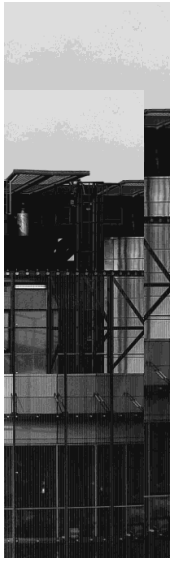


Ciberamenazas 2019
AGENTES

Javier Candau
Jefe Departamento Ciberseguridad
Centro Criptológico Nacional
ccn@cni.es

centro criptológico nacional

DIFUSIÓN LIMITADA

2 CCN-CERT

- Ley 11/2002 reguladora **del Centro Nacional de Inteligencia.**
- Real Decreto 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.
- Real Decreto 3/2010, 8 de Enero, que define el **Esquema Nacional de Seguridad** para la Administración Electrónica, modificado por el **RD 951/2015, de 23 de octubre.** Ampliación del ámbito de actuación con Ley 39/2015 Procedimiento Administrativo común de las AAPP y Ley **40/2015** Régimen Jurídico del Sector Público
- RDL 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información. Coordinación incidentes

Establece al CCN-CERT como CERT Gubernamental/Nacional competente

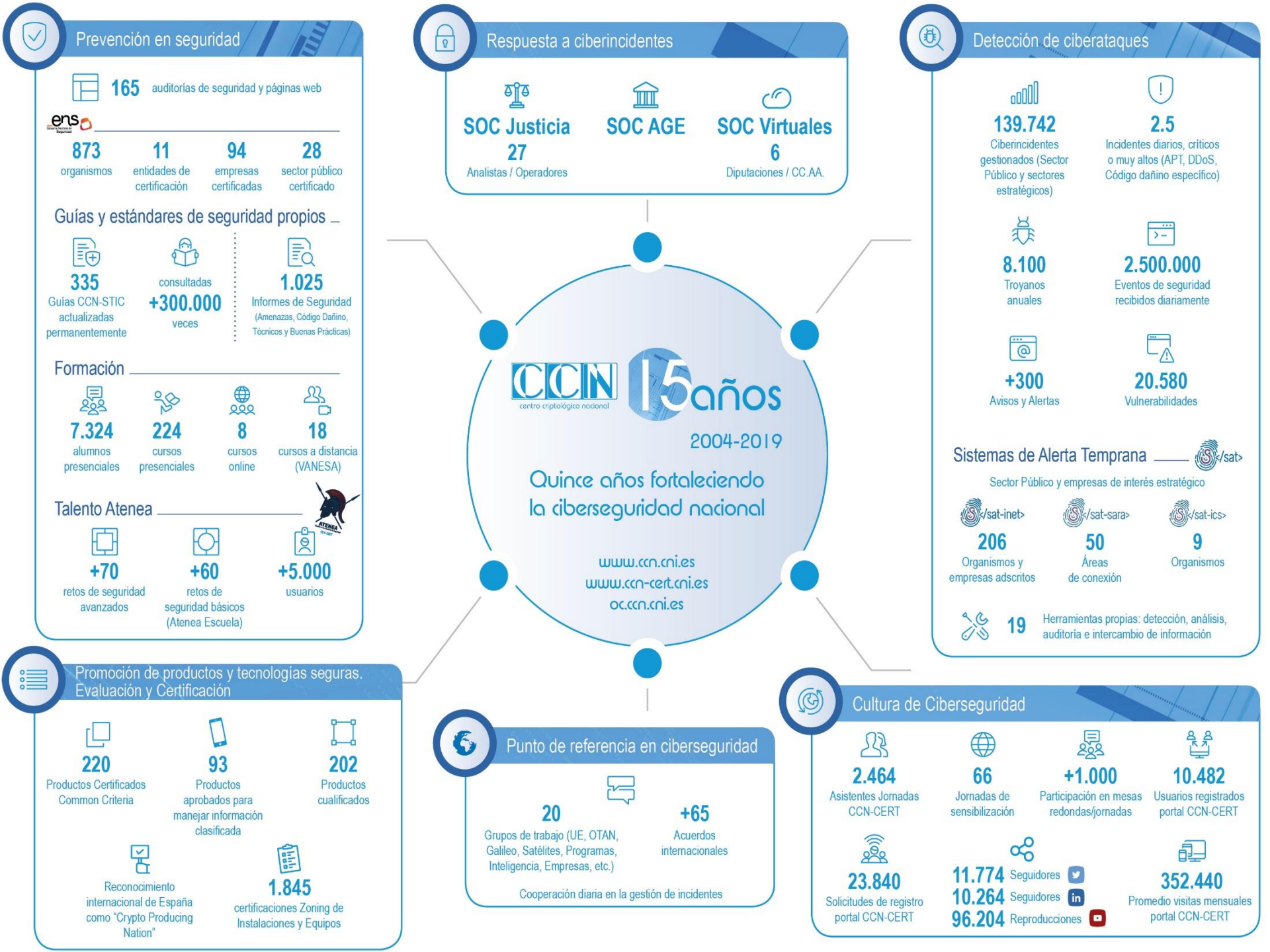
MISIÓN

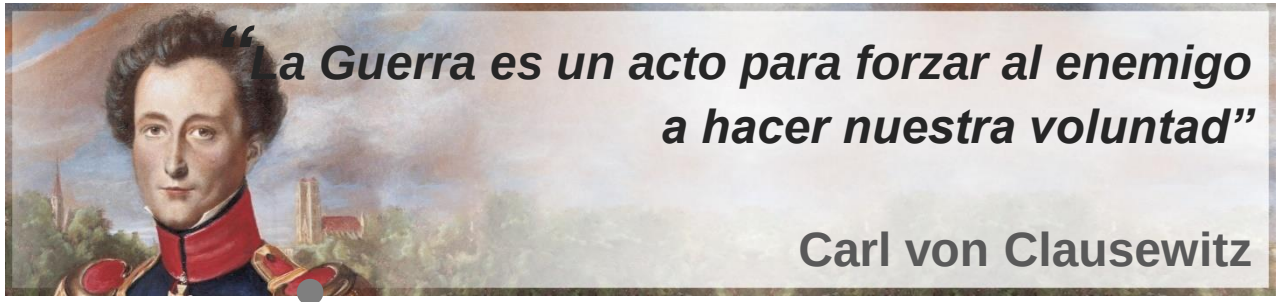
Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

Responsabilidad en ciberataques sobre:

