XVI JORNADAS STIC CCN-CERT

IV JORNADAS DE CIBER_DEFENSA: ESPDEF-CERT

TERROR EN EL CIBER MERCADO

(SCAMs en el Ultramarinos)

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN **CIBERESCUDO ÚNICO** PARA **ESPAÑA**


TERROR EN EL
CIBER MERCADO
(SCAMs en el Ultramarinos)

Cuando lo pides por Internet

¡Quiero la peli de StarWars!

Cuando te llega a casa

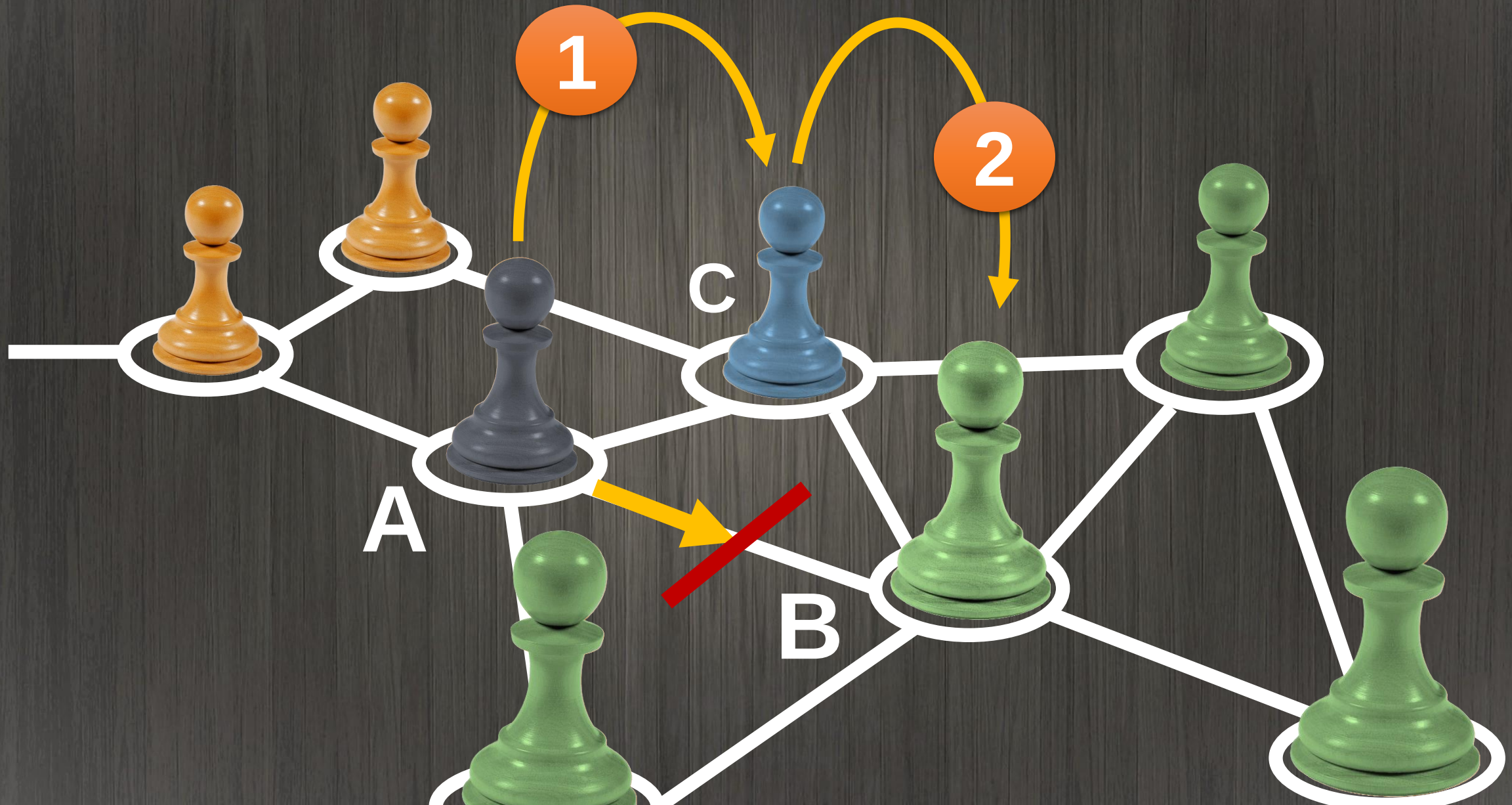
¡Quiero la peli de StarWars! 🤪

Hardware Wars (Ernie Fosselius1978) - Parodia

Ataques a la cadena de suministro.

- Un ataque a la cadena de suministro supone una violación y/o compromiso de los bienes, servicios o tecnología, que un proveedor suministra a un cliente, introduciendo y trasladando un riesgo para esos clientes.

La Propiedad Transitiva



Gartner

Top Trends in Cybersecurity, 2022

2025

↓

45%

13ABR2022

ENISA THREAT LANDSCAPE 2022

ENISA REPORT

1. Ransomware
2. Malware
3. Amenazas de ingeniería social
4. Amenazas contra los datos
5. Amenazas contra la disponibilidad
6. Desinformación
7. **Ataques a la cadena de suministro**

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

03NOV2022

TOP 10 emerging cybersecurity threats for 2030

enisa
European Network and Information Security Agency

Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! — ENISA (europa.eu)

11NOV2022

El problema

preocupación especial
sistemas OT

- Diseño no orientado a ciberseguridad
- Contraseñas predeterminadas
- Firmware /BIOS/ UEFI*… obsoletos
- Cifrado débil (o ausente)
- Acceso local desprotegido
- …

