Cisco Self-Defending Network
Redes Capazes de Auto Defesa

Daniel Barossi Garcia

CISSP, CCSP, CCIE

Mar 2006

Estratégia de Otimização de Processos e Negócios: O Papel Da Rede

EVOLUÇÃO DA ESTRATÉGIA DE REDES

CONECTIVIDADE  REDE INTELIGENTE

- OTIMIZAÇÃO DOS PROCESSOS DE NEGÓCIOS
  OTIMIZAÇÃO REQUER UMA REDE INTELIGENTE

POR QUE REDES INTELIGENTES?

- A Rede toca todas as partes do processo de negócios
- Aplicativos e serviços estão ***individualmente*** mais eficientes
- Aplicativos e serviços trabalham ***em conjunto*** para uma eficiência maior

O Novo Paradigma da Segurança - SDN

Cisco.com

SEGURANÇA

Self Defending Network

d Messaging
Services
Instant Messaging
Contact Center

A Internet sempre foi “Terra de Ninguém”

- A falta de regulamentação fez da Internet uma “terra de ninguém”
- Em 2004 vimos uma escalada no uso de programas destinados ao crime cibernético. Os ganhos financeiros são o principal motivador para esses crimes.

- Sete dos dez hackers mais ativos do mundo são brasileiros
- Brasil vira centro de crimes digitais, diz 'NY Times‘
- Evitar vírus de computador 'estressa mais que divórcio'

Fonte: BBC Brasil

Evolução das Ameaças

Cisco.com

O Verme Sapphire ou “Slammer”

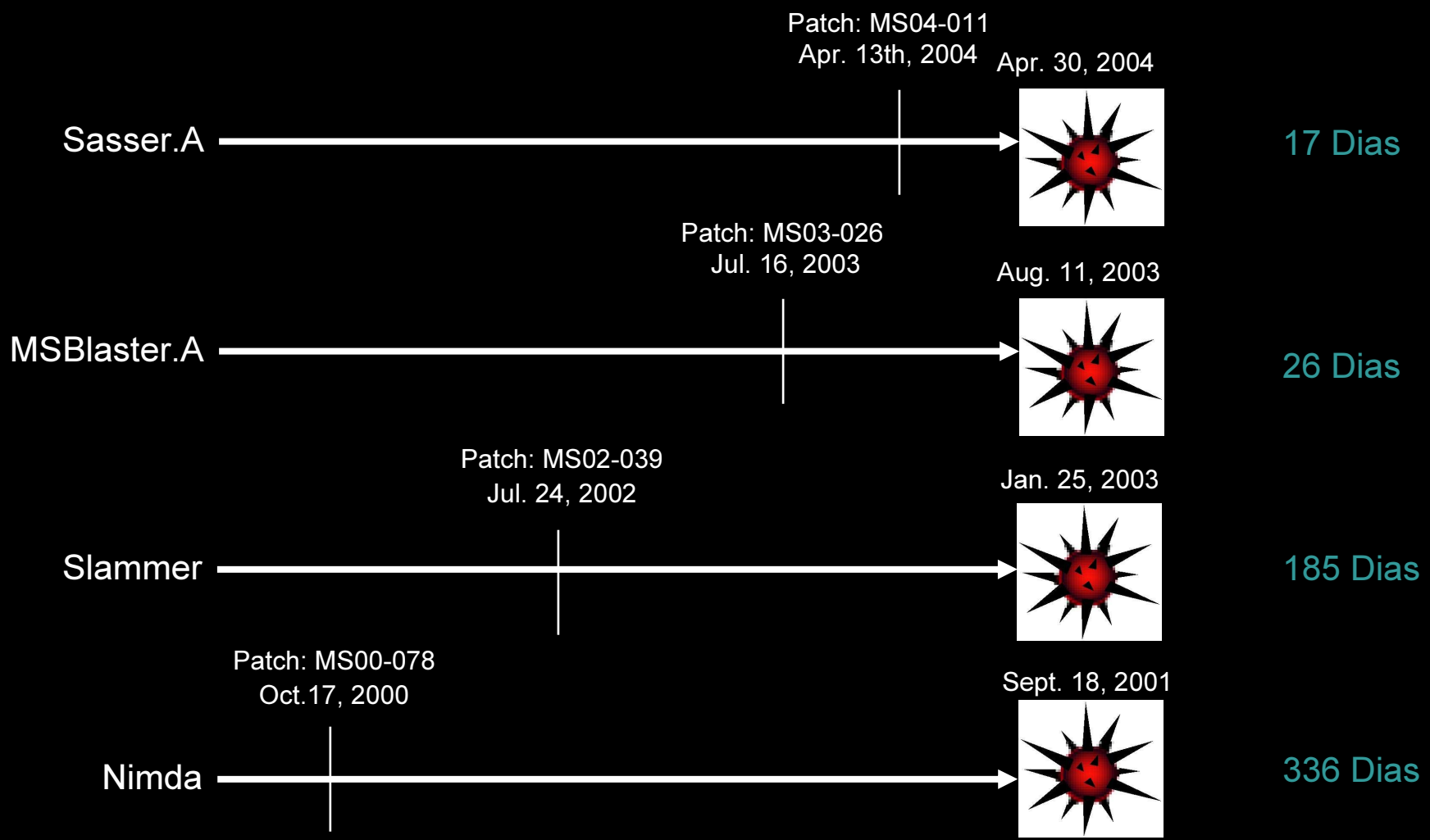
- Infeção dobrava a cada 8.5 segundos
- Infectou 75,000 hosts nos primeiros 11 minutos
- Causou parada de redes, cancelamento de voos e falhas em “Caixas Eletrônicos”

Minutos após o lançamento

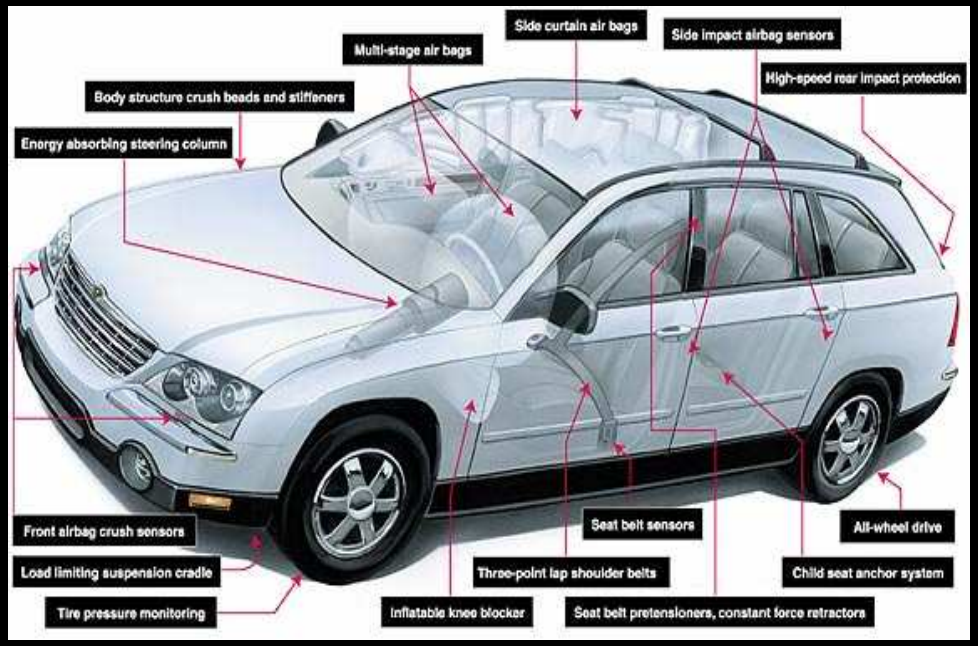
O Que Deu Errado?