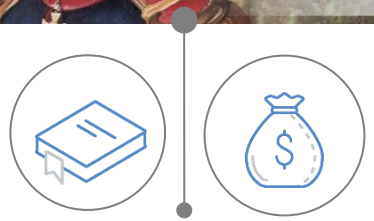
- **Sistemas clasificados**
- **Sistemas del Sector Público**
- Empresas y organizaciones de **sectores estratégicos (en coordinación con CNPIC).**


Prevención en seguridad
165 auditorías de seguridad y páginas web
ens
873 organismos
11 entidades de certificación
94 empresas certificadas
28 sector público certificado
Guías y estándares de seguridad propios
335 Guías CCN-STIC actualizadas permanentemente
consultadas +300.000 veces
1.025 Informes de Seguridad (Amenazas, Código Dañino, Técnicos y Buenas Prácticas)
Formación
7.324 alumnos presenciales
224 cursos presenciales
8 cursos online
18 cursos a distancia (VANESA)
Talento Atenea
+70 retos de seguridad avanzados
+60 retos de seguridad básicos (Atenea Escuela)
+5.000 usuarios
Respuesta a ciberincidentes
SOC Justicia
27
Analistas / Operadores
SOC AGE
SOC Virtuales
6
Diputaciones / CC.AA.
Detección de ciberataques
139.742
Ciberincidentes gestionados (Sector Público y sectores estratégicos)
2.5
Incidentes diarios, críticos o muy altos (APT, DDoS, Código dañino específico)
8.100
Troyanos anuales
2.500.000
Eventos de seguridad recibidos diariamente
+300
Avisos y Alertas
20.580
Vulnerabilidades
Sistemas de Alerta Temprana
/sat
Sector Público y empresas de interés estratégico
/sat-inet
206
Organismos y empresas adscritos
/sat-sara
50
Áreas de conexión
/sat-ics
9
Organismos
19 Herramientas propias: detección, análisis, auditoría e intercambio de información
CCN
centro criptológico nacional
15 años
2004-2019
Quince años fortaleciendo la ciberseguridad nacional
www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es
Promoción de productos y tecnologías seguras. Evaluación y Certificación
220
Productos Certificados Common Criteria
93
Productos aprobados para manejar información clasificada
202
Productos cualificados
Reconocimiento internacional de España como "Crypto Producing Nation"
1.845
certificaciones Zoning de Instalaciones y Equipos
Punto de referencia en ciberseguridad
20
Grupos de trabajo (UE, OTAN, Galileo, Satélites, Programas, Inteligencia, Empresas, etc.)
+65
Acuerdos internacionales
Cooperación diaria en la gestión de incidentes
Cultura de Ciberseguridad
2.464
Asistentes Jornadas CCN-CERT
66
Jornadas de sensibilización
+1.000
Participación en mesas redondas/jornadas
10.482
Usuarios registrados portal CCN-CERT
23.840
Solicitudes de registro portal CCN-CERT
11.774 Seguidores
10.264 Seguidores
96.204 Reproducciones
352.440
Promedio visitas mensuales portal CCN-CERT



"La Guerra es un acto para forzar al enemigo a hacer nuestra voluntad"

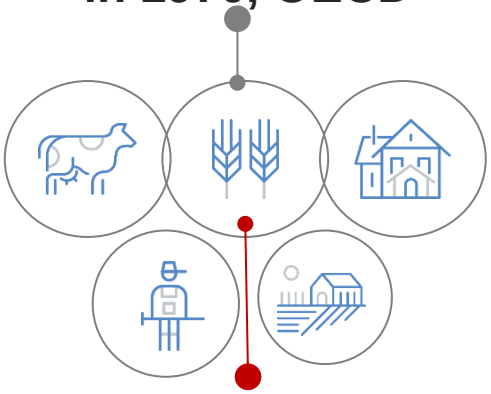
Carl von Clausewitz



Ideología ○ **Riqueza**

50% PIB

in 1970, OECD

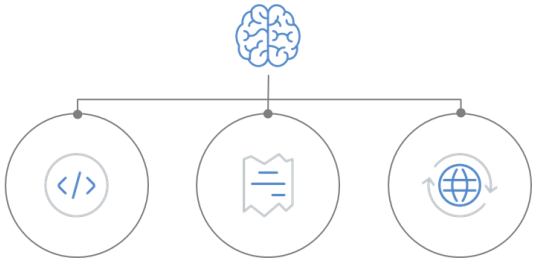


Territorio + Gente

Conquista = Guerra

Ventaja competitiva actual

Tecnología



Estas compañías significan

18%

Del Mercado de valores USA

Y USA significa

25%

Del PIB global

Microsoft Google amazon

Insignificante

Gente & Territorio

CCN centro criptológico nacional

Ciberguerra: Las nuevas armas.

Robo:	***"Tomar la propiedad de otro, con la intención de privarlo permanentemente de la misma."***	**2017.08**	**Equifax Ransomware**
Extorsión:	***"Practica de obtener algo, especialmente dinero a través de FUERZA o AMENAZA."***	**2017.05** **2017.06**	**WannaCry** **Bad Rabbit**
Propaganda Desinformación:	**"Influenciar los votantes de un país para beneficiar a una potencia extranjera."**	**2015** **2016** **2017** **2018**	**Brexit** **Elecciones USA** **Cataluña** **Brasil**
Espionaje:	***"Acto de manera secreta adquirir información sensible o clasificada."***	**2013.10** **2014** **2015**	**Teléfonos móviles de líderes europeos.** **SNAKE** **Snowden**
Sabotaje:	***"Intento deliberado de debilitar / deshabilitar los servicios esenciales, sistemas económicos o de defensa."***	**2010.07** **2012.08** **2015** **2017**	**Stuxnet** **Shamoon infectó 30,000 equipos de Aramco Interrumpió las operaciones más de 2 semanas.** **Blackenergy** **NotPetya**

Resultado final ● **Transferencia de Riqueza**

Ejemplo: Vulnerabilidad APACHE STRUTS

2017.01.29 Vulnerabilidad publicada. Se asigna CVE (Mitre)

- **CVE-2017-5638 Permite ejecución remota de código**
- **Comentada en muchos blog**
- **Se soluciona con una actualización**