- APTs especializadas: DragonFly

(*) UEFI: Unified Extensible Firmware Interface

El peligro

Video Credit: Annie’s Eden

Está pasando

19/08/2022 - Ista

60M lectores

22/08/2022 - General Bytes

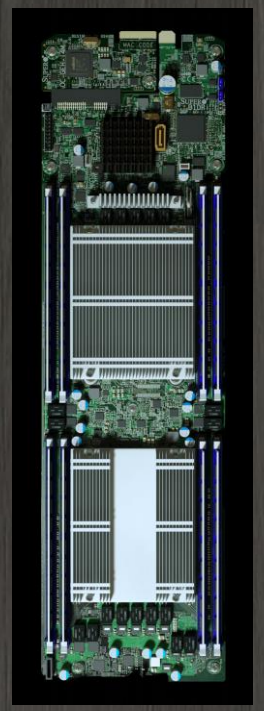
8.000 cajeros

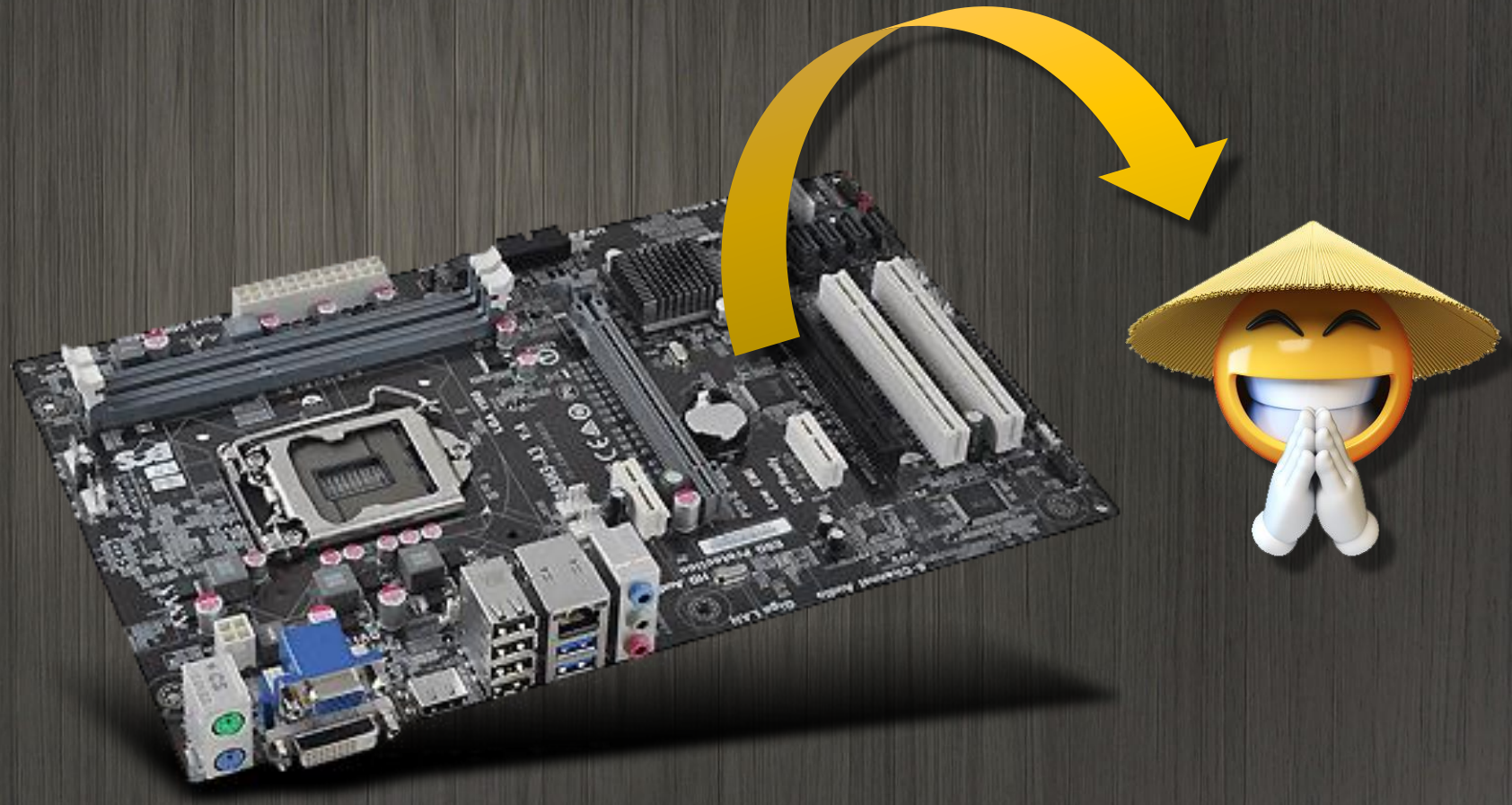
06/05/2021

18 estados

También afecta al Hardware

OCT-2018: China introdujo un chip para espiar 30 empresas americanas como Apple y Amazon





Bloomberg revela nueva evidencia sobre el hackeo a los servidores de Supermicro - Masterhacks Blog

Software Supply Chain Attacks

entonces ...

¿Open Source?

URL indexadas	Depósito
40,851,486	github.com
27,415,236	stackoverflow.com
26,861,477	npmjs.org
19,150,201	maven.org

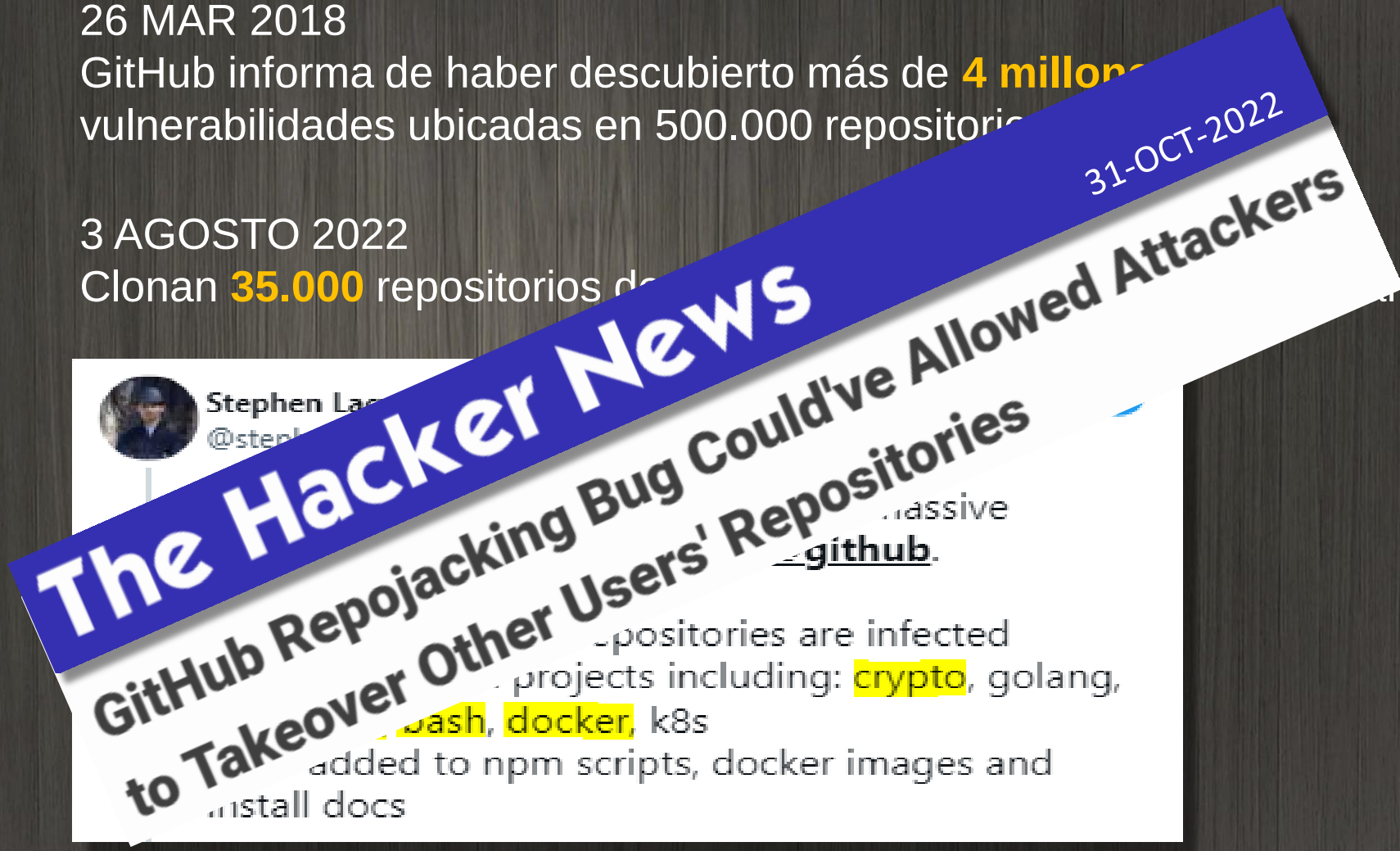
Copy & paste

3,512,317	nuget.org
3,368,946	debian.org
2,086,058	sourceforge.net
1,788,102	googlesource.com
1,551,408	bitbucket.org
1,433,665	gnome.org
734,254	gitee.com

