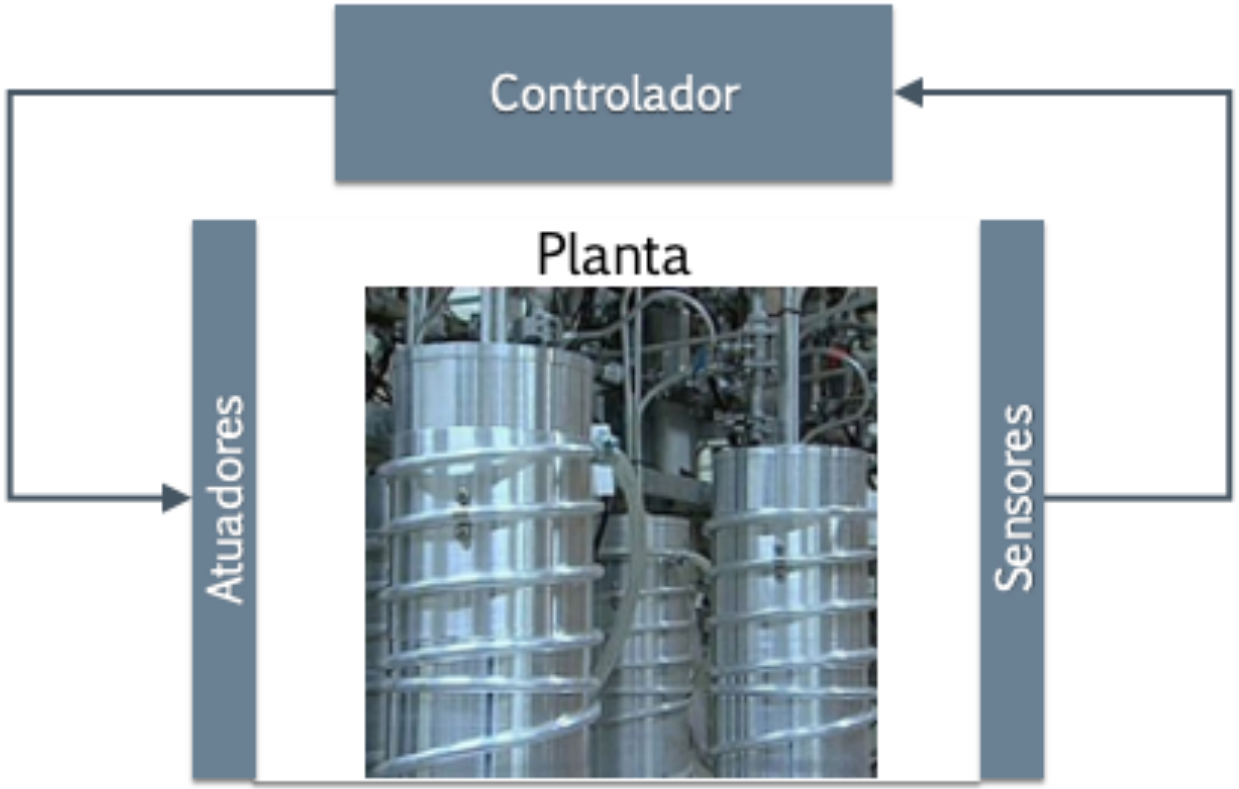
Sistemas de Controle em Rede



Plantas:

- Geração e distribuição de energia;
- Tratamento de água;
- Linhas de produção;
- Transporte;
- ...

