CCN
Centro Criptológico Nacional

CCN-CERT
Centro Criptológico Nacional

Abogacía Española
CONSEJO GENERAL

Jornada sobre Esquema Nacional de Seguridad

Ciberseguridad

Lo "cyber" proporciona titulares

TIMESONLINE

NEWS | COMMENT | BUSINESS | MONEY | SPORT | LIFE & STYLE | TRAVEL | DRIVING

UK NEWS | WORLD NEWS | POLITICS | WEATHER | PHOTO GALLERIES | TECH & WEB | TIMES ON

Where am I? › Home › News › World News

From Times Online

November 15, 2007

Chinese cyber-spies 'greatest threat' to US

Times Online and agencies in Washington

Chinese espionage poses the "single greatest risk" to the American technology sector, according to a congressional advisory panel.

In its annual report, the US-China Economic and Security Review Commission accused Beijing of pursuing an aggressive spying program to acquire critical US technology and adopting "destructive" tactics, including cyber attacks, to target American infrastructure.

"Chinese military strategies have embraced destructive warfare techniques, including the use of cyber attacks (which) if carried out strategically on a large scale could have catastrophic effects on the target countries' critical infrastructure," the panel reported.

"Chinese espionage activities in the United States are so extensive that they comprise the single greatest risk to the security of American technologies."

EXPLORE WORLD NEWS

- IRAQ NEWS
- US & AMERICAS NEWS
- EUROPE NEWS
- MIDDLE EAST NEWS
- ASIA NEWS
- AFRICA NEWS
- IRELAND NEWS

TIMES RECOMMENDS

- Remains found at Fossett crash site
- £130 phone with unlimited music
- By bus round the feuding Russian fringe

Terror activities for these outfits. He said that various social networking sites were helping these perpetra communicate, collaborate and network with the like-minded.

Cyberattackers shut down one Georgian government site and defaced another with images of Adolf Hitler.

traffic.

assault Web sit for whic

"Nobod happen Burling, an Atlar volunte nation c

Entertainment

Also in the news

Video and Audio

Have Your Say

Magazine

In Pictures

BBC Home Search

UK version | International version | About the versions

BBC NEWS | LIVE BBC NEWS CHANNEL

News Front Page

World

Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

England

Northern Ireland

Scotland

Wales

Business

Politics

Health

Education

Science & Environment

Technology

Entertainment

Also in the news

Video and Audio

Have Your Say

Magazine

In Pictures

Country Profiles

Special Reports

RELATED BBC SITES

SPORT

WEATHER

CBBC NEWSROUND

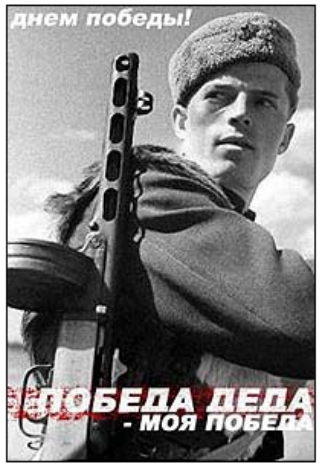
Last Updated: Thursday, 17 May 2007, 14:52 GMT 15:52 UK

E-mail this to a friend | Printable version

The cyber raiders hitting Estonia

As Estonia appeals to its Nato and EU partners for help against cyber-attacks it links to Russia, the BBC News website's Patrick Jackson investigates who may be responsible.

Estonia, one of the most internet-savvy states in the European Union, has been under sustained attack from hackers since the ethnic Russian riots sparked in late April by its removal of a Soviet war memorial from Tallinn city centre.