2017.03.08 Publicación de exploit

- **Toda la info en blog. Afecta 35 millones de servidores**

2017.03.10 Alerta CCN-CERT

2017.03.11 Ataques a Web AAPP

- **+ 75 organismos notificados**
- **+ 25 Incidentes / 4 críticos**

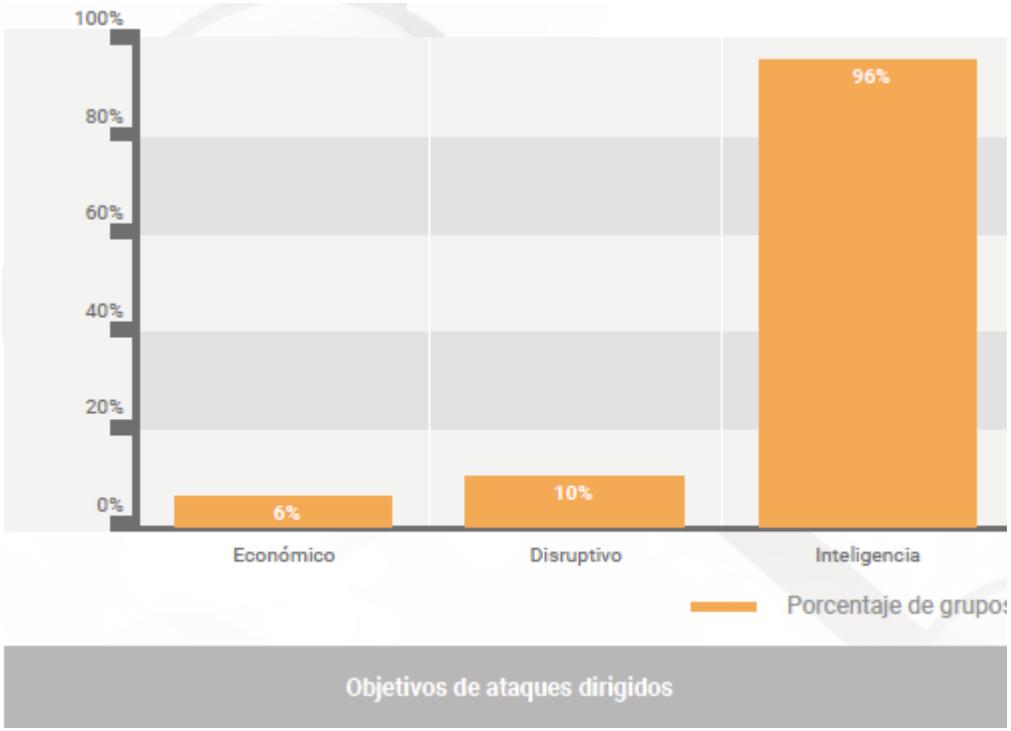
2017.03.13 Impacto:

- **Denegación de servicio**
- **Compromiso de información ???**
- **Cambio de certificados**
- **Bloqueo de la actividad de los Administradores**

- **2017.09.06 Vulnerabilidad publicada.**

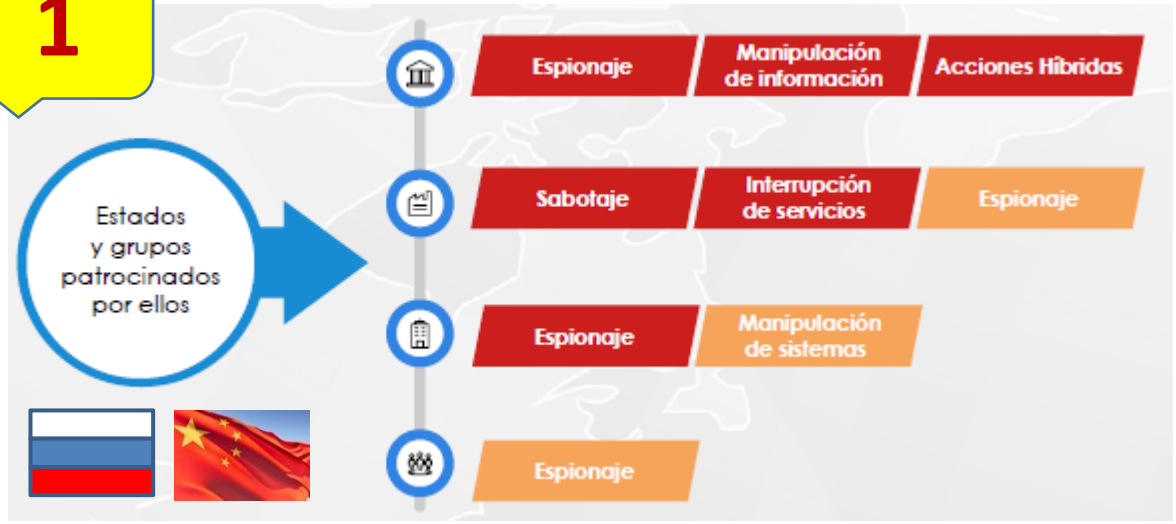
AGENTES DE LA AMENAZA 2019

Incremento de presencia de la amenaza



CCN
centro criptológico nacional

1

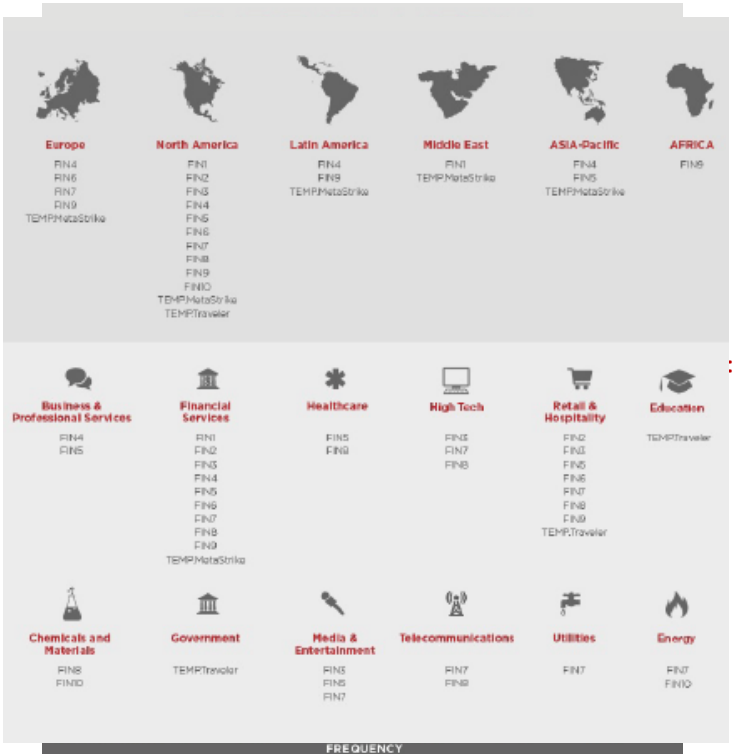

Estados y grupos patrocinados por ellos
Espionaje
Manipulación de información
Acciones Híbridas
Sabotaje
Interrupción de servicios
Espionaje
Espionaje
Manipulación de sistemas
Espionaje


