Botnet Remediation in ISP networks

Carlos Fragoso Mariscal

ESNOG · 6th October 2011 · Barcelona

Botnet Remediation on ISPs networks

- Context
- Detection
- Notification
- Remediation
- Study cases

Context

- Cybercrime is a major problem nowadays
- Cross-border incidents with impact on …
  - Users
  - Service providers (reputation, infrastructure…)
- Containment or cleaning requires …
  - Knowledge, skills and tools sometimes beyond average user
- Private/Public partnership needed
- Several key players directly involved
  - CERTs
  - LEAs
  - ISPs / Service Providers
  - AV/Security vendors
  - Academia
- Security means "*quality*" !!!

Detection

- Combination of methods, processes and tools
- Considerations
  - Time sensitive
  - Avoid false positives
  - Avoid disruption/transparent for end-users
  - Respect privacy (Personal Identifiable Information – PII)
- Threat classification
- Sources
  - Monitoring aggregate traffic
    - Flows
    - DNS
    - Relevant applications
  - 3rd party feeds
    - *Shadowserver, TeamCymru, Feedback loops…*
  - Feedback/notifications/complaints from users or customers
  - Active scanning
  - IDS or Honeypots

Notification

- Inform about the problem and next actions
- Considerations
  - Public Network Locations
  - Shared corporate/customer Ips
  - Contact data on service sign-up (prefered method)
  - End-user expertise
- Mechanisms
  - Email
  - Telephone call
  - Postal mail
  - Walled-garden (strict or leaky)
  - Instant messaging
  - Short Message Service (SMS)
  - Web browser

Remediation

- Remove, disable or render bot harmless
- Provide necessary tools and education
  - Security-oriented website
  - Security support forums (staff & volunteers)
  - Help for identification of affected device
- Remediation process should include
  - Help for backing up personal files (USB thumb/hard drives, cloud)
  - OS/SW patches downloading and/or AV updates
  - Autoupdate configuration explanation and check
  - Professional assistance options
  - Provide Software (*online* or CD/DVD) for remediation/cleaning
  - Inform corresponding LEA about infection
- An opportunity for professional remediation services
- What if a user refuses to remediate?

Study Cases

- Japan Cyber Clean Center (CCC)
  - *https://www.ccc.go.jp/en_ccc/*
- German Anti-Botnet
  - *https://www.botfrei.de/en/index.html*
- Australia IIA
  - *http://www.security.iia.net.au/*

References

- *“Recommendation for the Remediation of Bots in ISP Networks”*, IETF Internet Draft (Sep, 2011)
  - *http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-16*
- *“IIA Guide for ISPs”*, Internet Industry Association (AU)
  - *http://iia.net.au/index.php/initiatives/isps-guide.html*
  - *http://iia.net.au/images/resources/pdf/esecurity_code_consultation_version.pdf*
- *“Voluntary Notification to Consumers regarding botnets and malware*”, NIST RFI (USA)
  - *http://www.nist.gov/itl/csd/botnets-100411.cfm*
  - *http://www.federalregister.gov/articles/2011/09/21/2011-24180/models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of*
- *“CSIRC Working Group 8*”, FCC (USA)
  - *http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii*
- *“Internet Crime Complaint Center (IC3)” (USA)*
  - *http://www.ic3.gov*

cfragoso@cesicat.cat **www.cesicat.cat**

@cesicat