- Dispositivos tradicionais de segurança NÃO conseguem evitar que vermes como o SQL Slammer executem o ataque e se espalhem
  - Passam por firewalls permitindo tráfego
  - Não são detectados pelos anti-virus sem uma atualização
  - Não são detectados pela maioria dos dispositivos de IDS sem uma nova assinatura
  - Produtos HIDS tradicionais não protegeram adequadamente os servidores sem uma atualização das assinaturas
- Dispositivos tradicionais de segurança NÃO conseguem evitar que vermes como o Slammer afetem a rede
  - Produtos pontuais não evitam Denial of Service
  - Produtos pontuais não evitam a propagação entre servidores
  - Produtos pontuais não previnem ataques cgi-bin, buffer overflows, fragmented attacks, Unicode attacks, SQL, etc.

Tempo entre a disponibilidade do patch e das ferramentas para explorar as vulnerabilidades diminui



Como Você Quer a Sua Segurança?



Segurança como uma opção

- Segurança como um aditivo
- Integração extremamente complicada
- Não é economicamente viável
- Não pode focar na principal prioridade

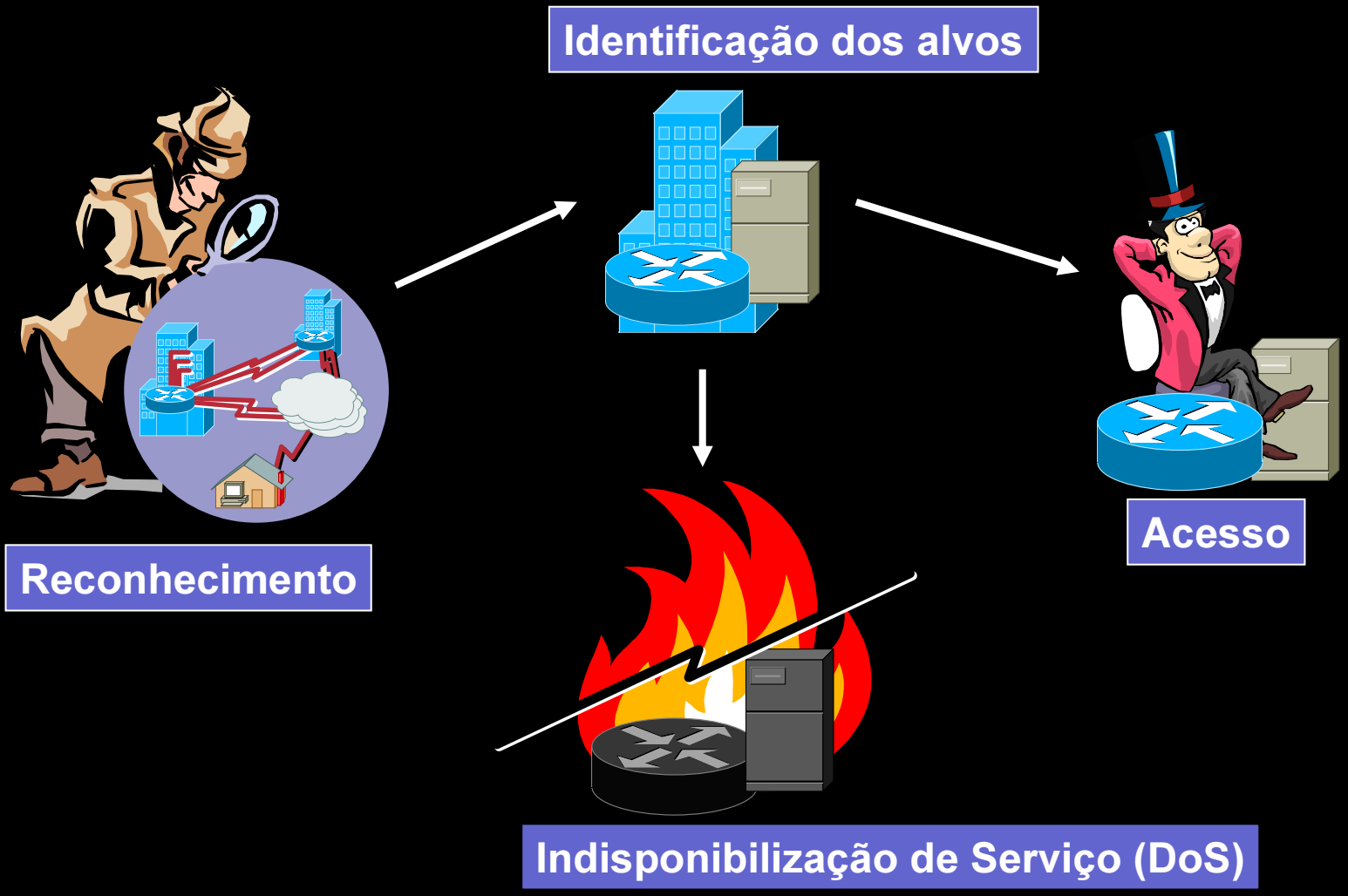
Segurança como parte do sistema

- Segurança Embutia à rede
- Colaboração inteligente
- Segurança apropriada
- Foco direto na principal prioridade

Firewall é Apenas Parte da Solução...

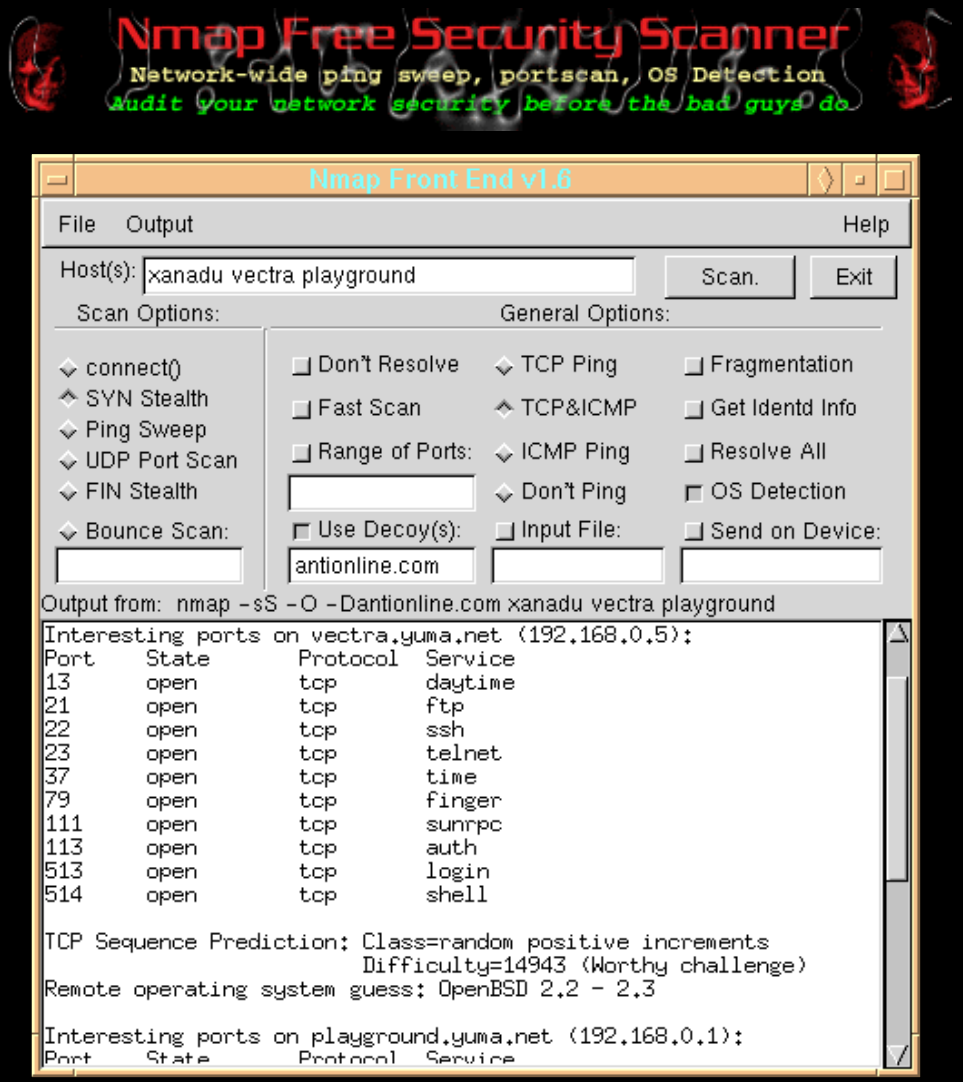
Existem Ferramentas Mais Apropriadas...

