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

5º Seminário de Defesa Cibernética

Brasília, DF

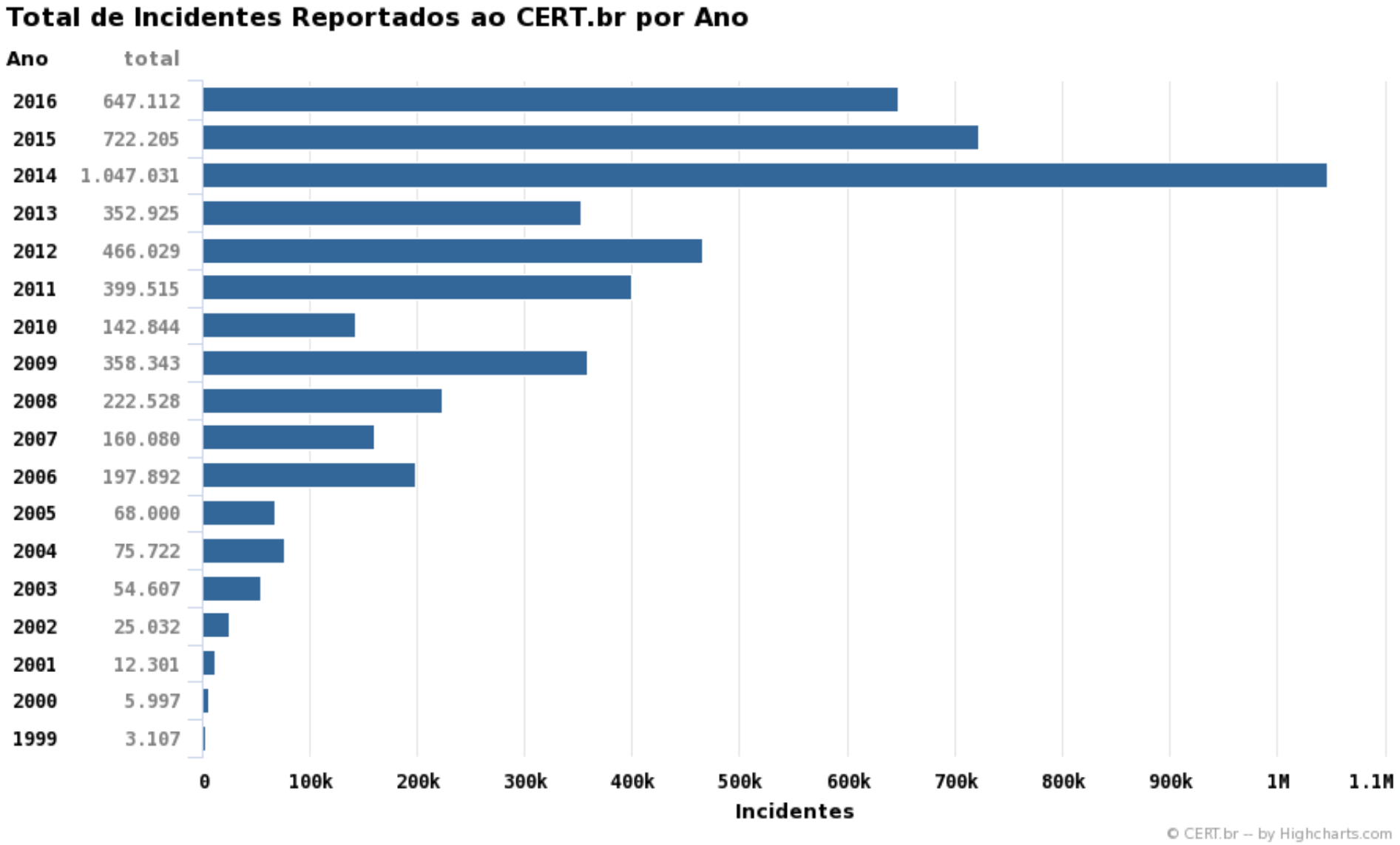
01 de agosto de 2017

Cenário de Ameaças Cibernéticas no Brasil

Cristine Hoepers, D.Sc.
Gerente Geral
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br