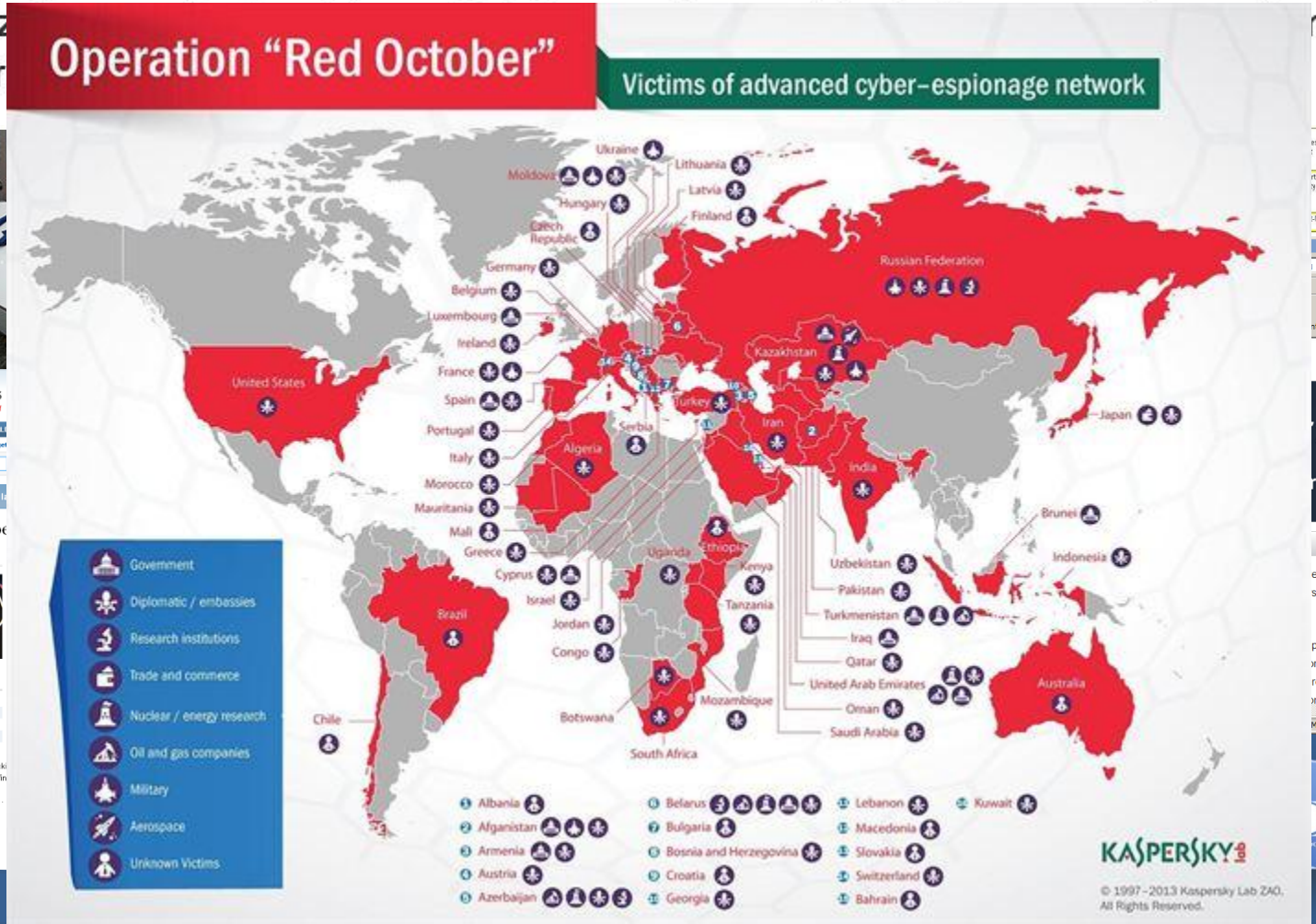
One Estonian website was defaced to show a Soviet soldier

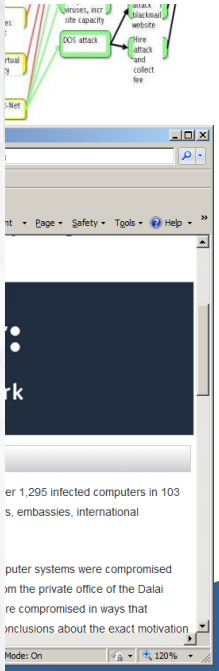
Websites of the tiny Baltic state's government, political parties, media and business community have had to shut down temporarily after being hit by denial-of-service attacks, which swamp them with external requests.

Some sites were defaced to redirect users to images of Soviet soldiers and quotations from Martin Luther King about resisting "evil".

And hackers who hit the ruling Reform Party's website at the height of the tension on 29 April left a spurious message that the Estonian prime minister and his government were asking forgiveness of Russians and promising to return the statue to its original site.

On January 14, 2013, Kaspersky Lab announced the discovery of “Red October”, a high-level cyber-espionage campaign that has been active for over 5 years. (https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies). This campaign has successfully infiltrated computer networks at diplomatic, governmental and scientific research organiz ns and networ





EL PAIS

INTERNACIONAL

Estados Unidos y China, ante la primera ciberguerra fría

Obama firmó una orden ejecutiva la pasada semana que le otorga poderes especiales

ANTONIO CAÑO | Washington | 19 FEB 2013 - 20:06 CET 135

Archivado en: Barack Obama Guerra electrónica Ataques informáticos China Ciberactivismo Seguridad internet Asia oriental Activismo Guerra Estados Unidos Internet Norteamérica Asia Telecomunicaciones Conflictos América Comunicaciones

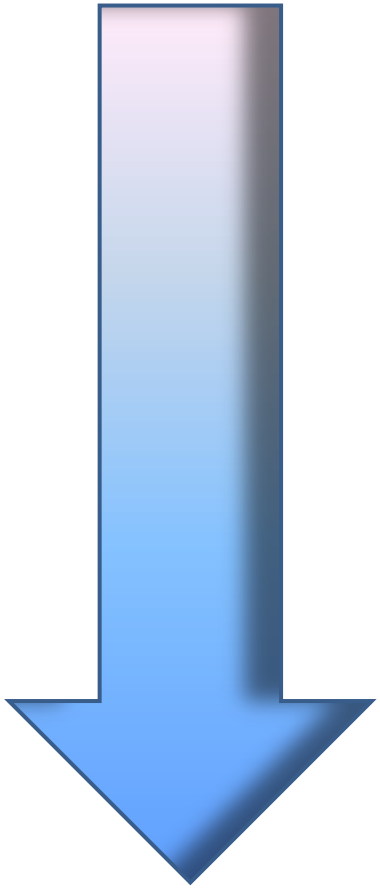
El presidente Barack Obama durante una intervención en Washington este martes. / JIM LO SCALZO (EFE)

La Casa Blanca describió este martes los reiterados ataques cibernéticos, que una investigación reciente vincula directamente con una unidad secreta del Ejército chino, como "un serio desafío para la seguridad y la economía de Estados Unidos", lo que es la señal de que una nueva guerra fría, en el desconocido e incontrolable espacio de Internet, ha comenzado entre las dos grandes potencias que se disputan la supremacía en el siglo XXI.