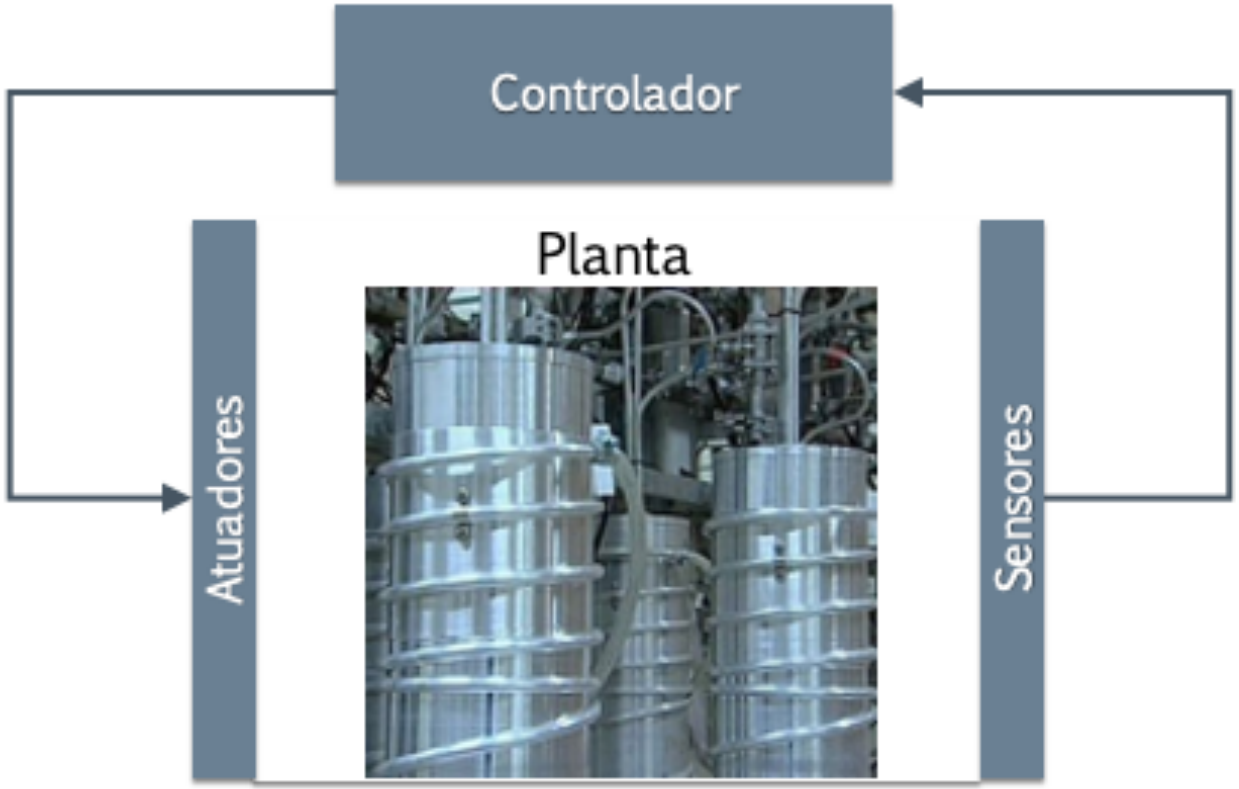
Sistemas de Controle em Rede



Sensores:

- Pressão;
- Temperatura;
- Velocidade;
- Vazão;
- ...