Ataques a repositorios

26 MAR 2018
GitHub informa de haber descubierto más de **4 millon**
vulnerabilidades ubicadas en 500.000 repositori

3 AGOSTO 2022
Clonan **35.000** repositorios d re



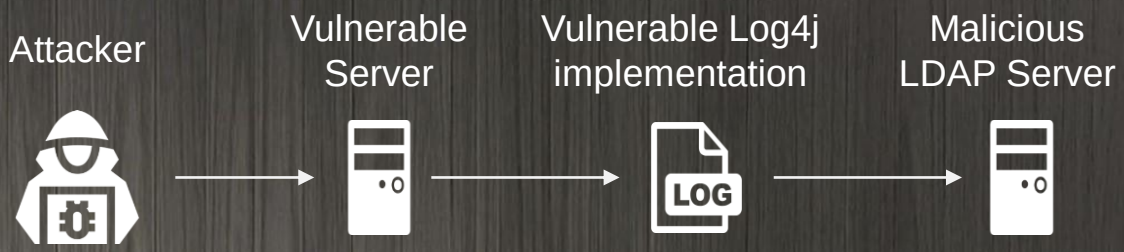
hxxp://ovz1.j19544519.pr46m.vps.myjino[.]ru.

LOG4J

9 DICIEMBRE 2021

CVSS: 10/10

Log4j JNDI Attack



CISCO

SAMSUNG

MINECRAFT

...

Ralph Goers

https://www.incibe-cert.es/blog/log4shell-analisis-vulnerabilidades-log4j

12 de diciembre de 2020

- NetFlow Traffic Analyzer
- User Device Tracker
- Network Topology Mapper
- Kiwi CatTools
- Kiwi Syslog Server
- **ORION** ← Network Management

APT29

solarwinds

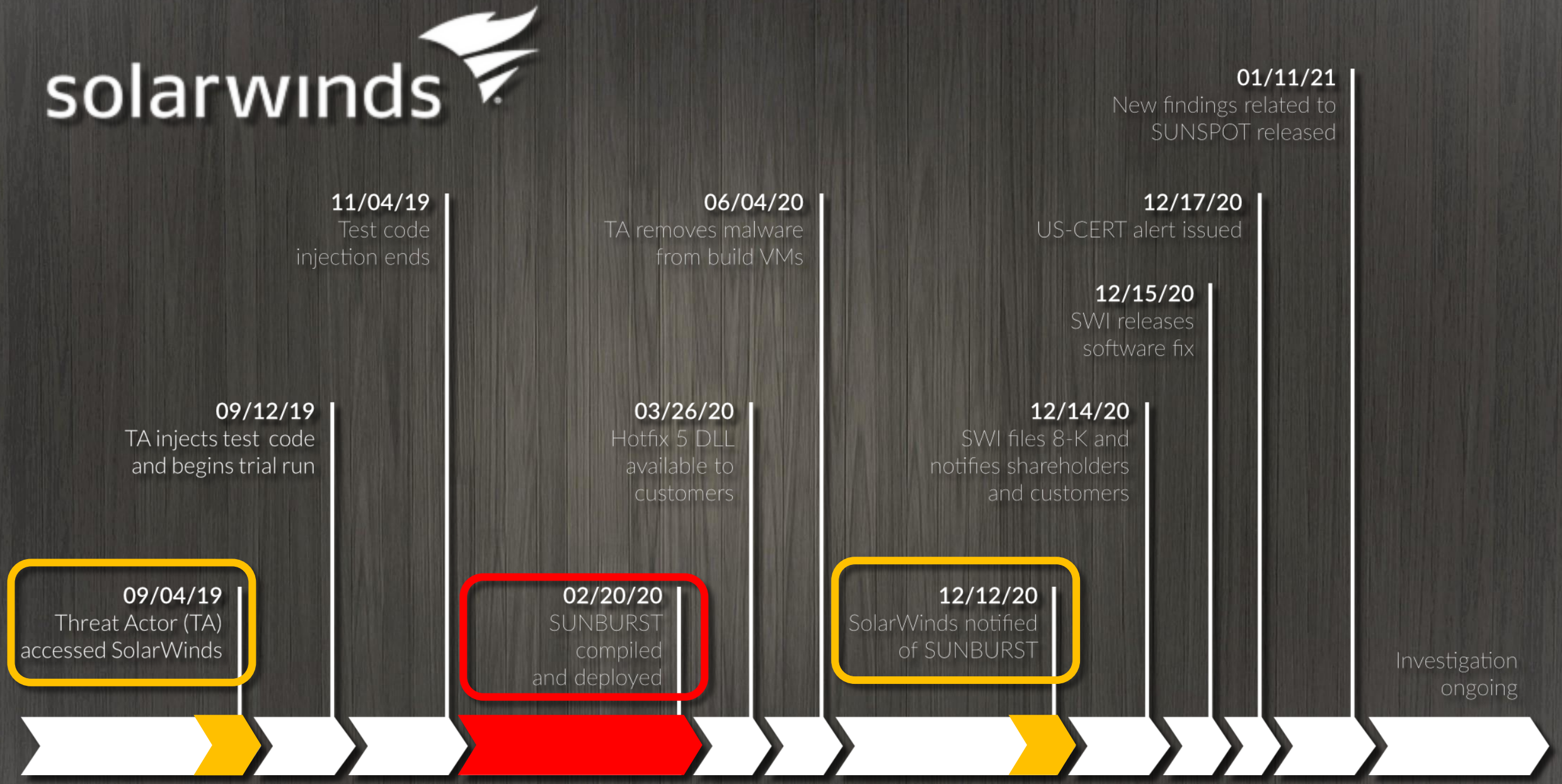
Vulnerabilidad: Solorigate (**Sunburst**)

Nobelium - APT29

18,000 / 33.000 organizaciones (**F500**)
7 países:

FireEye

Microsoft


solarwinds
09/04/19
Threat Actor (TA) accessed SolarWinds
09/12/19
TA injects test code and begins trial run
11/04/19
Test code injection ends
02/20/20
SUNBURST compiled and deployed
03/26/20
Hotfix 5 DLL available to customers
06/04/20
TA removes malware from build VMs
12/12/20
SolarWinds notified of SUNBURST
12/14/20
SWI files 8-K and notifies shareholders and customers
12/15/20
SWI releases software fix
12/17/20
US-CERT alert issued
01/11/21
New findings related to SUNSPOT released
Investigation ongoing

solarwinds

- "Microsoft assigned 500 engineers to investigate the attack“.
- "When we analyzed everything that we saw at Microsoft, we asked ourselves how many engineers have probably worked on these attacks. And the answer we came to was, well, certainly more than 1.000“.