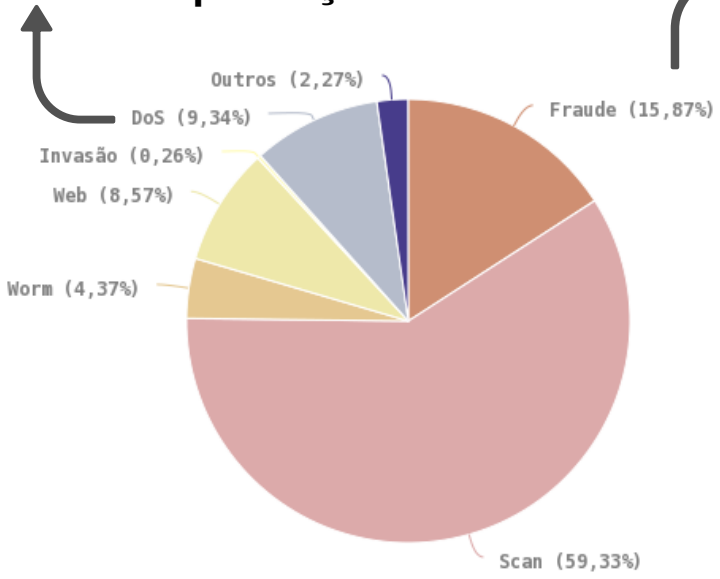
Estatísticas de notificações enviadas voluntariamente por administradores de sistemas e usuários finais para o *e-mail* cert@cert.br.

https://cert.br/stats/

Estatísticas 2016

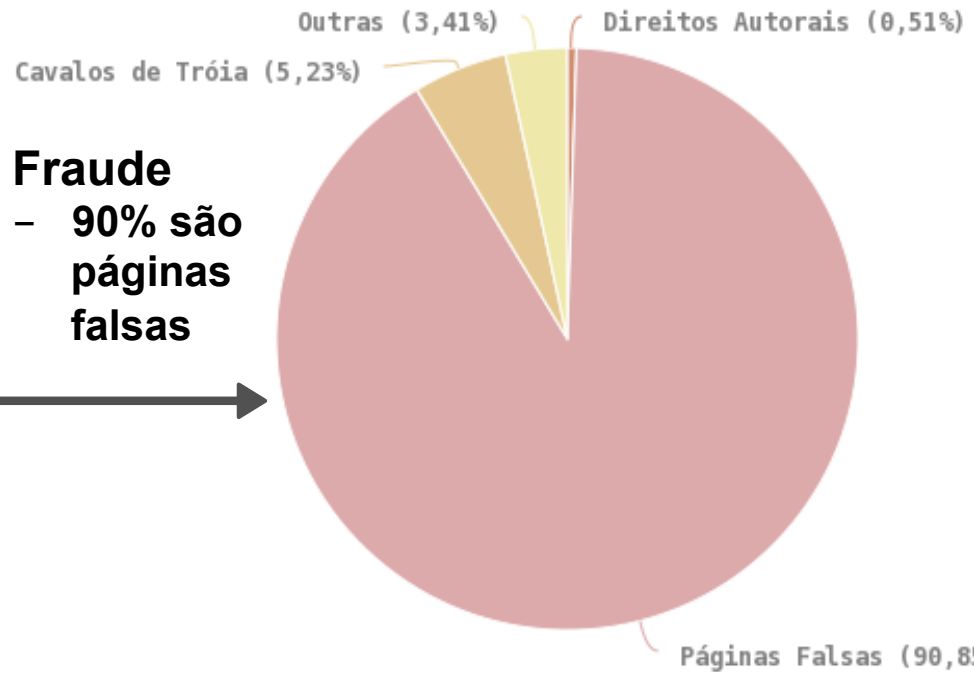
DDoS – aumento de 138%

- 300Gbps é o "normal"
- Até 1Tbps contra alguns alvos
- Tipos mais frequentes
  - botnets IoT
  - amplificação