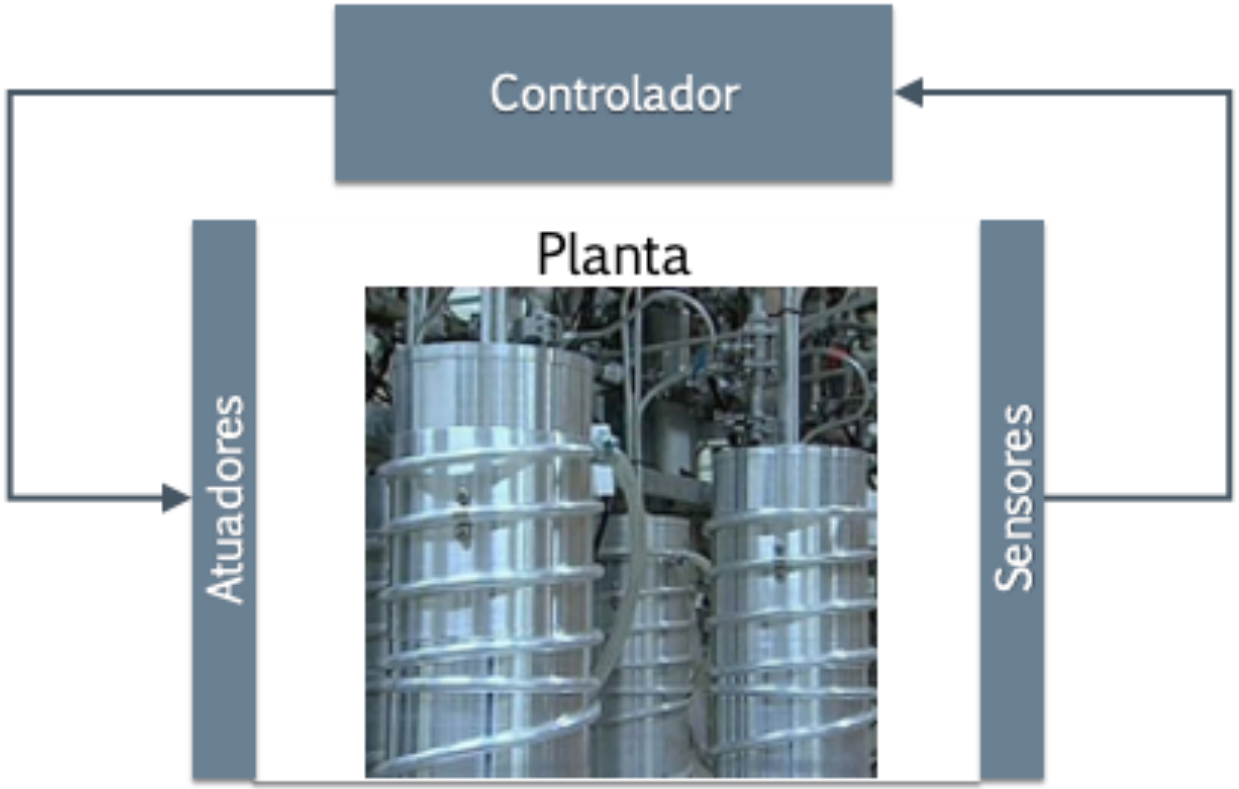
Sistemas de Controle em Rede



Atuadores:

- Motores;
- Válvulas;
- Bombas;
- ...