Sin acusar directamente a China, por

Evolución de la Amenaza

- Communication Security (COMSEC)
- Transmission Security (TRANSEC)
- Computer Security (COMPUSEC)
- Network Security (NETSEC)
- Electronic Security (ELSEC)
- Emission Security (EMSEC)
- Information Security (INFOSEC)
- Information Assurance (IA)
- Cibersecurity

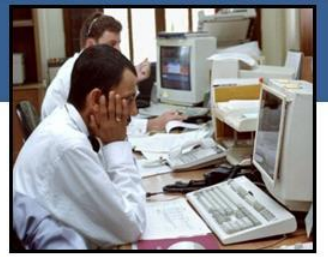


1. Diversidad de agentes, motivación

Ciberataques. Motivación

- ROBO DE INFORMACIÓN
- BENEFICIO ECONÓMICO
- PROVOCACIÓN DE DAÑOS
- REIVINDICACIÓN SOCIAL O POLÍTICA

Ciberataques. QUIÉN



Usuarios internos

1. Ciberespionaje / Robo propiedad intelectual
   - Objetivo: Administraciones públicas / Empresas estratégicas
   - China, Rusia, Irán, otros…
     Servicios de Inteligencia / Fuerzas Armadas / Otras empresas

2. Ciberdelito / cibercrimen
   - Objetivo: Robo información de tarjetas de crédito / Fraude Telemático / Blanqueo de dinero…
   - HACKERS y crimen organizado

3. Ciberactivismo
   - Objetivo: Ataques a servicios webs / Robo y publicación de datos e información sensible o de carácter personal.
   - ANONYMOUS y otros grupos

4. Uso de INTERNET por terroristas / **Ciberterrorismo**
   - Objetivo : Comunicaciones , obtención de información, propaganda o financiación // Ataque a Infraestructuras críticas

CCN-CERT
Centro Criptológico Nacional

Ciberataques: Características

Los ciberataques normalmente comparten las siguientes características comunes:

- **Bajo coste**
  Muchas herramientas de ataque se pueden descargar de forma gratuita o con un coste muy bajo para el daño que pueden causar.

- **Fácil empleo**
  Para muchos ataques no son necesarios grandes conocimientos técnicos.

- **Efectividad**
  Existe una probabilidad muy alta de alcanzar los objetivos buscados con estos ataques por la ausencia de políticas de seguridad o la limitación de recursos existentes en la parte defensiva debido a la falta de concienciación de las organizaciones gubernamentales, empresas y ciudadanos.

- **Bajo Riesgo para el atacante**
  Es muy difícil atribuir un ataque con las **herramientas de ocultación** del origen existentes actualmente en INTERNET y por la diferencia de **legislaciones** de los diferentes países.

2. Diversidad de sectores afectados

Energético
Industria Nuclear
Administración
Espacio
Financiero
Hídrico
Alimentación
Transportes
Sanidad
Industria Química
Instalaciones de Investigación
Tecnologías de la Información

Infraestructuras Críticas

Energético
Aeroespacial
Administración
Defensa
Farmacéutico
Financiero
Marítimo
Química
Minería
Ingeniería
Derechos Humanos
Comunicaciones

Sectores Estratégicos

CCN-CERT
Centro Criptológico Nacional

ESPIONAJE= Perdida de concursos, fluctuaciones de precios, variación en materias primas, fusiones y adquisiciones….

