nic.br cgi.br | 20 anos cert.br

SBSeg 2017

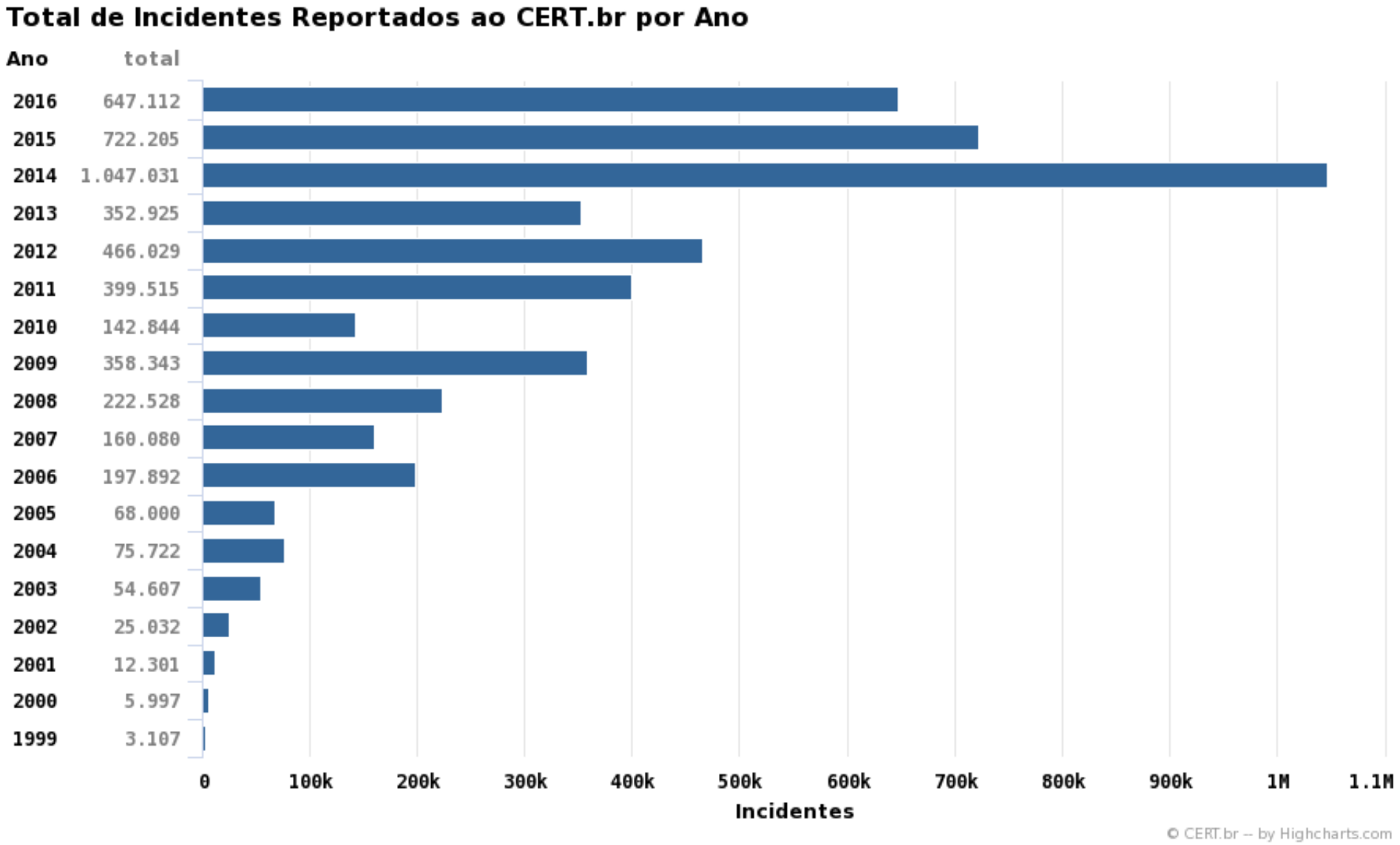
XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

Brasília, DF – 08 de novembro de 2017

O Que nos Mostram os Incidentes Mais Prevalentes no Brasil: Evolução ou Involução da Segurança nos últimos 20 anos?

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

cert.br nic.br cgi.br

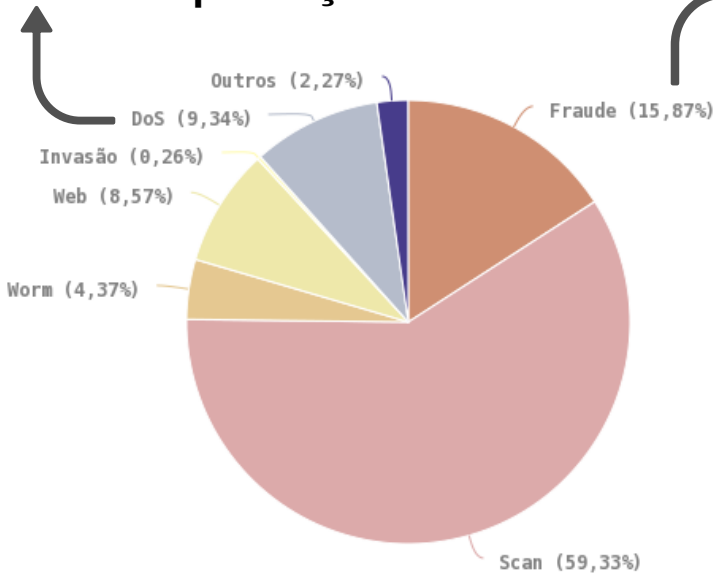


Estatísticas de notificações enviadas voluntariamente por administradores de sistemas e usuários finais para o *e-mail* cert@cert.br.

