



TERROR EN EL CIBER MERCADO

(SCAMs en el Ultramarinos)



UN CIBERESCUDO
ÚNICO PARA ESPAÑA



TERROR EN EL CIBER MERCADO

(SCAMs en el Ultramarinos)



Cuando lo pides por Internet

iQuiero la peli de StarWars!



Cuando te llega a casa

iQuiero la peli de StarWars!

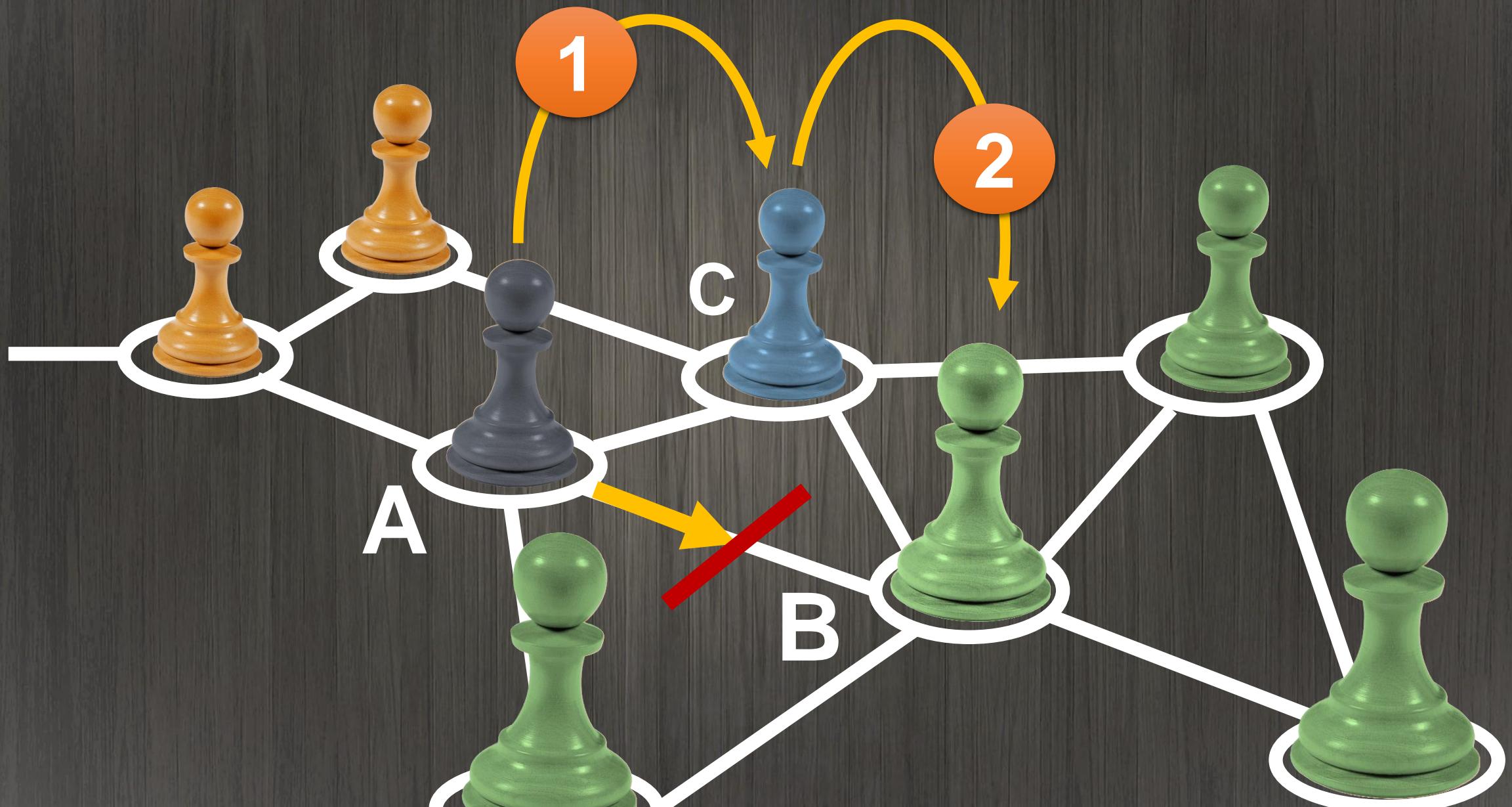


Ataques a la cadena de suministro.



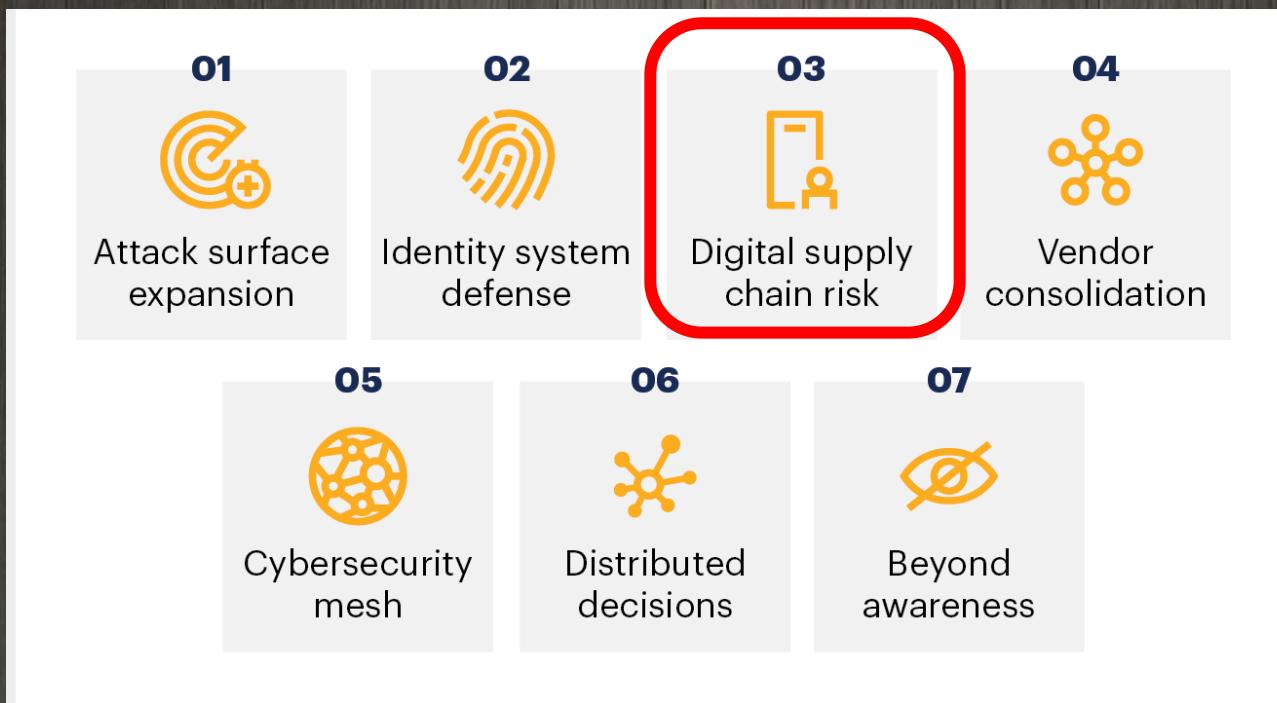
- Un ataque a la cadena de suministro supone una violación y/o **compromiso** de los bienes, servicios o tecnología, que un proveedor suministra a un cliente, **introduciendo** y **trasladando un riesgo** para esos clientes.