Cost of cyber espionage in UK

Citizens …… 3.100 M£

Companies… 21.000 M£

Government 2.200 M£

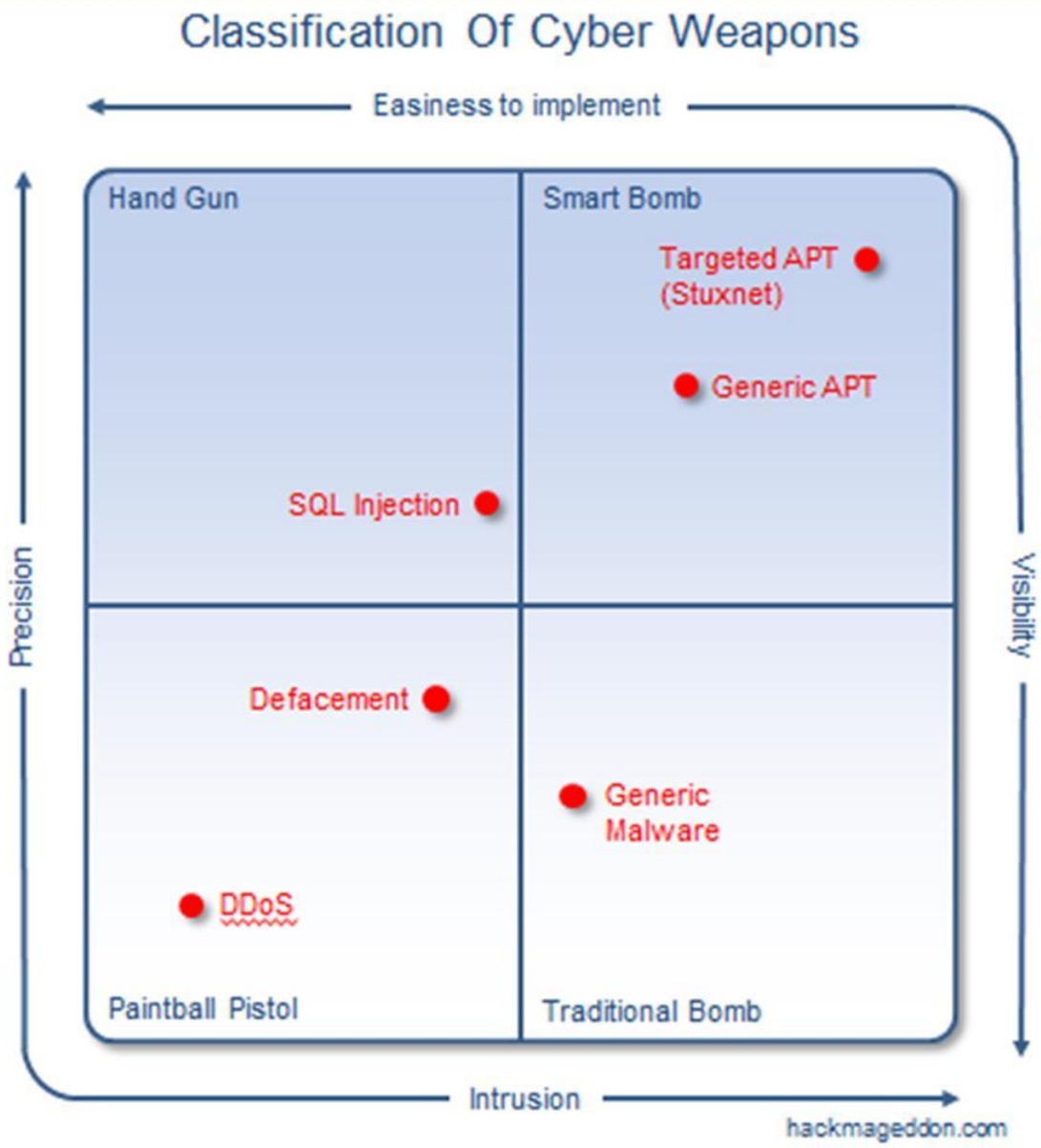
3. Impacto económico

Estrategia Europea de Ciberseguridad

El objetivo es "impulsar los valores europeos de libertad y democracia y velar por un **crecimiento seguro de la economía digital"**

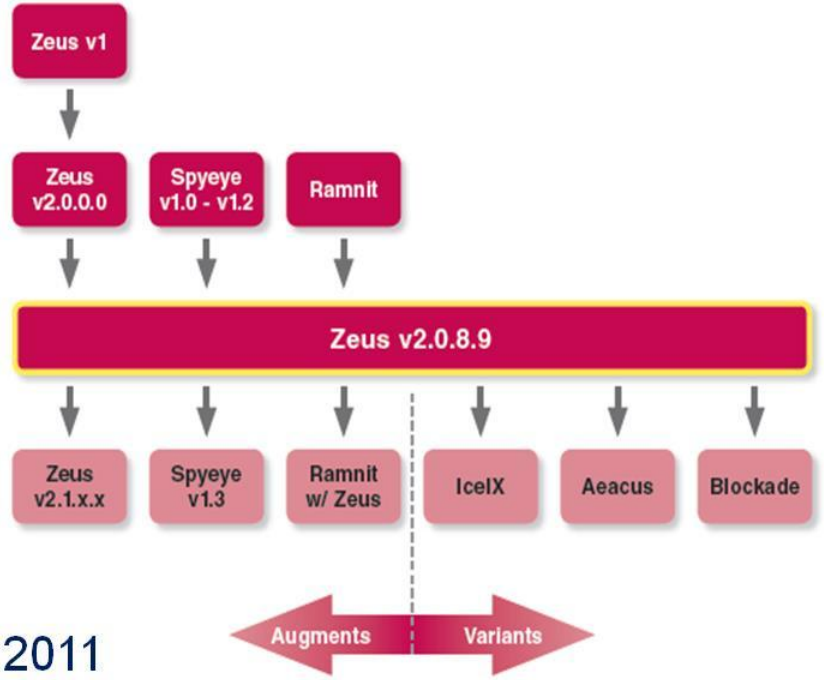
PRINCIPIOS

- Valores esenciales de la UE en el Ciberespacio
- Protección de los derechos fundamentales, de la libertad de expresión, de los datos personales y de la privacidad
- Acceso para todos
- Gobierno eficiente y democrático con todos los grupos de interés
- Responsabilidad compartida para asegurar la seguridad



4. Calidad, Complejidad, Eficacia

MALWARE 2012

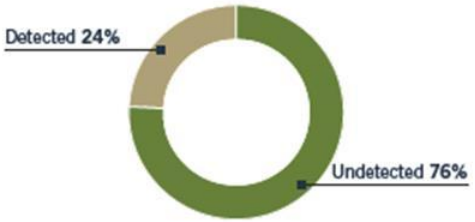


- ZeuS evolution → Source code available in Feb 2011
  - Improve versions.

- *Malware as a Service* → "licences and services".

- brokers.

