CCN
Centro Criptológico Nacional

microCLAUDIA

S2 GRUPO

microCLAUDIA | Introducción

Motivación: Impacto que han ocasionado las últimas campañas de ransomware, especialmente la combinación de varios malware como Emotet, Ryuk, Sodinokibi, Bitpaymer...

Objetivo: Proporcionar protección contra malware de tipo ransomware mediante el despliegue de vacunas

microCLAUDIA | Antecedentes

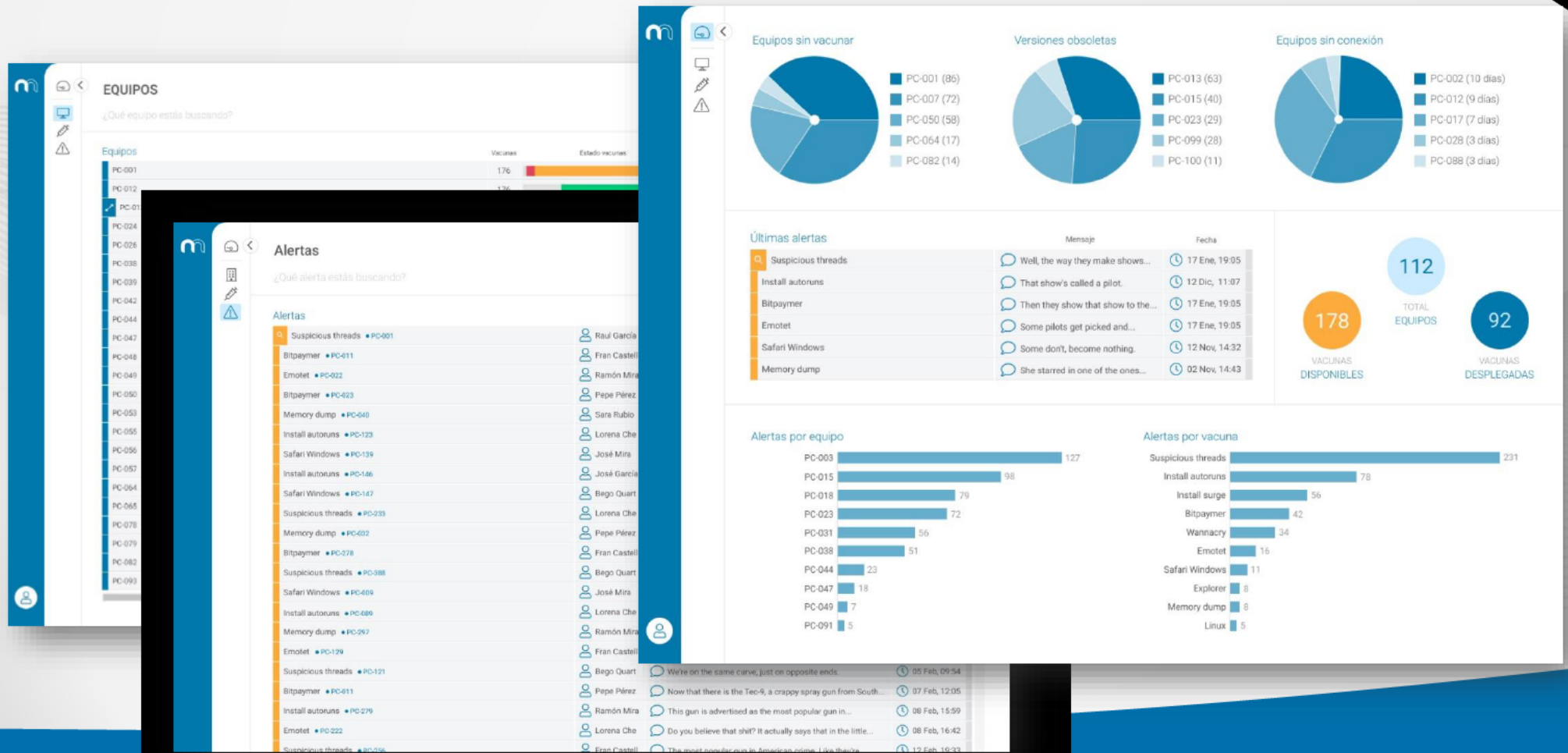
- El CCN-CERT desarrolló la herramienta **Emotet-Stopper**
- Este agente recoge diferentes mecanismos que permiten evitar la ejecución de las muestras de malware usadas en las campañas de phishing recientes
- Las técnicas utilizadas por el malware tienen una evolución constante que requiere:
  - Desarrollo de nuevas versiones del agente de vacunación
  - Necesidad de facilitar la distribución de actualizaciones