La Propiedad Transitiva



Gartner

Top Trends in Cybersecurity, 2022



2025
↓
45%

ENISA THREAT LANDSCAPE 2022

ENISA REPORT



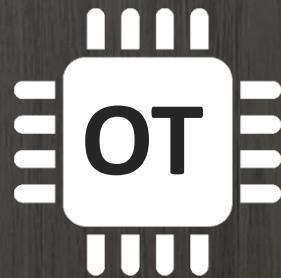
1. Ransomware
2. Malware
3. Amenazas de ingeniería social
4. Amenazas contra los datos
5. Amenazas contra la disponibilidad
6. Desinformación
7. **Ataques a la cadena de suministro**

TOP 10 emerging cybersecurity threats for 2030



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



El peligro



Video Credit: Annie's Eden

Está pasando

19/08/2022 - Ista



60M lectores

22/08/2022 - General Bytes



8.000 cajeros

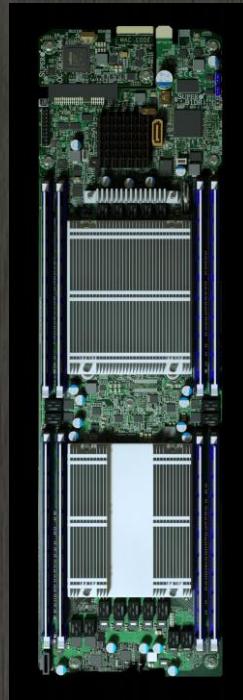
06/05/2021

COLONIAL PIPELINE

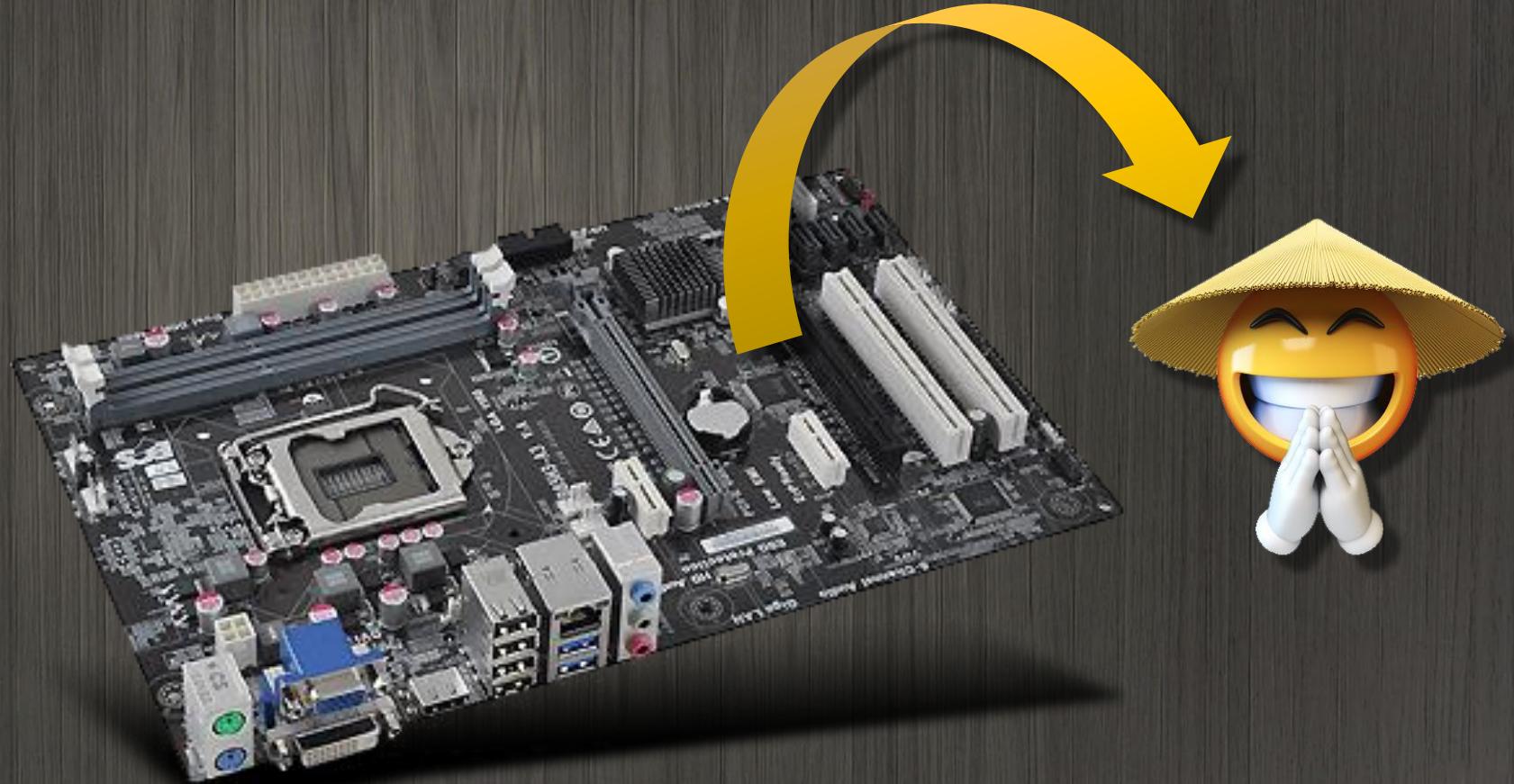


18 estados

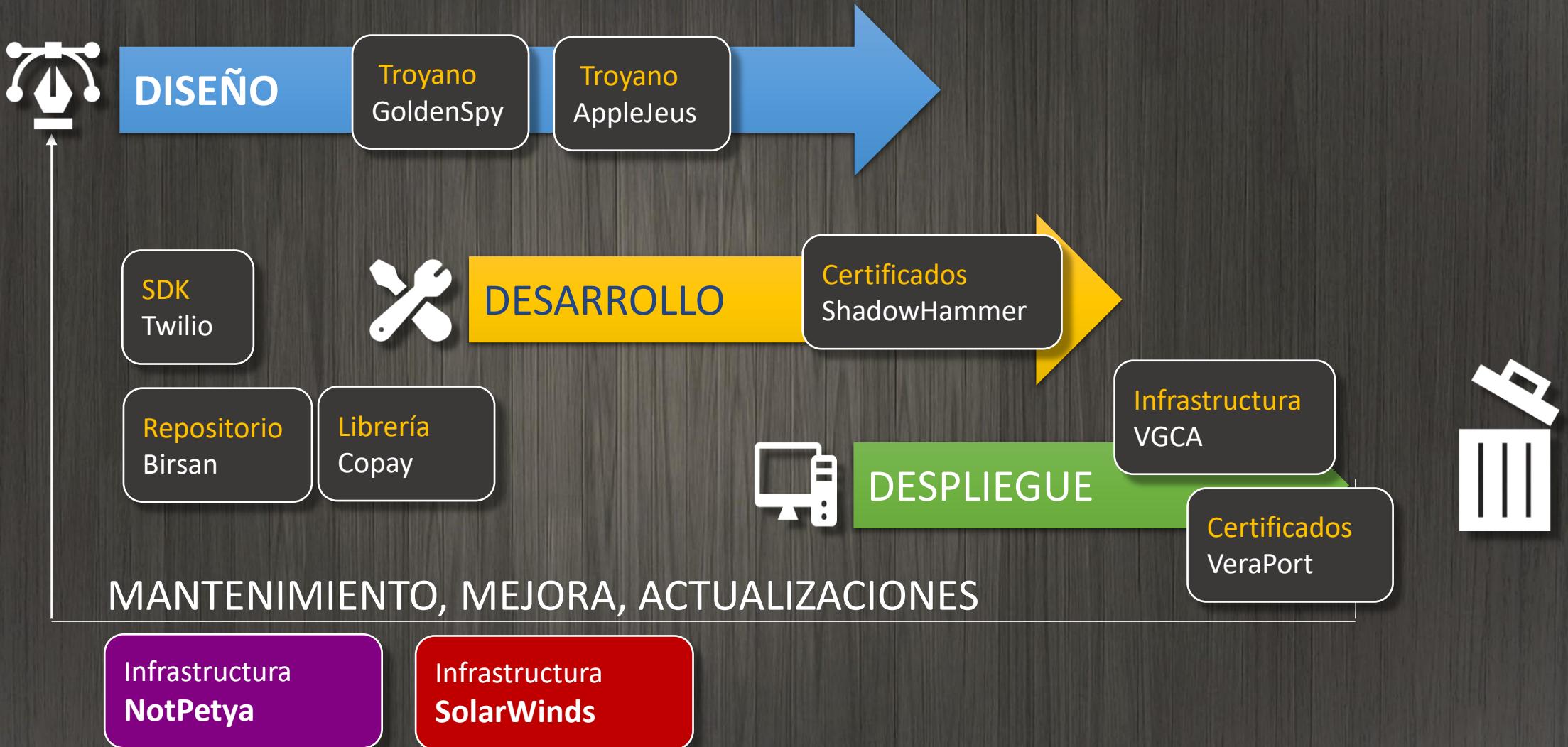
También afecta al Hardware



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



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

5,512,517	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 millones** de vulnerabilidades ubicadas en 500.000 repositorios.

3 AGOSTO 2022

Clonan **35.000** repositorios de

31-OCT-2022

The Hacker News

GitHub Repojacking Bug Could've Allowed Attackers to Takeover Other Users' Repositories

Stephen Lang @stephenlang

A massive GitHub bug could have allowed attackers to take over other users' repositories. The bug, which was discovered by Stephen Lang (@stephenlang), was first reported in August 2022. It was later fixed in October 2022. The bug was found in the GitHub API, which allows users to clone repositories. The bug was exploited by attackers to clone repositories from other users without their permission. This could have been used to steal sensitive information or even take over entire projects. The bug was fixed in October 2022, but it highlights the importance of regularly updating software and staying aware of security vulnerabilities.