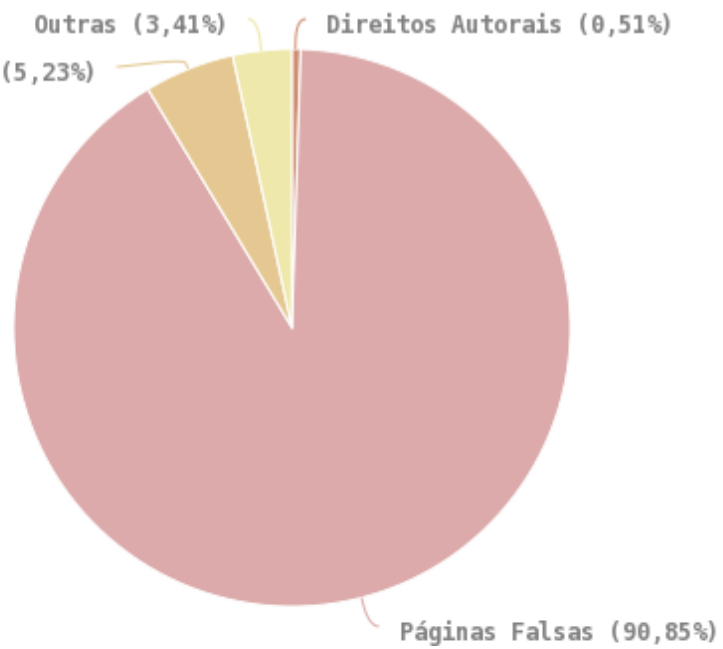
https://cert.br/stats/

Estatísticas 2016

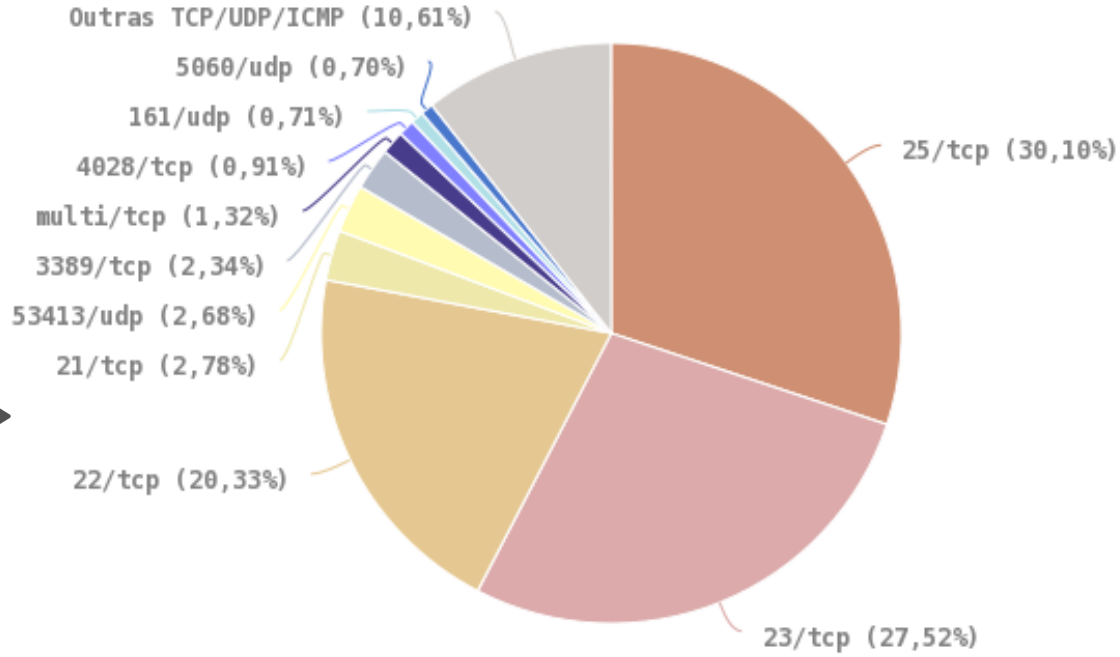
DDoS – aumento de 138%
- 300Gbps é o "normal"
- Até 1Tbps contra alguns alvos
- Tipos mais frequentes
  - botnets IoT
  - amplificação



Fraude
- 90% são páginas falsas



Scan
- Portas 22 e 23: força bruta de senhas de servidores e de IoT
- Porta 25: força bruta de senhas de *e-mail*



Atividades nos Honeypots Distribuídos: **Serviços mais Visados**

Força bruta de senhas (ataque usado por malwares de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- RDP (3389/TCP)
- POP3 (110/TCP)
- Outras TCP (2323, 23231, 2222)

Protocolos explorados pela botnet Mirai, na variante para CPEs (roteadores de banda larga)

- TCP: 7547, 5555, 37777, 6789, 81

Busca por protocolos que permitam amplificação

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Relembrar é viver...

Information about the PC CYBORG (AIDS) trojan horse

A-10

Published: 1989-12-19 00:00:00
Updated: 1989-12-19 00:00:00

THE COMPUTER INCIDENT ADVISORY CAPABILITY

CIAC

INFORMATION BULLETIN

Information about the PC CYBORG (AIDS) trojan horse

December 19, 1989, 1600 PST Number A-10

There recently has been considerable attention in the news media about a new trojan horse which advertises that it provides information on the AIDS virus to users of IBM PC computers and PC clones. Once it enters a system, the trojan horse replaces AUTOEXEC.BAT, and may count the number of times the infected system has booted until a criterion number (90) is reached. At this point PC CYBORG hides directories, and scrambles (encrypts) the names of all files on drive C: There exists more than one version of this trojan horse, and at least one version does not wait to damage drive C:, but will hide directories and scramble file names upon the first boot after the trojan horse is installed.

2 CA-1990-02: Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

A complet

There hav
entitled "C
ferred to a

At this poi
not have h
tempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a "virus" on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intrude

It is possit
tempts hav

2. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).

   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

VMS SYSTEM ATTACKS:

13. The intruder exploits system default passwords that have not been changed since installation.

    Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

CERT® Advisory CA-1991-04 Social Engineering

Original issue date: April 18, 1991
Last revised: September 18, 1997
Attached copyright statement

A complete revision history is at the end of this file.

I. Description

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received several incident reports concerning users receiving requests to take an action that results in the capturing of their password. The request could come in the form of an e-mail message, a broadcast, or a telephone call. The latest ploy instructs the user to run a "test" program, previously installed by the intruder, which will prompt the user for his or her password. When the user executes the program, the user's name and password are e-mailed to a remote site. We are including an example message at the end of this advisory.

These messages can appear to be from a site administrator or root. In reality, they may have been sent by an individual at a remote site, who is trying to gain access or additional access to the local machine via the user's account.

While this advisory may seem very trivial to some experienced users, the fact remains that MANY users have fallen for these tricks (refer to CERT Advisory CA-91.03).

1 CA-1996-01: UDP Port Denial-of-Service Attack

Original issue date: February 8, 1996
Last revised: September 24, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of programs that launch denial-of-service attacks by creating a "UDP packet storm" either on a system or between two systems. An attack on one host causes that host to perform poorly. An attack between two hnosts can cause extreme network congestion in addition to adversely affecting host performance.

The CERT staff recommends disabling unneeded UDP services on each host, in particular the chargen and echo services, and filtering these services at the firewall or Internet gateway.

Because the UDP port denial-of-service attacks typically involve IP spoofing, we encourage you to follow the recommendations in advisory CA-96.21.

21 CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks

Original issue date: September 19, 1996
Last revised: November 29, 2000
Updated vendor information for the Linux kernel.

A complete rev
portion of CA-

Two "undergro
by creating TC
nected to the In
that can be take
is possible to d

Any system cor
server, FTP ser
tacks launched
network server
sequences of the attack may vary depending on the system; however, the attack itself is funda-
mental to the TCP protocol used by all systems.

If you are an Internet service provider, please pay particular attention to Section III and Appendix A, which describes step we urge you to take to lessen the effects of these attacks. If you are the customer of an Internet service provider, please encourage your provider to take these steps.

Appendix A: Reducing IP Spoofed Packets

1. Filtering Information

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can take steps to reduce the number of IP-spoofed packets entering and exiting your network.

Currently, the best method is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network to prevent a source IP spoofing attack from originating from your site.


www.OpenSSH.com
RLOGIN
1982-99
LIVED LIFE
WITH JOY
TELNET
1971-99
WONT CRYPT
RSH
1982-99
++
Putting an end to unencrypted network logins


OpenSSH
Putting an end to unencrypted network logins
USS-BSD
RLOGIN
1982-99
LIVED LIFE
WITH JOY
TELNET
1971-99
WONT CRYPT
RSH
1982-99
++
SSHERIFF
www.OpenSSH.com

4 IN-2000-04: Denial of Service Attacks using Nameservers

Updated: Monday, January 15, 2001 (changed RFC 2267 to RFC 2827/BCP 38)
Date: Friday, April 28, 2000

Overview

Intruders are using nameservers to execute packet flooding denial of service attacks.

Description

We are receiving an increasing number of reports of intruders using nameservers to execute packet flooding denial of service attacks.

The most common method we have seen involves an intruder sending a large number of UDP-based DNS requests to a nameserver using a spoofed source IP address. Any nameserver response is sent back to the spoofed IP address as the destination. In this scenario, the spoofed IP address represents the victim of the denial of service attack. The nameserver is an intermediate party in the attack. The true source of the attack is difficult for an intermediate or a victim site to determine due to the use of spoofed source addresses.

Because nameserver responses can be significantly larger than DNS requests, there is potential for bandwidth amplification. In other words, the responses may consume more bandwidth than the requests. We have seen intruders utilize multiple nameservers on diverse networks in this type of an attack to achieve a distributed denial of service attack against victim sites.