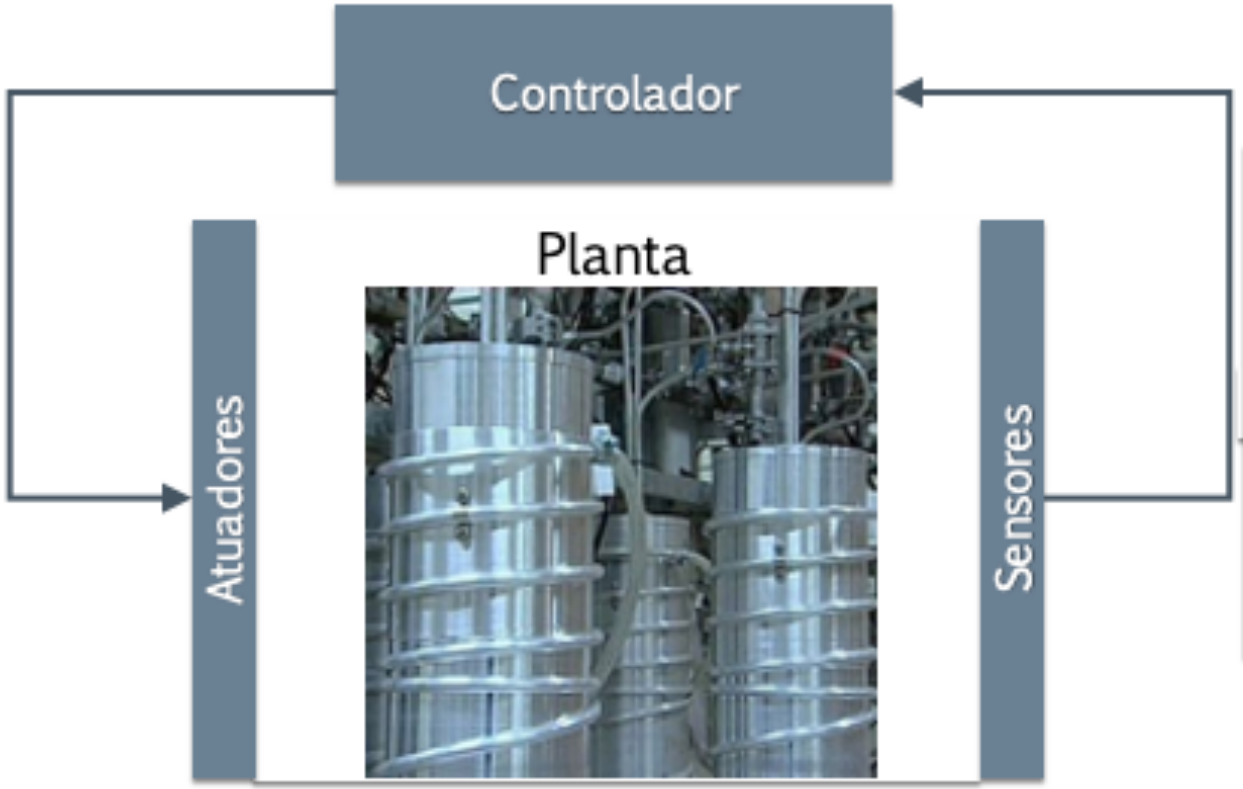
Sistemas de Controle em Rede



Controlador Lógico Programável (CLP):

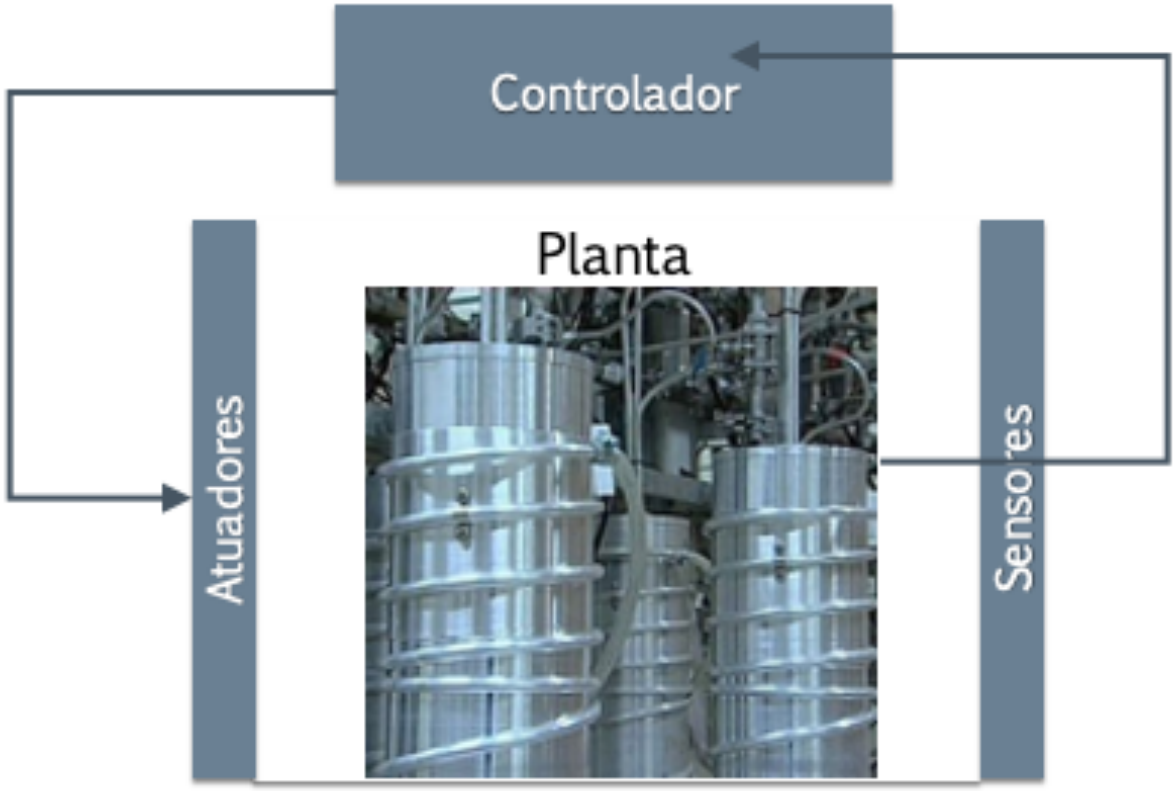
- Controle lógico combinacional / sequencial.
- Controle de plantas analógicas (via conversores A/D e D/A)