Passos típicos de um ataque



Exemplo de Scanner : NMAP

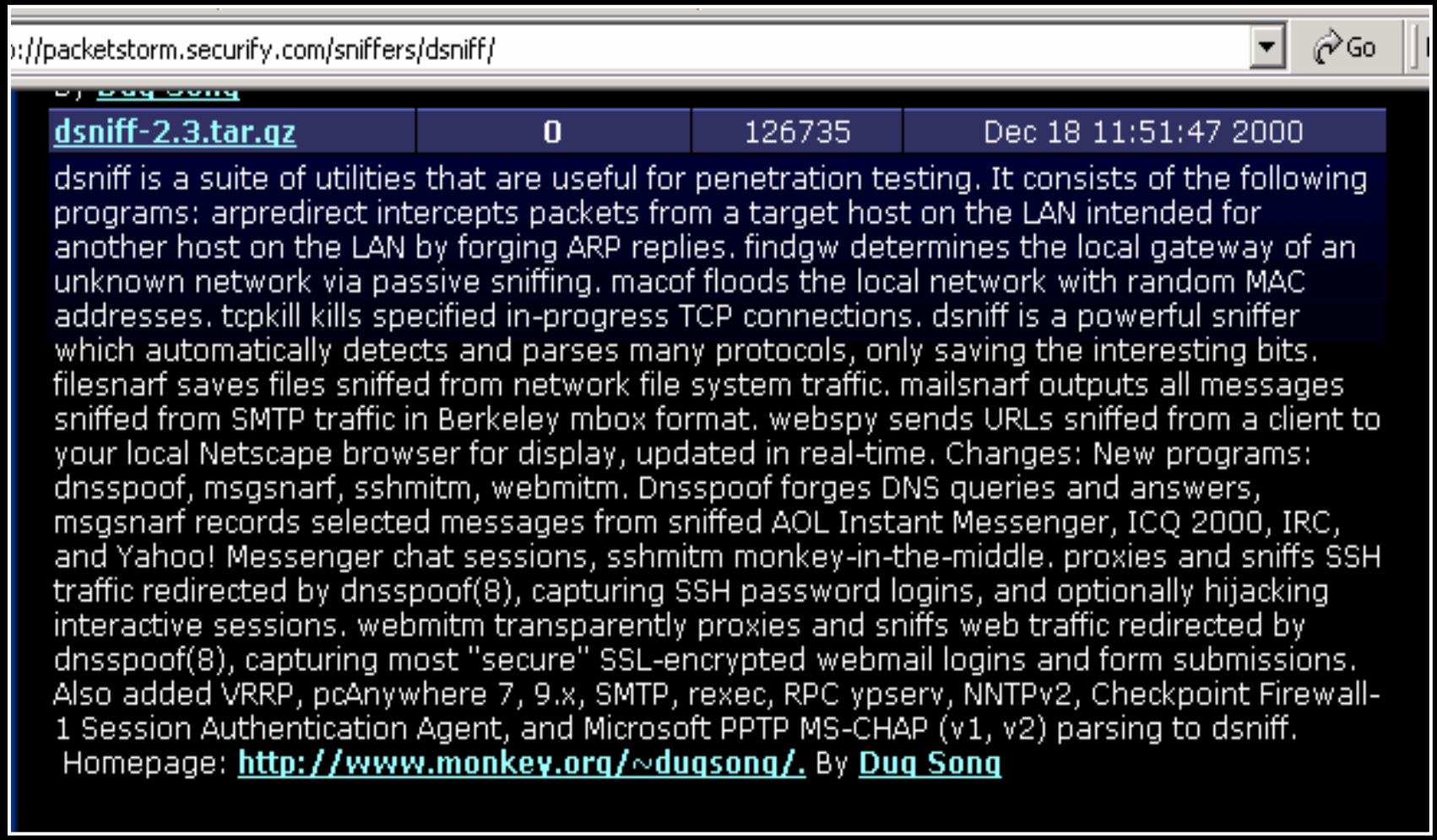
- **Sweep options**
  - Fast and slow scans
  - Port ranges (for services)
- **Device detection (some of the tests):**
  - UDP, TCP connect, TCP SYN, ftp proxy (bounce), reverse-ident, ICMP ping sweep, FIN, ACK Sweep, Idlescan (IPID-based)
- **OS detection (some of the tests):**
  - FIN probe RESET or ignored?
  - TCP ISN sampling
  - IPID sampling
  - Don’t frag set?
  - TCP initial window
  - ICMP error messaging integrity
  - TCP options responses



Após o Reconhecimento: Pesquisar vulnerabilidades

Novas técnicas e ferramentas disponíveis na WEB

Cisco.com



SANS: Windows Top10 Vulnerabilities

W8 LSAS Exposures

W8.1 Description

The Windows Local Security Authority Subsystem Service on Windows 2000, Server 2003 and Server 2003 64 Bit, XP and XP 64 Bit editions contains a critical buffer overflow that if exploited can lead to full system compromise. This overflow is outlined in the Microsoft Security Bulletin MS04-011. This attack can be accomplished remotely and anonymously over RPC on un-patched Windows 2000 and XP systems but requires administrative privileges to be effective.

While Windows Server 2003 and Windows XP 64 bit 2003 Edition products did contain the vulnerability, the /GS overflow protection that's was added to certain parts of the OS prevented Sasser from doing any significant damage or a full system compromise.

The Local Security Authority Subsystem Service (LSASS) plays an important role in system authentication and Active Directory functionality. It is here in the interface process with Active Directory that the logging function of the LSASRV.dll can be overflowed with an inordinately long string. Potentially this vulnerability can lead to full system compromise.

The gravity of the fact that this vulnerability can be easily exploited remotely is demonstrated by the recent propagation of the LSASS based Sasser and Korgo worms. Also known as W32.Sasser (http://www.cert.org/current/archive/2004/07/12/archive.html#sasser, http://www.microsoft.com/security/incident/sasser.mspx) and W32.Korgo (http://www.cert.org/current/archive/2004/07/12/archive.html#korgo). Many recent malicious "bot" worms use this vulnerability for infection as well and their importance as a developing security issue is growing daily and often overlooked.

The vulnerability has been assigned CVE number CAN-2003-0533. It is strongly encouraged that network administrators not only patch their systems against this vulnerability but implement all necessary access controls at network ingress points to stop Windows RPC based abuses from entering vulnerable environments.

W8.2 Operating Systems Affected

Windows 2000, Windows XP and Professional, Windows XP 64-Bit Edition, Windows 2003

W8.3 CVE/CAN Entries

CVE-1999-0227
CAN-2003-0507, CAN-2003-0533, CAN-2003-0663, CAN-2003-0818

W8.4 How to Determine if You Are Vulnerable:

This vulnerability can either be checked across the network or locally on the system itself. A network check is best-suited to security and network administrators who need to detect vulnerable machines within a network or an IP range. A localized check suits end-users who need

SANS UNIX U1: BIND (ainda o BIND...)