[hxxp://ovz1.j19544519.pr46m.vps.myjino\[.\]ru](http://ovz1.j19544519.pr46m.vps.myjino[.]ru)

LOG4J



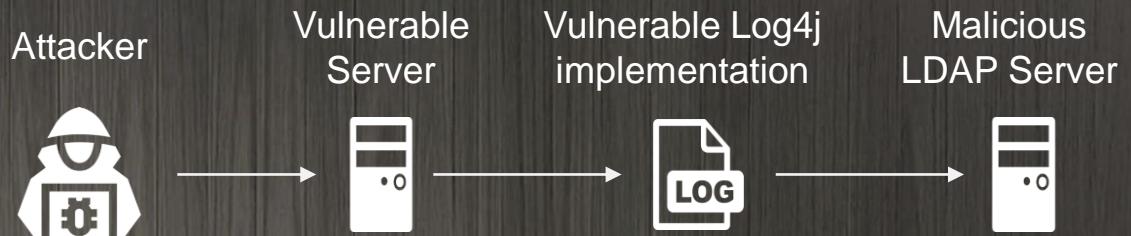
9 DICIEMBRE 2021

CVSS: 10/10



• • •

Log4j JNDI Attack



Ralph Goers



12 de diciembre de 2020

solarwinds

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

APT29



Vulnerabilidad: Solorigate (**Sunburst**)

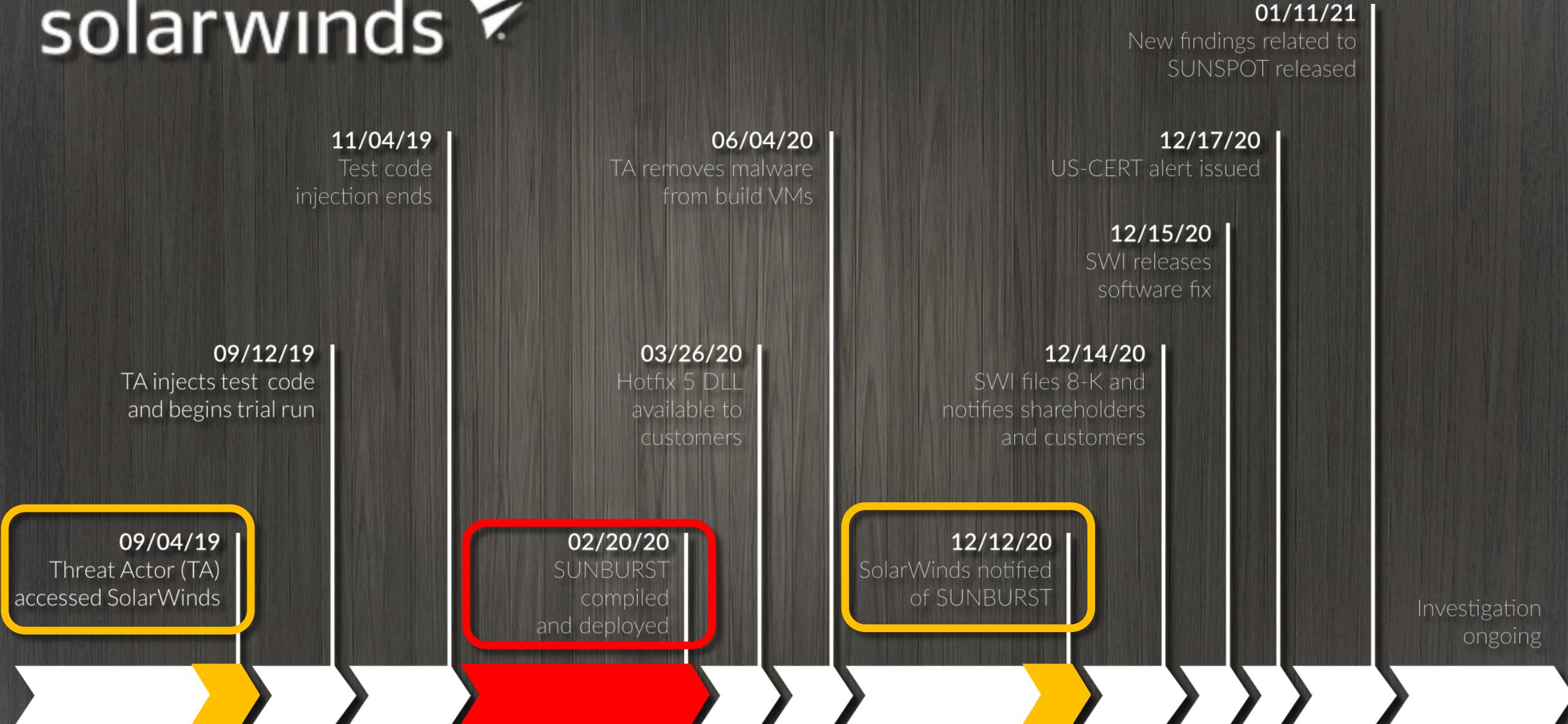


Nobelium - APT29

18,000 / 33.000 organizaciones (**F500**)

7 países:







- "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

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

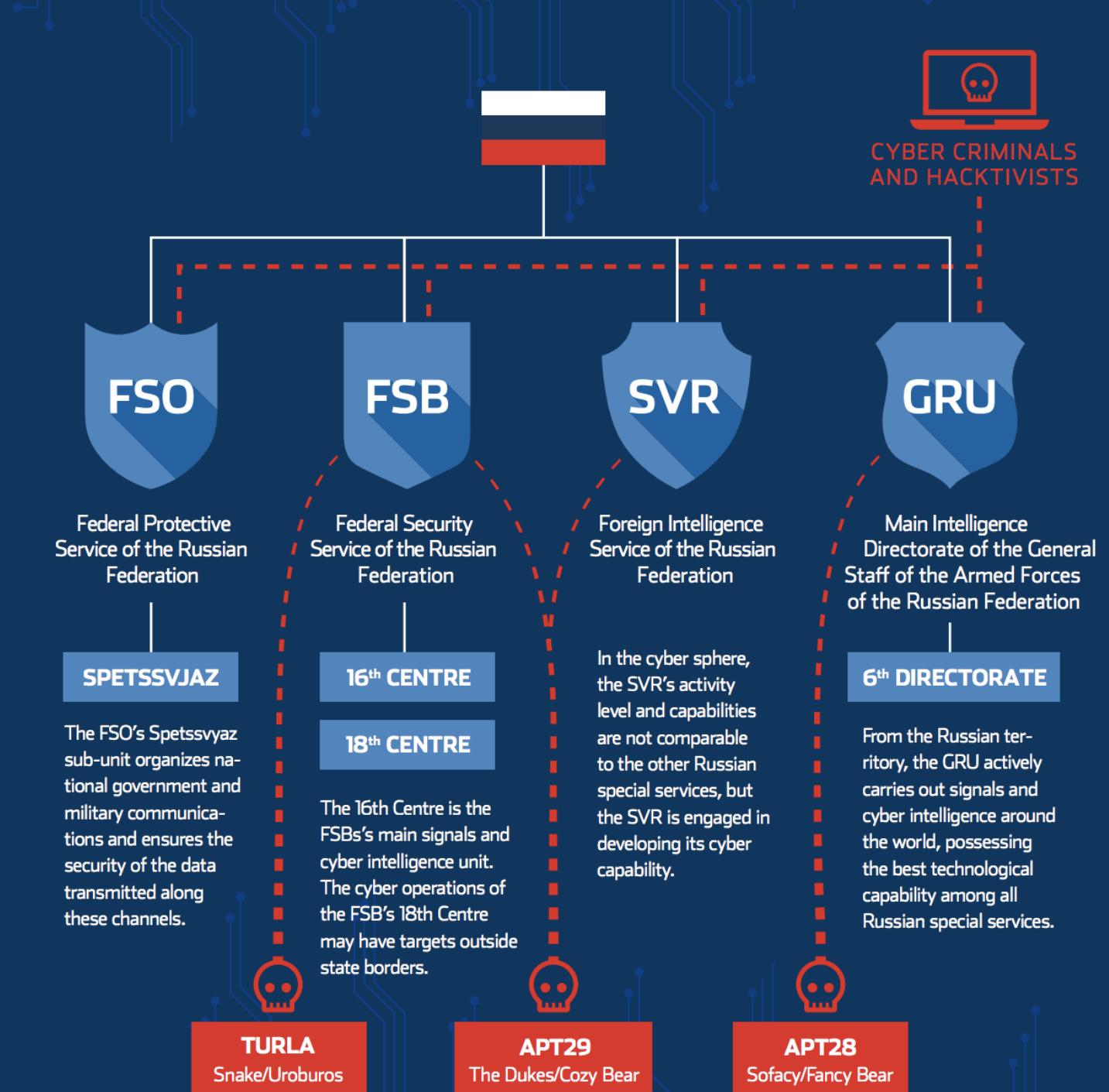
cCleaner - Axiom, Deputy Dog, APT 17

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.
 - Detectar actividad anómala y **Responder** rápidamente.
-
- Necesitamos **MÉTODO**
 - Necesitamos **TECNOLOGÍAS**
 - Necesitamos **PROCEDIMIENTOS**

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



Taxonomía

proveedor

Técnicas de ataque para comprometer la Cadena de suministro

- Infección de malware
- Ingeniería social
- Ataque de fuerza bruta
- Software de explotación Vulnerabilidad
- Configuración de explotación Vulnerabilidad
- Fuente abierta Inteligencia (OSINT)

Activos del proveedor que son objetivo

- Software preexistente
- Bibliotecas de software
- Código
- Configuraciones
- Datos
- Hardware
- Componentes
- Gente
- Proveedor

cliente

Técnicas de ataque utilizadas para comprometer al cliente

- Relación de confianza [T1199]
- Drive-by compromise [T1189]
- Suplantación de identidad – Phishing [T1566]
- Infección de malware
- Ataque físico o Modificación
- Falsificación

Activos del cliente que son objetivo

- Datos
- Información Personal
- Propiedad intelectual
- Software
- Procesos
- Banda Ancha
- Financiero
- Gente

Atentos a lo que compramos...



