VIII JORNADAS STIC CCN-CERT

La defensa del patrimonio tecnológico frente a los ciberataques

10 y 11 de diciembre de 2014

Gestión de incidentes

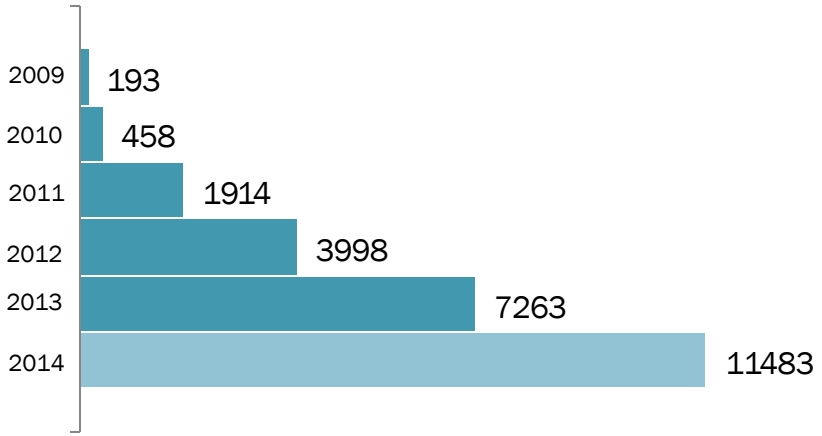
CCN-CERT

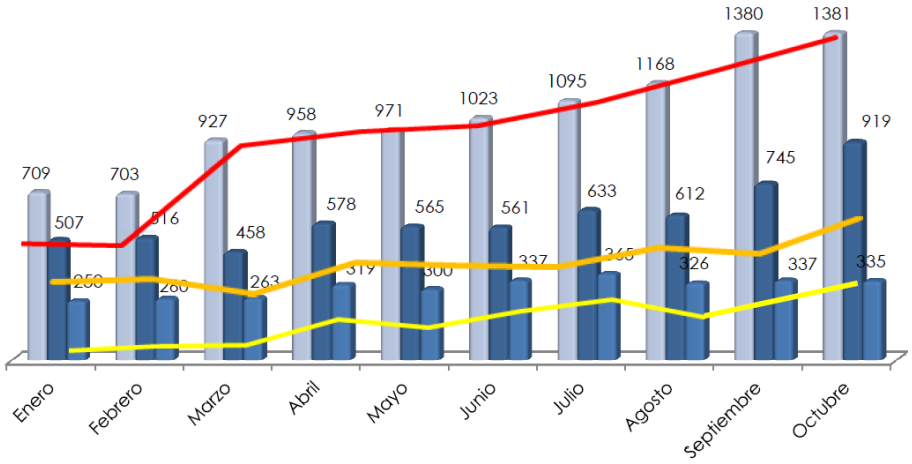
info@ccn-cert.cni.es

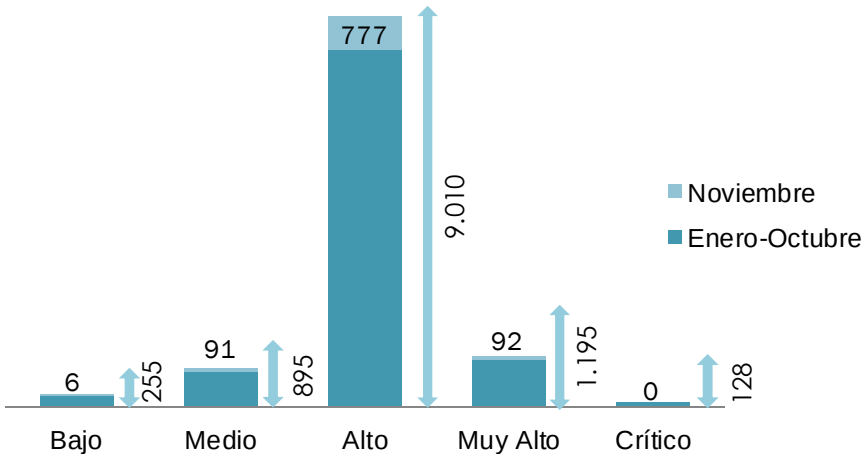
Equipo CCN-CERT

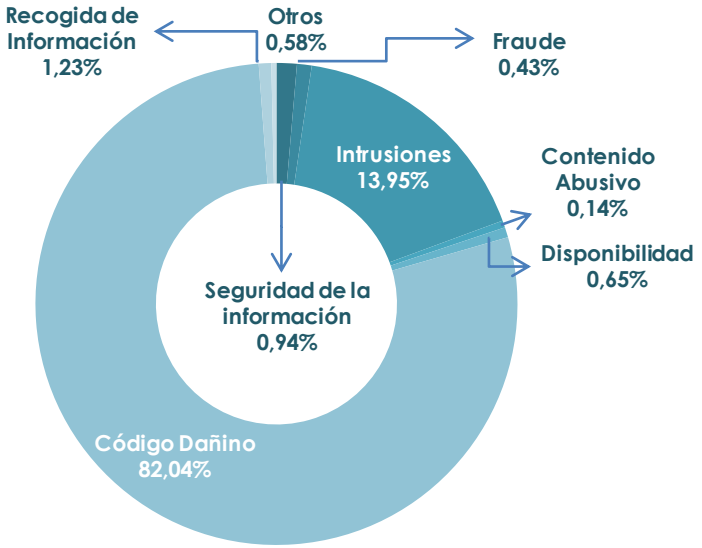
Índice

Estadísticas de incidentes (noviembre 2014)