Para ello, basándose en el conocimiento adquirido en el desarrollo de la herramienta CLAUDIA, nace **microCLAUDIA** como centro de vacunación.

microCLAUDIA

Sistema de vacunación de puestos de usuario

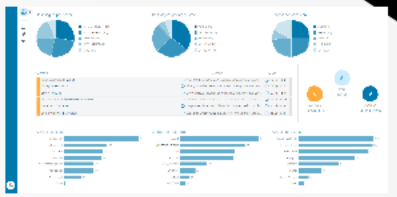
microclaudia es la especialización de claudia para la **vacunación** de equipos ante nuevas campañas y amenazas de malware



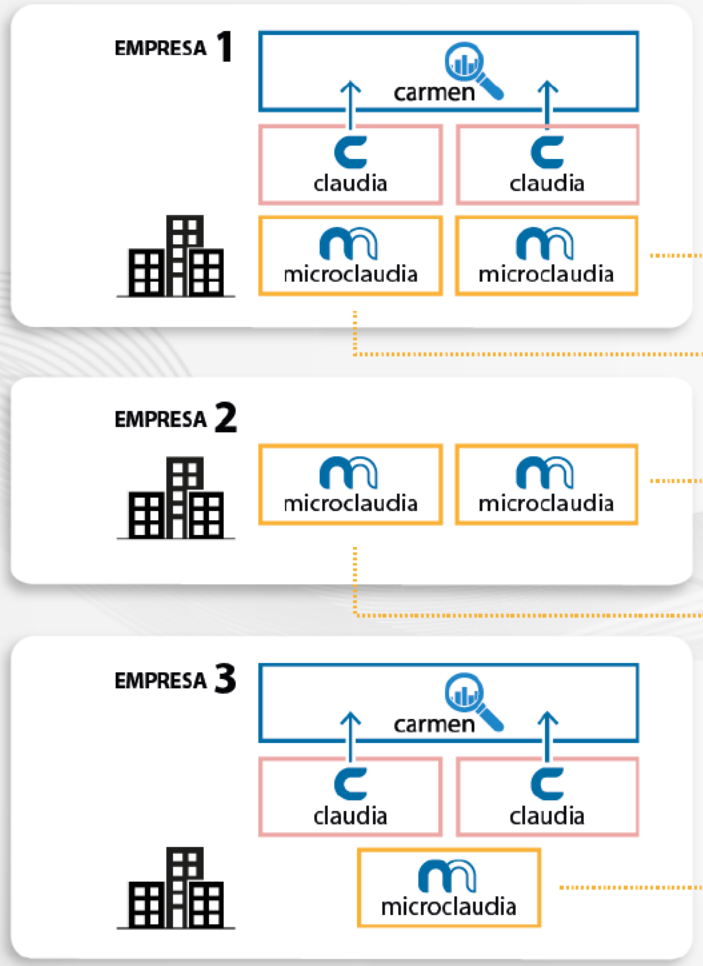
microCLAUDIA | Arquitectura

Instalación de un agente en el puesto de usuario que comunica con el servicio central de **microclaudia**

Los puestos que tienen el agente de **claudia** comunican con la instancia de **carmen** del propio Organismo



Equipo CCN y
Equipo S2 GRUPO



INTERNET

https

Servicio central de microclaudia ubicado en las instalaciones de CCN

Servicio independiente de generación de vacunas y publicación

microCLAUDIA | Instalación del agente

Requisitos

- **Software de instalación**
- **Clave de activación es única por organización**
- **Instrucciones de instalación**

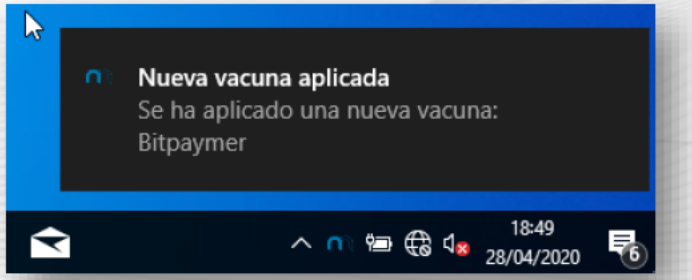
Modos de instalación

- Manual: Ejecución del instalador con permisos de administrador en un equipo (indicando el campo de clave y, si aplica, la configuración del proxy)