CVE-ID	
CVE-2000-0784	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

sshd program in the Rapidstream 2.1 Beta VPN appliance has a hard-coded "rsadmin" account with a null password, which allows remote attackers to execute arbitrary commands via ssh.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20000816 Remote Root Compromise On All RapidStream VPN Appliances
- URL:http://archives.neohapsis.com/archives/bugtraq/2000-08/0216.html
- BID:1574
- URL:http://www.securityfocus.com/bid/1574

Assigning CNA

N/A

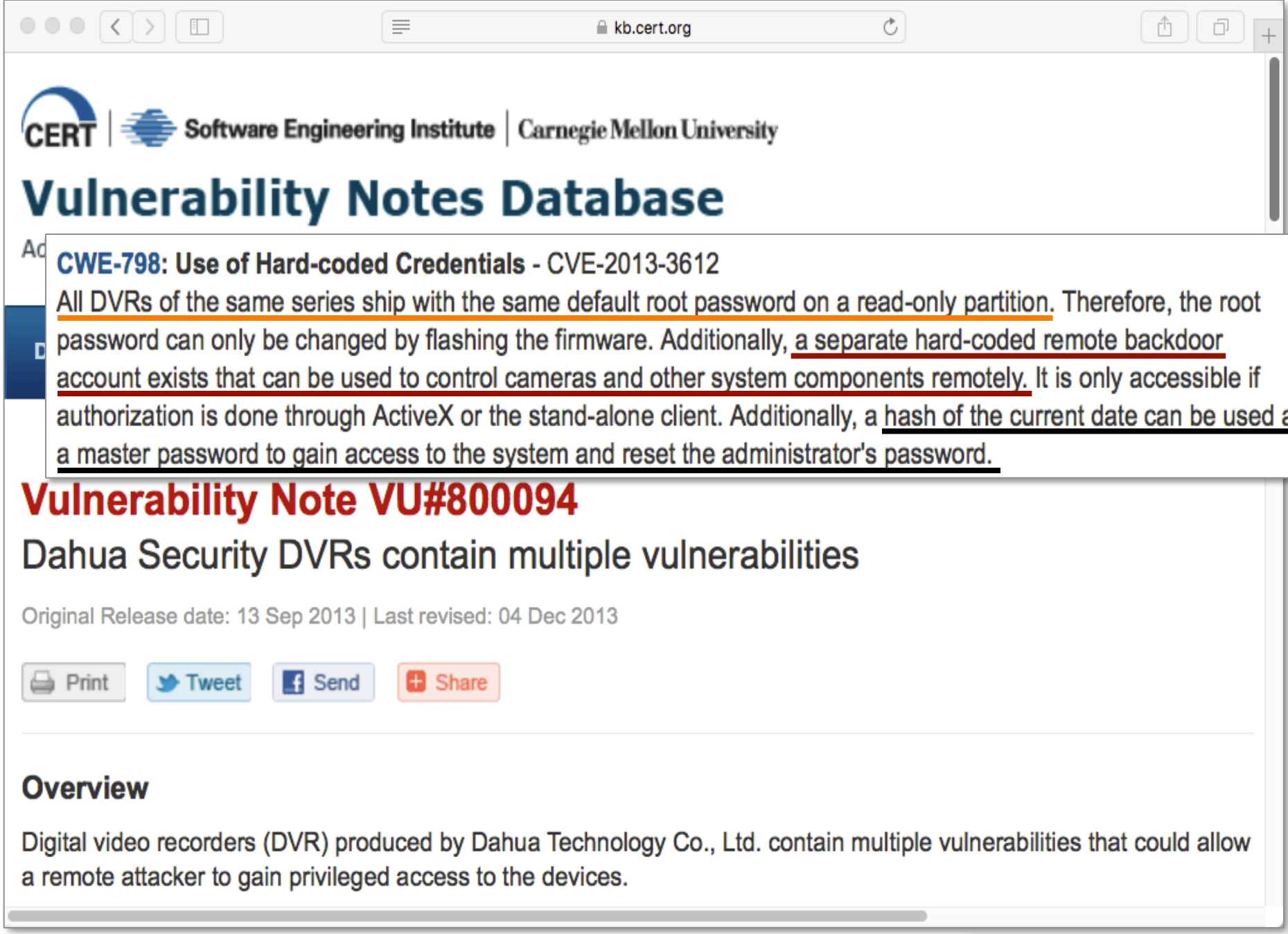
Date Entry Created

20000919	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

20 anos depois...

"Those who don't study history are doomed to repeat it. Yet those who *do* study history are doomed to stand by helplessly while everyone else repeats it."

Fonte:
http://imgc-cn.artprintimages.com/images/P-473-488-90/90/9031/84KB500Z/posters/tom-toro-those-who-don-t-study-history-are-doomed-to-repeat-it-yet-those-who-do-s-cartoon.jpg


kb.cert.org
CERT | Software Engineering Institute | Carnegie Mellon University
Vulnerability Notes Database
CWE-798: Use of Hard-coded Credentials - CVE-2013-3612
All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.
Vulnerability Note VU#800094
Dahua Security DVRs contain multiple vulnerabilities
Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013
Print
Tweet
Send
Share
Overview
Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Roteadores 4G-WiFi Utilizados em Infraestruturas Críticas Também São Afetados

Utilizados, entre outros, em: gasodutos, oleodutos, semáforos, iluminação pública, *smart grids*, carros de polícia e ambulâncias

SIERRA WIRELESS

Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

http://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---mirai/

DDoS attack halts heating in Finland amidst winter

A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland. In both of the events the attacks disabled the computers that were controlling heating in the buildings.

Both of the buildings where managed by Valtia. The company who is in charge of managing the buildings overall c and maintenance. According to CEO, Simo Rounela, in both cas circulation were temporarily disa

Building Automation security is not a priority

The devices under attack were built by the company Fidelix. According to company representative Antti Koskinen, there have been other attacks in the country before the case in Lappeenranta. He also states to Helsingin Sanomat that when people want convenience and ease of use it often opens up vulnerabilities.

http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

Vulnerabilidades em IoT:
O que chama mais atenção

Segurança não é prioridade

- mesmo em dispositivos de segurança!

Raríssimos consideram ciclo de atualizações de segurança

Todos repetem os erros do passado

- falta de autenticação
  - quando tem, são senhas fracas
- protocolos sem criptografia
- "*backdoors*" dos fabricantes são a norma
  - usualmente senhas padrão, que não podem ser alteradas, nem as contas desabilitadas