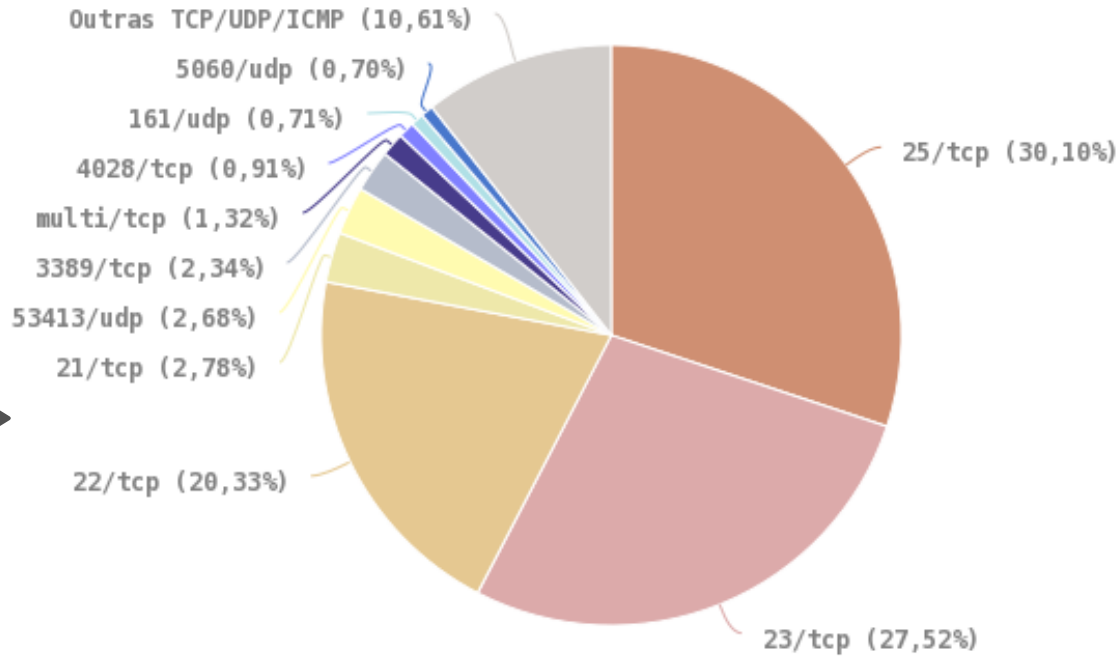
Fraude

- 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*

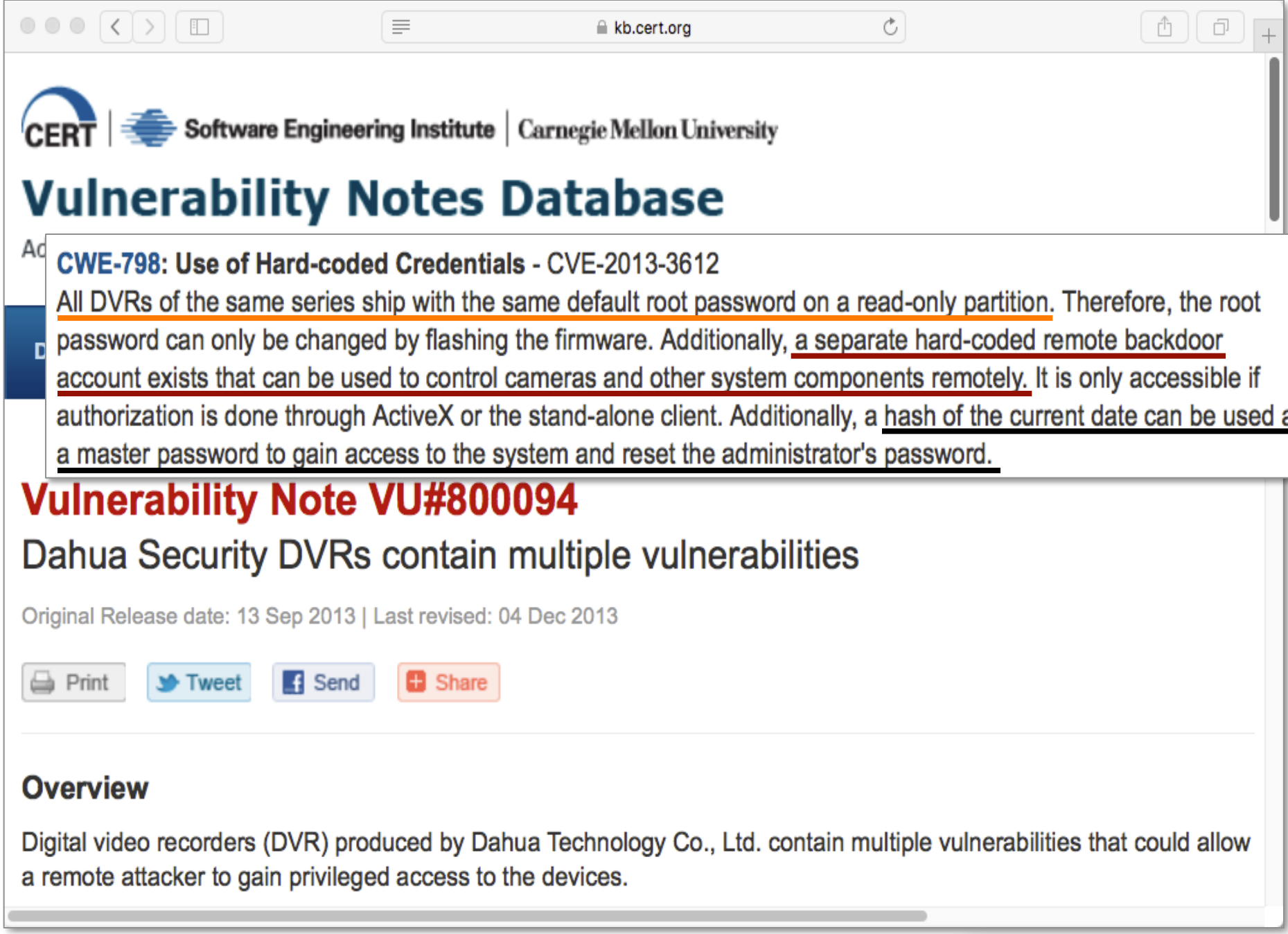


Atividades nos Honeypots Distribuídos
Serviços mais Visados

- **Força bruta de senhas (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 (*Consumer Premise Equipments*)**
  - **TCP: 7547, 5555, 37777, 6789, 81**
- **Busca por protocolos que permitam amplificação**
  - **UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP**
- **SIP (VoIP)**

Ataques Envolvendo IoT

cert.br nic.br cgi.br


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.