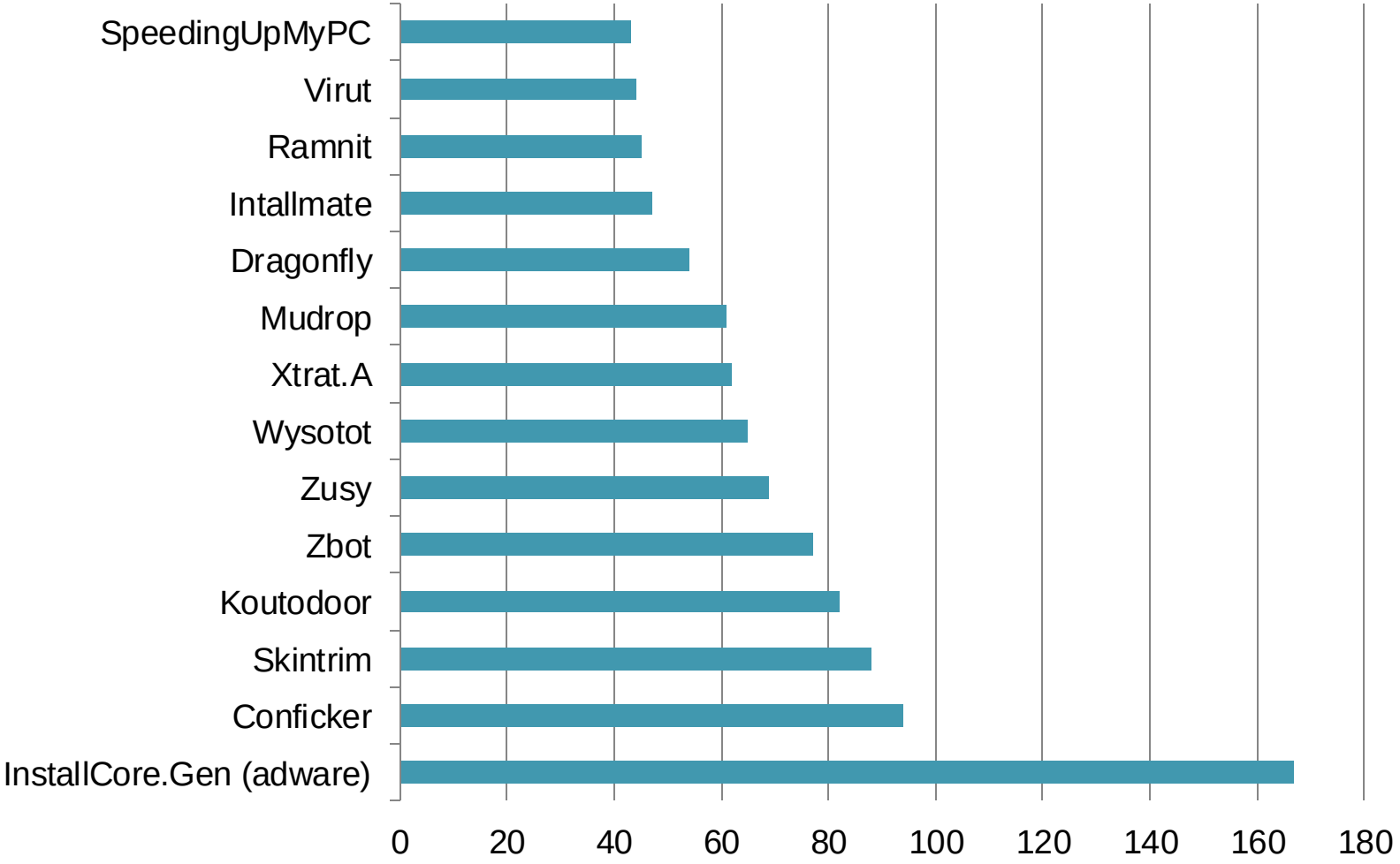






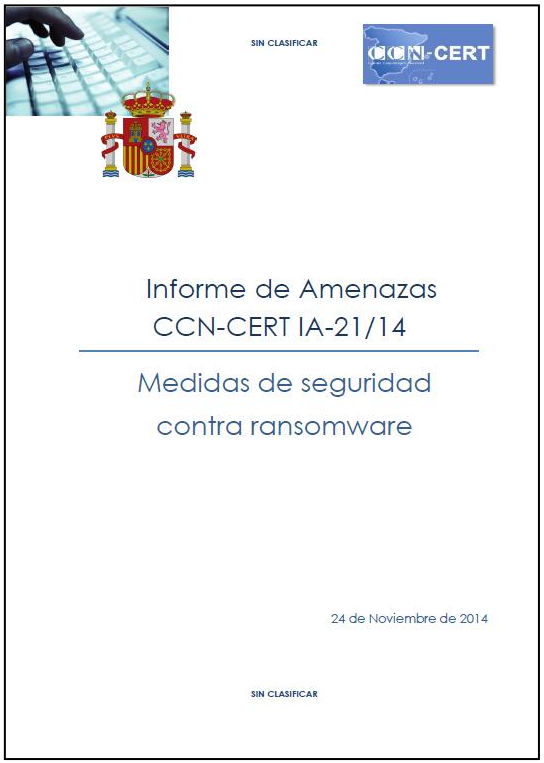


Código dañino más visto en 2014



Ransomware

- Múltiples oleadas de infección por ransomware en los últimos meses.
- A través de campañas de phishing
  - Correos
  - ...
- Publicación de Informe de Amenazas IA-21/14 sobre Medidas de seguridad contra ransomware
- **¡Copias de seguridad de la información importante!**



Campañas APT destacadas

- Rusia
  - SNAKE / UROBUROS / TURLA
  - Energetic BEAR / Dragonfly
  - APT28



- China
  - GRUPO A APT1,