Em resumo, como são criadas as **Botnets de Dispositivos IoT**

Evolução sendo acompanhada em nossa rede de sensores desdes 2013

- infectam CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc

***Malware* se propaga geralmente via Telnet**

- protocolo para conexão remota, sem criptografia

Exploram Senhas Fracas ou Padrão

- muitas vezes são "*backdoors*" dos fabricantes

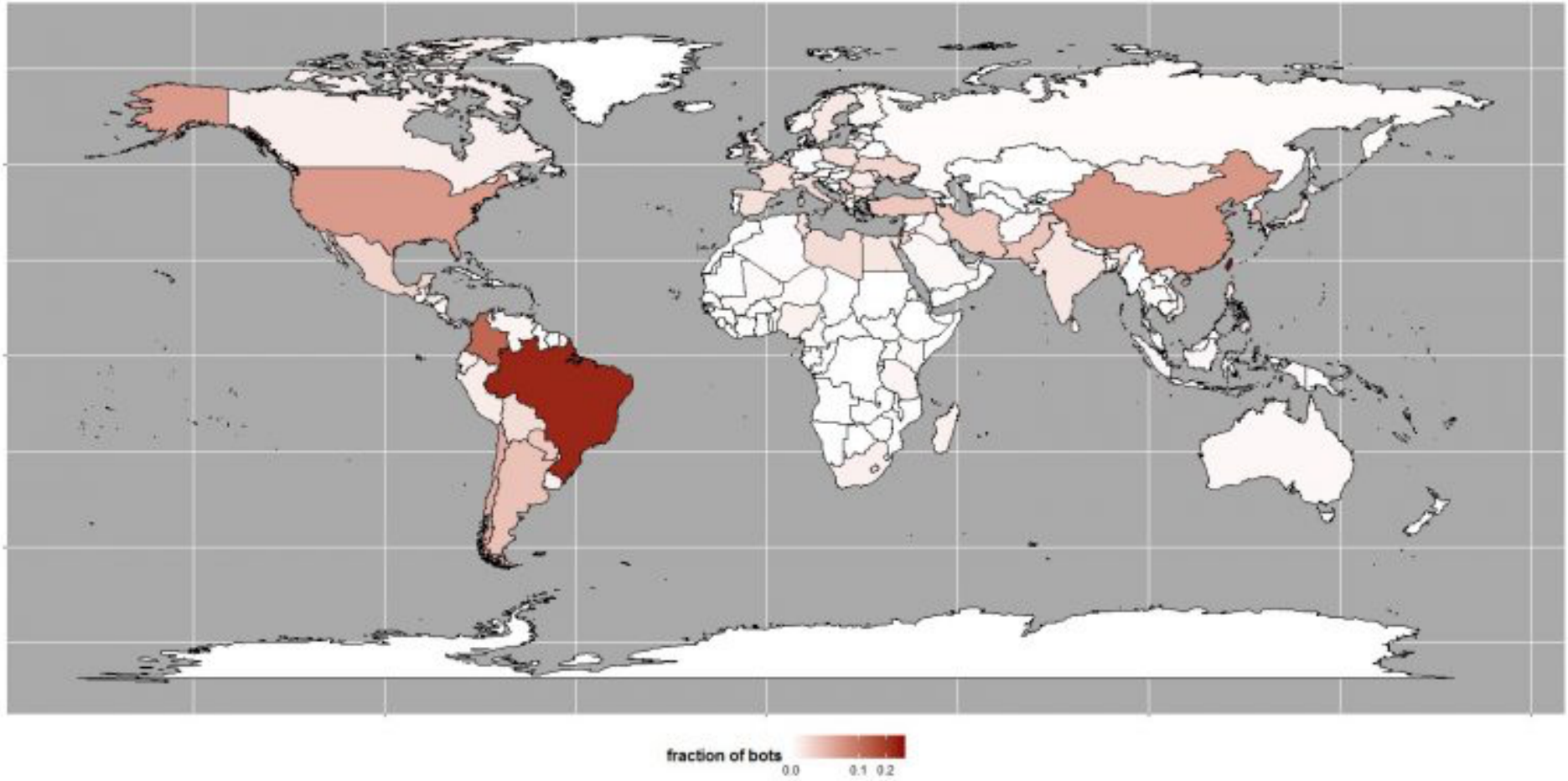
Foco em dispositivos com versões "enxutas" de Linux

- para sistemas embarcados
- arquiteturas ARM, MIPS, PowerPC, etc

Famílias prevalentes, vistas em nossos *honeypots*

- Mirai e gafgyt/bashlite

Variante mais antiga de botnet IoT sendo monitorada: **gafgyt (ou também Lizkebab, bashlite, Torlus)**



Fonte: Estatísticas da distribuição global, Level3, 25 de agosto de 2016
http://blog.level3.com/security/attack-of-things/

Setembro/2016, variante Mirai é identificada

- 22 e 23/09 – 620Gbps contra o Blog do Brian Krebs
- 21/10 – DDoS contra a Dyn
- 27/11 – Surgimento da variante para CPEs

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

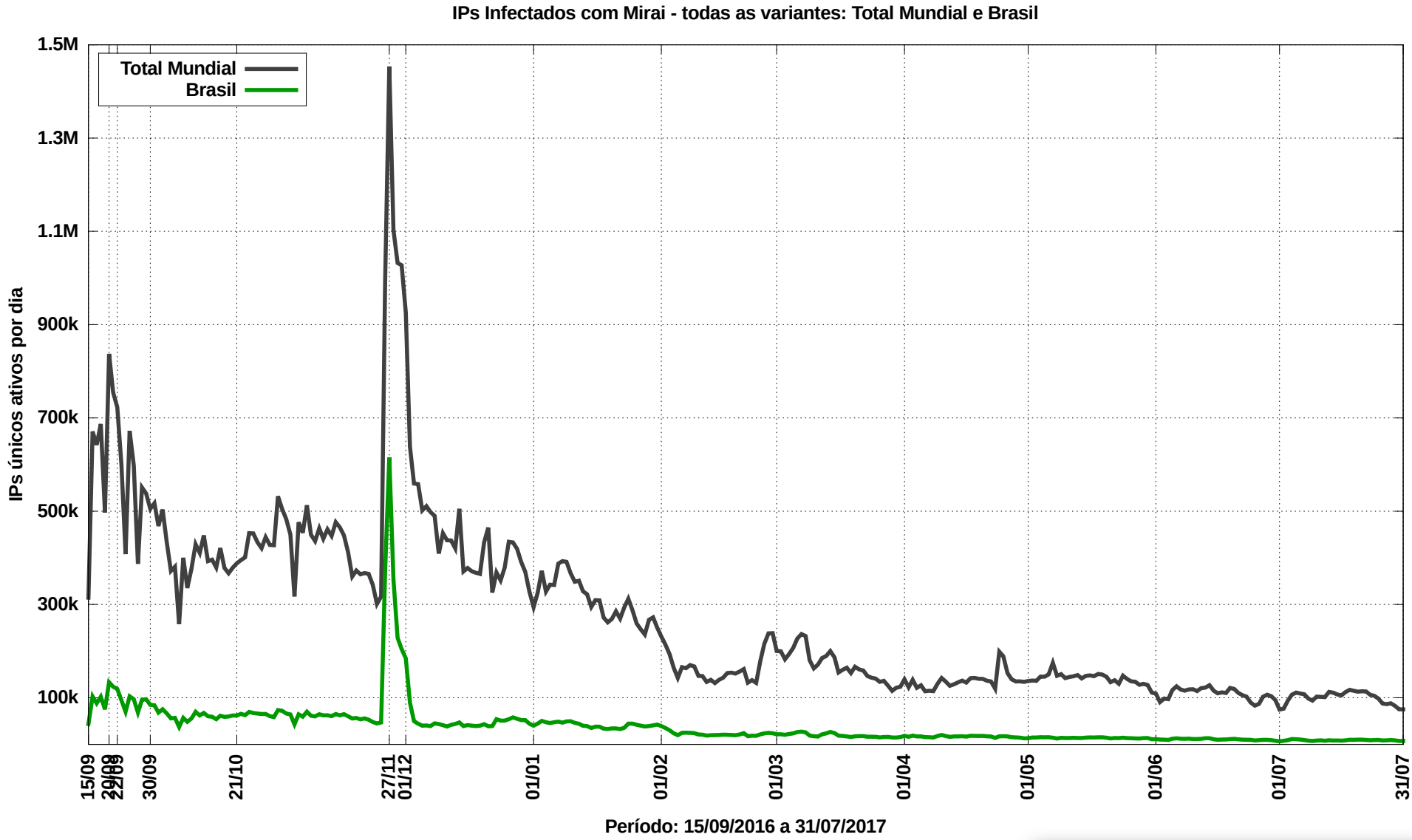
'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication

Brad Chacos | *@BradChacos* Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.bbc.co.uk/news/amp/37439513
http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html
http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

Dados dos sensores do CERT.br:
IPs únicos infectados com Mirai, por dia



Números de IoT em nossos *honeypots* – julho/2017

1.263 binários únicos novos (assinaturas SHA256 únicas)