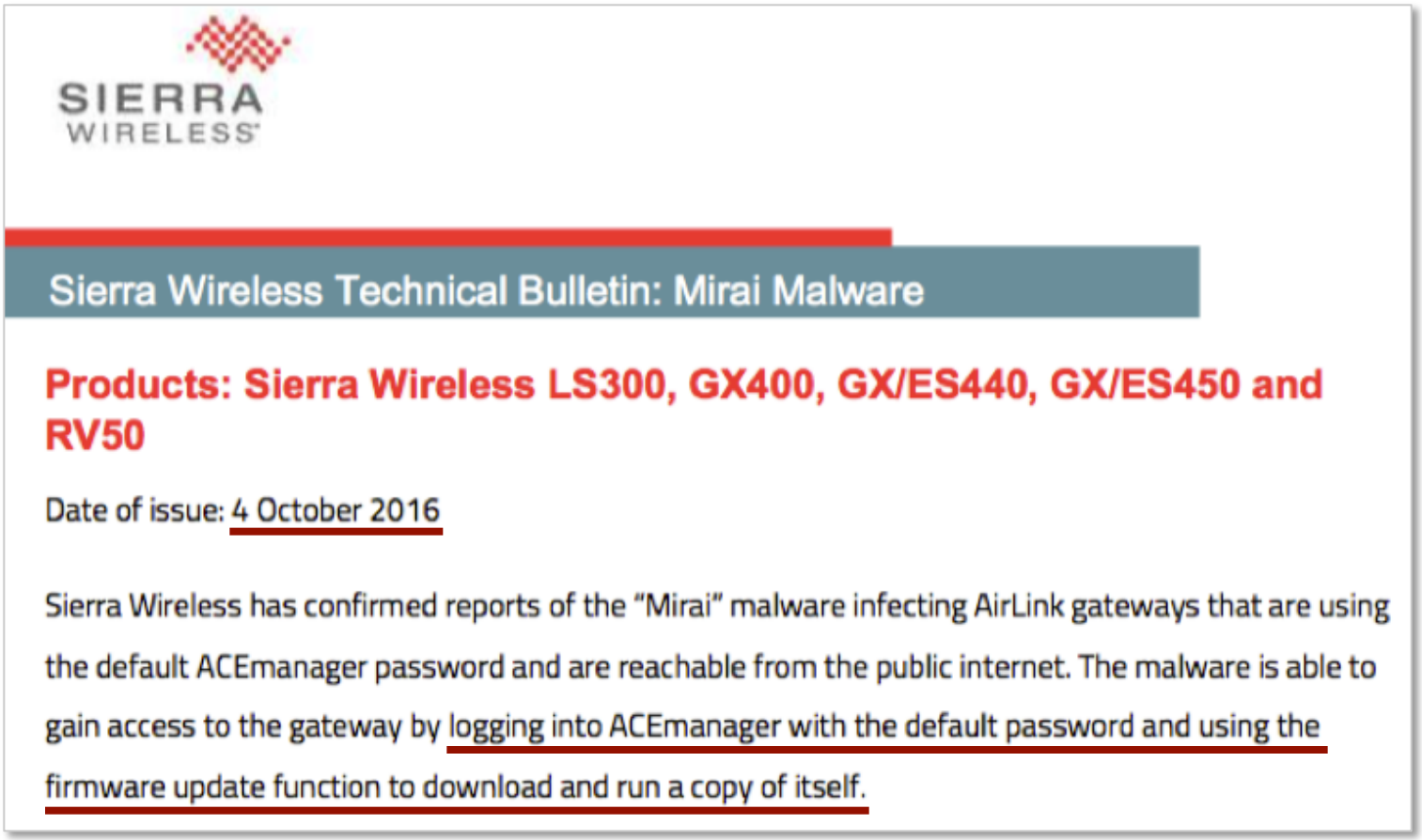
CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