Sistemas de Controle em Rede



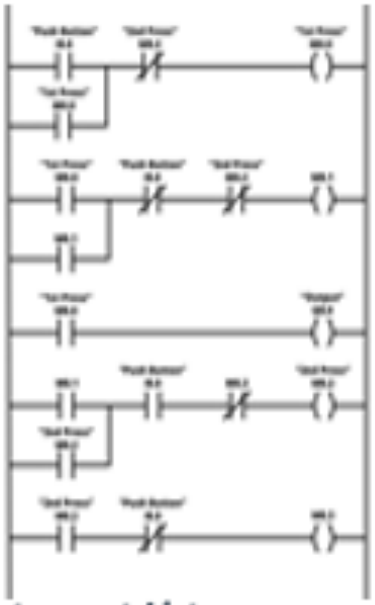
- Controlador Lógico Programável

Sistemas de Controle em Rede



Controlador Lógico Programável (CLP):

Ladder



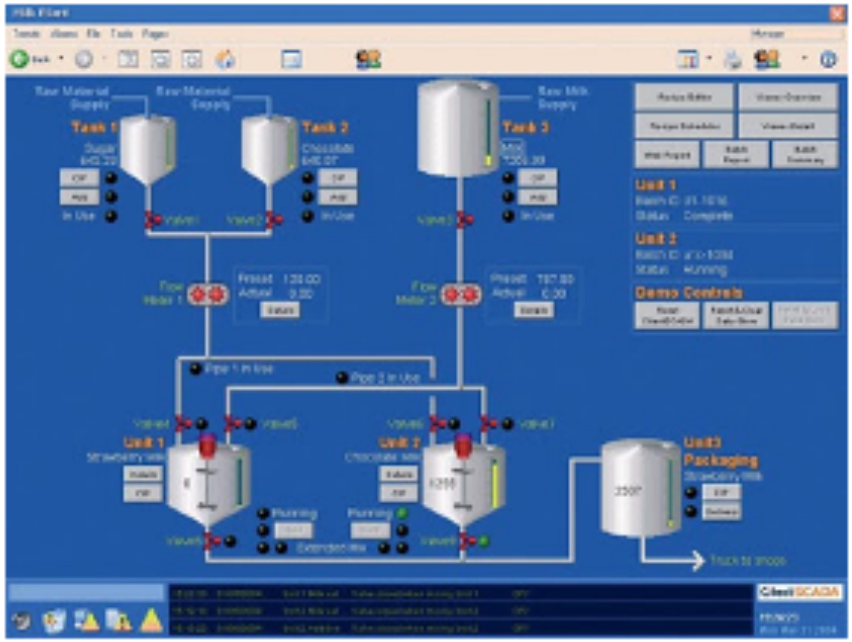
*STL**

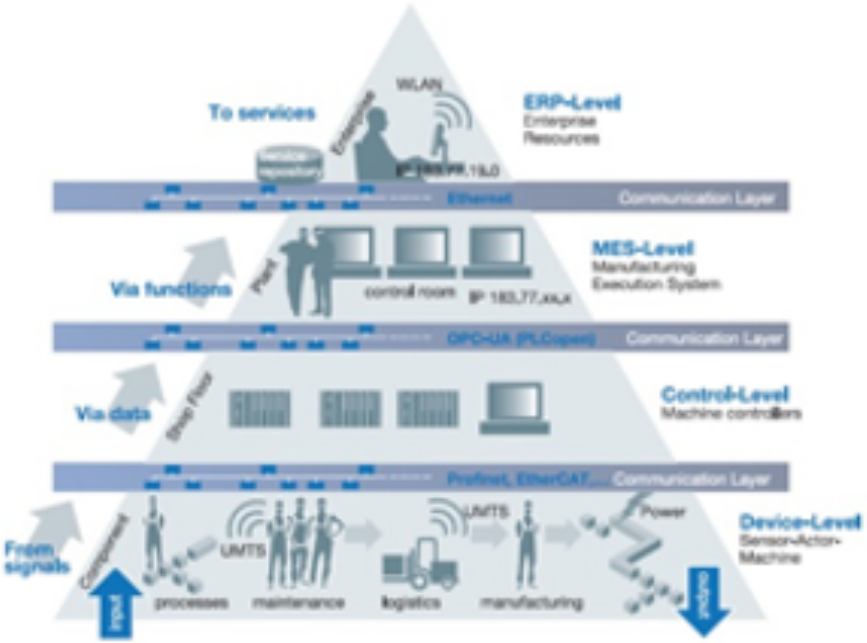
```
M117:  L      LW0
       L      164
       <=I
       SPBN   M101