vs



.. Y a lo que vendemos

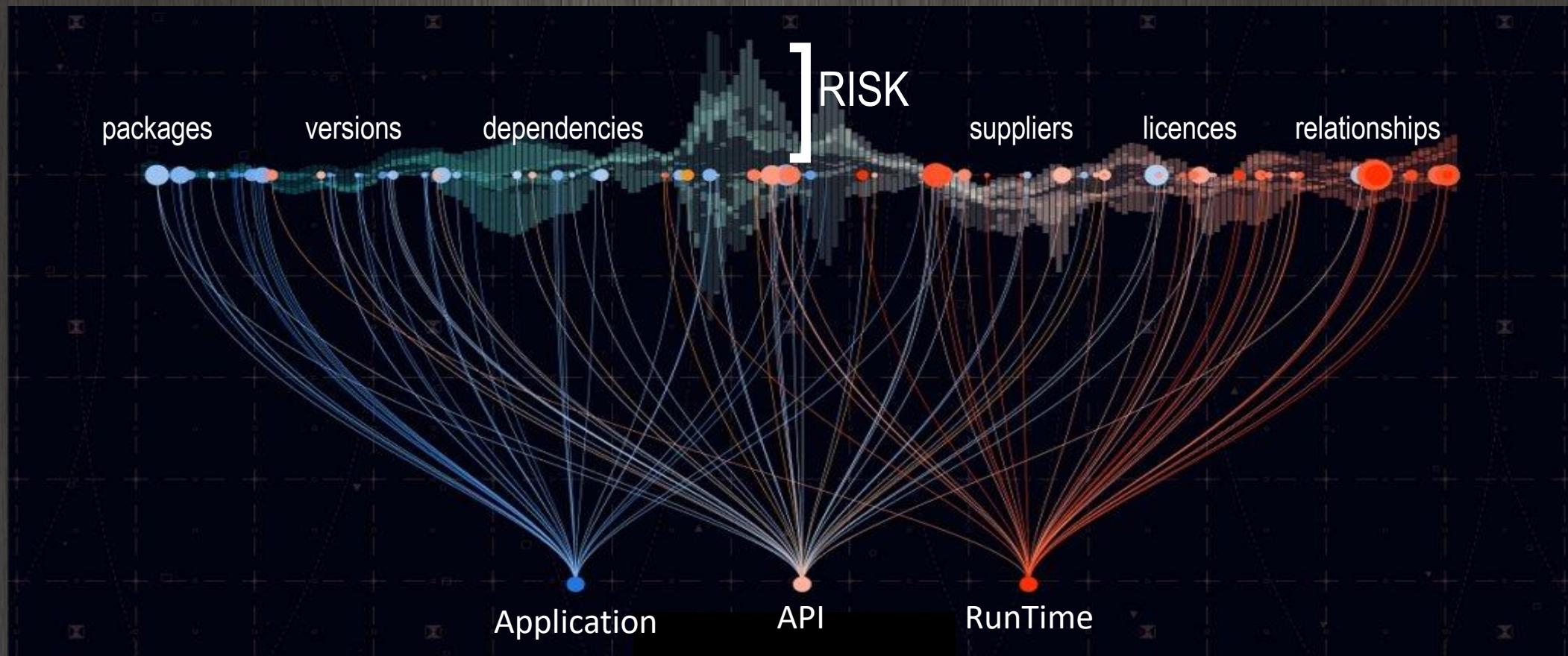


Y si descargamos ...

- ¿Ejecuta un Shell Script en tiempo de instalación?
- ¿Tiene código nativo?
- ¿Conecta con la red? Con Internet? Con qué dominios?
- ¿Lee variables de entorno? Cuales?
- ¿Hay código ofuscado?
- ¿Recolecta datos de telemetría?

SBOM: Software Bill Of Materials

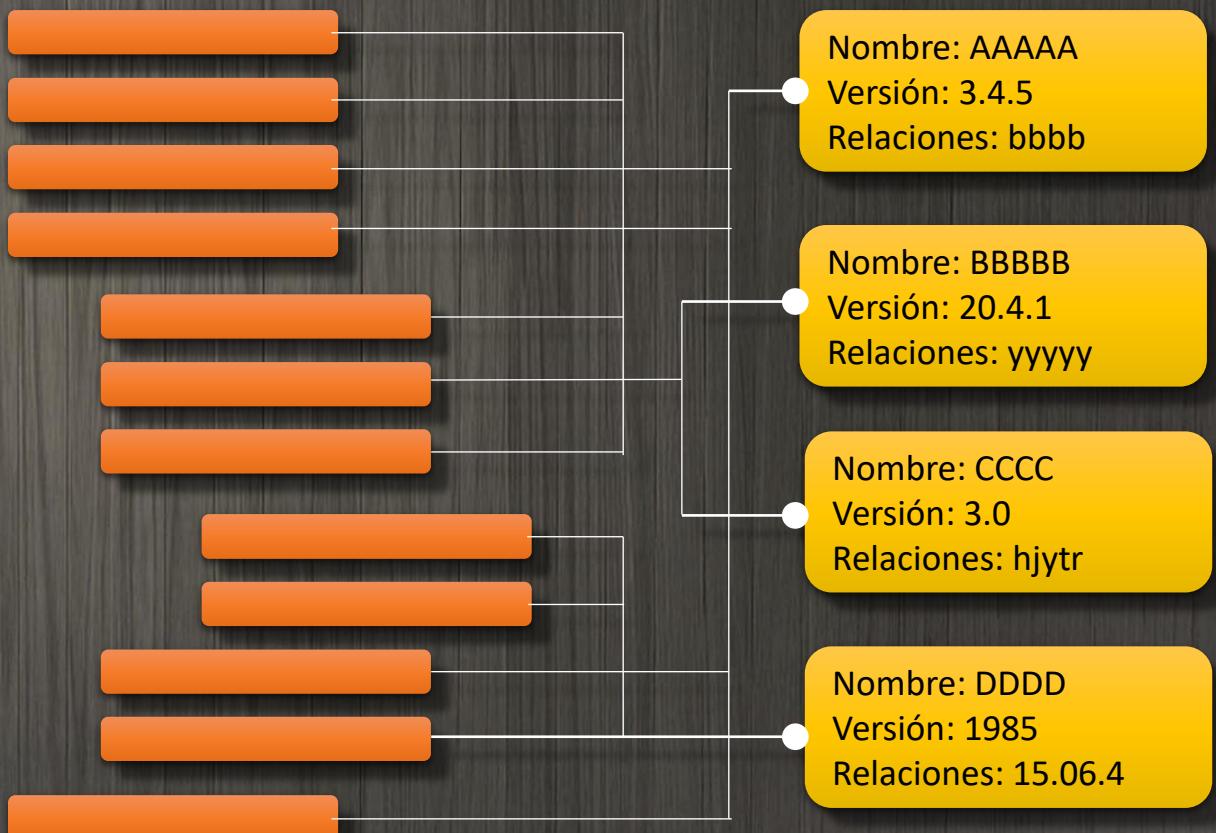
El SBOM es un registro (inventario) que contiene el detalle y las relaciones jerárquicas de los componentes usados en el desarrollo de un software dado.