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

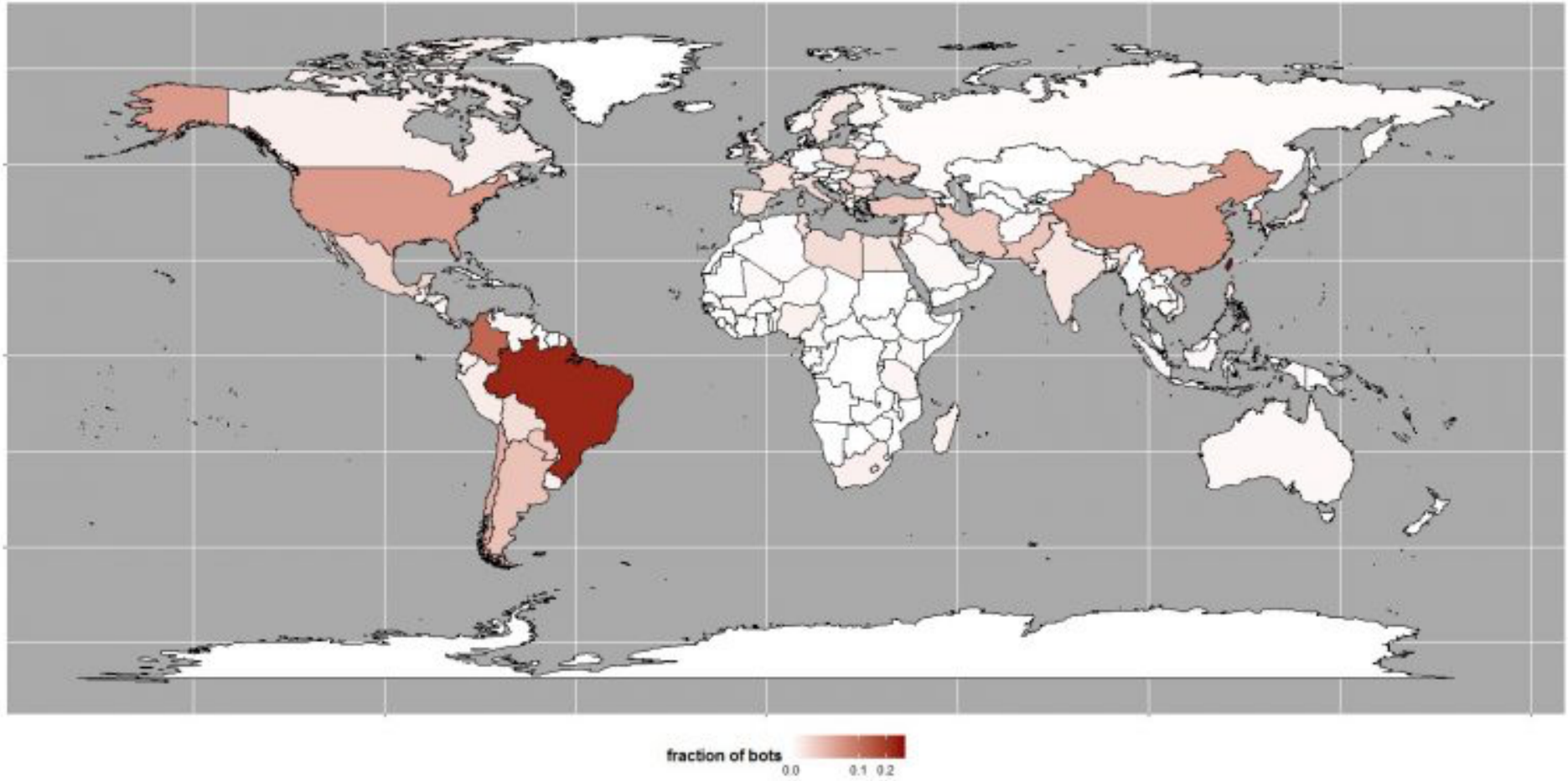
- mesmo em dispositivos de segurança!

