Incident Response dealing with the whole country

Javier Berciano
Head of incident response
What is INCIBE?

Leading company in cybersecurity and digital trust development for:

- The public
- Companies, especially those in strategic sectors
- The academic research network in Spain (RedIRIS)

It leads different cybersecurity interventions at a national and international level.
CERTSI (Security and Industry CERT)

Year 2012 Partnership Framework Agreement:

State Secretariat for Security + State Secretariat for Information Society and Digital Agenda = CERTSI

CNPIC + INCIBE = LEA technology support
CERTSI (Security and Industry CERT)

A benchmark for the technical resolution of cybersecurity incidents that affect essential services

Prevention  Mitigation  Response

individuals  companies  critical infrastructure operators  academic and research network

FIRST Regional Symposium for Europe 2017, Valencia
MICS

Detection & Analysis
Intelligence
Value

CERT SERVICES

DETECTION TOOLS
ANALYSIS TOOLS
3rd PARTIES
Spamtraps
Honeypots

- SMB
- SSH
- Telnet
- FTP
- RDP
- HTTP
- VNC

Glastopf

Kipp
Skanna and .ES .NET .NAME .COM... hosted in Spain
Fast-Flux
MICS

DETENTION TOOLS

ANALYSIS TOOLS

3rd PARTIES

CERT SERVICES

Detection & Analysis

Intelligence

Value

FIRST Regional Symposium for Europe 2017, Valencia
Information feeds

- Microsoft Digital Crimes Unit
- Symantec
- Anubis Networks
- Shadowserver
- Team CYMRU
- Spamhaus

bots  C&C  URLs  IPs

FIRST Regional Symposium for Europe 2017, Valencia
Information feeds

- CERT.PL
  - bots
  - C&C
  - URLs
  - IPs

- PhishTank
  - URLs

- Tor
  - IPs
  - URLs

- MDL

- abuse.ch
  - URLs

- ADMINUSLABS
  - C&C

- AM Trckr
  - C&C

- APWG
  - URLs

- Arbor Networks
  - URLs
Information feeds

- zone-it
- CLEAN MX
- RSA
- CYBERCRIME
- OpenPhish
- S21 SEC
- Fraunhofer FKIE
- Bambenek Consulting
Information feeds

More than **10,000,000** events per day

92% bot infections

Two main sources Anubis Networks and Microsoft-DCU

Both provide all connections to a C2 as evidence
FIRST Regional Symposium for Europe 2017, Valencia
The **objective** of the Antibotnet Service is the mitigation of botnets from the point of view of the **disinfection** of the users’ devices infected: **bots**. Also the service is way to inform and aware users about this problems.

This service is a result of the work developed day to day by INCIBE in collaboration with other national and international entities in fighting against botnets:

- An average of **9,2 million evidences of botnet connections** from Spain daily.
- An average of **59,500 unique IPs affected** daily in Spain.
- Data from close to **900 external sinkholes**, which correspond approximately with **129 families** of botnets.

Spain is pioneer in this kind of initiative alongside countries such Germany, Japan or Sweden.
Antibotnet service

Information analysis and validation

Identify end customer and notification

Feed (bots)

CyberSecurity Intelligence Engine

Botnet information and database

Detection

3rd parties

Treath analysis

Metrics

Botnet information and disinfections tools

Awareness and prevention

END USER

ANTIBOTNET SERVICE

URL + Botnet Ticket

CertisI

Security and Industry CERT

FIRST Regional Symposium for Europe 2017, Valencia
Antibotnet Service is offered to end-users through **five different ways**:

- **Online Service:** End-users can check online if their public IP is involved in botnet activity.
- **Plugin Service:** Plugin available for Google Chrome, Firefox and Internet Explorer to check the IP periodically and automatically, in order to alert the end-user in case of a positive is detected.
- **CONAN Mobile:** Application for Android devices, which helps to check the level of security of mobile devices developed by INCIBE. This app integrates the functionality of the Antibotnet Service, giving botnet alerts in case a positive is detected on wifi networks.
- **ISP Notification:** The Spanish ISP Telefónica collaborates with us notifying end-users by email about botnet related incidents that affect their internet connection. INCIBE gives to Telefónica every day a feed containing bot evidences related to their ASNs. With this information, Telefónica can identify end-user lines affected and therefore notify.
- **API for companies:** API that allows IT personal to integrate the service in their network monitoring systems. This service is oriented to companies.
Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/19)
- DNS (UDP/53) (*Open Resolver Project*)
- Kad (UDP/6429)
- MS-SQL (UDP/1434)
- NetBIOS (UDP 137 to 139)
- NTP Mode 6 (UDP/123) (*Open NTP Project*)
- NTP Mode 7 (UDP/123)
- QOTD (UDP/17)
- Quake Network Protocol (UDP/26000 and UDP/27960)
- SNMPv2 (UDP/161) (*Open SNMP Project*)
- SSDP (UDP/1900) (*Open SSDP Project*)
- Steam Protocol (Many – UDP/27015)
Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/137)
- DNS (UDP/53) (O)
- Kad (UDP/6429)
- MS-SQL (UDP/1434)
- NetBIOS (UDP 13)
- NTP Mode 6 (UDP)
- NTP Mode 7 (UDP)
- QOTD (UDP/17)
- Quake Network 
- SNMPv2 (UDP/16)
- SSDP (UDP/1900)
- Steam Protocol

Protocols That Should not be Exposed:

- DB2 (UDP/523)
- Elastic Search (TCP/9200)
- HDFS (TCP/50070, TCP/50075, TCP/50090, TCP/50105, TCP/50030, TCP/50060)
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/11211)
- MongoDB (TCP/27017, TCP/27018, TCP/27019, TCP/28017)
- NAT-PMP (UDP/5351)
- NetBIOS (TCP/137 to 139)
- Portmapper (UDP/111)
- RDP (TCP/3389 and UDP/3389)
- REDIS (TCP/6379)
- rlogin (TCP/451)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)
Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/1)
- DNS (UDP/53) (O)
- Kad (UDP/6429)
- MS-SQL (UDP/1433)
- NetBIOS (UDP 137)
- NTP Mode 6 (UDP)
- NTP Mode 7 (UDP)
- QOTD (UDP/17)
- Quake Network f
- SNMPv2 (UDP/16)
- SSDP (UDP/1900)
- Steam Protocol

Protocols That Should not be Exposed:

- DB2 (UDP/523)
- Elastic Search (TCP/9200)
- HDFS (TCP/50070, TCP/50075, TCP/50090, TCP/50105, TCP/50030, TCP/50060)
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/11211)
- MongoDB (TCP/27017, TCP/27018, TCP/27019, TCP/27017)
- NAT-PMP (UDP/5351)
- NetBIOS (TCP/137 to 139)
- Portmapper (UDP/111)
- RDP (TCP/3389 and UDP/3389)
- RDIS (TCP/6379)
- rlogin (TCP/451)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)

Protocols That are Vulnerable:

- ISAKMP (UDP/500)
- Netcore/Netis Router (UDP/53413)
- SSL/FREAK (TCP/443)
- SSLv3 (TCP/443)
- Synful Knock (TCP/80)
Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/149)
- DNS (UDP/53) (O)
- Kad (UDP/6429)
- MS-SQL (UDP/1433)
- NetBIOS (UDP 137)
- NTP Mode 6 (UDF)
- NTP Mode 7 (UDF)
- QOTD (UDP/17)
- Quake Network (UDP/28000)
- SNMPv2 (UDP/161)
- SSDP (UDP/1900)
- Steam Protocol (TCP/27840)