Dados do último final de semana de julho:

```
180 artefatos
    165 ELFs
     15 shell scripts (downloaders)

Divisão por 32/64 bits, little/big endian e processador:
 31  ELF 32-bit LSB executable, ARM, version 1
 28  ELF 32-bit LSB executable, Intel 80386, version 1
 13  ELF 32-bit LSB executable, MIPS, MIPS-I version 1
 14  ELF 32-bit LSB executable, Renesas SH, version 1
  3  ELF 32-bit LSB shared object, Intel 80386, version 1
 23  ELF 32-bit MSB executable, MIPS, MIPS-I version 1
 12  ELF 32-bit MSB executable, Motorola 68020, version 1
 16  ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1
 11  ELF 32-bit MSB executable, SPARC, version 1
 14  ELF 64-bit LSB executable, x86-64, version 1

Dos ELFs, por tipo de malware:
 143  gafgyt/bashlite
   9  mirai
  13  unknown ELF
```

blog.cloudflare.com

Reflections on reflection (attacks)

24 May 2017 by Marek Majkowski.

Share 116 Like 16 Tweet

Recently Akamai published an article about CLDAP reflec
saw attacks from Connectionless LDAP servers back in N
them because our systems were automatically dropping

Count	Proto	Src port	
3774	udp	123	NTP
1692	udp	1900	SSDP
438	udp	0	IP fragmentation
253	udp	53	DNS
42	udp	27015	SRCDS
20	udp	19	Chargen
19	udp	20800	Call Of Duty
16	udp	161	SNMP
12	udp	389	CLDAP
11	udp	111	Sunrpc
10	udp	137	Netbios
6	tcp	80	HTTP
5	udp	27005	SRCDS
2	udp	520	RIP

Kromtech Security Center Discovers Massive ElasticSearch Infected Malware Botnet

< Back to blog

By Bob Diachenko

2017-09-12

One of our recent researches was focused on the publicly accessible ElasticSearch (ES) nodes and we discovered suspicious indices names that did not have any relations to ElasticSearch file structure.

Among the many "red flags" some of the file names referenced to AlinaPOS and JackPOS malware. These are the type of POS (Point-of-Sale) malware that attempts to scrape credit card details using a range of different techniques. As an example of how this malware is so effective, JackPOS attempts to trick the system that it is java or a java utility. It can copy itself directly into the %APPDATA% directory or into a java based sub-directory inside %APPDATA%. JackPOS uses the MAC address as a bot ID and can even encode the stolen credit card data to go undetected as it is extracted. This malware first became widespread in 2012, but it is still effective today and available for sale online.

Why did it happen?

The lack of authentication allowed the installation of malware on the ElasticSearch servers. The public configuration allows the possibility of cyber criminals to manage the whole system with full administrative privileges. Once the malware is in place criminals could remotely access the server's resources and even launch a code execution to steal or completely destroy any saved data the server contains.

Não tem nada de novo?

Ataques Envolvendo CPEs para Alteração de DNS

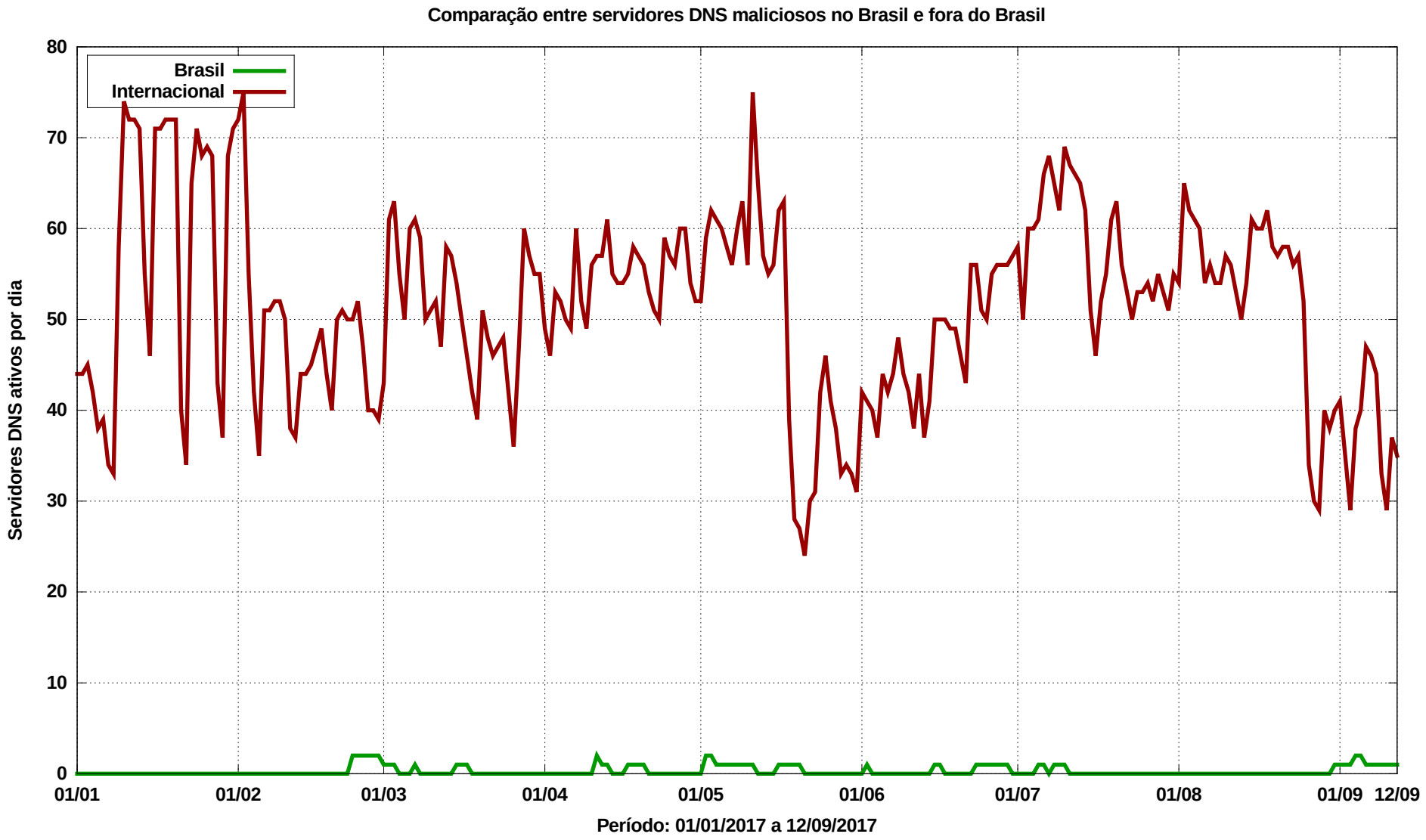
Comprometidos

- via força bruta de senhas (geralmente via telnet)
  - via rede ou via *malware* nos computadores das vítimas
- explorando vulnerabilidades
- via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos
  - Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos ataques

- **alterar a configuração de DNS para que consultem servidores sob controle dos atacantes**
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

Servidores DNS Maliciosos *Online*, por Dia



Ataques Envolvendo Sequestro de Rotas BGP para Perpetrar Fraudes Financeiras

Características do protocolo BGP

- Sistemas Autônomos anunciam seus blocos de rede (/16, /20, /22, etc)
- "*Peers*" aprendem e repassam esses anúncios
- "vencem" as rotas para anúncios de blocos mais específicos ou com caminho (*AS path*) menor

Anatomia dos ataques

- Atacantes comprometem roteadores de borda de pequenos provedores
- Anunciam prefixos de rede mais específicos da instituição vítima (em geral /24)
  - "*peers*" do provedor comprometido vão aprendendo a nova rota
  - clientes das redes que aprenderam a nova rota passam a ser roteados para o local errado
- Início em março de 2017 e ainda está ocorrendo

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

COMPLETELY BROKEN —

Millions of high-security crypto keys crippled by newly discovered flaw

Factorization weakness lets attackers impersonate key holders and decrypt their data.