J-31
F-35C
F-35A


Agentes de la amenaza
Víctima
Gobierno / Admón. Pública
Empresas
Infraestructuras críticas
Ciudadanos
Peligrosidad
Alta
Media
Baja

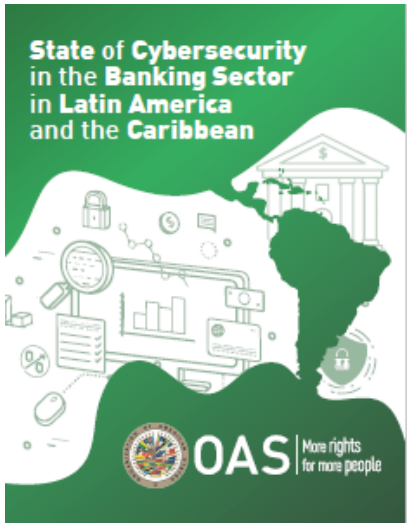

Goblin Panda
Vixen Panda
Deep Panda
Emissary Panda
Pirate Panda
Numbered Panda
Lotus Panda
Pitty Panda
Gothic Panda
Predator Panda
Dynamite Panda
Temper Panda
Pale Panda
Violin Panda
Hurricane Panda
Sabre Panda
Samurai Panda
Dagger Panda
Aurora Panda
Maverick Panda
Keyhole Panda
Stone Panda
Spicy Panda
Comment Panda ...
Energetic Bear
Snake
Octubre Rojo
Agent BTZ
Inception
APT28
Cosmic Duke
Monkey Duke
Cozyduke
Equation Group
Stuxnet
Duqu
Gauss
Flame
RCS
NSO-Pegasus
Machete
Siesta / The Mask
Animal Farm
Regin
Desert Falcons

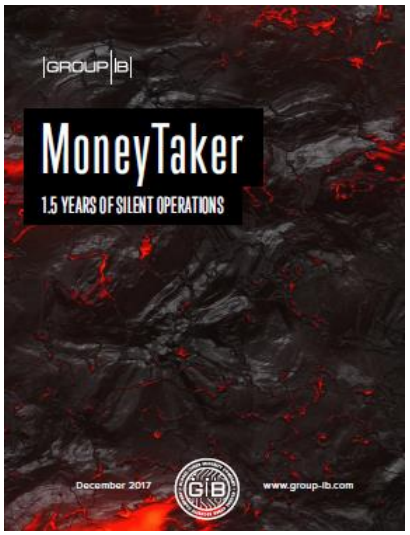
2

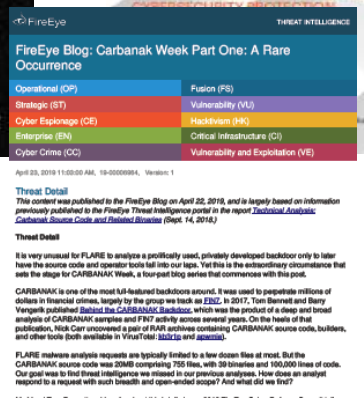


: Carbanak = Cobalt Gang

Fuente: Fireeye



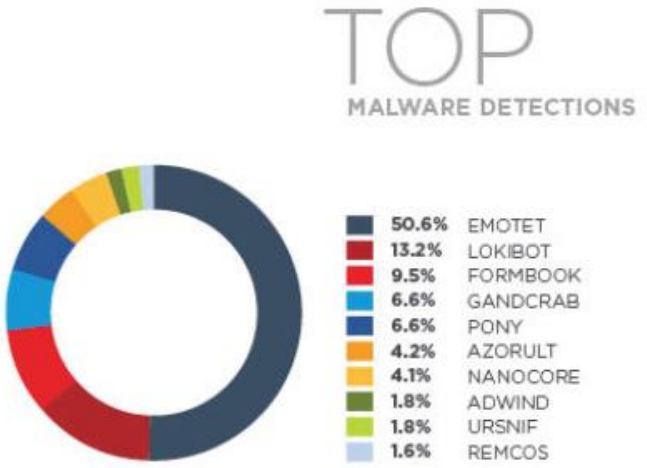




CCN
centro criptológico nacional

Tipos de Ataque al Sector Financiero

Ataques a móviles / Robo credenciales banca on-line
Ataques a puntos de venta
Ataques a sistemas de gestión tarjetas
Ataque a servicios web
Ransomware (Extorsión)
Minería de criptomonedas
Ataques a SWIFT
DDoS (Extorsión)
….



FIREEYE

1Q 2019

Ataques dirigidos a operativa del banco

TTP,s más comunes:

- Spear phishing (uso OSINT)
- Rapidez en descubrir la operativa
- Escalado de privilegios
- Borrado de memoria / logs
- Uso de malware fileless
- Persistencia muy ofuscada

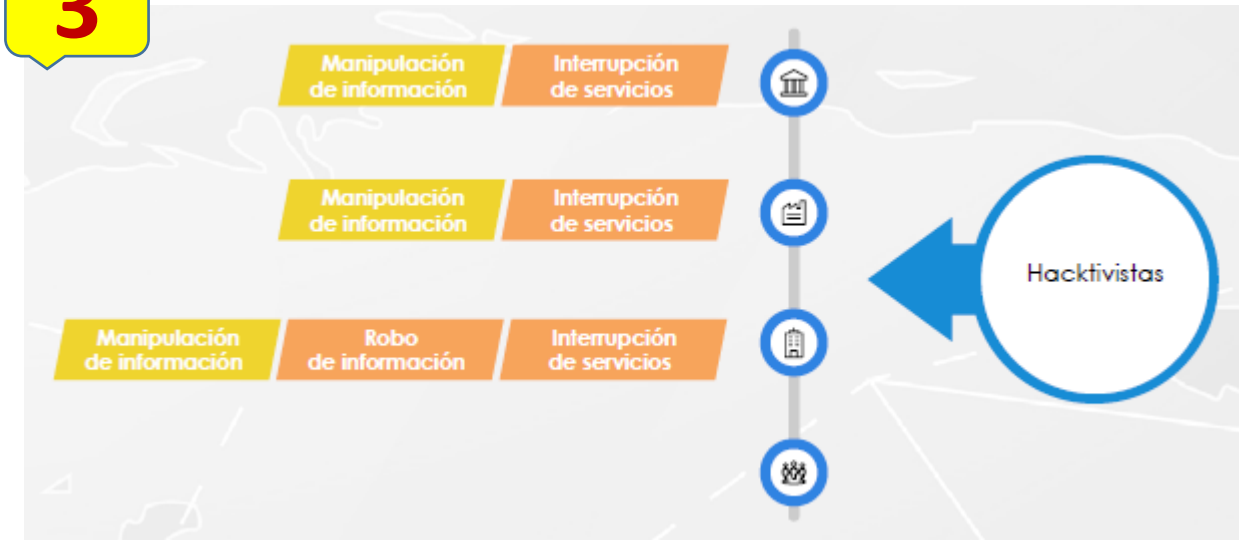
CCN
centro criptológico nacional

Grupos de Ataque al Sector Financiero (2019)