U9 BIND/DNS

U9.1 Description

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of the Domain Name Service (DNS), the system that allows one to locate a server on the Internet (or a local network) by using its name (e.g., www.sans.org) without having to know its specific IP address. The ubiquity of BIND has made it a frequent target of attack. While BIND developers have historically been quick to repair vulnerabilities, an inordinate number of outdated or misconfigured servers remain

A number of factors contribu
aware of security upgrades,
unnecessarily, and bad conf
overflow or DNS cache poisc
denial of service, discussed
specific DNS packets to forc
cause the BIND daemon to s
Advisory CA-2002-19, in wh
libraries. By sending maliciou
execute arbitrary code or ev

In addition to the risk a vuln
machine may provide a platf
be used as a repository of il

U9.2 Operating Systems A

Nearly all Unix and Linux sys
enabled. Binary versions of E

U9.3 CVE Entries

CVE-1999-0009, CVE-1999-
CVE-1999-0024, CVE-2001-
CAN-2002-0400

Carnegie Mellon Software Engineering Institute

CERT® Coordination Center

Home | Site Index | Search | Contact | FAQ

vulnerabilities, incidents & fixes | security practices & evaluations | survivability research & analysis | training & education

Options

Advisories

Vulnerability Notes Database

Incident Notes

Current Activity

Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CERT® Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries

Original release date: June 28, 2002
Last revised: September 9, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

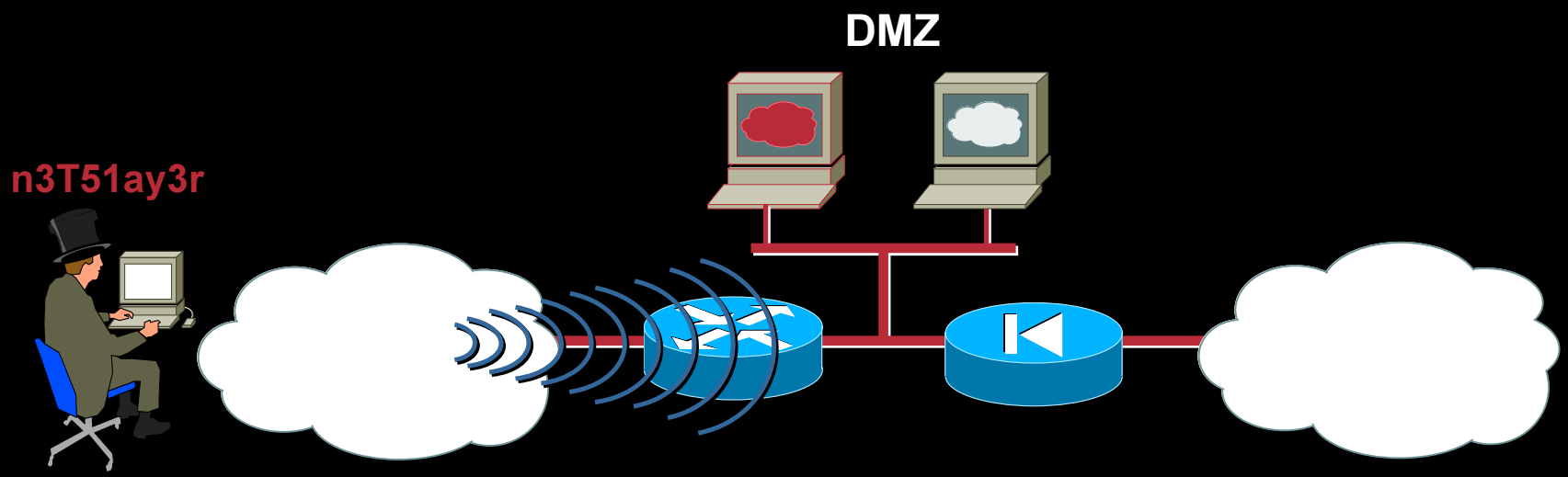
Applications using vulnerable implementations of the Domain Name System (DNS) resolver libraries, which include, but are not limited to

- Internet Software Consortium (ISC) Berkeley Internet Name Domain (BIND) DNS resolver library (libbind)
- Berkeley Software Distribution (BSD) DNS resolver library (libc)
- GNU DNS resolver library (glibc)

Overview

Buffer overflow vulnerabilities exist in multiple implementations of DNS resolver libraries. Operating systems and applications that utilize vulnerable DNS resolver libraries may be affected. A remote attacker who is able to send malicious DNS responses could potentially exploit these vulnerabilities to execute arbitrary code or cause a denial of service on a vulnerable system.

Ao ataque !

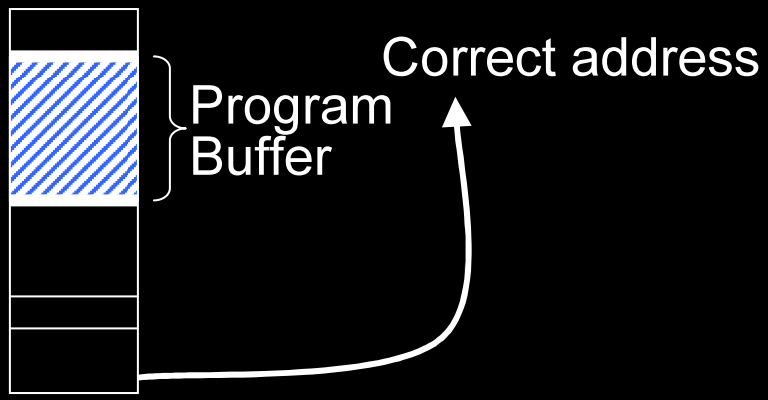


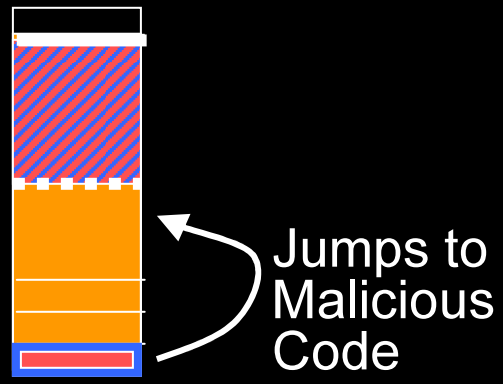
- Reconhecimento, pesquisa de vulnerabilidades…
- Versão antiga (e vulnerável) do BIND descoberta em um servidor
- Acesso “root” obtido, logs apagados e “rootkit” instalado
- (Só o começo da brincadeira…)

Um problema cada vez mais comum: Buffer Overflow

Exemplo: SNMP

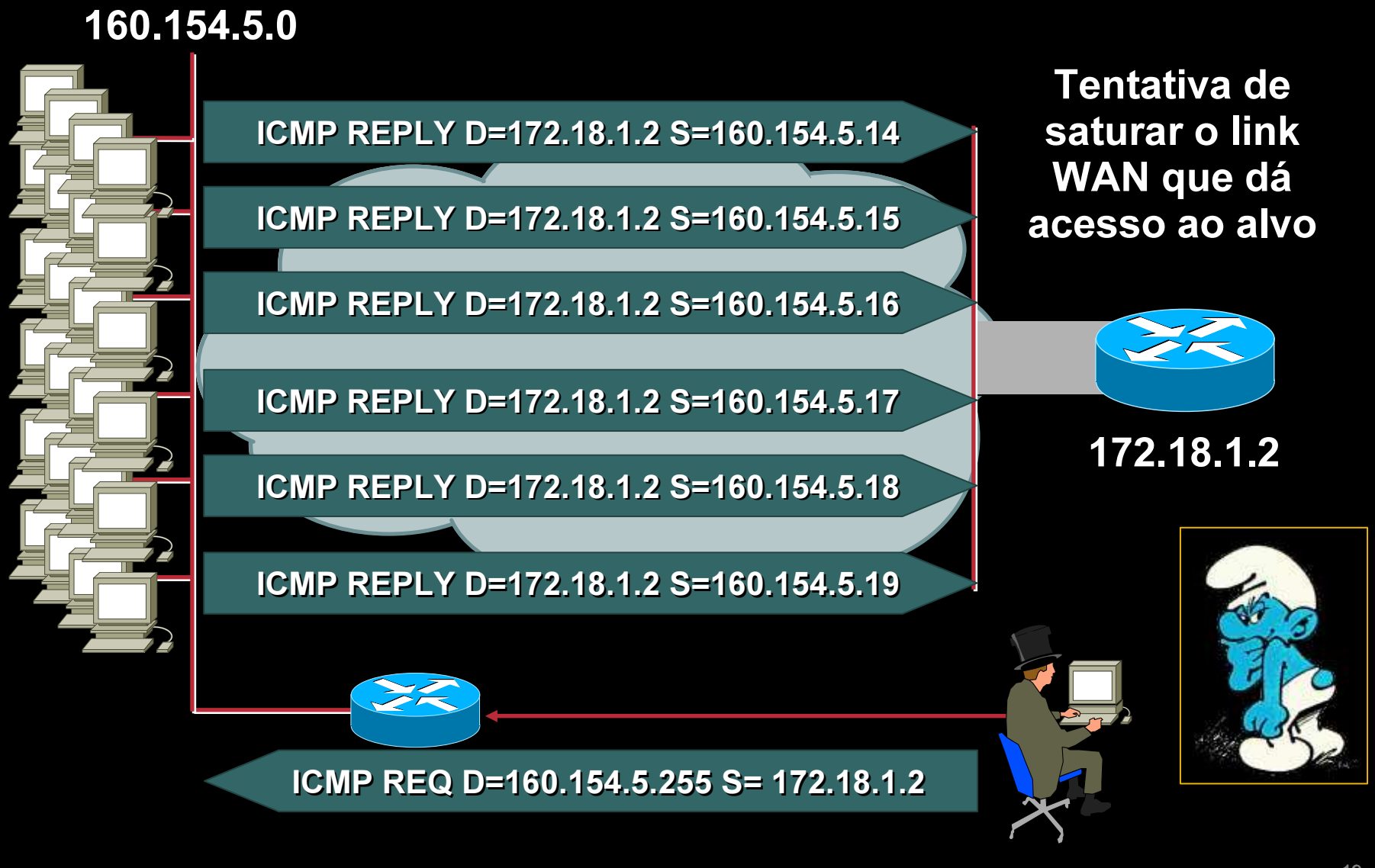
Se alguns parâmetros de pacotes em versões vulneráveis do protocolo SNMP forem muito grandes, eles poderão causar um "buffer overflow"