DAN GOODIN - 10/16/2017, 9:00 AM

The flaw resides in the Infineon-developed RSA Library version v1.02.013, specifically within an algorithm it implements for RSA primes generation. The library allows people to generate keys

This is the second time in four years that a major crypto flaw has been found hitting a crypto scheme that has passed rigorous certification tests. In 2013,

Enlarge / 750,000 Estonian cards that look like this use a 2048-bit RSA key that can be factored in a matter of days.

E *Ransomware*?

Sim é um problema :-)

- poucas notificações formais
- muito pânico causado por cobertura apressada/incompleta

Prevalência acentuada por um conjunto de fatores

- falta de gestão de configuração e política de atualização
- falta de política de *backup* *offline* e *offsite*
- popularidade de *kits* para geração de códigos maliciosos
- popularidade de criptomoedas

Únicas defesas

- *backup*
- conscientização e educação

https://cartilha.cert.br/ransomware/

Desafios para Melhorar o Cenário

cert.br nic.br cgi.br

Alguns Desafios para o Futuro

Qualificação profissional

- redes, administração de sistemas, **desenvolvimento de *software* seguro**

Resistir a ataques DDoS

- AS próprio, melhor conectividade, conexão a um IX
- em alguns casos a migração para CDNs é a única solução

Segurança na infraestrutura de roteamento

- roteamento fuciona por confiança nos anúncios
- em discussão na comunidade o uso de RPKI e S-BGP
  - Em resumo: tabelas de rotas passam a ser assinadas

Requisitos mais rígidos para escolha de fornecedores

- *software*, *hardware*, IoT

Adoção de DNSSEC

- novos protocolos, como DANE, em estudo

Migrar para o Protocolo IPv6

- os endereços IPv4 na América Latina esgotaram em 10/06/2014

Um caminho para melhorar os próximos 20 anos: **Cooperação para um ecossistema saudável**

Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel

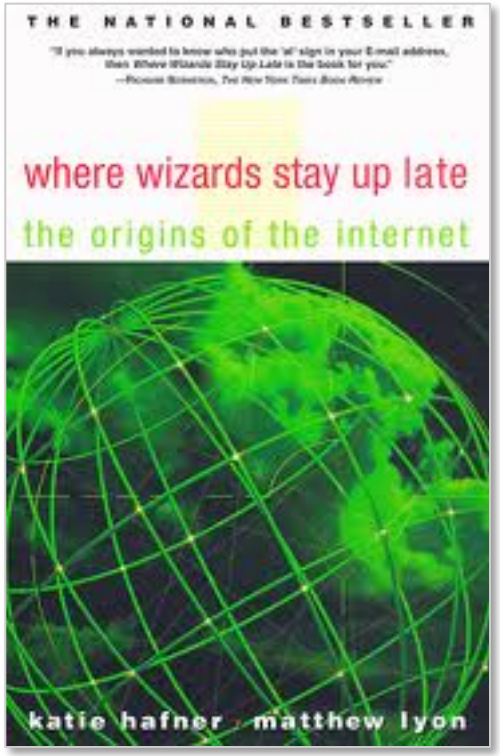
- **universidades**
  - **precisam incluir questões de segurança em todas as disciplinas**
- **desenvolvedores / *vendors***
  - **precisam pensar em segurança desde as etapas iniciais de desenvolvimento**
- gestores
  - precisam considerar segurança como um investimento e alocar recursos adequados
- administradores de redes e sistemas e profissionais de segurança
  - não emanar “sujeira” de suas redes
  - adotar boas práticas
- usuários
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções

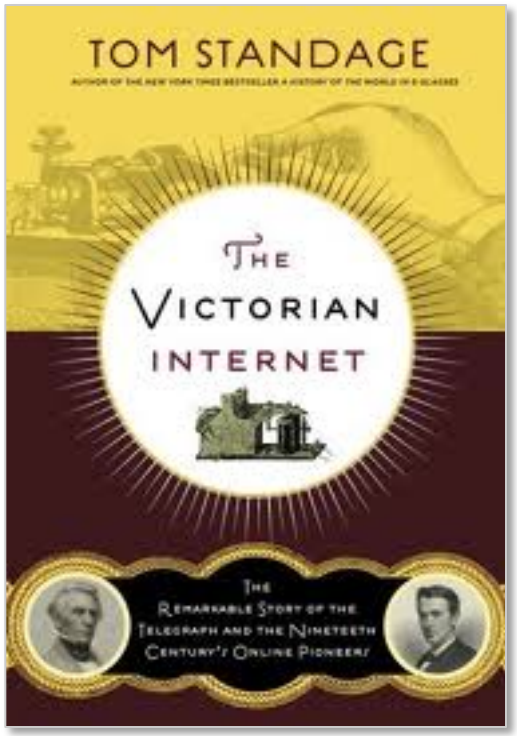
Ainda assim ataques e incidentes de segurança ocorrerão

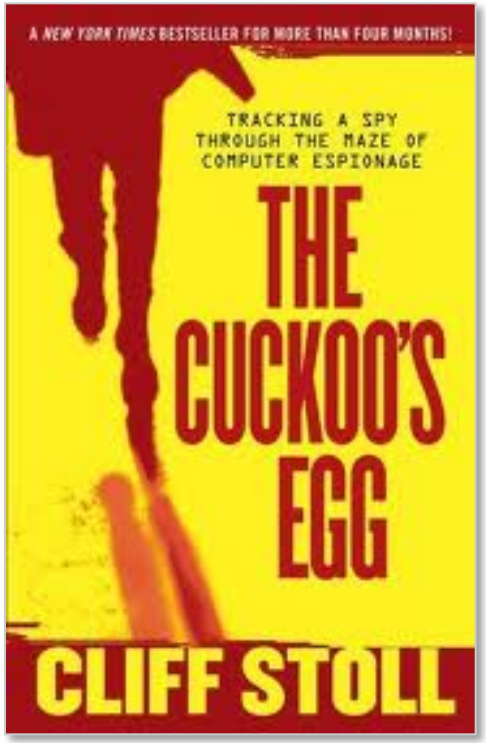
- https://cert.br/csirts/ https://www.first.org/members/

Leituras Recomendadas

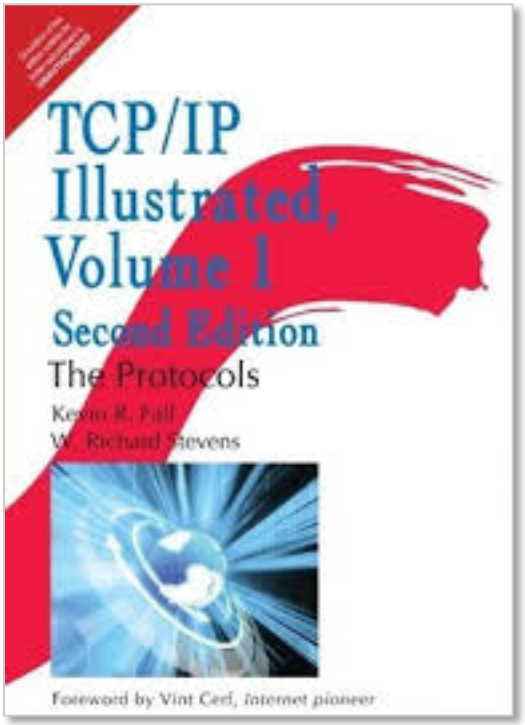
História da Internet e Primeiros Incidentes