- Automático: mediante cualquier utilidad de despliegue de software del que se disponga, GPO, SCCM, etc. llamando al mismo ejecutable desde la línea de comandos y con permisos de administrador. Esto es transparente para el usuario

microCLAUDIA | Modo de funcionamiento

- Conexión al servidor central de vacunación
- Descarga automática de la configuración de las vacunas
- Reconocimiento y ejecución de vacunas firmadas (también en modo offline)
- Icono y notificaciones en la bandeja del sistema
- Auto actualización del agente



¿Qué es una vacuna?

Mecanismo que impide que el malware se ejecute en un equipo

microCLAUDIA | Vacunación. Caso prácticos

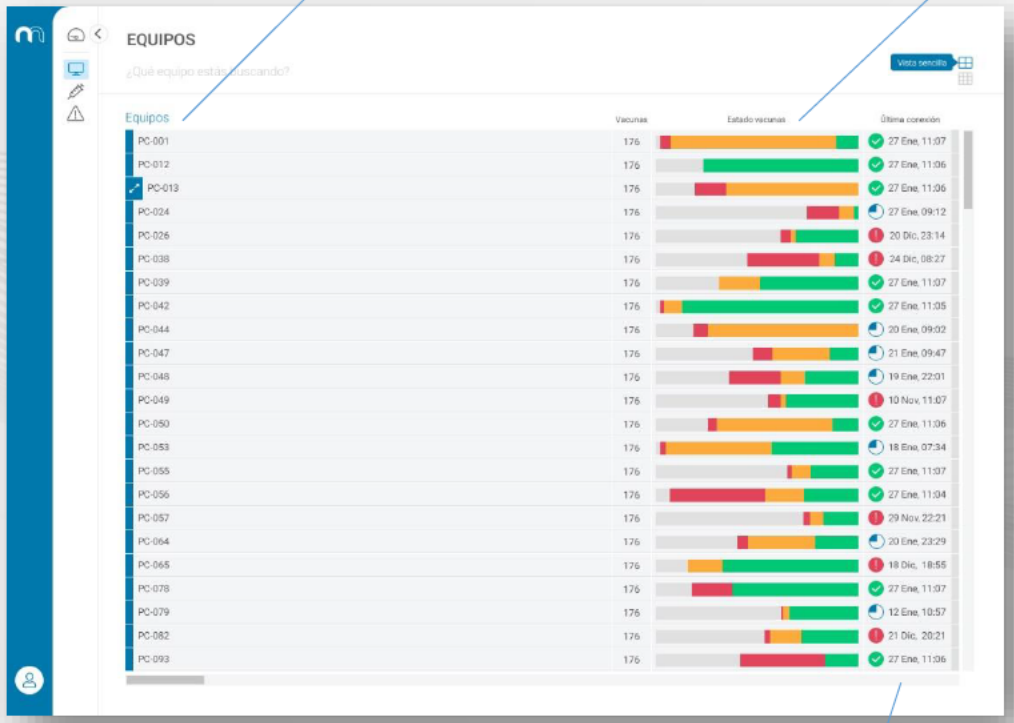
- **Emotet (Phising)**
  - Ataque indiscriminado que supone la vía de infección más común
  - El 95% de los casos de ransomware del año pasado usaron esta vía de infección
  - Diferente a *spear phishing*, que es un ataque dirigido
- **WannaCry (mutex)**
  - Ataque indiscriminado
  - Mucha repercusión mediática
- **Sodinokibi (mutex)**
  - Ataque dirigido a empresas / organizaciones
- **BitPaymer (file)**
  - Ataque dirigido a grandes empresas / organizaciones