1. **SILENCE GROUP** (01.2019 correos dirigidos bancos Europa del Este)
2. **LAZARUS (BLUENOROF)** (2018 Banco de Chile). Ataque SWIFT
3. **FIN 5 (rawPOS).** Accesos ilegítimos con credenciales válidas
4. **FIN 6 (Skeleton Spider).** Ataque puntos de venta y Ransomware (lockergoga)
5. **COBALT GANG (CARBANAK – FIN 7**). Ataque SWIFT
6. **MONEYTAKER** (Ataque a bancos de RU, US y UK)
7. **RETEFE GROUP** (Ataque a clientes ON LINE de bancos SW y GE)

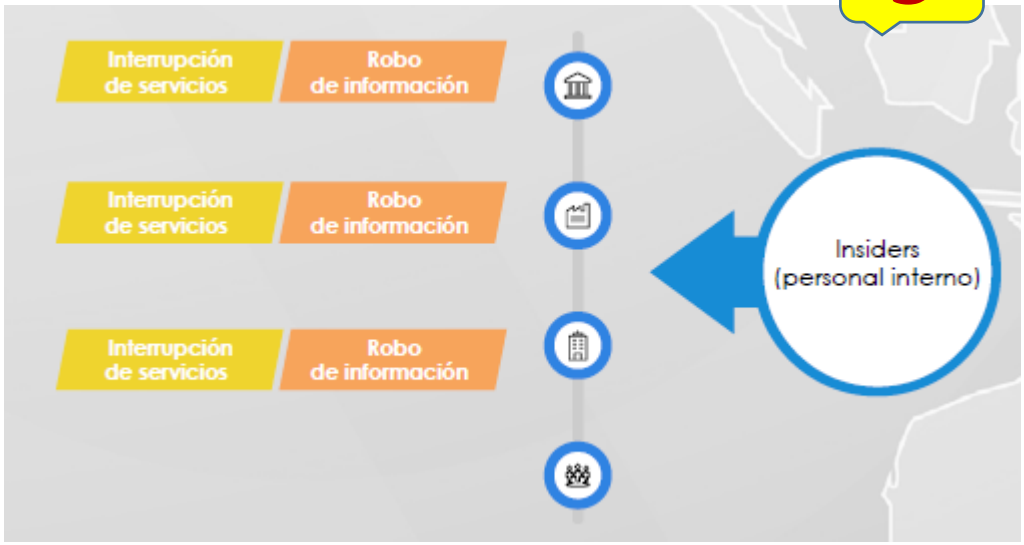
8. RIM SPIDER (ransomware)
9. INDRIK SPIDER (ransomware)
10. NARWHAL SPIDER (infección equipos)
11. PICHY SPIDER
12. WIZARD SPIDER (trickbot)

3



4

5



CCN
centro criptológico nacional

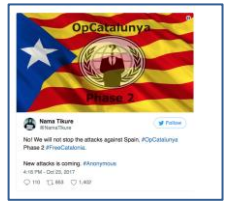
EJEMPLOS 2017

Demostración fuerza

Wannacry 2.0 (mayo 2017)

OwnCloud (febrero 2017)

LexNet (julio 2017)



Struts (marzo 2017)

Saguaro (enero 2017)

Sabotaje

notPetya (junio 2017)

#OpCatalunya (oct. 2017)

Desinformación

2017

Emissary Panda (febrero 2017)

APT28 (julio 2017)

Emissary Panda (julio 2017)

Hidden Cobra (nov. 2017)

APT10 (abril 2017)

Snake (julio 2017)

Grizzly Steppe (enero 2017)

Espionaje

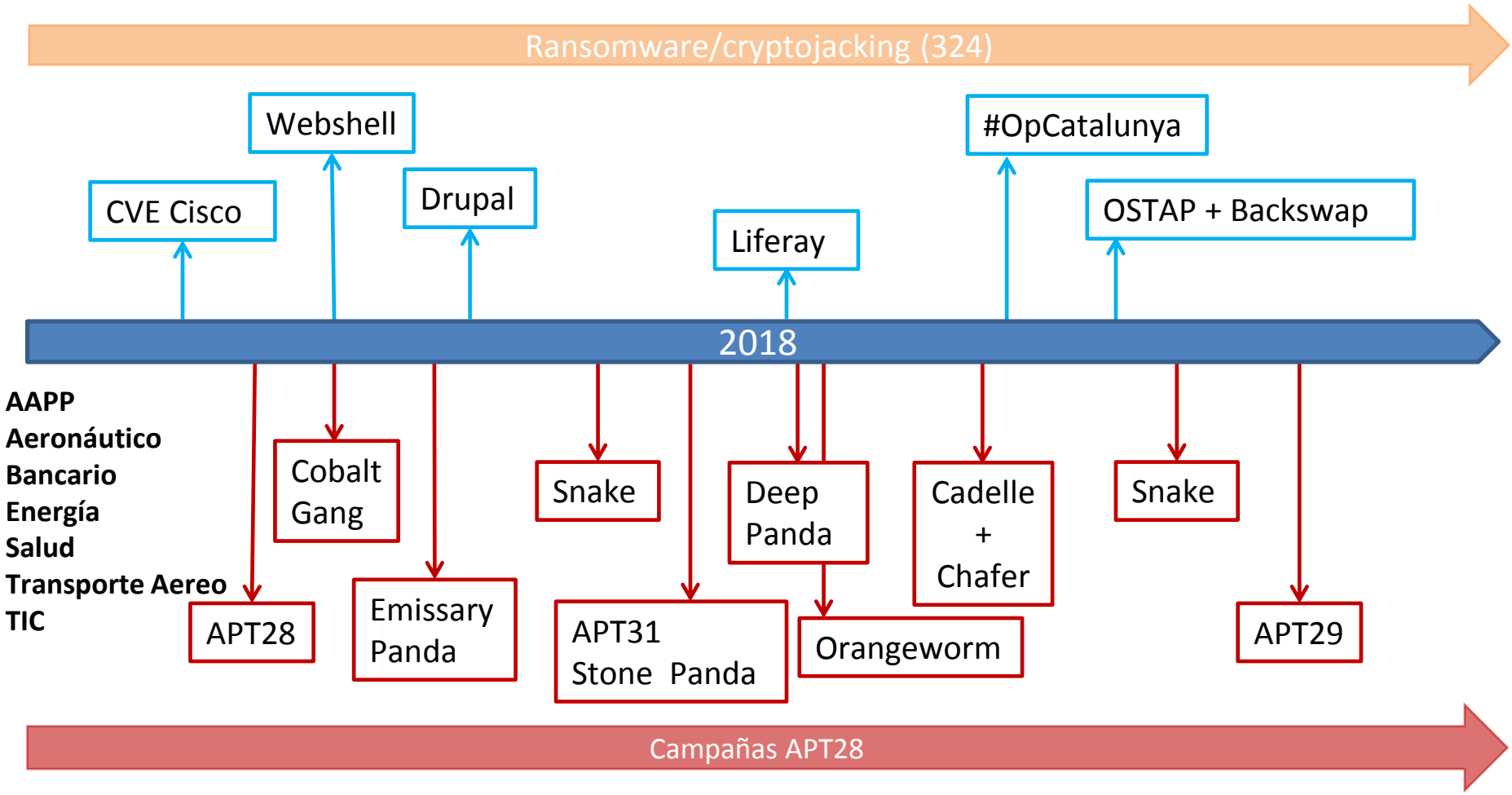
Snake (sep. 2017)