       L      LW0
       L      1
       >=I
       L      LW0
       L      2
       =      L14.2
       <=I
       U      L 14.2
       SPBN   M102
       L      LW0
       ITD
```

* ***Statement List*** *programming language*

Sistemas de Controle em Rede

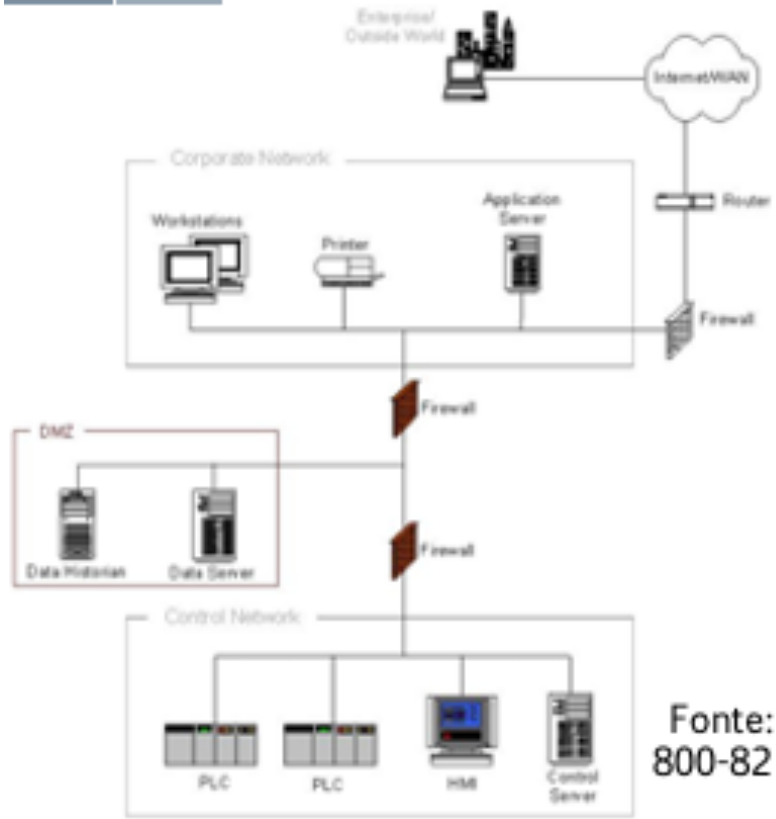
Supervisory Control and Data Acquisition (SCADA)