  - GRUPO B Leounica
  - GRUPO C
  - GRUPO E MSUpdater,
  - GRUPO T

Campañas APT destacadas

- Hispanoparlantes
  - CARETO (The Mask)
  - MACHETE
- Otros países
  - REGIN
  - …//…

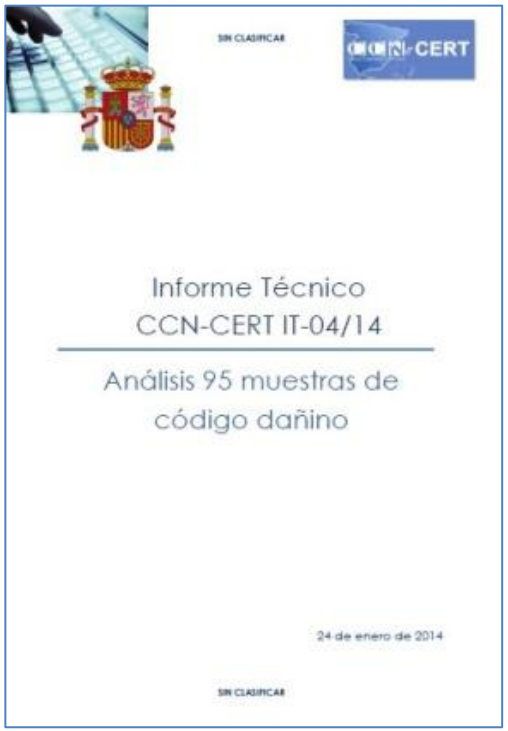
Snake/Uroburos/Turla

- Detectado con CARMEN
- Diferentes vectores y diferentes fases de infección
- Incidentes gestionados en 2014
  - Diversos incidentes relacionados con *Watering hole attacks* en Administración Local
  - Incidentes relacionados con fases iniciales de la infección en diferentes organismos de la Administración / Empresas