Desinformación Elecciones USA

RESUMEN 2017

CCN centro criptológico nacional

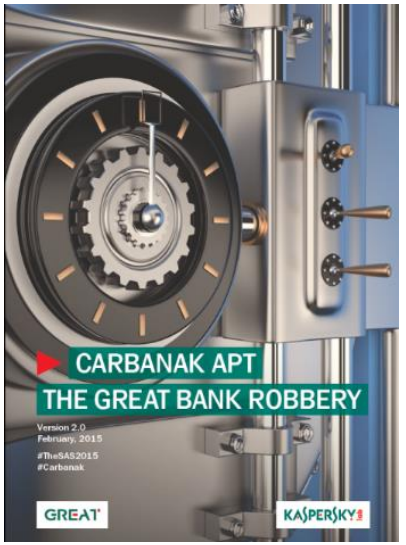
EJEMPLOS 2018



RESUMEN 2018

Cobalt Gang

- **Antecedentes**
  - Grupo conocido desde 2014[1].
  - Ataque “à la APT” **pero** el objetivo es el dinero.
    - 2014: ~20M€
    - 2015-2016: >25M€
    - 2017: ~20M€ (sólo en bancos rusos)
    - 2018?
  - Cambio a Cobalt Strike en 2015[2].
  - Robo a través de cajeros, red SWIFT y modificación de cuentas bancarias.



[1] Kaspersky Labs – “Carbanak APT, the great bank robbery”
[2] https://www.cobaltstrike.com

ALERTAS

Detectada una campaña del Grupo Cobalt Gang contra el sector bancario

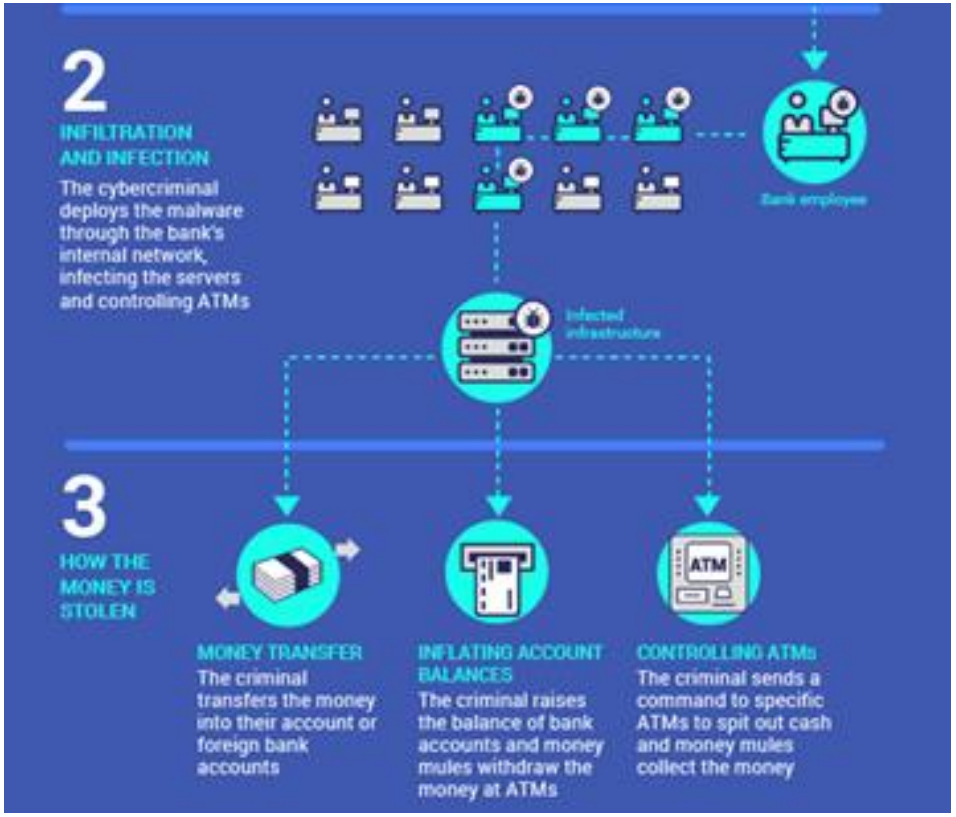
Publicado el: **23/03/2018**

Nivel de criticidad: **Crítico**

El Equipo de Respuesta a incidentes del Centro Criptológico Nacional, CCN-CERT, alerta sobre la existencia de una campaña muy agresiva contra el sector bancario, por parte del grupo Cobalt Gang. Este grupo, relacionado con el cibercrimen, inició su actividad en el año 2016 y, desde entonces, ha realizado numerosas campañas en las que ha sustraído importantes cantidades de dinero a las entidades afectadas.

El grupo utiliza, entre otras herramientas, la denominada Cobalt Strike y su primera incursión suele realizarse a través de las técnicas de *Spear-phising* y explotando las vulnerabilidades del sistema.