Brad Smith - Microsoft president

https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

CYBER KILL CHAIN | método

Behind the scenes

ICS - DragonFly, Energetic Bear → FSB

SolarWinds – Nobelium, Cozy Bear, APT29 → SVR

NotPetya - SandWorm, BlackEnergy, Voodoo Bear → GRU

Log4J - Aquatic Panda, APT-35

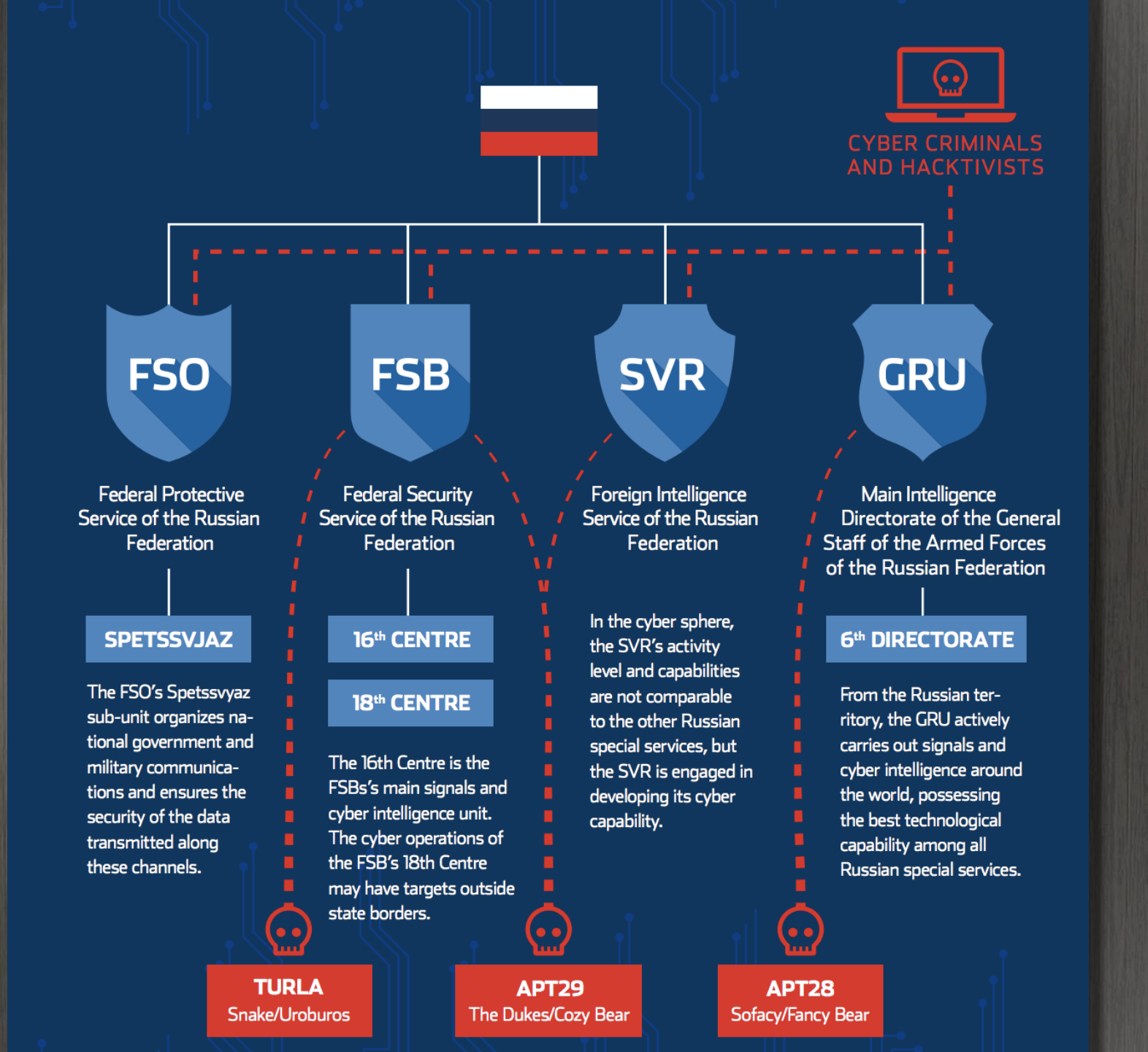
Ccleaner - Axiom, Deputy Dog, APT 17

Sermicro - ???

Colonial Pipeline - DarkSide

Who´s who

- FSB: Federal Security Service
- SVR: Foreign Intelligence Service
- GRU: General Staff Main Intelligence Directorate



¿Cómo debemos actuar?

- Conocer nuestros activos y entorno (y sus vulnerabilidades).
- Proteger los datos y ser resilientes.
- Detectar actividad anómala y Responder rápidamente.

- Necesitamos **MÉTODO**
- Necesitamos **TECNOLOGÍAS**
- Necesitamos **PROCEDIMIENTOS**

Atentos a lo que compramos...

Y si lo descargamos ...

- ¿Ejecuta algún Script al instalar?
- ¿Conecta con la red?
- ¿Conecta con Internet? Qué dominio?
- ¿Lee variables de entorno? Cuales?
- ¿Hay código ofuscado?
- ¿Recolecta datos de telemetría?

.. Y atentos a lo que vendemos



ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

- WHAT IS A SUPPLY CHAIN ATTACK?
  - **TAXONOMY** OF SUPPLY CHAIN ATTACKS
  - ATTACK TECHNIQUES USED TO COMPROMISE
  - …
- THE LIFECYCLE OF A SUPPLY CHAIN ATTACK
- ANALYSIS OF SUPPLY CHAIN INCIDENTS → **24 examples**
- RECOMMENDATIONS
- CONCLUSIONS