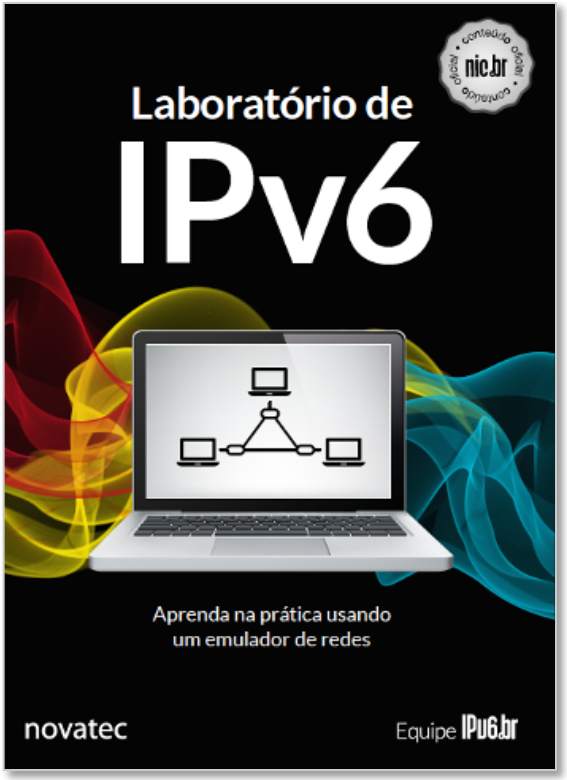


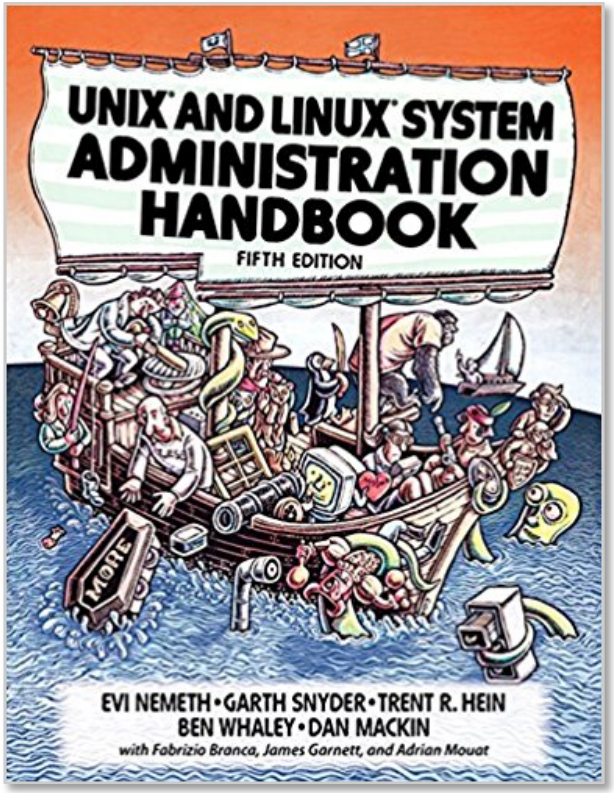




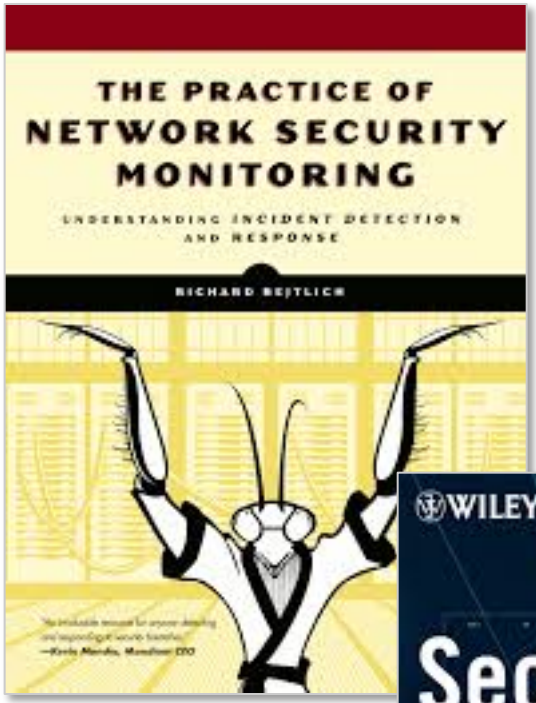
Redes e IPv6

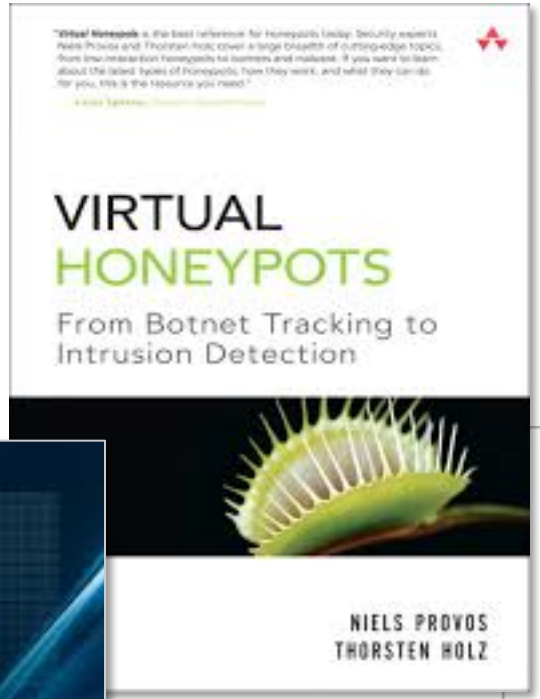

TCP/IP
Illustrated,
Volume 1
Second Edition
The Protocols
Kevin R. Fall
W. Richard Stevens
Foreword by Vint Cerf, Internet pioneer

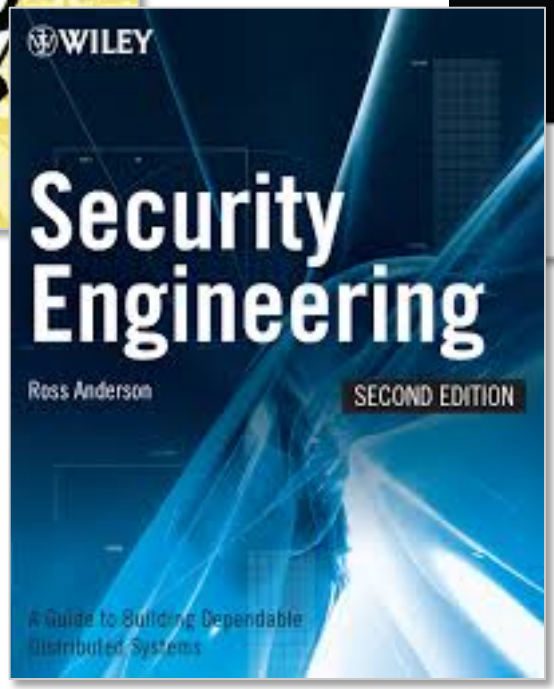

Laboratório de
IPv6
nic.br
Aprenda na prática usando
um emulador de redes
novatec
Equipe IPv6.br