#Samples by compile month													
Year	01	02	03	04	05	06	07	08	09	10	11	12	Total
2006	1				3								4
2007				1		1				1			3
2008			2		1	2	1				2		8
2009	1	1					1			3	2	2	10
2010	1	1		1		1				1	2		7
2011			1			4	1			3	1	3	13
2012	2		1			1				1	2	7	14
2013	1	13	5	2	5	4	3	2	1	2	1		39
2014	2												2
Total	8	15	9	4	9	13	6	2	1	11	10	12	100

Grupo ByC CHINA

- Incidentes notificados
  - [CCN-CERT#140127491] Detectado contacto DNS ciberataque BYC
  - [CCN-CERT#140128142] Detectado contacto DNS ciberataque BYC
  - [CCN-CERT#140128134] Detectado contacto DNS ciberataque BYC
  - [CCN-CERT#140218084] Detectado contacto CompressNet de ciberataque BYC
  - [CCN-CERT#140207201] Detectado contacto desde IP ciberataque BYC
  - [CCN-CERT#140212052] Detectado contacto DNS ciberataque BYC
  - [CCN-CERT#140213539] Detectado contacto SMTP ciberataque BYC
  - [CCN-CERT#140214256] Detectado contacto SMTP ciberataque BYC
  - [CCN-CERT#140217251] Detectado contacto SMTP ciberataque BYC
  - [CCN-CERT#140221368] Detectado contacto DNS ciberataque BYC
  - [CCN-CERT#140128151] Aviso de seguridad
- 11 familias de malware
  - Win32/Ziyanzho.D
  - Win32/Ziyanzho.C ó HTool-Pipecmd
  - Network Shell with Injection
  - KeyloggerDownloader
  - HackTool:Win32/Onaht
  - Win32/Ziyanzho.B
  - TROJ_LOCATI.ZZXX
  - Jsp File Browser
  - UPSmgr Installer
  - Win32/Ziyanzho.A
  - Trojan.Win32.Ziyanzho.A



Sectores que reciben más ataques en ESPAÑA

Energético

Industria Nuclea

Administración

Espacio

Financiero

Hídrico

Al ion

Transporte

Sanid ndustria Química

ones de Investigación

Tecnologías de la Información

Disponibilidad

Infraestructuras Críticas

Energético

Administración

efensa

macéutico

Minería

Marítimo

Ingeniería

ciones

Derechos Humanos

Confidencialidad

Protección Patrimonio Tecnológico

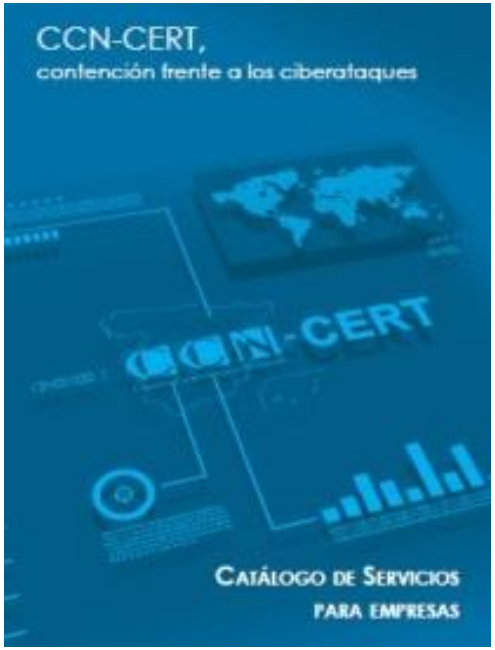
Sectores Más atacados

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Catálogo de Servicios

Actualmente hay 80 empresas adscritas al servicio de información.



- Envío de reglas / Alertas / Buenas Prácticas
- Acceso eventos CCN-CERT
- Acceso Parte privada portal
- LUCIA
- SAT INTERNET
- CARMEN
- Ingeniería Inversa / Análisis forense

LUCIA

CARMEN

SAT

Canales cifrados PGP/GPG