July 2021

Taxonomía

proveedor

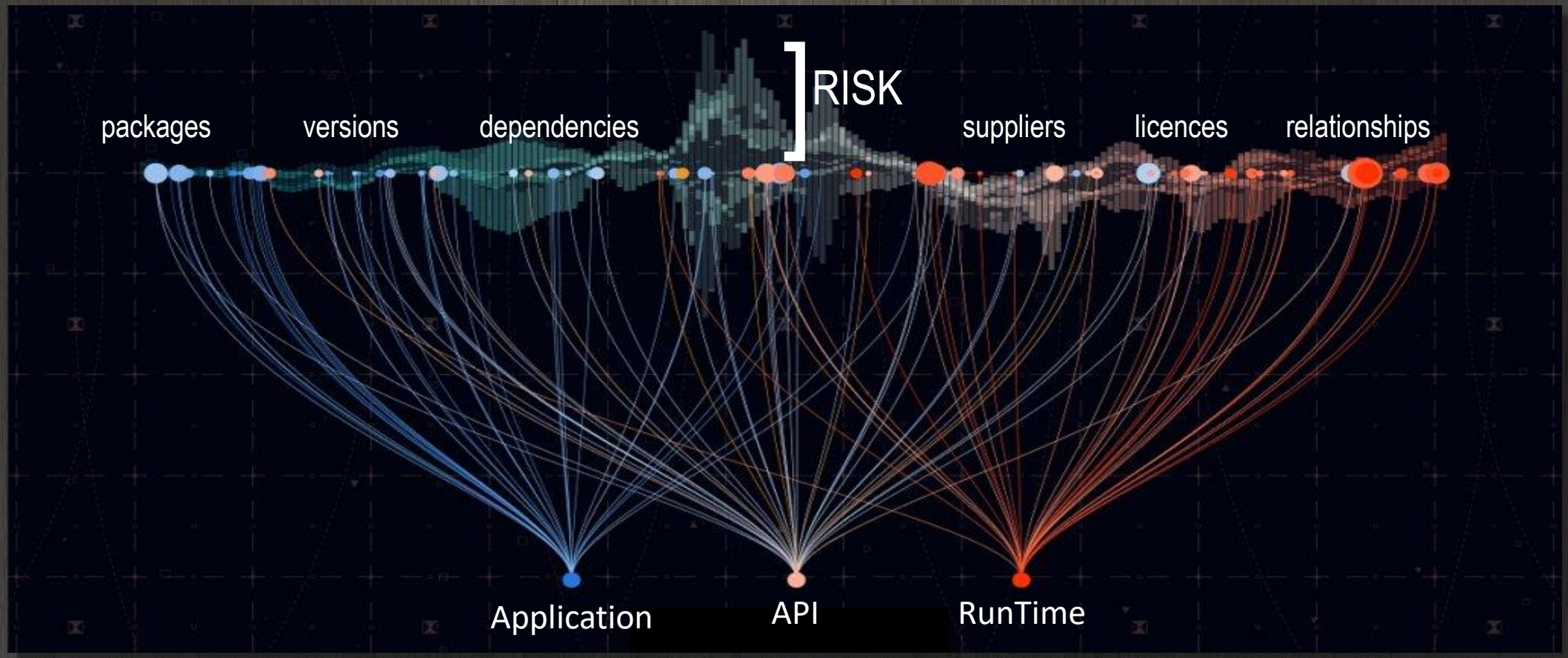
Técnicas de ataque para comprometer la Cadena de suministro	Activos del proveedor que son objetivo
▪ Infección de malware ▪ Ingeniería social ▪ Ataque de fuerza bruta ▪ Software de explotación Vulnerabilidad ▪ Configuración de explotación Vulnerabilidad ▪ Fuente abierta Inteligencia (OSINT)	▪ Software preexistente ▪ Bibliotecas de software ▪ Código ▪ Configuraciones ▪ Datos ▪ Hardware ▪ Componentes ▪ Gente ▪ Proveedor

cliente

Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente que son objetivo
▪ Relación de confianza [T1199] ▪ Drive-by compromise [T1189] ▪ Suplantación de identidad – Phishing [T1566] ▪ Infección de malware ▪ Ataque físico o Modificación ▪ Falsificación	▪ Datos ▪ Información Personal ▪ Propiedad intelectual ▪ Software ▪ Procesos ▪ Banda Ancha ▪ Financiero ▪ Gente

SBOM: Software Bill Of Materials

El SBOM es un registro (inventario) que contiene el detalle y las relaciones jerárquicas de los componentes usados en el desarrollo de un software dado.

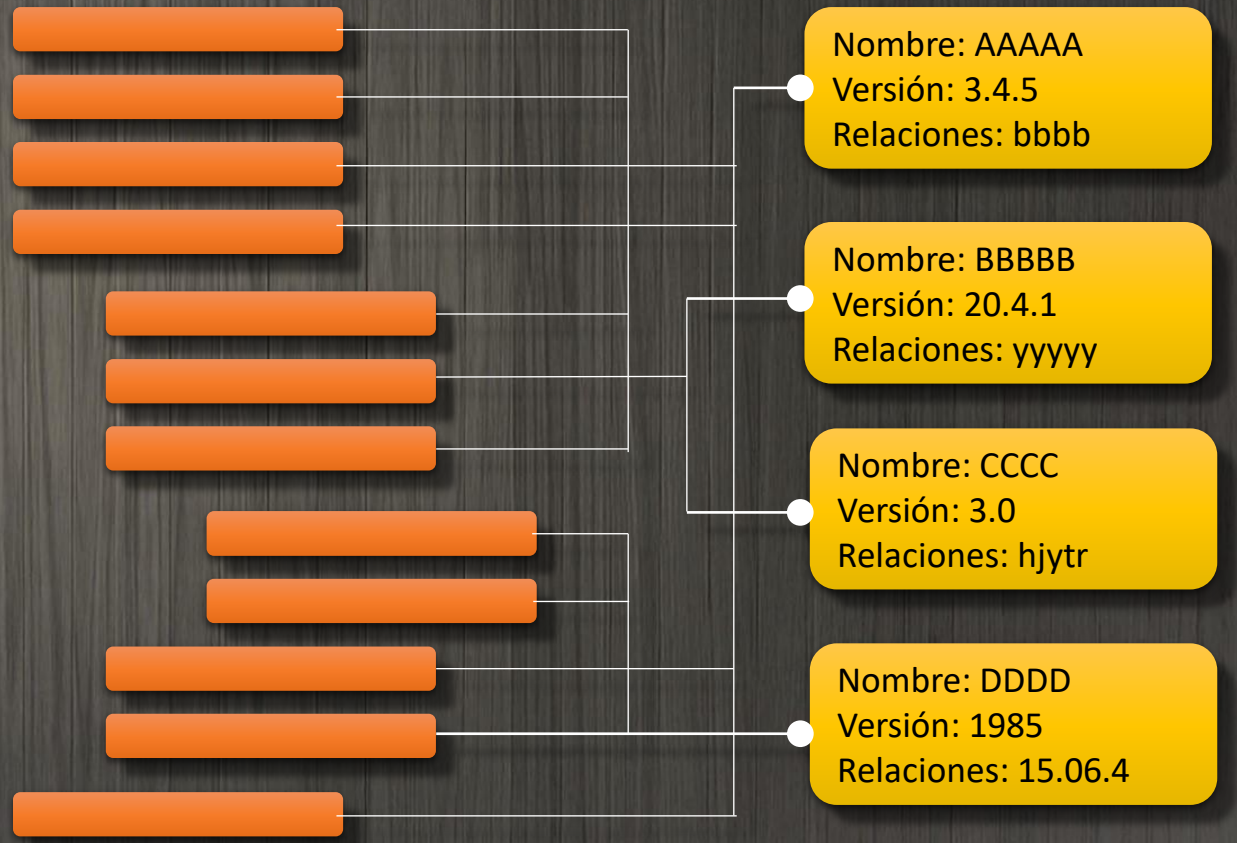


SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration (ntia.gov)

Registro de componente SBOM

Agencia Nacional de Telecomunicaciones e Información (NTIA)

- Autor de datos
- Nombre del componente
- Nombre del proveedor
- Versión
- **Hash del componente**
- Identificadores únicos
- Timestamp
- **Relaciones**



Software Composition Analysis **(SCA)**

El análisis de composición de software (SCA) es un proceso que detecta componentes de código abierto utilizados en el código base de una aplicación.