Protocols That SI

- DB2 (UDP/523)
- Elastic Search (TCP/9200)
- HDFS (TCP/50070, UDP/50070)
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/11211)
- MongoDB (TCP/27017)
- NAT-PMP (UDP/53)
- NetBIOS (TCP/137)
- Portmapper (UDP/111)
- RDP (TCP/3389 and UDP/445)
- REDIS (TCP/6379)
- rlogin (TCP/513)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)

- UPDATED: 2016-11-02 – Added LDAP
- UPDATED: 2016-09-22 – Added RDP
- UPDATED: 2016-09-21 – Added ISAKMP
- UPDATED: 2016-05-18 – Added XDMCP
- UPDATED: 2016-05-18 – Added DB2
- UPDATED: 2016-03-09 – Added TFTP
- UPDATED: 2016-02-17 – Added mDNS
- UPDATED: 2015-09-20 – Added Synful Knock
- UPDATED: 2015-09-15 – Added Portmapper
- UPDATED: 2015-06-01 – Added Elastic Search
- UPDATED: 2015-03-09 – Added SSL/FREAK
- UPDATED: 2015-02-13 – Added MongoDB
- UPDATED: 2015-02-08 – Added Open SSDP and Open SNMP project links
- UPDATED: 2015-01-29 – Added MS-SQL
- UPDATED: 2015-01-23 – Added MemCached
- UPDATED: 2015-01-21 – Added REDIS
- UPDATED: 2015-01-07 – Added NAT-PMP
- UPDATED: 2014-11-17 – Added SSLv3
- UPDATED: 2014-08-28 – Added Netcore/Netis
- UPDATED: 2014-07-01 – Added Quake and Steam
- UPDATED: 2014-06-26 – Added IPMI and Gameover Zeus
- UPDATED: 2014-06-12 – Added port numbers
- UPDATED: 2014-03-26 – Added NetBIOS
- UPDATED: 2014-03-06 – Added SSDP
PyRTIR

- Uses the 1.0 Request Tracker REST API
- Main goal is to complement and improve our day to day incident handling
- Easily expandable. It is structured in plugins, and each of them performs a different work into RTIR.
- Plugins:
  - Phishing
  - Defacement
  - StealRAT
  - XSS
  - Stats
- Whois data and yara rules
Yara detected websites: Examples
RTIR Custom Actions

On create action for Incident Reports, get URL, extract domains and IP (IPv4, IPv6) and set values in custom fields if it's not listed in the blacklist.

On conditional action for Incidents, push data from Incident into JSON and:
- Put Incident metadata into SIEM.
- Post metadata in JSON to ElasticSearch
Custom forms

Unify access to another internal party tools in RTIR. Examples:
- Internal WHOIS.
- GPG public keys management.
- SIEM integration
Easy life for operator

Several options to launch Investigations:
• domain or IP: get WHOIS data and parse email contacts.
• automatic: based on category of the Incident, get a template and parse it, get emails from WHOIS query and create Investigations by URL.
Export data

Feedback for SIEM
Executive indicators
Cyber Security Situational Awareness

JSON format
- By email
- POST to ElasticSearch
La imagen muestra una página del Informe de Indicadores Ejecutivos del FIRST Regional Symposium for Europe 2017, Valencia. El informe incluye gráficos y tablas que detallan los incidentes registrados en diferentes categorías durante el año. Las categorías incluyen Empresa, RedIRIS, Ciudadano, Infraestructuras críticas e Internacional. El informe proporciona una visión global de la cantidad de incidentes reportados en cada categoría y mes.
Information Sharing with strategic companies, universities and National CERT/CSIRT
ICARO: goals

- Share knowledge with strategic companies
- Increase detection capabilities on private sector
- Define a neutral Spanish hub
- Increase automation in early warning
MISP (Malware information Sharing Platform)
Thank you!

Javier Berciano
javier.berciano@incibe.es

www.incibe.es    www.certsix.es
@certsi_