microCLAUDIA | Visibilidad de la Organización

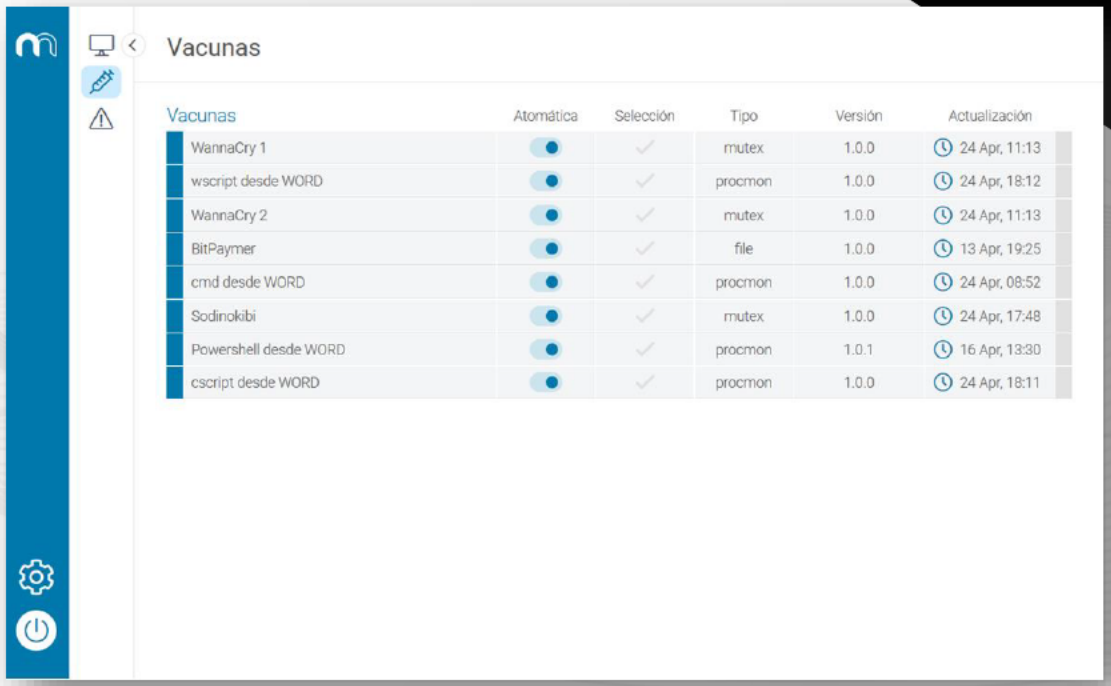
Posibilidad de supervisar el parque de equipos sobre los que aplicar las vacunas

Comprobación de la lista de vacunas aplicadas y de su estado por activo

Acceso a las vacunas publicadas disponible

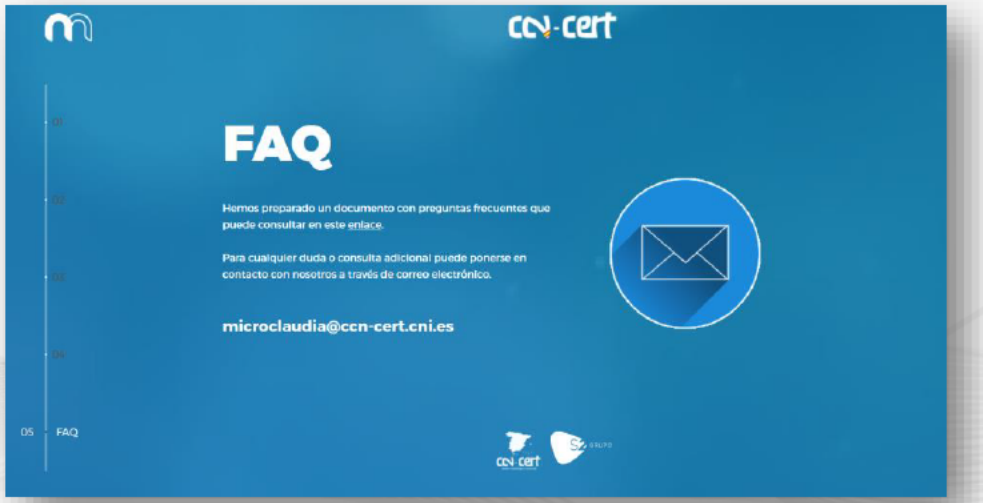


CMDB de agentes y fecha de última comunicación



microCLAUDIA | Información adicional

En el sitio web https://microclaudia.ccn-cert.cni.es se ofrece un apartado de preguntas frecu



Para cualquier duda o aclaración adicional, así como para la solicitud del software y clave de activación de microClaudia se pueden dirigir a microclaudia@ccn-cert.cni.es

GRACIAS

microCLAUDIA