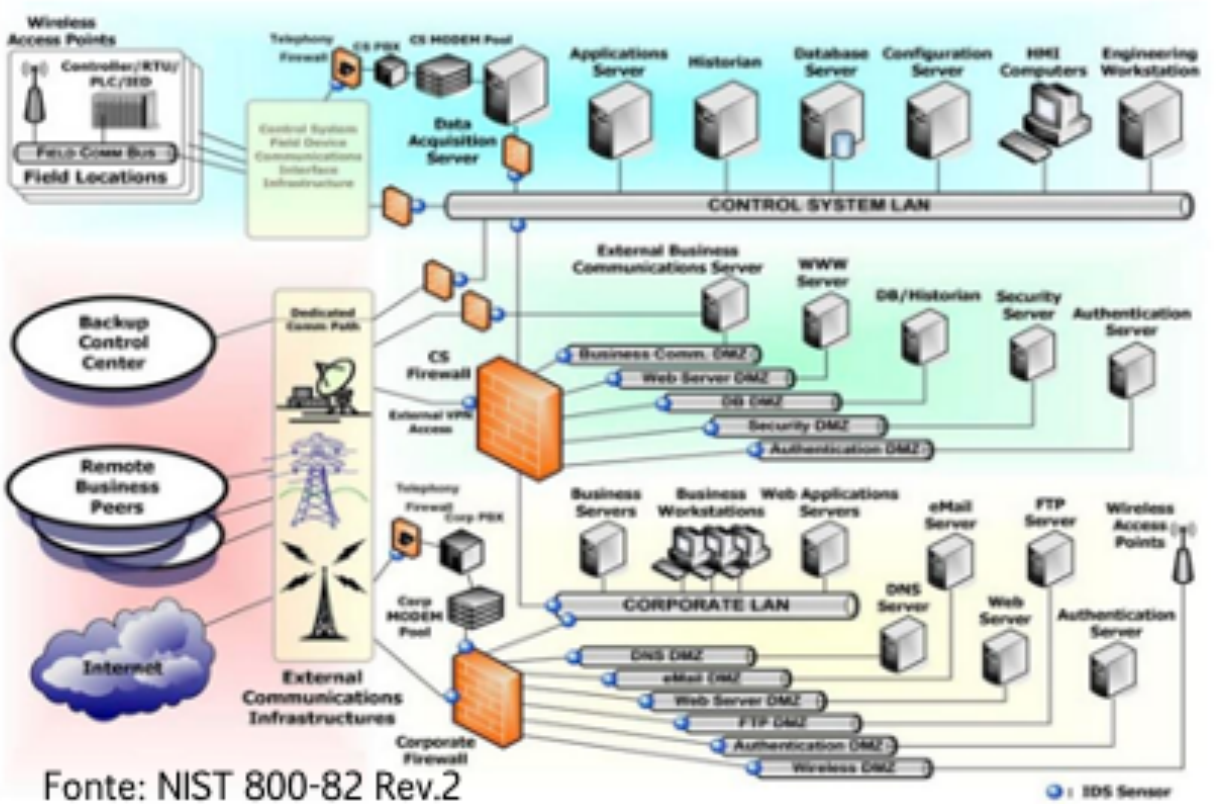


Sistemas de Controle em Rede

Segurança em sistemas SCADA



Fonte: NIST 800-82 Rev.2



Fonte: NIST 800-82 Rev.2