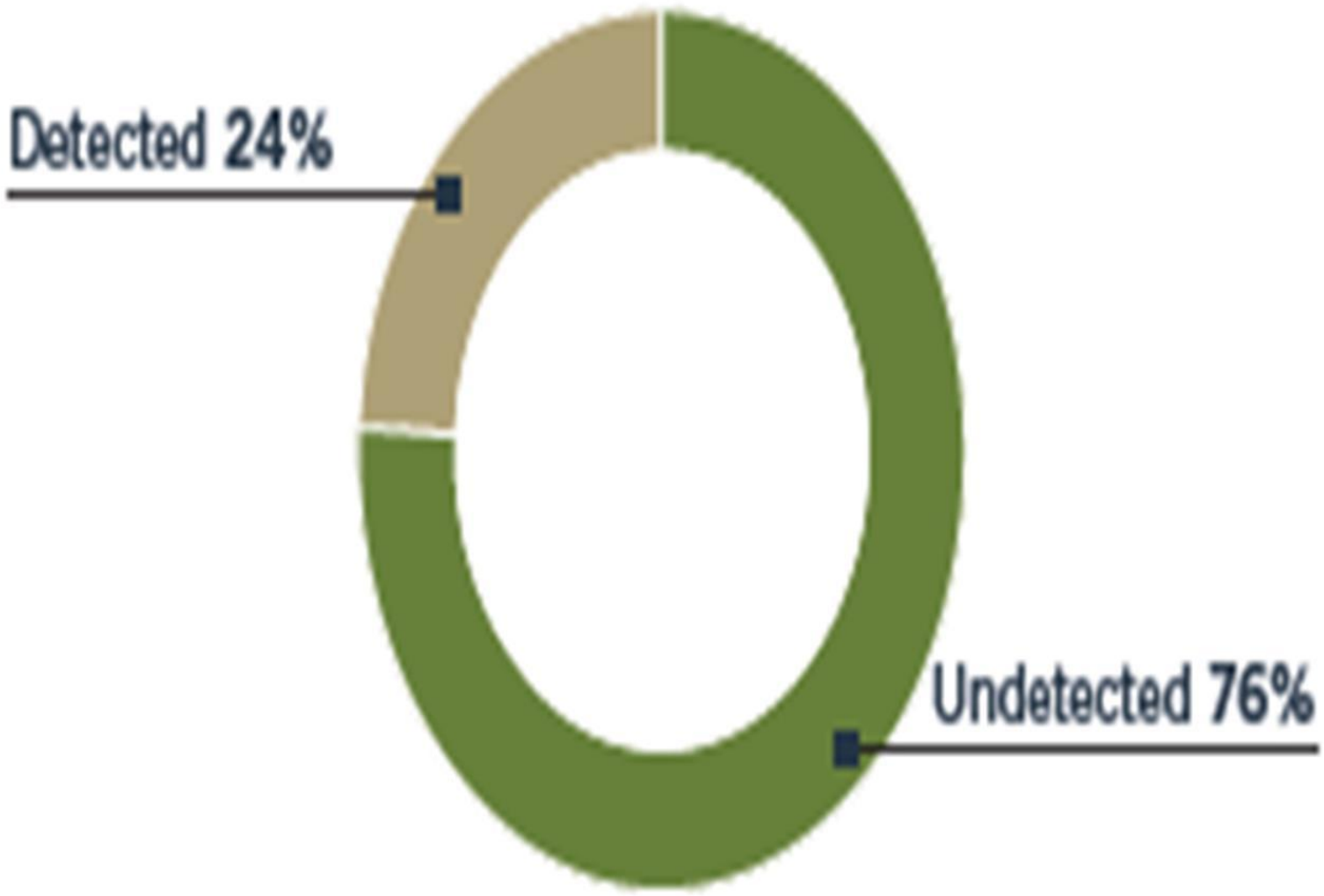
- New Target→ SMART telephones.