RESULTADOS:

- Lista de materiales (SBOM)
- Lista de Licencias
- Vulnerabilidades conocidas

MITRE ATT&CK™

ENTERPRISE

Supply Chain Compromise

- T1195.001 - Compromise Software Dependencies & Development Tools
- T1195.002 - Compromise Software Supply Chain
- T1195.003 - Compromise Hardware Supply Chain

ICS

Supply Chain Compromise

- T0862 - No sub-techniques

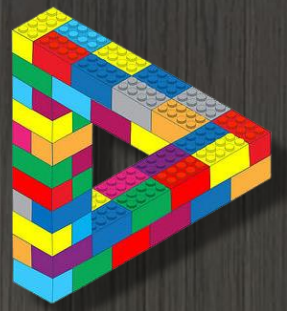
MOBILE

Supply Chain Compromise

- T1474 - No sub-techniques

Audit
Code Signing
SC-Management
Update Software
Vuln-Scan

Sistema de Confianza (SoT)

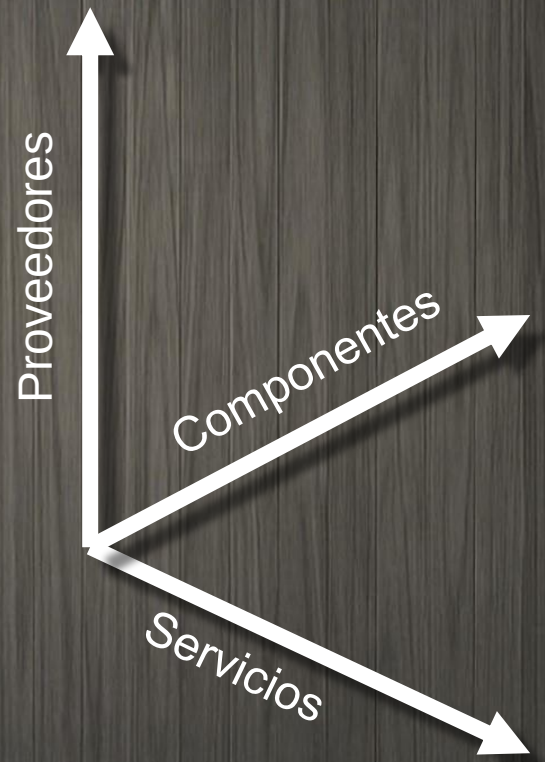


MITRE

RSA 2022 (7Jun)

Influencias externas
Estabilidad financiera
Reputación
Formalismo / Malicia
Cultura de Seguridad
Cultura de Calidad
Susceptibilidad

- Reputation
- Agreements
- Ownership
- Partners
- Leadership
- Personnel
- Training
- History
- Financial health
- Product Strategy
- Legal/Law Issues
- Facilities Security
- Cyber Security
- Software Assurance
- Hardware Assurance
- Market position



Higiene
Falsificación
Infección maliciosa

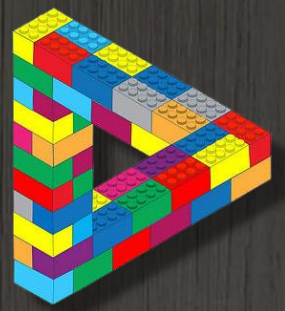
Seguridad
Fiabilidad
Calidad
Integridad

https://sot.mitre.org/

Sistema de Confianza (SoT)