- **Modus operandi & malware:**
  - Obtención de credenciales de usuarios privilegiados, creación de nuevos.
  - Reconocimiento de red → servidores de interés.
  - Cobalt Strike Beacon en modo SMB/*named pipe* **(14.03.2018)**.
  - Uso y abuso de Powershell: como servicio o ejecutado via CSB.
  - Despliegue por etapas, con ofuscación:
    - 1ª etapa: servicio Powershell + script ofuscado
    - 2ª etapa decodifica y descomprime (Gzip) otro script PS
    - 3ª etapa: script (OSINT) que inyecta *shellcode* (espacio de memoria proceso legítimo) → modo *named pipe* (interno) o modo HTTP (hacia los C2)



CCN
centro criptológico nacional

TENDENCIAS 2019

Herramientas cada vez más adaptadas a la víctima aprovechando la superficie de exposición que ofrecen las tecnologías, especialmente **dispositivos móviles**, **IoT** y **entornos cloud explotando la confianza que tiene el usuario** en las mismas a través de las vulnerabilidades del **firmware** y ataques a la **cadena de suministro**.

- **Ciberespionaje**: incremento actividad ataques patrocinados por estados.
  - Demostración de fuerza en el entorno internacional.
  - Socavar la confianza y minar la estabilidad de los sistemas políticos y sociales.
  - Guerra híbrida. DESINFORMACIÓN
  - **Ataques a la cadena de suministro**
  - **Sofisticación del código.** Umbral de detección muy bajo. Ofuscación.
- **Cibercrimen**: incremento en la actividad y selectividad sobre objetivos más rentables.
  - Ransomware como instrumento de financiación pero no la principal amenaza,
  - Miners como beneficio económico más estable y directo frente ransomware.
  - **Ataques complejos al sector financiero.**
  - Venta de servicios a terceros (botnets IoT, vulnerabilidades 0-day, malware fileless, …).
- **Hacktivismo**: continuarán sacando provecho de la inestabilidad social mediante ataques de denegación de servicio y desfiguraciones de sitios web.
- **Ciberyihadismo**: en principio, limitado a la propaganda y presencia de identidades en redes sociales, así como ataques no complejos contra objetivos de bajo perfil.

- **La Nube como objetivo.** Migración de grandes empresas
- **Técnicas fileless**: tendencia claramente al alza.
  - Empleo de herramientas propias del sistema atacado.
  - Hacer propias herramientas publicadas en internet.
- **Ataques IoT**: Antes …. **botnet Mirai** (cámaras IP, routers, televisores, domótica, etc.). Ahora: ataques más complejos y dirigidos.
  - 1. Causar daños al usuario (manipulación, robo daros, acceso a redes personales)
  - 2. Como medio para atacar otros objetivos (Alquiler de botnets (DDoS o desplegar ransomware/miners).
- **Incremento del cryptojacking**:
  - Presencia destacada de criptomonedas alternativas.
  - Acciones de fraude, encubiertas por sistemas de adquisición de tokens . Escasa o nula regulación en materia de ICOs (Initial Coin Offering).
- **Esquema blockchain:**
  - Empezará a generalizarse su implantación en el sector financiero.
  - Procesos de votación (elecciones) ????
- **Ataques a personas.** Eslabón más débil.

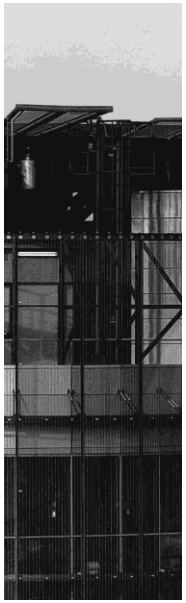
- **Adopción del 5G** (¿?)
- **Aprendizaje automático**. Para detectar malware
- **Incremento actividad legislativa** (modelo GDPR)

DECALOGO

1. **Aumentar la capacidad de Vigilancia.**
2. **Herramientas de Gestión Centralizada.**
3. Política de seguridad.
4. Aplicar configuraciones de seguridad y **actualización.**
5. Empleo de productos confiables y certificados.
6. Concienciación de usuarios.
7. Compromiso de dirección (Aceptación Riesgo)
8. Legislación y Buenas Prácticas.
9. **Intercambio de Información.**
10. **Trabajar como si se estuviera comprometido**.

CCN
centro criptológico nacional

Muchas Gracias



E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

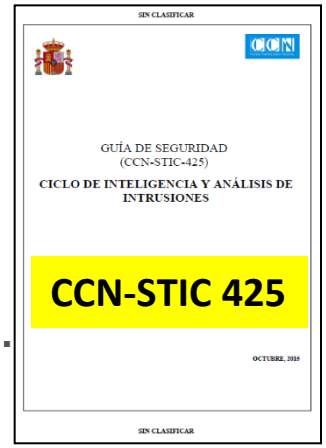
oc.ccn.cni.es

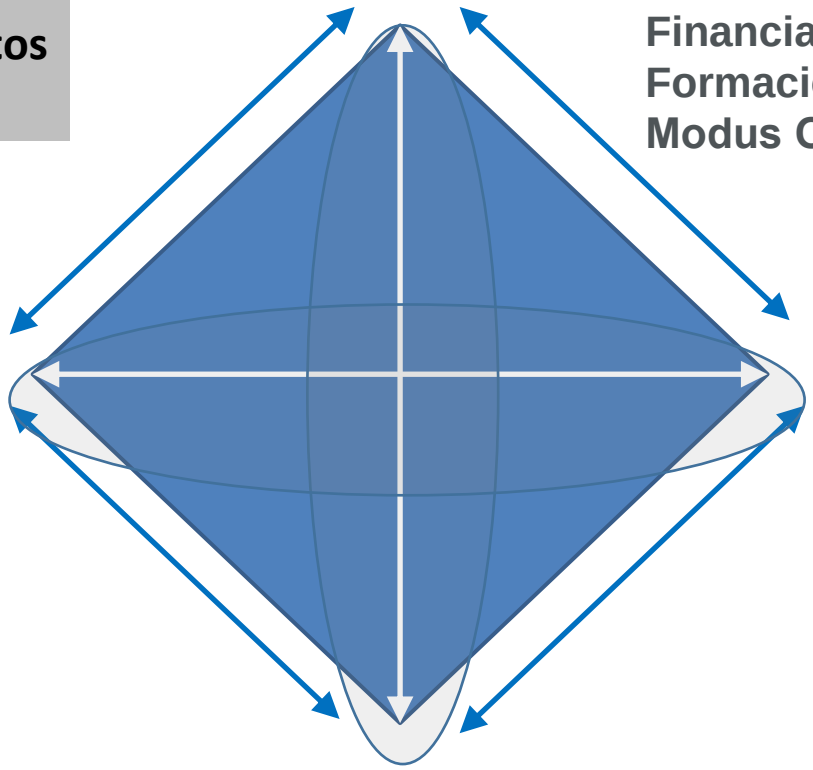
Modelo Diamante. Taxonomía de un ataque

Estudio de Tácticas / Técnicas / Procedimientos (TTP)

Atacantes

Actores
Motivación
Financiación
Formación
Modus Operandi….