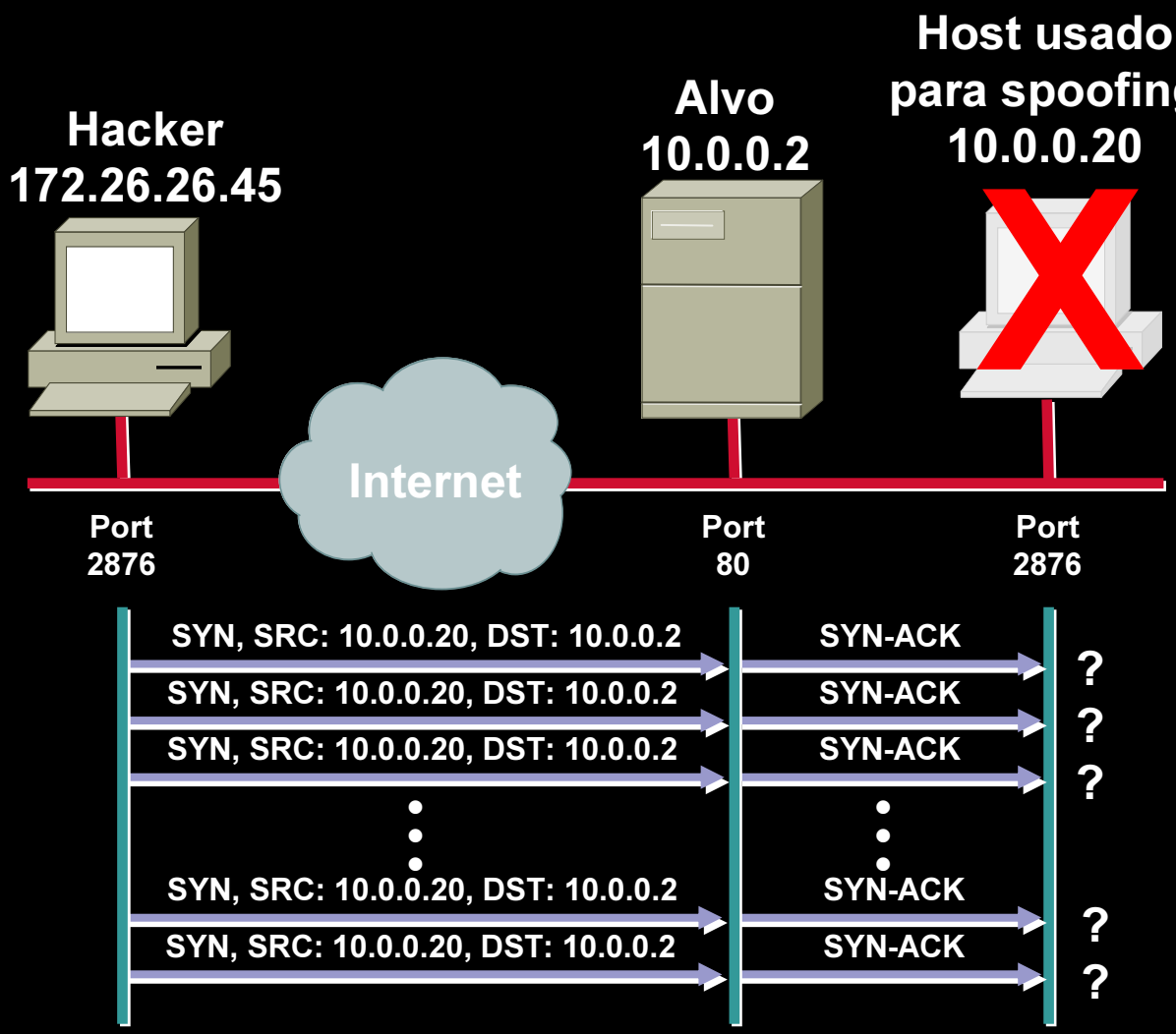
Bad address to jump to when the current function ends

Smurf Attack: um exemplo de “Denial of Service”