Definición APT / Ataques Dirigidos

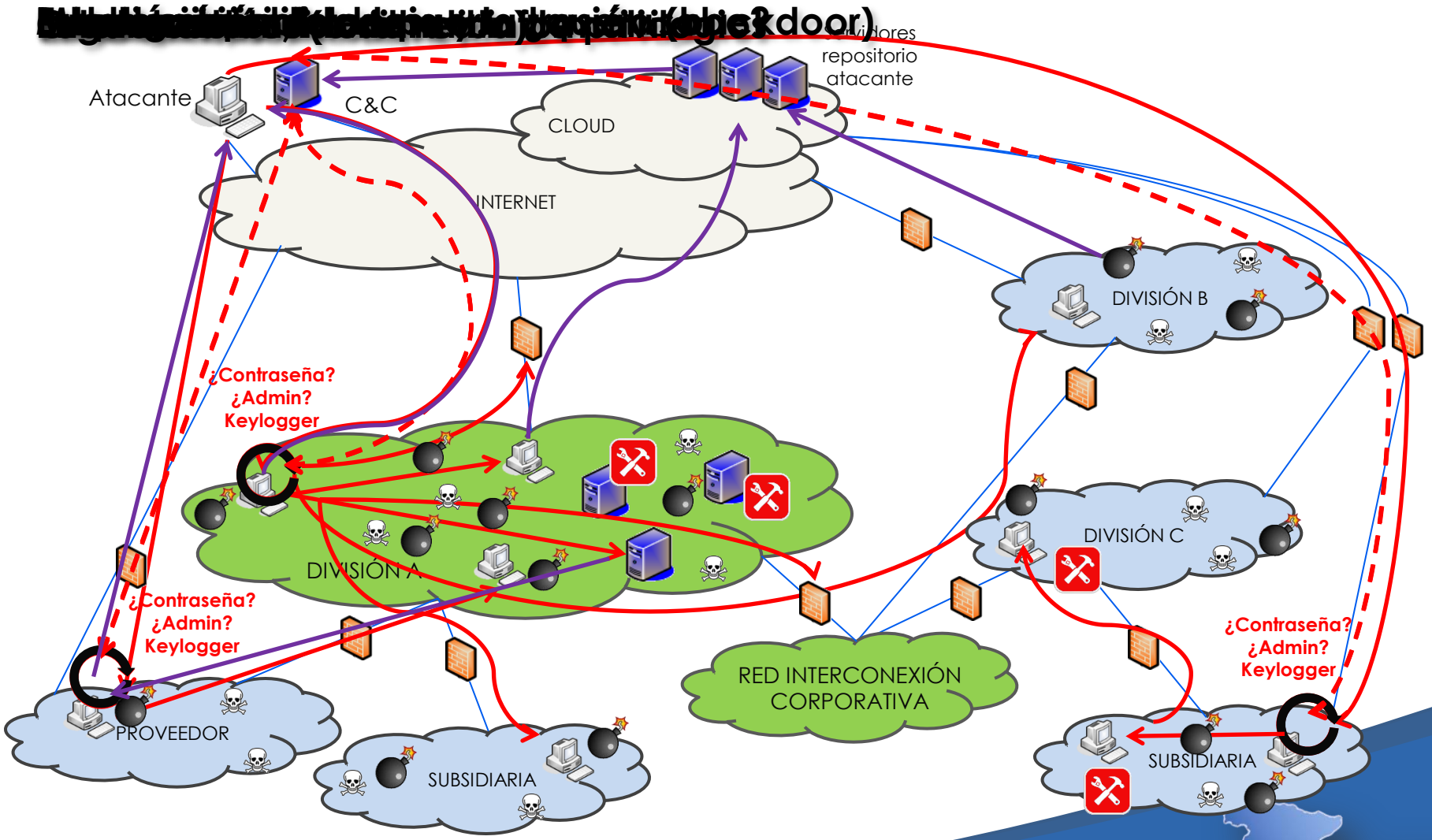
- **Ataque Dirigido**
  - Ciber Ataque "a medida" contra un objetivo concreto (administración, empresa, red, sistema)
- **Threat**
  - El atacante tiene la intención y capacidades para ganar acceso a información sensible almacenada electrónicamente
- **Persistent**
  - Una vez infectado, se mantiene el acceso a la red/sistema durante un largo periodo de tiempo
  - Difícil de eliminar
- **Advanced**
  - Habilidad de evitar la detección
  - Adaptabilidad al objetivo
  - Disponibilidad de recursos (tecnológicos, económicos, humanos)

CCN-CERT
Centro Criptológico Nacional



APT

Fases de una APT



SIGUIENTE

TAXONOMÍA DE UN APT

Atacantes

Actores
Financiación
Formación
Modus Operandi
.../.../...

Infraestructuras

Sistemas C&C
Nodos
Saltos
IP,s / Dominios
.../.../...

Capacidades

Exploits
Vectores de infección
Cifrado / RAT
Persistencia
.../.../...

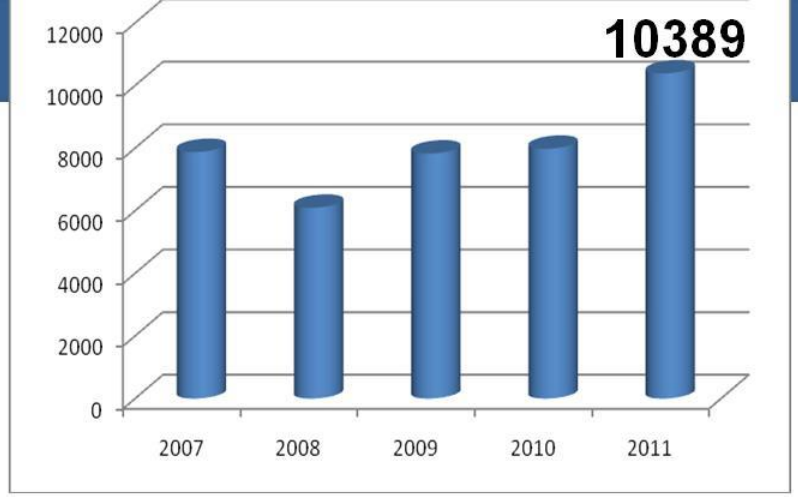
Víctimas

Sectores afectados
Métodos detección
.../.../...