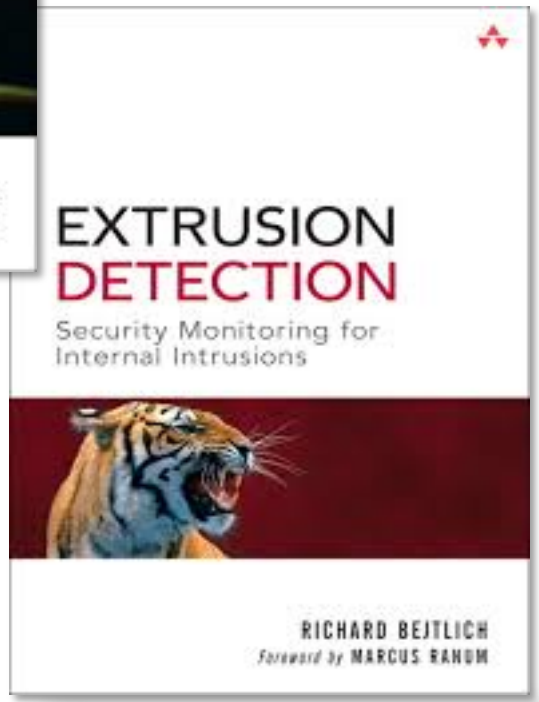

UNIX AND LINUX SYSTEM
ADMINISTRATION
HANDBOOK
FIFTH EDITION
MORE
EVI NEMETH • GARTH SNYDER • TRENT R. HEIN
BEN WHALEY • DAN MACKIN
with Fabrizio Branca, James Garnett, and Adrian Mouat

Segurança

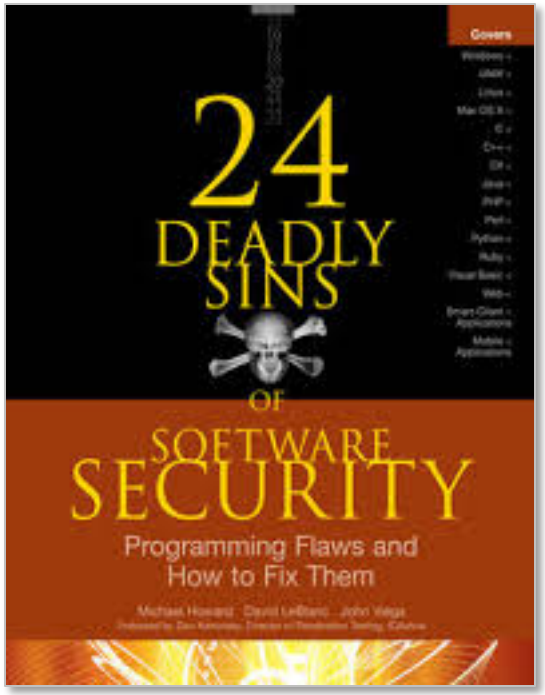

THE PRACTICE OF
NETWORK SECURITY
MONITORING
UNDERSTANDING INCIDENT DETECTION
AND RESPONSE
RICHARD BEJTLICH

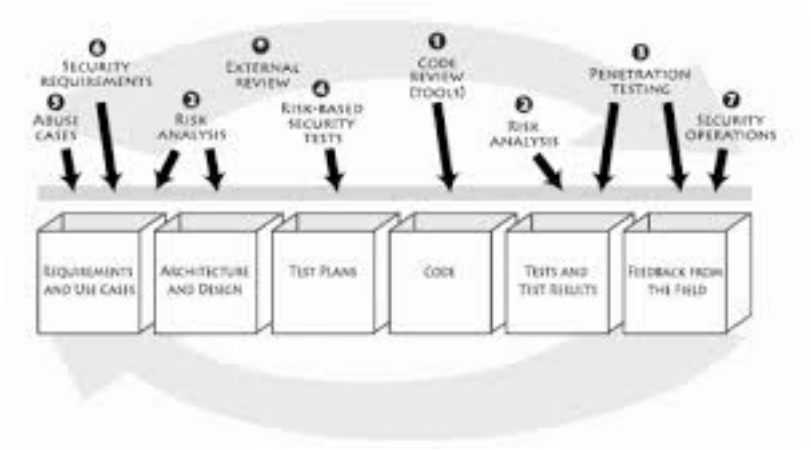

VIRTUAL
HONEYPOTS
From Botnet Tracking to
Intrusion Detection
NIELS PROVOS
THORSTEN HOLZ

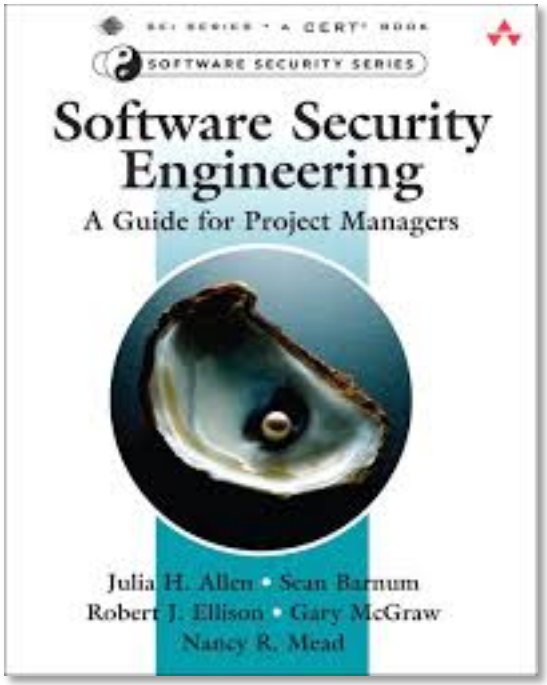

WILEY
Security
Engineering
Ross Anderson
SECOND EDITION

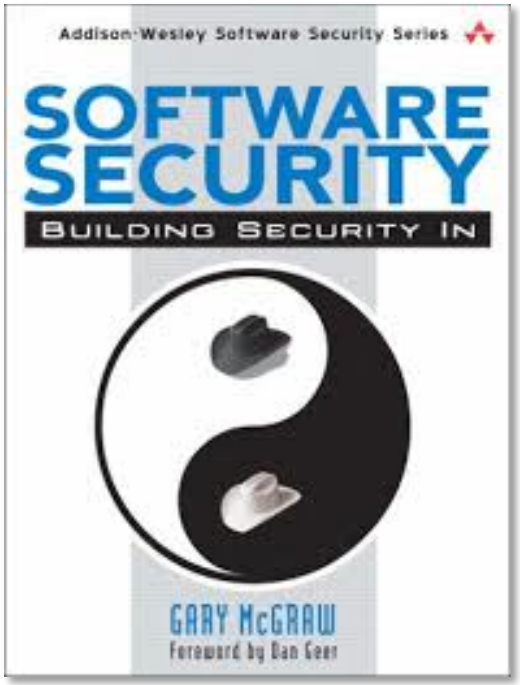

EXTRUSION
DETECTION
Security Monitoring for
Internal Intrusions
RICHARD BEJTLICH
Foreword by MARCUS RANUM

Segurança de *Software* (1/2)









Segurança de *Software* (2/2)

The Building Security In Maturity Model

https://www.bsimm.com/

CERT Secure Coding

https://cert.org/secure-coding/

- **Wiki com práticas para C, Perl, Java e Java para Android**

  https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

Últimas notícias, análises, blogs

- **Krebs on Security**
  http://krebsonsecurity.com/
- **Schneier on Security**
  https://www.schneier.com/
- **Ars Technica Security**
  http://arstechnica.com/security/
- **Dark Reading**
  http://www.darkreading.com/
- **SANS NewsBites**
  http://www.sans.org/newsletters/newsbites/
- **SANS Internet Storm Center**
  http://isc.sans.edu/

Revistas e congressos

- **Usenix ;login: Magazine**

  https://www.usenix.org/publications/login
- **Usenix Conferences Proceedings**

  https://www.usenix.org/publications/proceedings
  - **Usenix Security ‘17 com todos os vídeos, *slides* e artigos: https://www.usenix.org/conference/usenixsecurity17/technical-sessions**
- **IEEE Security & Privacy**

  http://www.computer.org/portal/web/computingnow/securityandprivacy

Obrigada

www.cert.br

cristine@cert.br

@certbr

08 de novembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br