MITRE

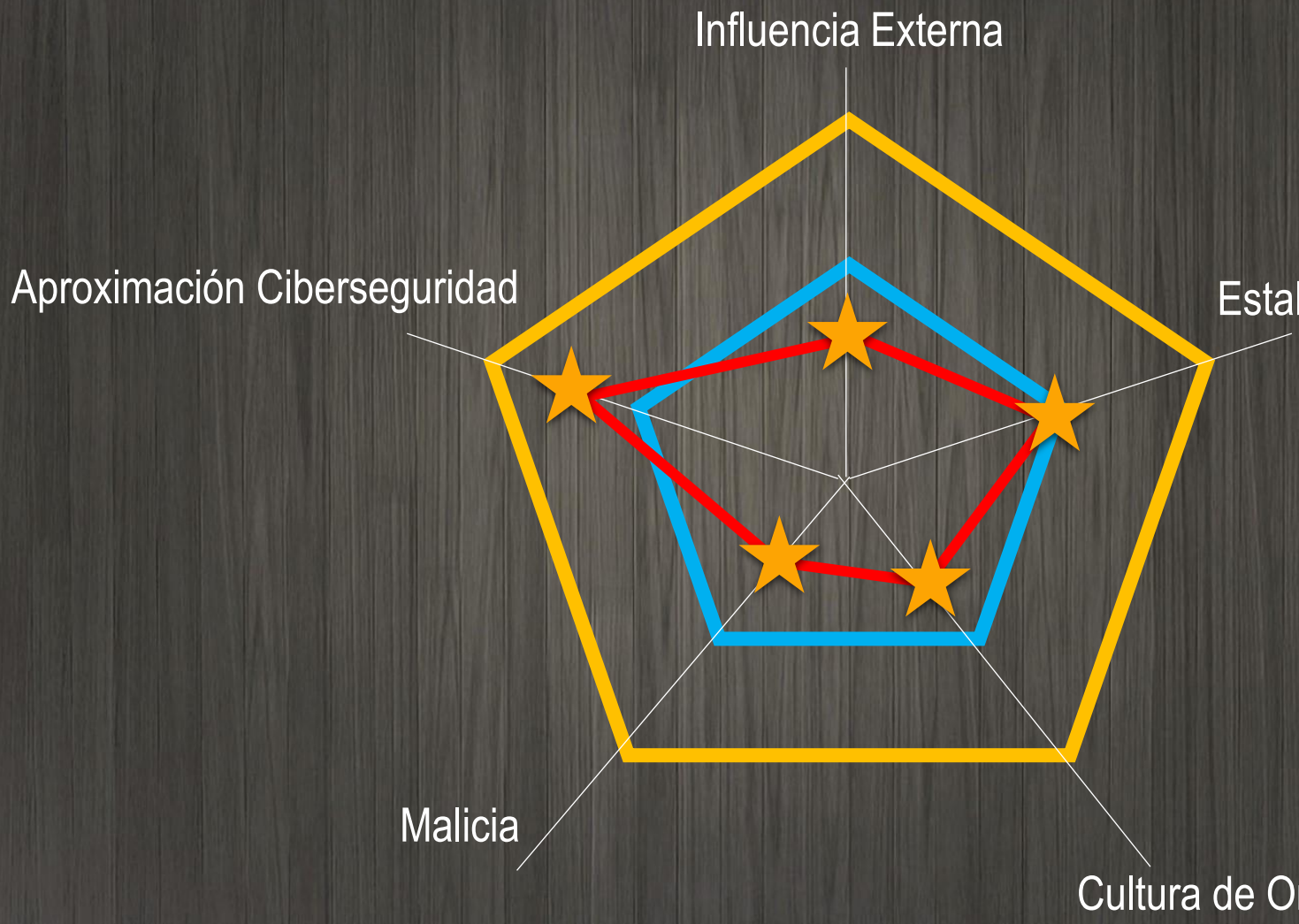
Supplier Risks							Supply Risks			Service Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service Delivered	Reliability of Service Delivered	Security of Service Delivered
Foreign relationships	Questionable debt management	Corporate ownership reputation	Customers	Company has a low CMMI rating	Foreign Intelligence Service (FIS) influence	Concerns regarding facility access	Product quality	Facilities integrity	Copycat manufacturing	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree
Operational location concerns	Questionable financial stewardship	Diversity and inclusion	Industry sector	Internal company QC, SCRM policy & practice	Fraud and corruption	Concerns regarding software access	Product resilience	Functional integrity	Mislabeling	Service Infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance
Foreign registration/ incorporation	Questionable future outlook	Geographic concentration	Location	Subcontractor supply chain health / risk	Legal/law issues	Concerns regarding hardware access	Product security	Geopolitical integrity	Packaging integrity	Service specific integrity	Service specific quality	Service specific reliability	Service specific security
Geopolitical instability	Questionable profitability	Mergers & acquisitions frequency	Personnel		Sanction list status	Cyber threat activity		Logistics / transportation integrity	Technical authenticity				
Key Management Personnel (KMP) and non-person entity relationships	Vulnerability of financial stability to foreign influence	Natural disasters	Technical susceptibility			Data security status		Maintenance integrity	Unsanctioned manufacturing				
National corruption	Vulnerability of financial stability to market factors	Operational volatility				Type/ level /frequency of security training		Manufacturing process integrity					
National governance	Vulnerability to takeover	Sustainability				Vulnerabilities		Packaging integrity					
Organization ownership and control								Reputational integrity					
Politically Exposed Persons (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													

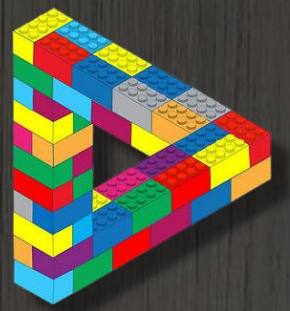


Taxonomía SoT

Perfil de empresa: 5 categorías de riesgo

MITRE





(no se muestran factores de riesgo)

CONCLUSIONES

- Entender los riesgos
- Define tus estándares y establece controles
- Evalúa el riesgo de tus proveedores
- Especifica buenos **REQUISITOS** (RQs) en tus pliegos

KEY NOTE 1

Comunicar los incidentes de forma transparente y colaborar unos con otros, es la única forma de proteger eficazmente nuestras ciber-infraestructuras de las amenazas existentes

