Notable trends in Brazil: BGP hijacking for financial fraud and the evolution of Mirai

Cristine Hoepers
General Manager
cristine@cert.br
This slide set is TLP: WHITE
BGP Hijacking for Financial Fraud
Case 1

Period:
- 2017-03-26 13h
- 2017-03-26 16h

Prefixes:
- /24 of the Internet Banking
- Two /24 of a public DNS service
- One /24 of a big CDN

Routers:
- Juniper ACX
- Mikrotik 1009

GRE tunnels to:
- Hosting provider A (HTTP)
- Hosting provider B (DNS)
Case 2

Period:
• 2017-03-29 22h
• 2017-03-30 09h

Prefix:
• /24 of the Internet Banking

Router:
• Mikrotik

Tunnel:
• unknown
Case 3 – has not replied to notifications

Period:
• 2017-04-11 2h
• 2017-04-11 3h

Prefix:
• /24 of the Internet Banking

Router:
• unknown

Tunnel:
• unknown
Case 4

Period:
- 2017-04-21 11h
- 2017-04-21 13h

Prefixes:
- Old /24 of the Internet Banking
- New /24 of the Internet Banking

Router/server:
- Compromised a Ubuntu server, used to manage the router
- Mikrotik router compromised via Ubuntu GRE tunnel to:
  - Hosting provider C (HTTP)
Case 5 – denies that it has ever happened

Period:
• 2017-05-24 19h
• 2017-05-24 20h
• 2017-05-29 16h
• 2017-05-29 ??h

Router/server:
• Unknown

Prefixes:
• Old /24 of the Internet Banking
• New /24 of the Internet Banking

GRE tunnel:
• unknown
Recommendations

1. Monitoring:
   • BGPmon
     - https://bgpmon.net
   • BGPStream
     - https://twitter.com/bgpstream
     - http://bgpstream.caida.org
   • Scripts to query looking glass servers
     - Ex: telnet://lg.saopaulo.sp.ix.br

2. Announce a more specific prefix (/24)
   • for the networks that host critical services
     - example: internet banking

3. Connect to an Internet eXchange point
   • shortest path possible to the neighboring networks
Mirai Evolution
Source of the Mirai data

- Traffic captured in our distributed network of honeypots
  https://honeytarg.cert.br/honeypots/

- Identifies a very specific Mirai scanning signature
  - scanning for ports 23, 2323, 7547, 5555, 23231, 37777, 6789, 22, 2222 and 81

- It is the metric being used for Mirai by CyberGreen
  https://stats.cybergreen.net/
Daily unique IPs actively scanning, with Mirai signature

Period: 2016-09-15--2017-05-20

Unique IPs infected with Mirai: World and LAC Region

World — black line
LAC Region — blue line
Daily unique IPs actively scanning, with Mirai signature

Period: 2016-09-15--2017-05-20

Unique IPs infected with Mirai: 5 RIRs

LACNIC
ARIN
RIPE
APNIC
AfriNIC
Unique IPs infected with Mirai: Top 10 CCs, LAC Region

Period: 2017-01-01--2017-05-20

Daily unique IPs actively scanning, with Mirai signature

Country Codes:
- BR
- AR
- EC
- MX
- CO
- CL
- PE
- UY
- VE
- CR
Thank You
www.cert.br

June 16, 2017

@certbr
cristine@cert.br