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

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/

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

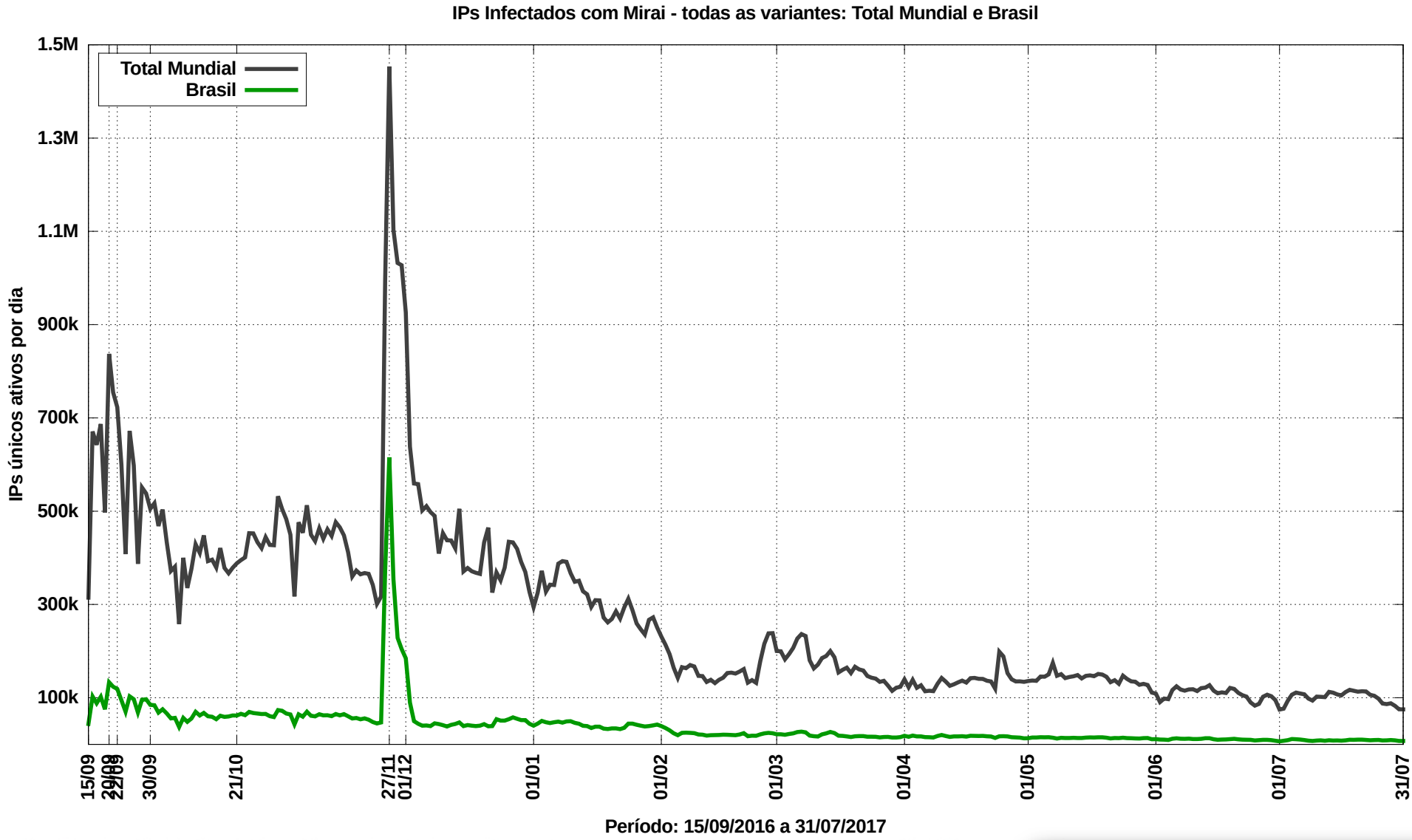
Foco em dispositivos com versões "enxutas" de Linux

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

Famílias prevalentes, vistas em nossos *honeypots*

- Mirai e gafgyt/bashlite

Dados atualizados 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:

```
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
```

Binário Mirai:
Informações de C&C Ofuscadas

```
0000ee40  35 36 37 38 00 00 00 00  ff ff 40 00 44 47 46 51  |5678......@.DGFQ|
0000ee50  0c 4f 4e 22 00 00 00 00  22 35 00 00 99 c7 00 00  |.ON"....."5.....|
0000ee60  4e 4b 51 56 47 4c 4b 4c  45 02 56 57 4c 12 22 00  |NKQVGLKLE.VWL.".|
0000ee70  4a 56 56 52 51 18 0d 0d  5b 4d 57 56 57 0c 40 47  |JVVRQ...[MWVW.@G|
0000ee80  0d 7d 7b 54 58 47 52 74  40 4e 46 16 22 00 00 00  |.}{TXGRt@NF."...|
0000ee90  0d 52 50 4d 41 0d 22 00  0d 47 5a 47 22 00 00 00  |.RPMA."..GZG"...|
0000eea0  02 0a 46 47 4e 47 56 47  46 0b 22 00 0d 44 46 22  |..FGNGVGF."..DF"|
0000eeb0  00 00 00 00 0c 43 4c 4b  4f 47 22 00 0d 51 56 43  |.....CLKOG"..QVC|
0000eec0  56 57 51 22 00 00 00 00  70 67 72 6d 70 76 02 07  |VWQ"....pgrmpv..|
0000eed0  51 18 07 51 22 00 00 00  6a 76 76 72 64 6e 6d 6d  |Q..Q"...jvvrdnmm|
0000eee0  66 22 00 00 6e 6d 6e 6c  6d 65 76 64 6d 22 00 00  |f"..nmnlmevdm"..|
0000eef0  7e 5a 17 1a 7e 5a 16 66  7e 5a 16 67 7e 5a 16 67  |~Z..~Z.f~Z.g~Z.g|
0000ef00  7e 5a 16 11 7e 5a 17 12  7e 5a 16 14 7e 5a 10 10  |~Z..~Z..~Z..~Z..|
0000ef10  22 00 00 00 58 4d 4e 4e  43 50 46 22 00 00 00 00  |"...XMNNCPF"....|
0000ef20  65 67 76 6e 6d 61 63 6e  6b 72 22 00 51 4a 47 4e  |egvnmacnkr".QJGN|
0000ef30  4e 22 00 00 47 4c 43 40  4e 47 22 00 51 5b 51 56  |N"..GLC@NG".Q[QV|
0000ef40  47 4f 22 00 51 4a 22 00  0d 40 4b 4c 0d 40 57 51  |GO".QJ"..@KL.@WQ|
0000ef50  5b 40 4d 5a 02 6f 6b 70  63 6b 22 00 6f 6b 70 63  |[@MZ.okpck".okpc|
0000ef60  6b 18 02 43 52 52 4e 47  56 02 4c 4d 56 02 44 4d  |k..CRRNGV.LMV.DM|
0000ef70  57 4c 46 22 00 00 00 00  4c 41 4d 50 50 47 41 56  |WLF"....LAMPPGAV|
0000ef80  22 00 00 00 0d 40 4b 4c  0d 40 57 51 5b 40 4d 5a  |"....@KL.@WQ[@MZ|
0000ef90  02 52 51 22 00 00 00 00  0d 40 4b 4c 0d 40 57 51  |.RQ".....@KL.@WQ|
0000efa0  5b 40 4d 5a 02 49 4b 4e  4e 02 0f 1b 02 22 00 00  |[@MZ.IKNN...."..|
```