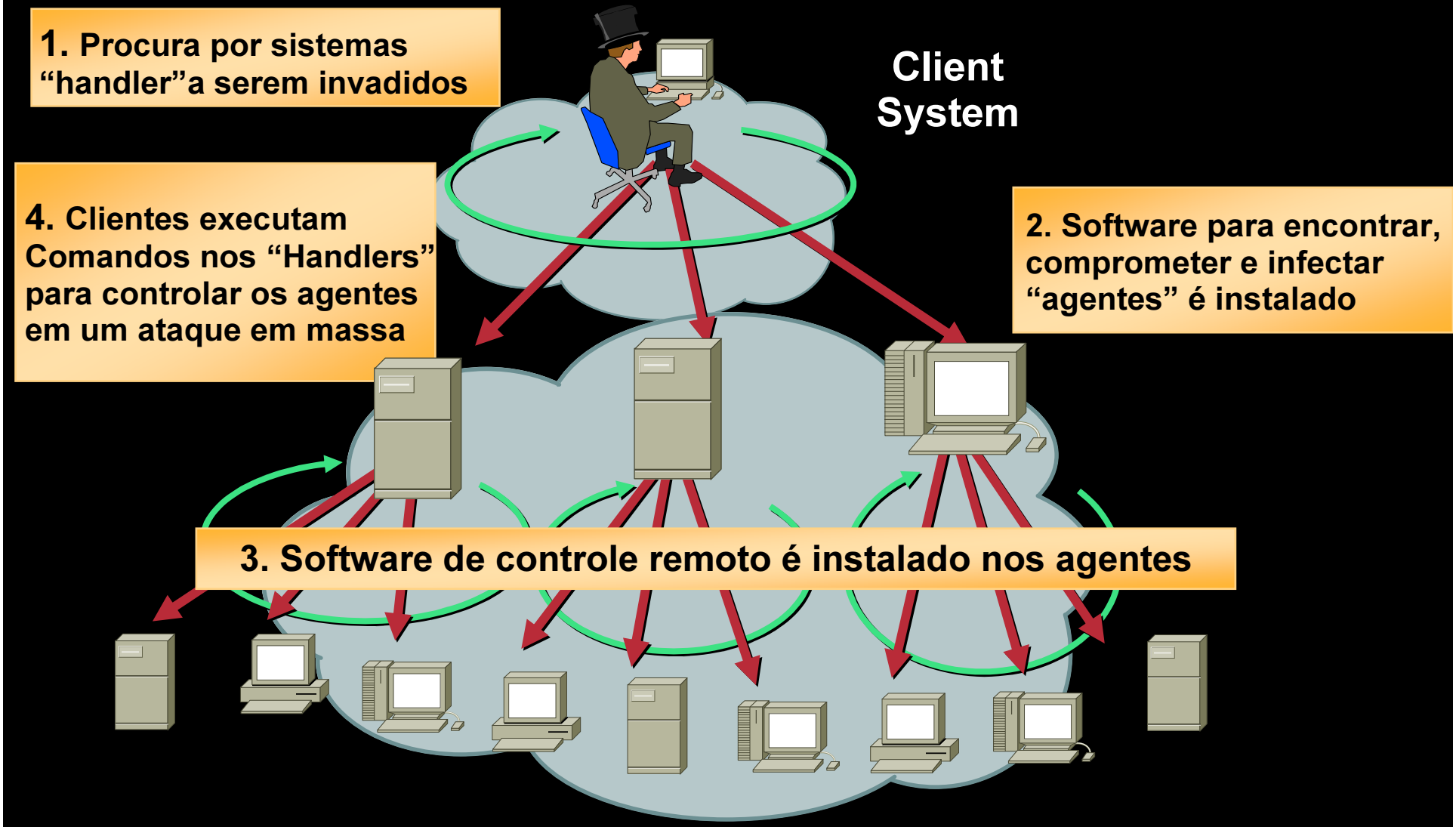


SYN Flood: mais um clássico “Denial of Service”

- O hacker forja o endereço IP de origem, usando um endereço não existente.
- O alvo responde aos pacotes SYN enviando pacotes SYN/ACK para o suposto host (endereço forjado)
- O alvo satura seus buffers com conexões TCP incompletas (pois nunca receberá resposta do host não existente) e para de responder às requisições legítimas.

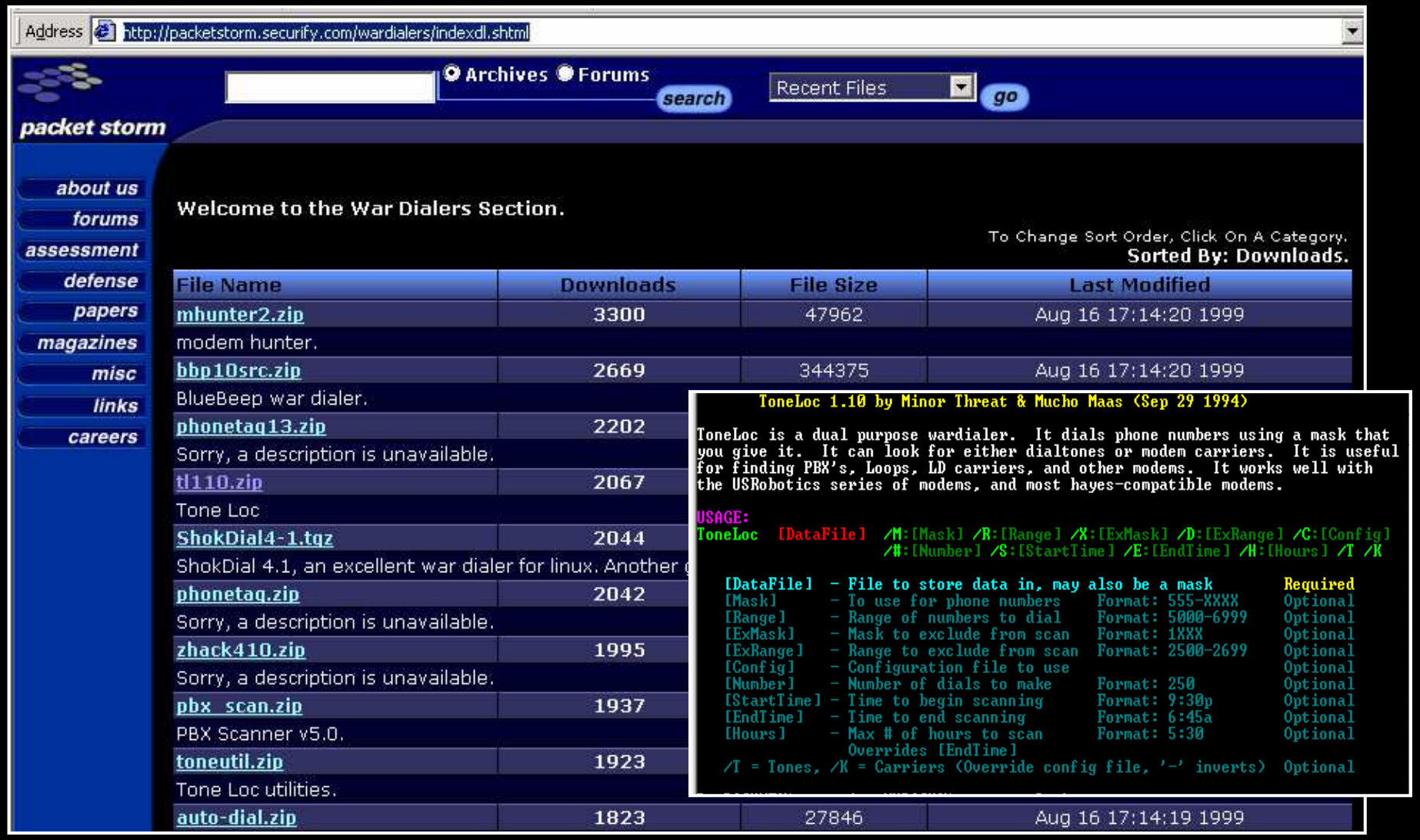


Distributed Denial of Service



War Dialers: o acesso remoto pode ser o ponto fraco

Cisco.com



“Drive-By Hacking”

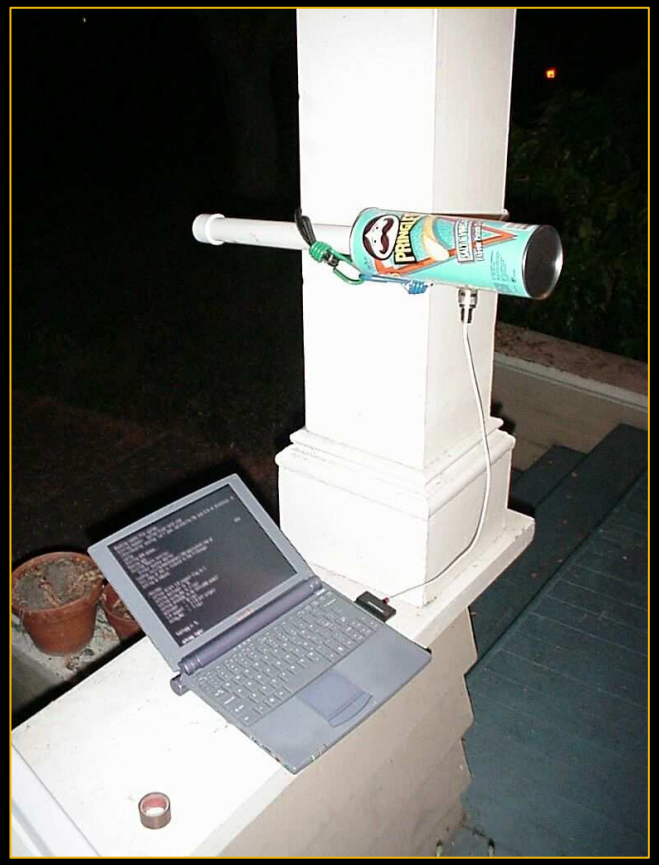
…Is Possible as It Has Been Proven by “

- Cruising with a car + laptop + WLAN card
- + GPS scanning for (unprotected) 802.11 wireless networks
- + Perl script to log the SSID, AP’s MAC address, best S/N ratio and location (GPS)

www.personaltelco.net/index.cgi/WarDriving

Hacking a grandes distâncias

> "Over a clear line of sight, with short antenna cable runs, a 12db to 12db can-to-can shot should be able to carry an 11Mbps link well over ten miles."
>
> Rob Flickenger, O'Reilly Systems Administrator