Valoración de la Amenaza

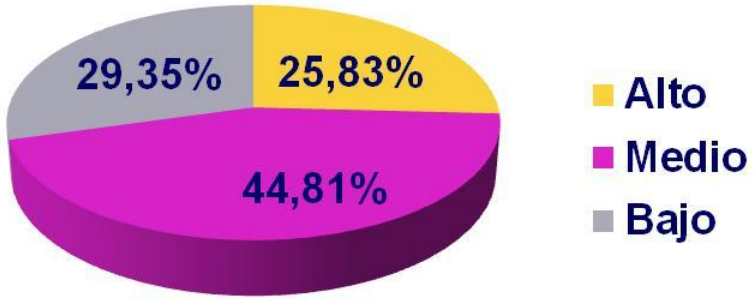
	Target			
Actor	*Civilians/NGOs*	*Companies*	*Vital infra-structure*	*Government*
States	Large	Very large	Large	Very large
Terrorists	Small	Average	Small	Small
Hacktivists	n/a	Average	n/a	Average
Script kiddies	n/a	n/a	n/a	n/a
Criminals/ mercenaries	Average	Very large	Large	Large

Vulnerabilidades



- More and less 9000 vulnerabilities
- HIGH = Remote code execution
- No motivation in security investigators

- ZERO DAY Vulnerability
  - Black market



5. Somos cada vez más vulnerables

- En 2020 habrá entre 50.000 y 70.000 millones de dispositivos interconectados. (Fuente: Comisión Europea, CISCO)
- M2M Machine to Machine. Aumento de la superficie de ataque a las Infraestructuras Críticas

Ciberataques: Factores tecnológicos

Los siguientes factores tecnológicos incrementan la posibilidad de estos ataques:

- La **complejidad** creciente de la tecnología hace más difícil determinar el grado de seguridad de un determinado producto o sistema.
- La **rapidez de la evolución tecnológica** y las exigencias y competitividad del mercado ocasionan que, con frecuencia, se desplieguen productos con vulnerabilidades y fallos de seguridad que son aprovechados por los agresores.
- Existe un mayor riesgo para productos fabricados en países fuera de la órbita occidental, pues es más **difícil controlar** la introducción de elementos inseguros.
- Hay una relativa **falta de madurez** de la industria de las tecnologías de la información y las comunicaciones, al no considerar la seguridad como un factor de diseño de los productos o sistemas.
- Incremento de la **interconexión** de todo tipo de sistemas utilizando Internet.

Existen evidencias de que determinados países tienen programas de capacitación técnica para lograr realizar ciberataques. En algunos casos, dicha capacitación técnica es considerada y abordada como una **capacidad militar** más con la que se plantean lograr la superioridad

Vulnerabilidades. Precios

Producto	Rango de precios
Adode Reader	3.800 – 23.000€
Mac OS X	15.300 – 38.300 €
Android	23.000 – 46.000 €
Plug-ins Java para navegador	30.600 – 76.700 €
Plug-ins Flash para navegador	30.600 – 76.700 €
Microsoft Word	38.300 – 76.700 €
Windows	46.000 – 92.000 €
Firefox	46.000 – 122.600 €
Safari	46.000 – 225.000 €
Chrome	61.300 – 153.000 €
Internet Explorer	61.300 – 153.000 €
iOS	76.700 – 191.600 €

LA ARTICULACIÓN DE LA RESPUESTA DE LOS ESTADOS

ESTRATEGIAS DE CIBERSEGURIDAD:

Antes de 2011:

- EE.UU. (2008 y 2010)
- Rusia (2010)126
- Reino Unido (2009)127
- Australia (2008)
- Canadá (2009)
- Estonia (2008)
- Singapur (2009)

Durante 2011:

- República Checa
- Finlandia (borrador)
- Alemania
- Israel (proyecto)
- Letonia (proyecto)
- Nueva Zelanda
- Suráfrica
- Dinamarca (borrador)
- Francia
- India
- Japón (proyecto)
- Holanda
- Polonia (proyecto)
- Corea del Sur
- Reino Unido (actualización)
- EE.UU. (anuncio de las tres políticas principales: Departamento de Defensa, Departamento de Estado y la Casa Blanca)

Del análisis de las acciones realizadas en ciberseguridad por Estados Unidos, Canadá, Francia, Reino Unido, Alemania, Noruega, Holanda, Estonia o Australia se extraen las siguientes conclusiones:

- Se realiza una **aproximación global** al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberseguridad; gobiernos centrales, regionales y locales, FAS, FCSE, infraestructuras críticas y ciudadanos
- Se considera que garantizar la seguridad del ciberespacio constituye un **aspecto esencial** para el funcionamiento de una sociedad avanzada (UK)
- Se reconoce que es un **problema emergente**, que el escenario es **incierto**, que es una de las prioridades para la seguridad nacional.
- Se reconoce que el ciberespacio es un escenario en el que es preciso disponer de **capacidades nacionales que aseguren la ventaja en su uso**

- En las naciones analizadas, se han adoptado **decisiones organizativas** para incrementar la **coordinación** entre los organismos con responsabilidades en ciberseguridad, tanto a nivel de gestión y planificación como a nivel operativo, estableciendo en cada caso el organismo que asume el liderazgo.
- Se potencian las **capacidades de monitorización y alerta temprana**, se concentran y se fortalecen los equipos de respuesta ante incidentes (especialmente las gubernamentales) por considerarlos los mejor posicionados para resolver el problema de las nuevas amenazas de forma más eficiente.
- **Se impulsan esquemas nacionales de seguridad (requisitos de seguridad mínimos a implantar en las redes gubernamentales)** y se intentan disminuir las interconexiones gubernamentales con Internet.
- Se priorizan y fortalecen las capacidades de inteligencia por el mejor conocimiento que poseen de la amenaza con el objetivo de hacer frente a ataques complejos.