Binário Mirai:
Informações de C&C Visíveis

```
0000ee40  17 14 15 1a 22 22 22 22  dd dd 62 22 xx xx xx xx  |....""""..b" CnC|
0000ee50  2e xx xx 00 22 22 22 22  00 17 22 22 bb e5 22 22  |.xx.""""..""..""|
0000ee60  6c 69 73 74 65 6e 69 6e  67 20 74 75 6e 30 00 22  |listening tun0."|
0000ee70  68 74 74 70 73 3a 2f 2f  79 6f 75 74 75 2e 62 65  |https://youtu.be|
0000ee80  2f 5f 59 76 7a 65 70 56  62 6c 64 34 00 22 22 22  |/_YvzepVbld4."""|
0000ee90  2f 70 72 6f 63 2f 00 22  2f 65 78 65 00 22 22 22  |/proc/."/exe."""|
0000eea0  20 28 64 65 6c 65 74 65  64 29 00 22 2f 66 64 00  | (deleted)."/fd.|
0000eeb0  22 22 22 22 2e 61 6e 69  6d 65 00 22 2f 73 74 61  |""""anime."/sta|
0000eec0  74 75 73 00 22 22 22 22  52 45 50 4f 52 54 20 25  |tus."""REPORT %|
0000eed0  73 3a 25 73 00 22 22 22  48 54 54 50 46 4c 4f 4f  |s:%s."""HTTPFLOO|
0000eee0  44 00 22 22 4c 4f 4c 4e  4f 47 54 46 4f 00 22 22  |D.""LOLNOGTFO."" |
0000eef0  5c 78 35 38 5c 78 34 44  5c 78 34 45 5c 78 34 45  |\x58\x4D\x4E\x4E|
0000ef00  5c 78 34 33 5c 78 35 30  5c 78 34 36 5c 78 32 32  |\x43\x50\x46\x22|
0000ef10  00 22 22 22 7a 6f 6c 6c  61 72 64 00 22 22 22 22  |."""zollard."""" |
0000ef20  47 45 54 4c 4f 43 41 4c  49 50 00 22 73 68 65 6c  |GETLOCALIP."shel|
0000ef30  6c 00 22 22 65 6e 61 62  6c 65 00 22 73 79 73 74  |l.""enable."syst|
0000ef40  65 6d 00 22 73 68 00 22  2f 62 69 6e 2f 62 75 73  |em."sh."/bin/bus|
0000ef50  79 62 6f 78 20 4d 49 52  41 49 00 22 4d 49 52 41  |ybox MIRAI."MIRA|
0000ef60  49 3a 20 61 70 70 6c 65  74 20 6e 6f 74 20 66 6f  |I: applet not fo|
0000ef70  75 6e 64 00 22 22 22 22  6e 63 6f 72 72 65 63 74  |und."""ncorrect|
0000ef80  00 22 22 22 2f 62 69 6e  2f 62 75 73 79 62 6f 78  |."""/bin/busybox|
0000ef90  20 70 73 00 22 22 22 22  2f 62 69 6e 2f 62 75 73  | ps."""/bin/bus|
0000efa0  79 62 6f 78 20 6b 69 6c  6c 20 2d 39 20 00 22 22  |ybox kill -9 ."" |
```