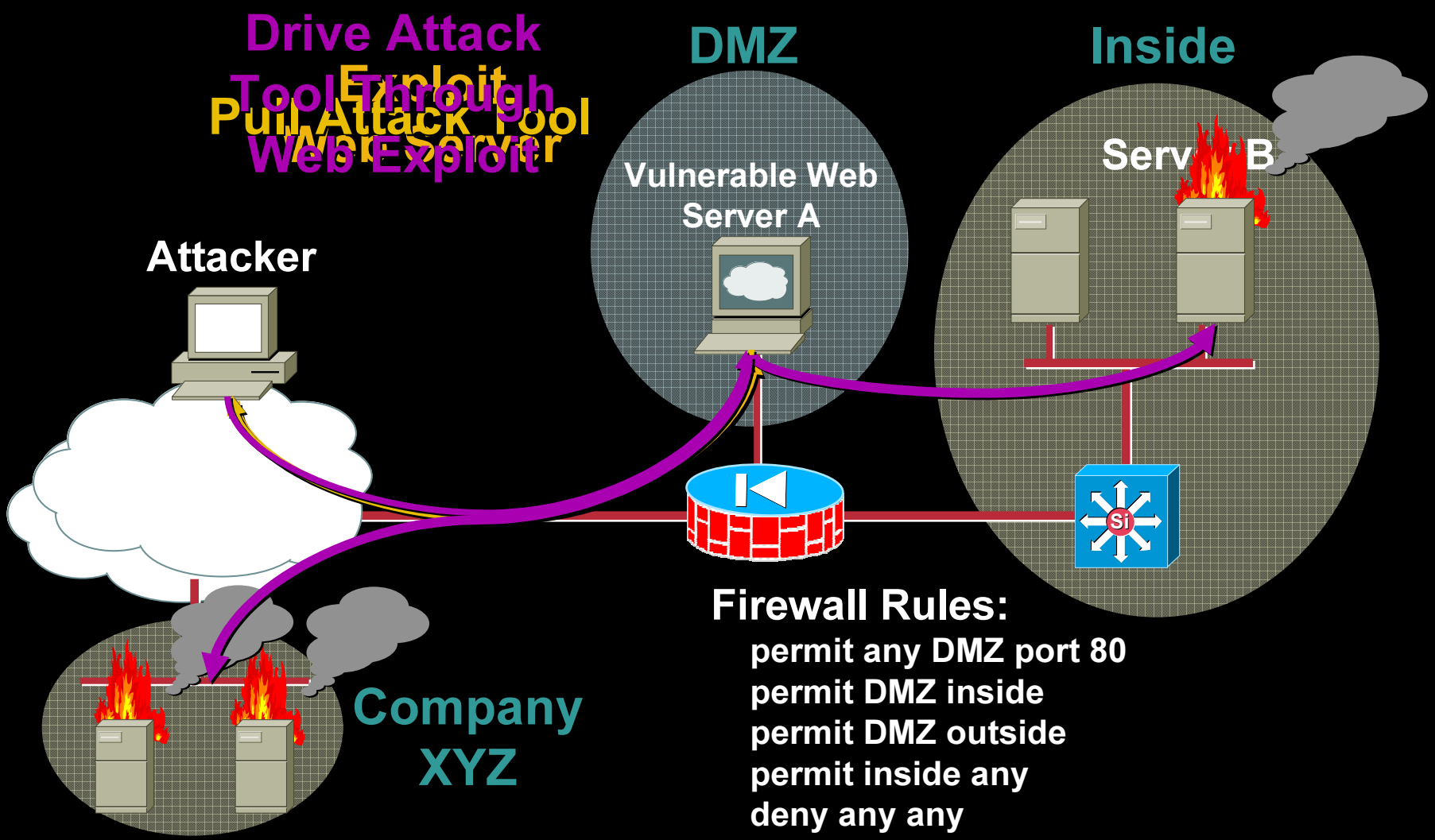


- "Pringles" YAGI Antenna
  - Custo: US$10
  - Alcance: 10 Milhas
  - Já foi possível atacar alvo em lado oposto do Rio Hudson (separando New Jersey e New York)

Moral: Não confie tanto em distância!

http://www.oreillynet.com/cs/weblog/view/wlg/448

Atacando através do Firewall



Precisamos mudar a abordagem de segurança

Cisco.com

Passado	Necessário Hoje
Reativo	Automático, Pró-ativo
Standalone	Integrado, Múltiplas Camadas
Produtos Pontuais	Network / Sistema Final

A Abordagem de Segurança Estratégica!!!

Estratégia Self-Defending Networks

Segurança Integrada

Sistema de Segurança Colaborativo

Sistema de defesa pró-ativo (ATD)

Evolução da Estratégia de Segurança Cisco

Cisco.com

SDN Fase III *"Defesa Adaptável contra ameaças"*

- Reconhecimento mútuo entre Serviços de Segurança & inteligência de Rede & aplicativos
- Aumenta a eficiência da Segurança, permite respostas pró-ativas.
- Consolidação de serviços, aumento da eficiência operacional
- Reconhecimento e inspeção de aplicativos para garantir a otimização dos serviços.

SDN Fase II *"Sistema de Segurança Colaborativo"*

- Segurança se torna um Sistema: Endpoints + Rede + Políticas
- Múltiplos serviços e dispositivos trabalhando de forma coordenada para evitar ataques. Gerenciamento ativo
- NAC, IBNS, SWAN

SDN Fase I *"Segurança Integrada"*

- Transforma cada elemento de rede em um ponto de defesa Roteadores, Switches, dispositivos. Endpoints
- Conectividade Segura (V3PN, DMVPN), Defesa contra ameaças, Identidade e confiabilidade
- Proteção à Rede em si

Sistema Colaborativo

Controle de Admissão é Fundamental

- Muito fácil para um individuo obter acesso físico e lógico a uma Rede
  - Username e password não é mais suficiente
- Uma porta de rede pode estar habilitada ou desabilitada
  - Precisamos de mais opções!
- 802.1x é parte da solução…
- …com Controle de Admissão à rede
  - Foco em reduzir os danos causados por ameaças crescentes como os vírus e vermes

Exemplo de Self-Defending Network

Serviços de Rede Baseado em Identidade

Aplica políticas e habilita a porta do switch

- Set port to enable
- set port vlan 10

Cliente 802.1x

VLAN 10

VLAN de Engenharia

Segurança de Acesso

Em ação

4000 Series

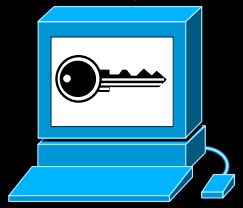
3550/2950 Series

6500 Series

Access Points

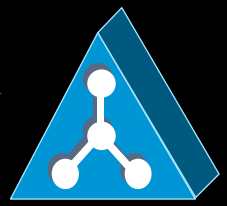
Credenciais verificadas
Login autorizado
Envia Políticas