- Se declara como necesidad estratégica la **formación y concienciación** de servidores públicos, empresas y ciudadanos. Se presentan diversas soluciones para conseguir este objetivo
- Se impulsan las actividades **de investigación e innovación** en este campo mediante alianzas con Universidades y centros de investigación
- Se proporciona una **dotación presupuestaria** para la implantación de las estrategias con la vocación política de mantenerla en el tiempo
- Se impulsa la **cooperación internacional** como un factor imprescindible dada la globalidad de muchos aspectos de la amenaza

ENS Principios

1. La seguridad como un proceso integral
2. Gestión de la seguridad basada en los riesgos
3. Prevención, reacción y recuperación
    1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
    2. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
4. Líneas de defensa
5. Reevaluación periódica
6. La seguridad como función diferenciada

Líneas de Defensa

4. Líneas de defensa

   1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

      a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

      b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

      c) Minimizar el impacto final sobre el mismo.

   2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

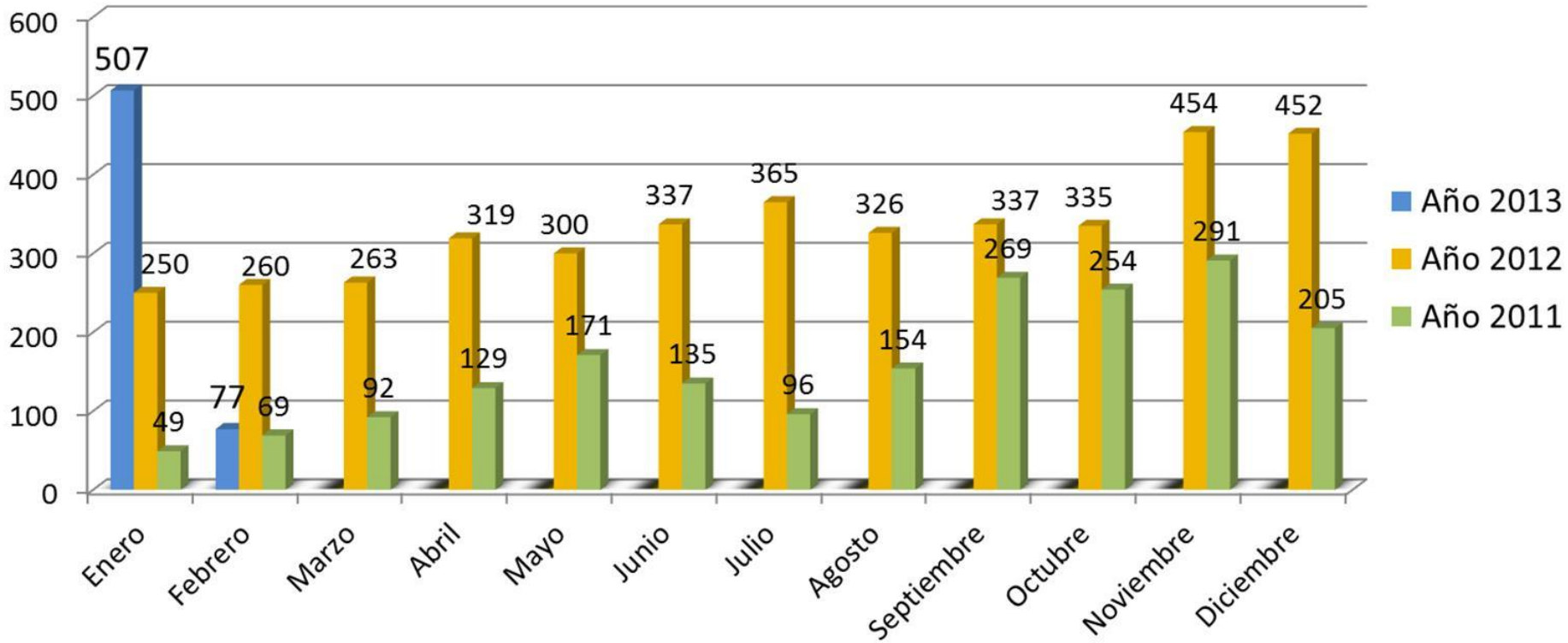
- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

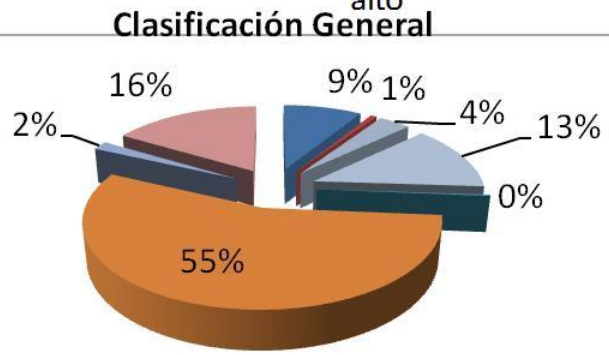
Gracias

CCN-CERT
Centro Criptológico Nacional

Total de incidentes por Mes

3998 en 2012





Recogida de información
Fraude
Disponibilidad
Intrusiones
Contenido Abusivo
Código Dañino
Otros
Seguridad de la información

CCN-CERT