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

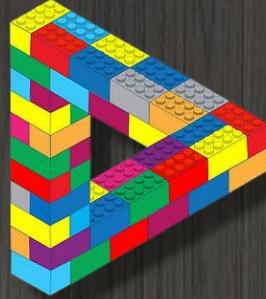
Supply Chain Compromise

- T1474 - No sub-techniques



Audit
Code Signing
SC-Management
Update Software
Vuln-Scan

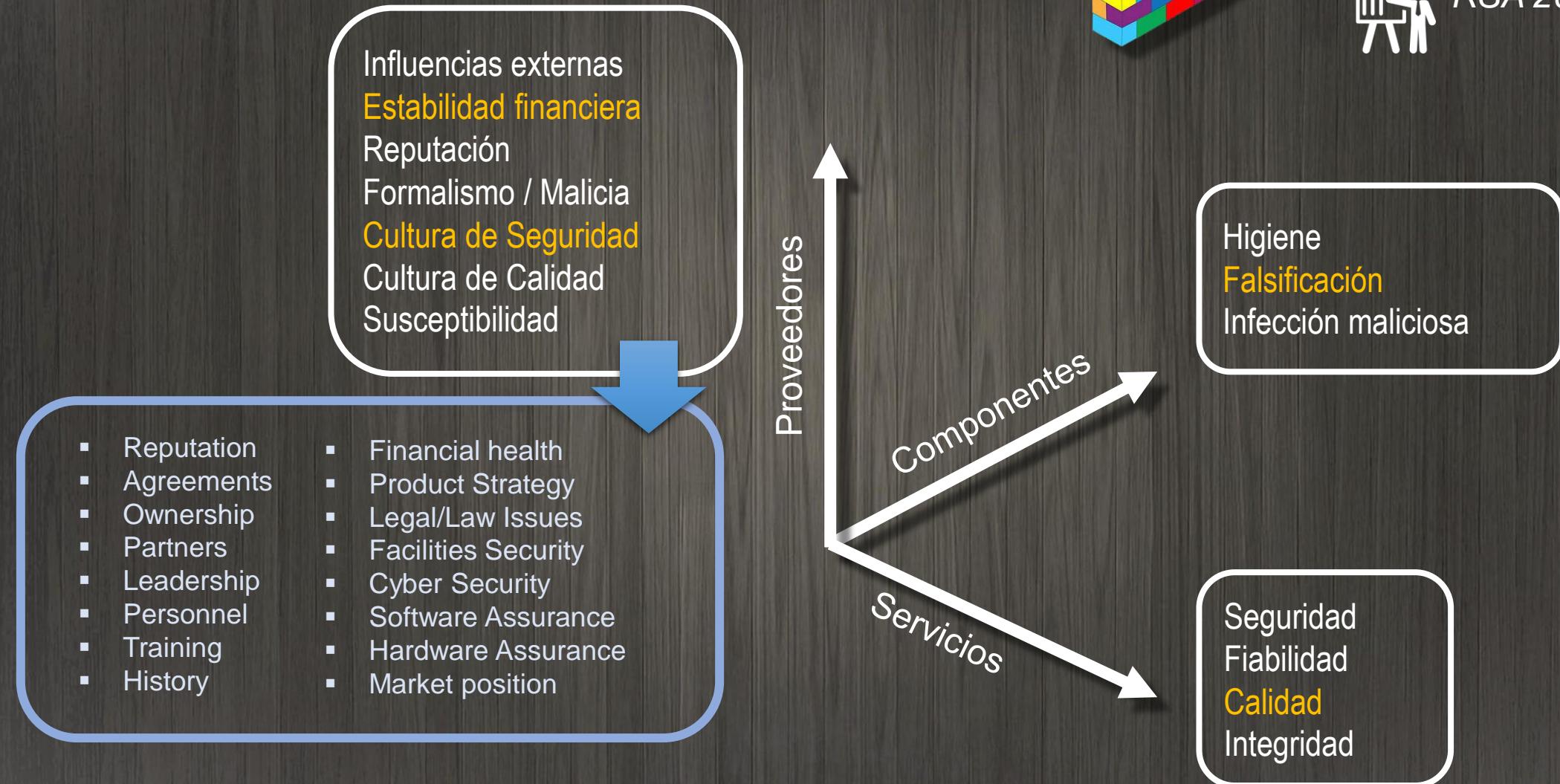
Sistema de Confianza (SoT)



MITRE



RSA 2022 (7Jun)