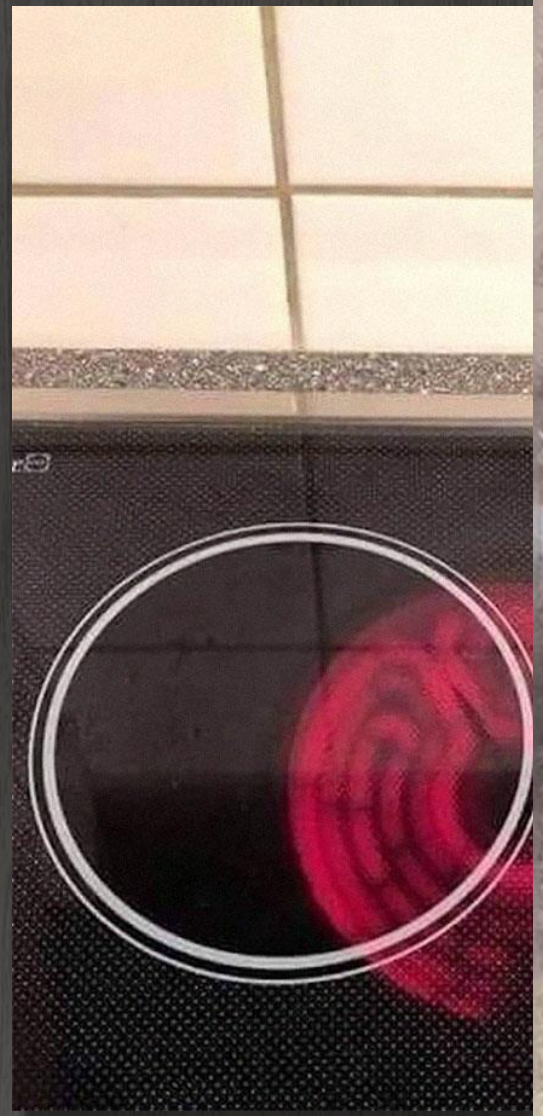
KEY NOTE 2

доверяй, но проверяй

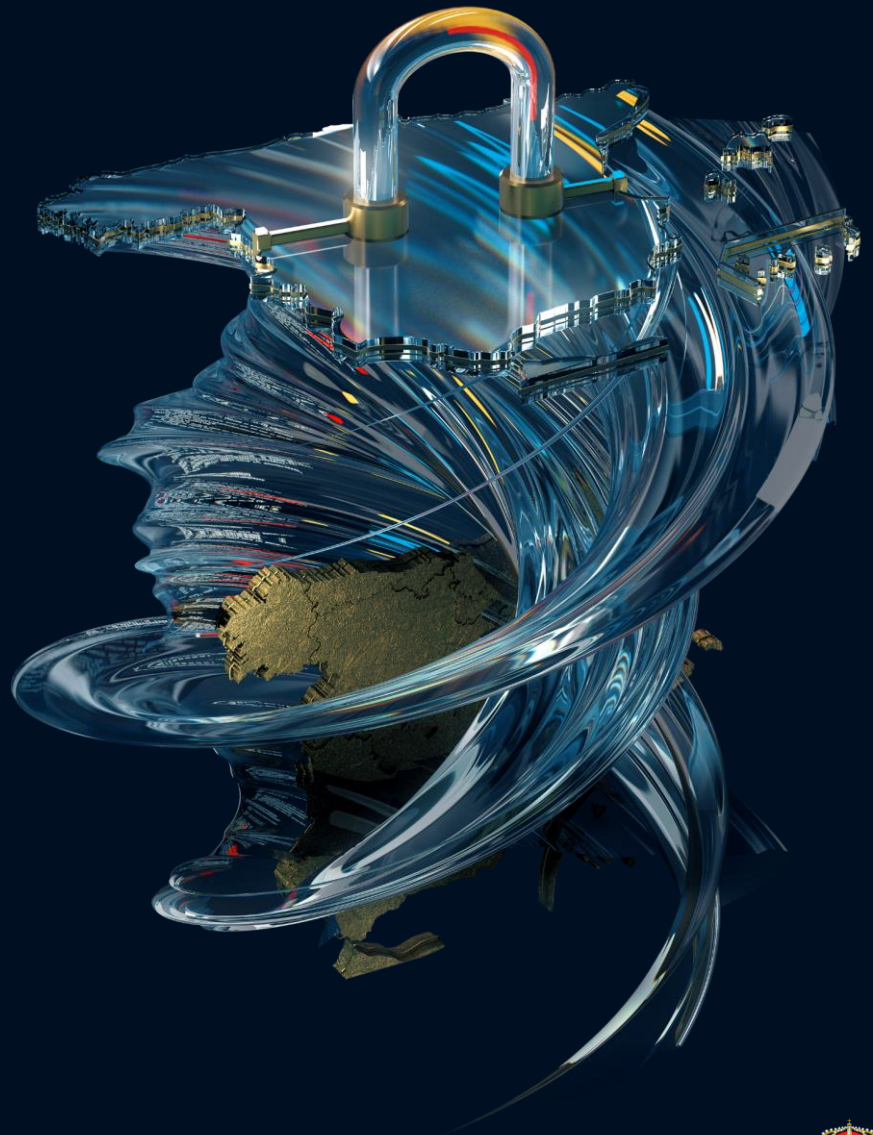
Doveryay, no proveryay

confía …, pero verifica

KEY NOTE 3:



ten buenos partners



MUCHAS GRACIAS

Emilio Rico Ruiz

GRUPO TRC®

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN CIBERESCUDO ÚNICO PARA ESPAÑA

Primer ataque a la cadena de suministro

Wenzel Peter. Adán y Eva en el Paraíso Terrenal
Museo Vaticano: Oleo sobre Lienzo

TOMAS FALSAS

Supply Chain attack: Hardware

DOCUMENTACION DE REFERENCIA:

- ISO 31000
- CCN-STIC-480F Seguridad en el control de procesos y scada (Apdo 6 cadena de suministro)
- NIST - IR 8276 Key practices in Cyber Supply Chain Risk Management
- NIST - SP 161-800-161r1
- NIST - Best practices in Cyber Supply Chain Risk Management
- NCSC (UK) Supply Chain Security Guidance
- CISA ICT Supply Chain Risk Management
- MITRE Supply Chain Attack Framework and Atack Patterns
- MCO - Framework for a Third Party Risk Management Program
- The LINUX Foundation - Software Bill of Materials (SBOM) and Cybersecurity Readiness (Jan2022)

- ENISA - Threat Landscape for Supply Chain Attacks
- ENISA - Threat Landscape 2022
- ENISA - TOP 10 emerging cybersecurity threats for 2030

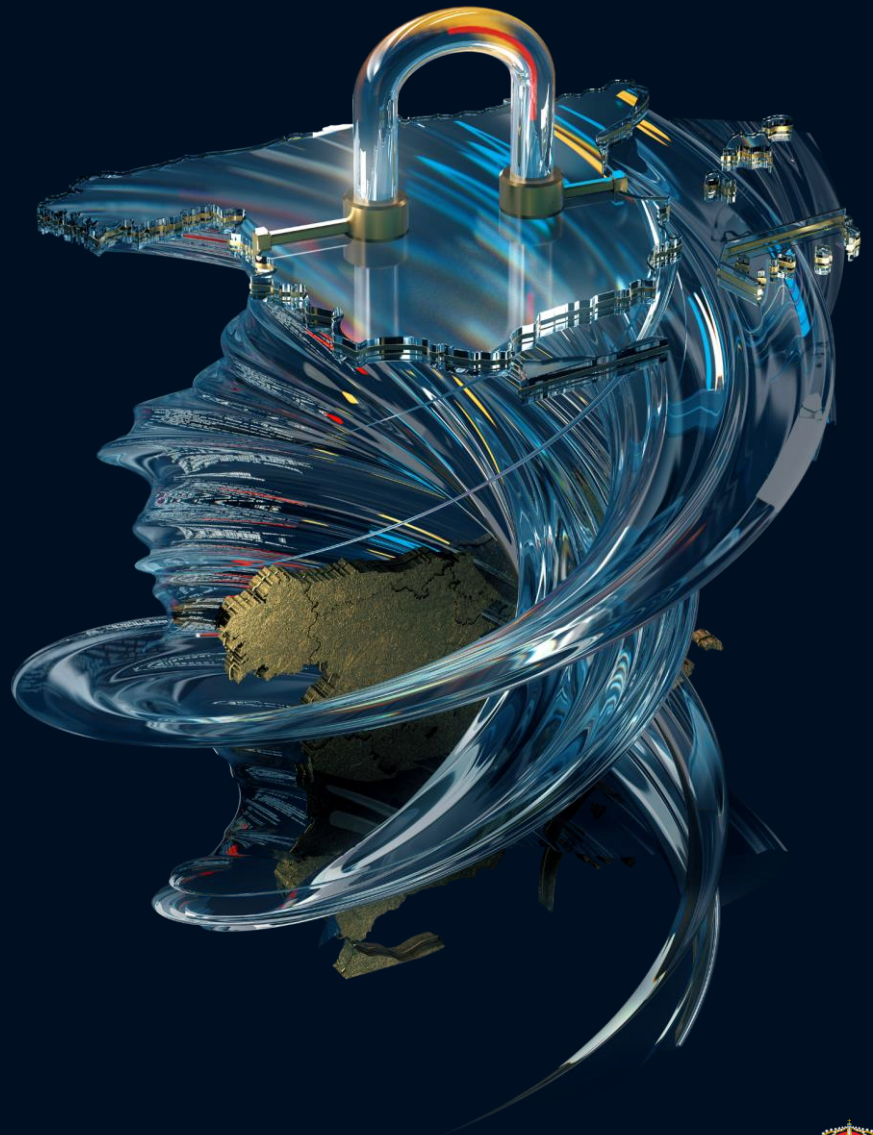
- *Executive Order 14028 of May 12, 2021: Improving the Nation's Cybersecurity*
- Catalogo de productos del CCN

TOMAS FALSAS

доверяй, но проверяй

Doveryay, no proveryay

confía, pero verifica



MUCHAS GRACIAS

Emilio Rico Ruiz

GRUPO TRC®

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN CIBERESCUDO ÚNICO PARA ESPAÑA