Infraestructuras

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

Capacidades

Exploits propios
Vectores infección
Cifrado / RAT
Persistencia….

Víctimas

Sectores afectados
Métodos detección…

The Diamond Model of Intrusion Analysis
www.activeresponse.org

CIBERSEGURIDAD

La habilidad de proteger y defender las redes o sistemas de los **ciberataques.** Estos según su motivación pueden ser:

CIBERESPIONAJE

Ciberataques realizados para obtener secretos de estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal.

CIBERDELITO / CIBERCRIMEN

Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito.

CIBERACTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social.

CIBERTERRORISMO

Actividades dirigidas a causar pánico o catástrofes realizadas en las redes y sistemas o utilizando éstas como medio.

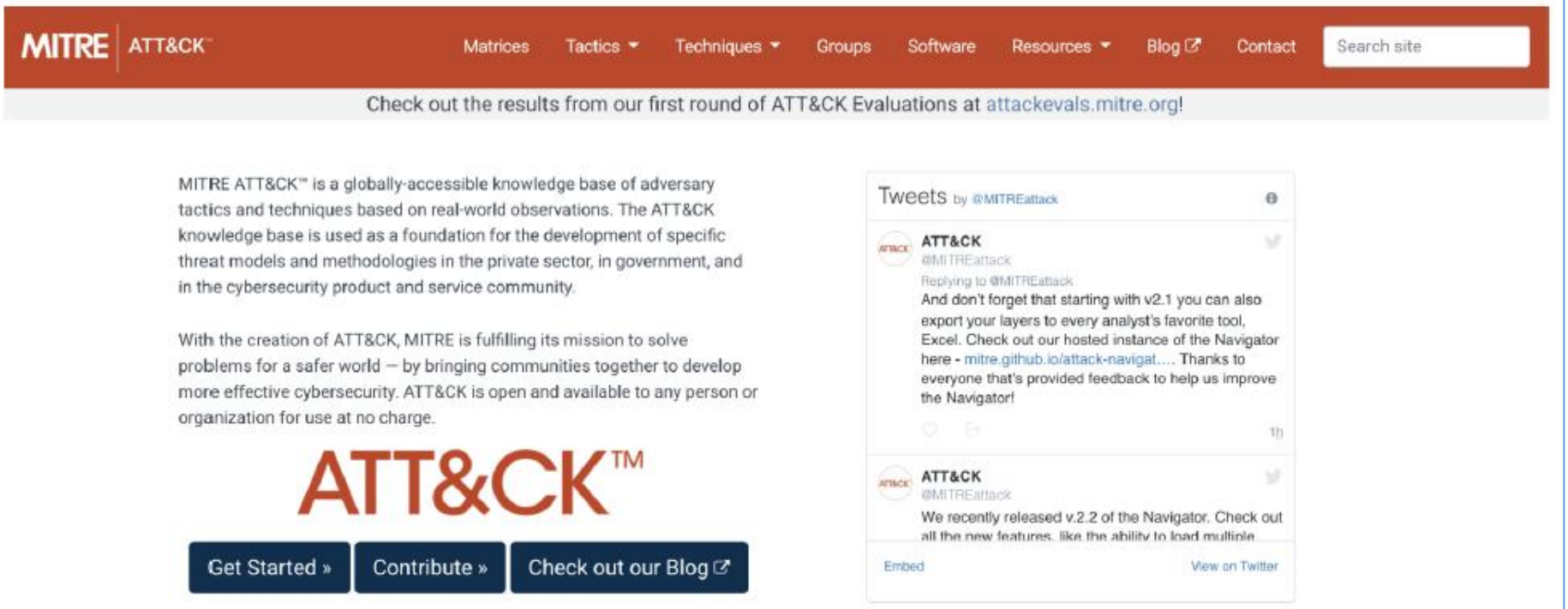
CIBERCONFLICTO / CIBERGUERRA / GUERRA HÍBRIDA

Operación dirigida por un Estado que utiliza tácticas abiertas y encubiertas con el objetivo de desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como **diplomacia** y acciones de **inteligencia tradicional**, **actos subversivos** y de sabotaje, **influencia política y económica**, instrumentalización del **crimen organizado**, **operaciones psicológicas**, **propaganda** y **desinformación** y **ciberataques**

CIBERATAQUE

Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.

MITRE ATT&CK


MITRE ATT&CK
Matrices
Tactics
Techniques
Groups
Software
Resources
Blog
Contact
Search site
Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!
MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
ATT&CK™
Get Started »
Contribute »
Check out our Blog
Tweets by @MITREattack
ATT&CK
@MITREattack
Replying to @MITREattack
And don't forget that starting with v2.1 you can also export your layers to every analyst's favorite tool, Excel. Check out our hosted instance of the Navigator here - mitre.github.io/attack-navigat.... Thanks to everyone that's provided feedback to help us improve the Navigator!
1h
ATT&CK
@MITREattack
We recently released v.2.2 of the Navigator. Check out
Embed
View on Twitter

Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2018-10-17T00:14:20.652Z

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

Example: Comparing Groups APT 28 vs. Deep Panda

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery			Data from Network Shared Drive		
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	Graphical User Interface		Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	InstallUtil	Data from Removable Media		
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	MSBuild			Data Encoding
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Process Hollowing	Input Capture		Fallback Channels
Authentication Package	Exploitation of Vulnerability				Remote Services	Regsvcs/Regasm	Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Regsvr32	Video Capture		Multiband Communication
Component Object Model Hijacking	DLL Injection	Component Object Model Hijacking		Process Discovery	Shared Webroot	Rundll32		Scheduled Transfer	Multilayer Encryption
Basic Input/Output System		Indicator Removal from Tools		Query Registry	Taint Shared Content	Scheduled Task			Remote File Copy
Change Default File Association		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	Scripting			Standard Application Layer Protocol
Component Firmware		Install Root Certificate		Security Software Discovery		Service Execution			Standard Cryptographic Protocol
External Remote Services		InstallUtil		System Information Discovery		Windows Management Instrumentation			Standard Non-Application Layer Protocol
Hypervisor		Masquerading		System Owner/User Discovery					Uncommonly Used Port
Logon Scripts		Modify Registry		System Service Discovery					Web Service
Modify Existing Service		MSBuild		System Time Discovery					
Netsh Helper DLL		Network Share Removal							
Redundant Access		NTFS Extended Attributes							
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
		Regsvr32							
Winlogon Helper DLL		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Legend

APT 28

Deep Panda