Manipulação de DNS e Sequestro de Rotas para Perpetrar Fraudes Financeiras

cert.br nic.br cgi.br

Ataques Envolvendo CPEs para Alteração de DNS

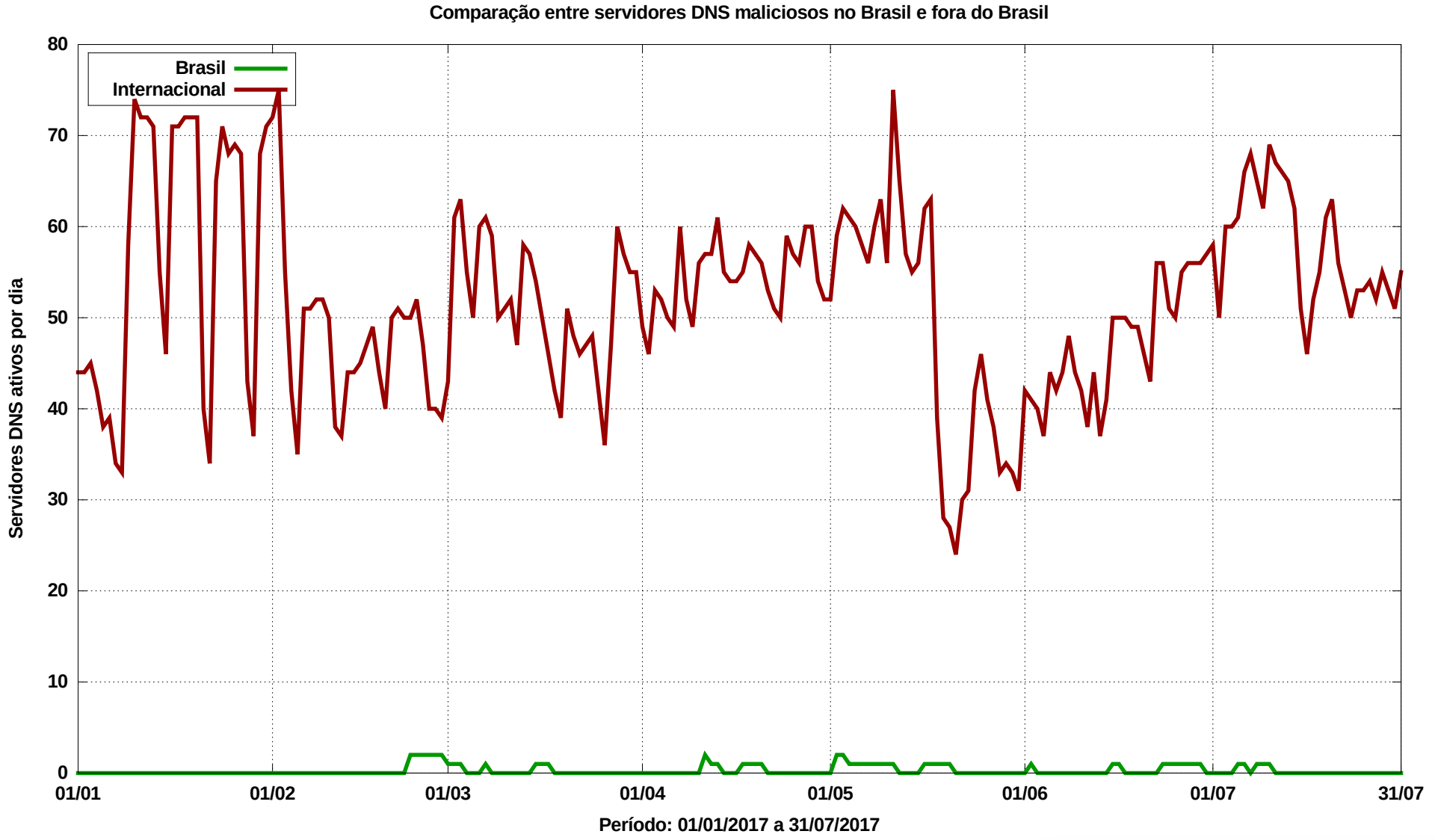
Comprometidos

- 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

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

Características dos Sequestros de Rota Detectados

Períodos:

- **variando de minutos a horas**
- **inicialmente à noite, escalando para feriados e finais de semana**

Prefixos sequestrados:

- **/24 de serviços Internet Banking**
- **/24 de provedores de nuvem**

Equipamentos:

- **roteadores de borda de pequenos e médios provedores**
- **1 caso via rede de gerência**

Levantados túneis GRE:

- **para destinos em provedores de *hosting***
- **protocolos HTTP e DNS no destino**

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 nas instituições
- 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

Segurança é Inerentemente Multissetorial: **Cooperação para um ecossistema saudável**

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

- desenvolvedores
  - 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/

Obrigado

www.cert.br

cristine@cert.br jessen@cert.br @certbr

01 de agosto de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br