Verifica Credenciais



Login

Login Verificado



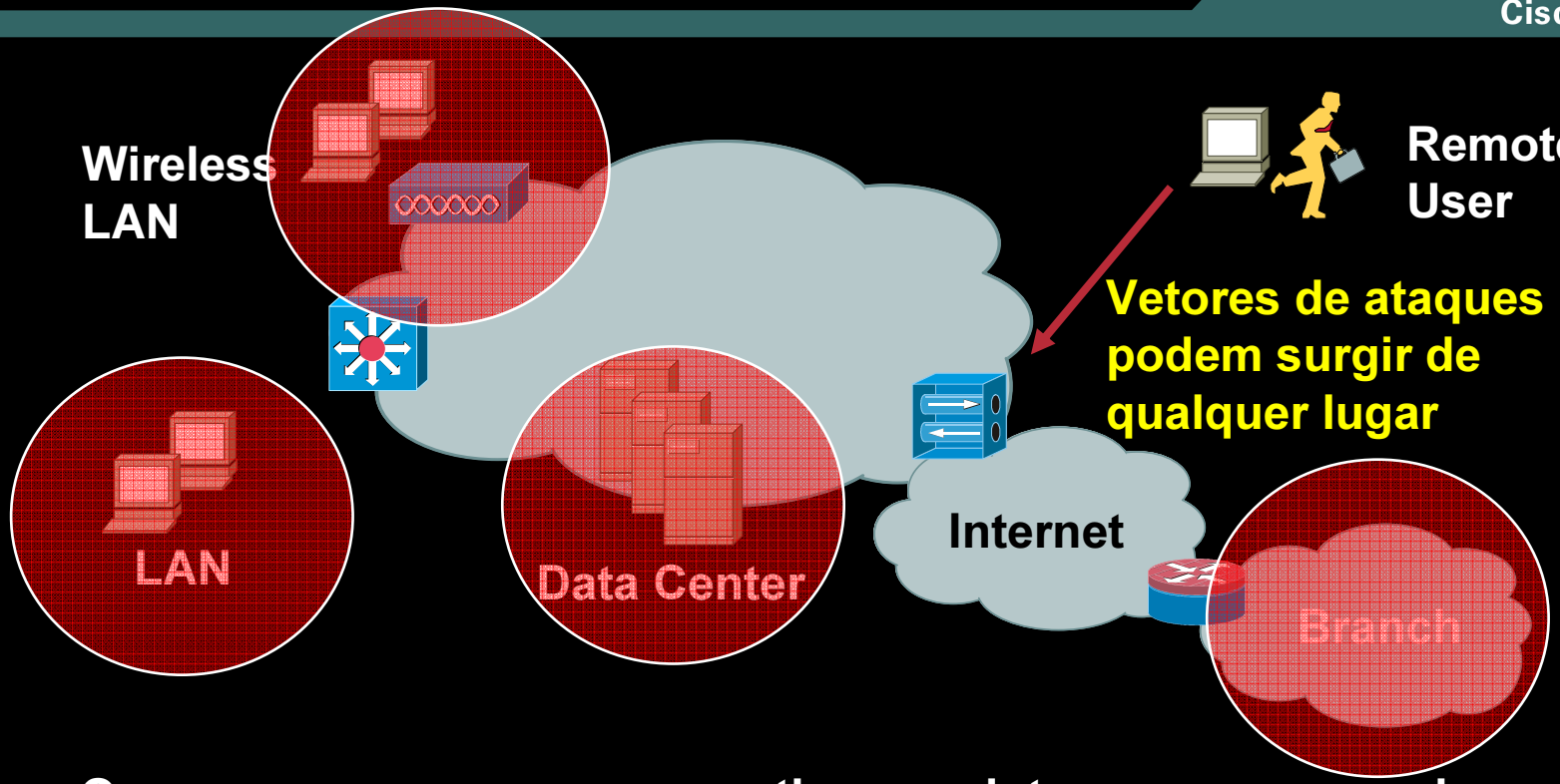
CiscoSecure ACS

Servidor Radius AAA

Servidor de autenticação 802.1x

Active Directory

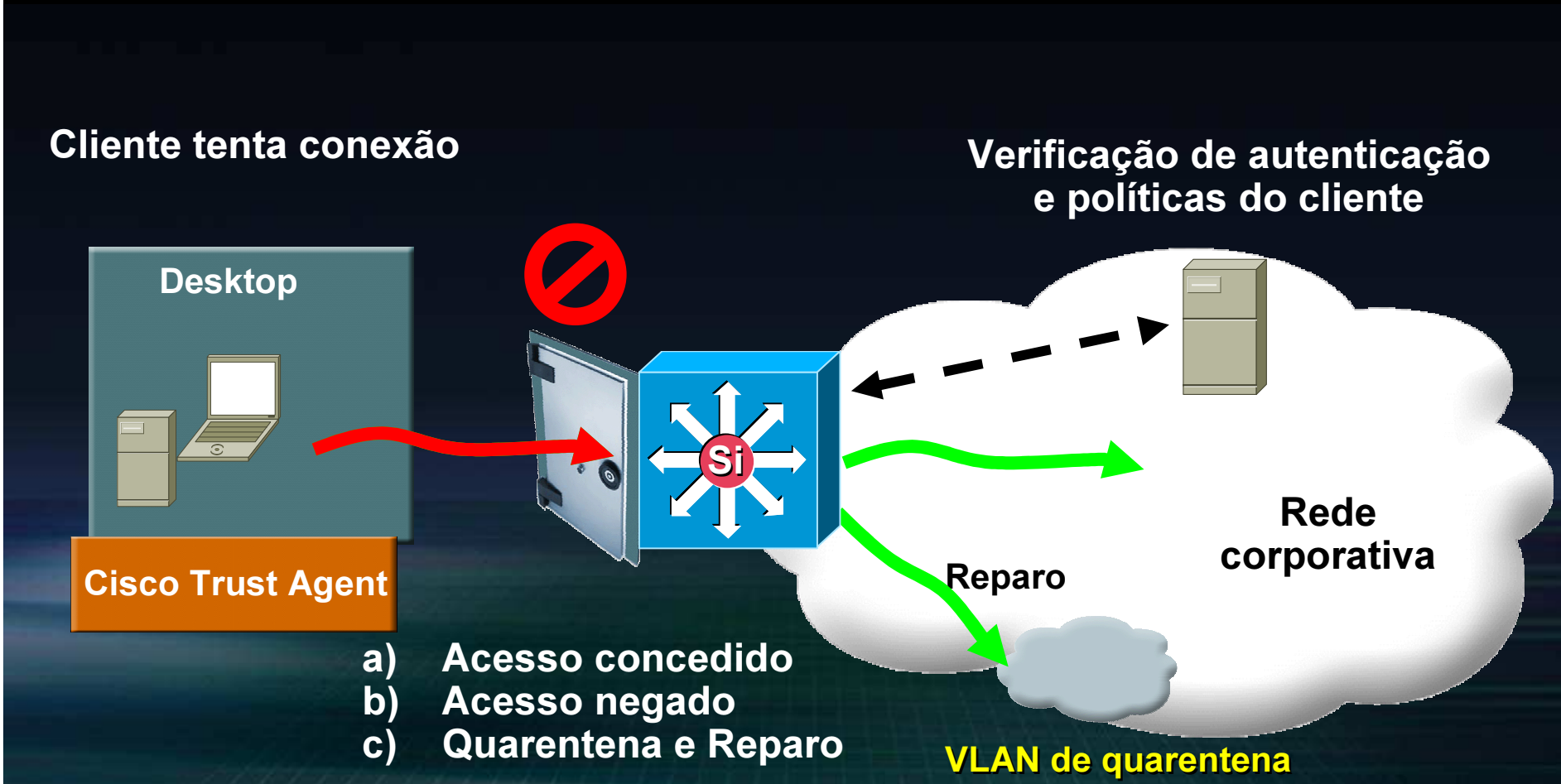
Infecção dos Internet Worm



- Os vermes se propagam e continuam a interromper os serviços, causando downtime e aplicação constante de patch
- Servidores e desktpos Non-compliant são comuns
- Localizar e isolar sistemas infectados consome muito recurso e tempo
- Múltiplos tipos de usuários, métodos de acesso, e endpoints compões um problema

Controle de Admissão na Rede Cisco: Primeira Solução de Segurança baseada em Confiança e Identidade

Cisco.com



Colaboração da Indústria
Fator crítico para o sucesso

Participantes do Programa Cisco Network Admission Control (NAC)

"ANYONE CAN BUILD A STOP SIGN – OR EVEN A TRAFFIC LIGHT – BUT IT TAKES A DIFFERENT MIND-SET ENTIRELY TO CONCEIVE OF A CITY-WIDE TRAFFIC CONTROL SYSTEM."

Bruce Schneier, "Beyond Fear"