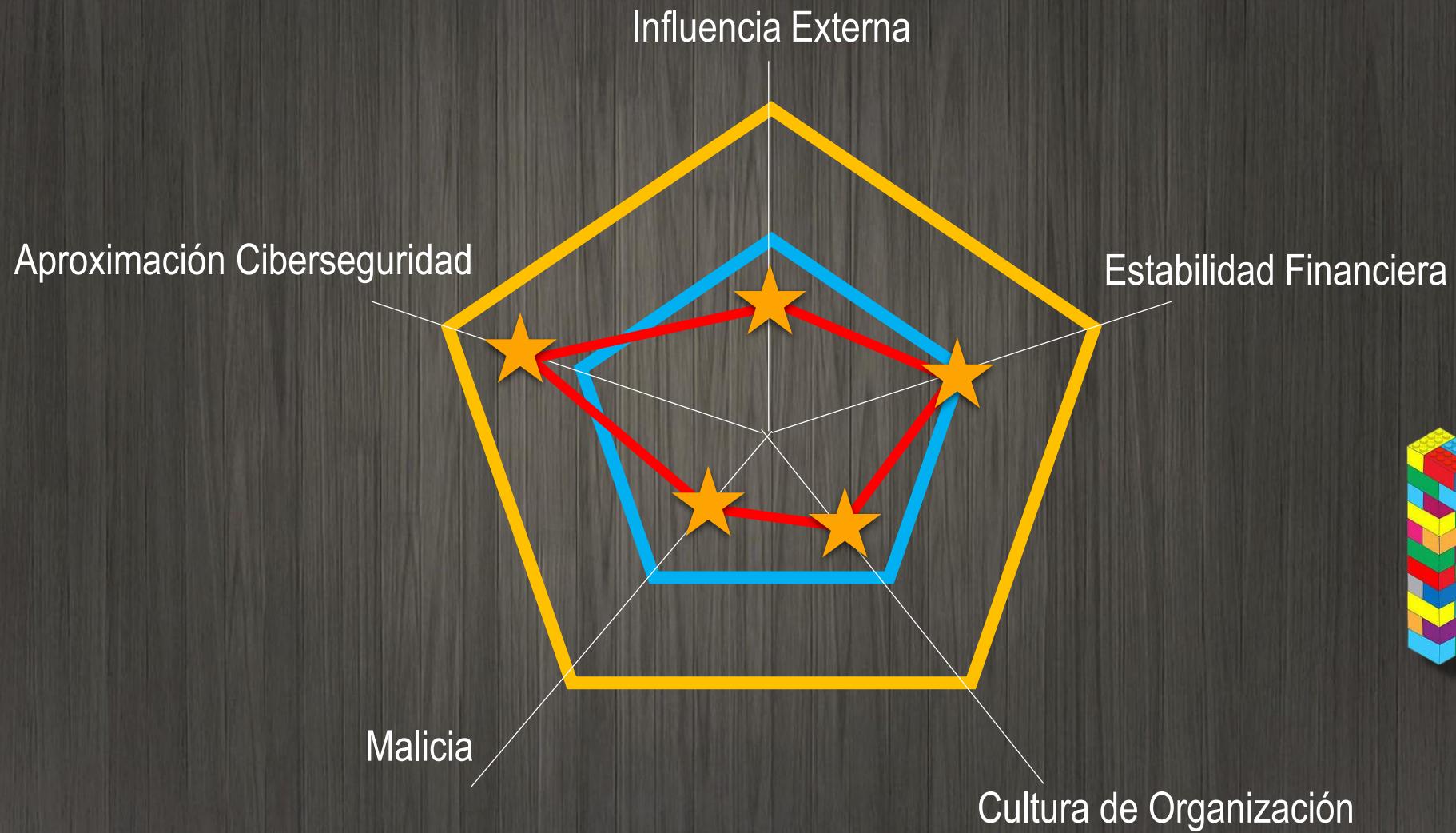


Sistema de Confianza (SoT)

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	Type/ level /frequency of security training	Vulnerabilities	Logistics / transportation integrity	Technical authenticity	Taxonomy SoT																	
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	Sustainability		Type/ level /frequency of security training			Manufacturing process integrity	Taxonomy SoT																		
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



(no se muestran factores de riesgo)



MULTI-TASKING



PROBLEM SOLVING

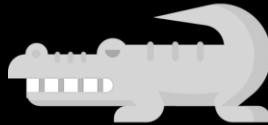


HARD WORKING



WILL TRAVEL

SUPPLY CHAIN[®] ANALYST



Contents
may vary
in color



100%
ORGANIC



CONCLUSIONES

1. Entender los riesgos
2. Define tus estándares y establece controles
3. Evalúa el riesgo de tus proveedores
4. 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

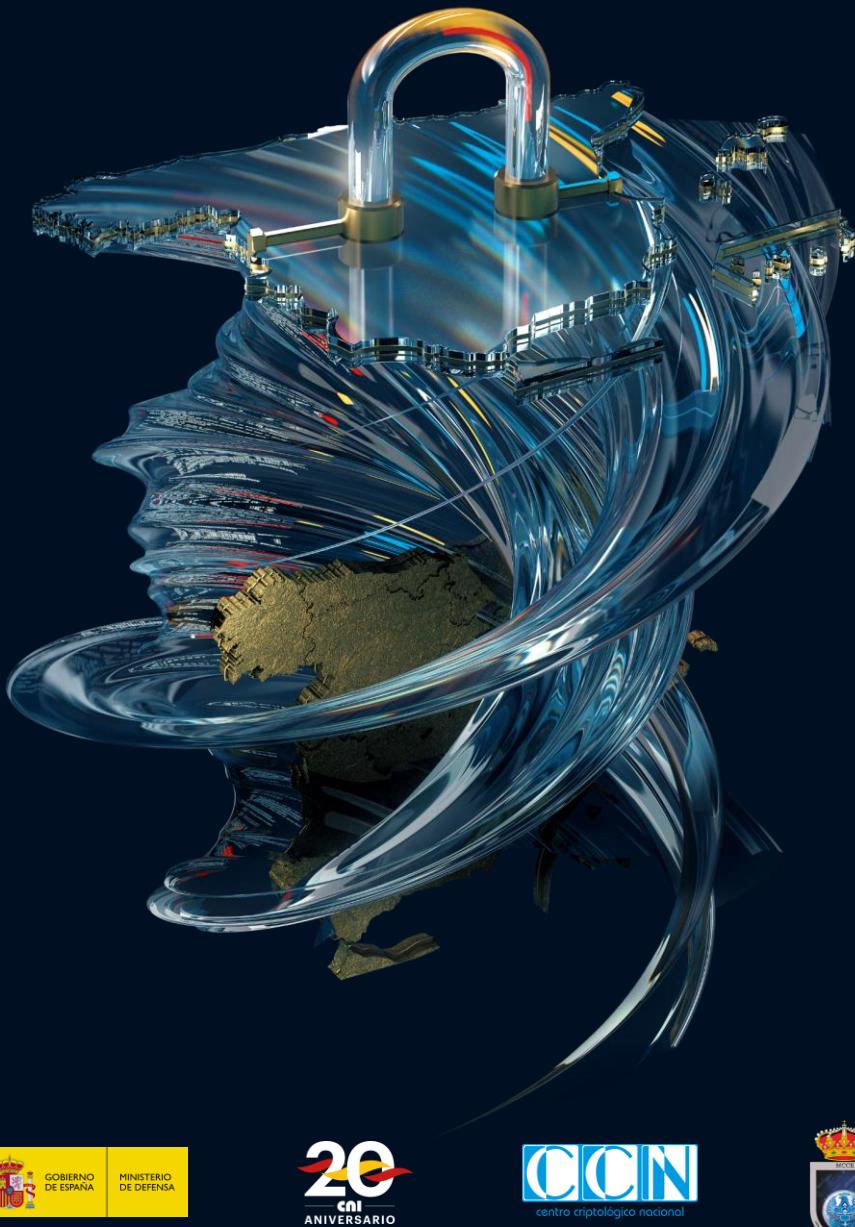
Doveryay, no proveryay

confía ..., pero verifica

KEY NOTE 3: Aún así

ten buenos partners





MUCHAS
GRACIAS



Emilio Rico Ruiz

GRUPO
TRC®



20
cni
ANIVERSARIO

CCN
centro criptológico nacional



CCN-cert
centro criptológico nacional



UN CIBERESCUDO
ÚNICO PARA ESPAÑA