centro criptológico nacional

Cryptojacking

¿Qué es?
Uso ilegítimo de un dispositivo electrónico, sin el consentimiento ni conocimiento del usuario, por parte de criminales para minar criptomonedas.

Pero, ¿qué es minar criptomonedas?
Emplear los recursos de un dispositivo para validar transacciones y a cambio recibir una compensación económica en esa criptomoneda.

¿Qué hacer para desinfectar un cryptominer?

- Desconectar el equipo de la red.
- Analizar el equipo con antivirus actualizado.
- Analizar el equipo con tecnologías Antimalware.
- Formateo del equipo.

Y..¿cómo se minan criptomonedas?
A través de cryptominers, que es el malware utilizado para minar criptomonedas sin la autorización del propietario del dispositivo.

¿Qué herramientas de detección puedo utilizar?
Aquellas que monitoricen los recursos del sistema y realicen un análisis del equipo. Además, este proceso se puede complementar con un examen facilitado por la herramienta Malwarebytes.

¿Sabías que...?
Durante el año 2017 se produjo un incremento del 34.000% en ataques relacionados con el cryptojacking.

¿Cómo detectar un cryptominer?
Comprobando los siguientes síntomas:

- Lentitud general de la máquina o de la conexión a internet.
- Procesador con una alta carga de cómputo sin tener aplicaciones abiertas.
- Sobrecalentamiento de los componentes.
- Procesos no conocidos ejecutándose.

¿Cuál puede ser la forma de distribuir el malware?

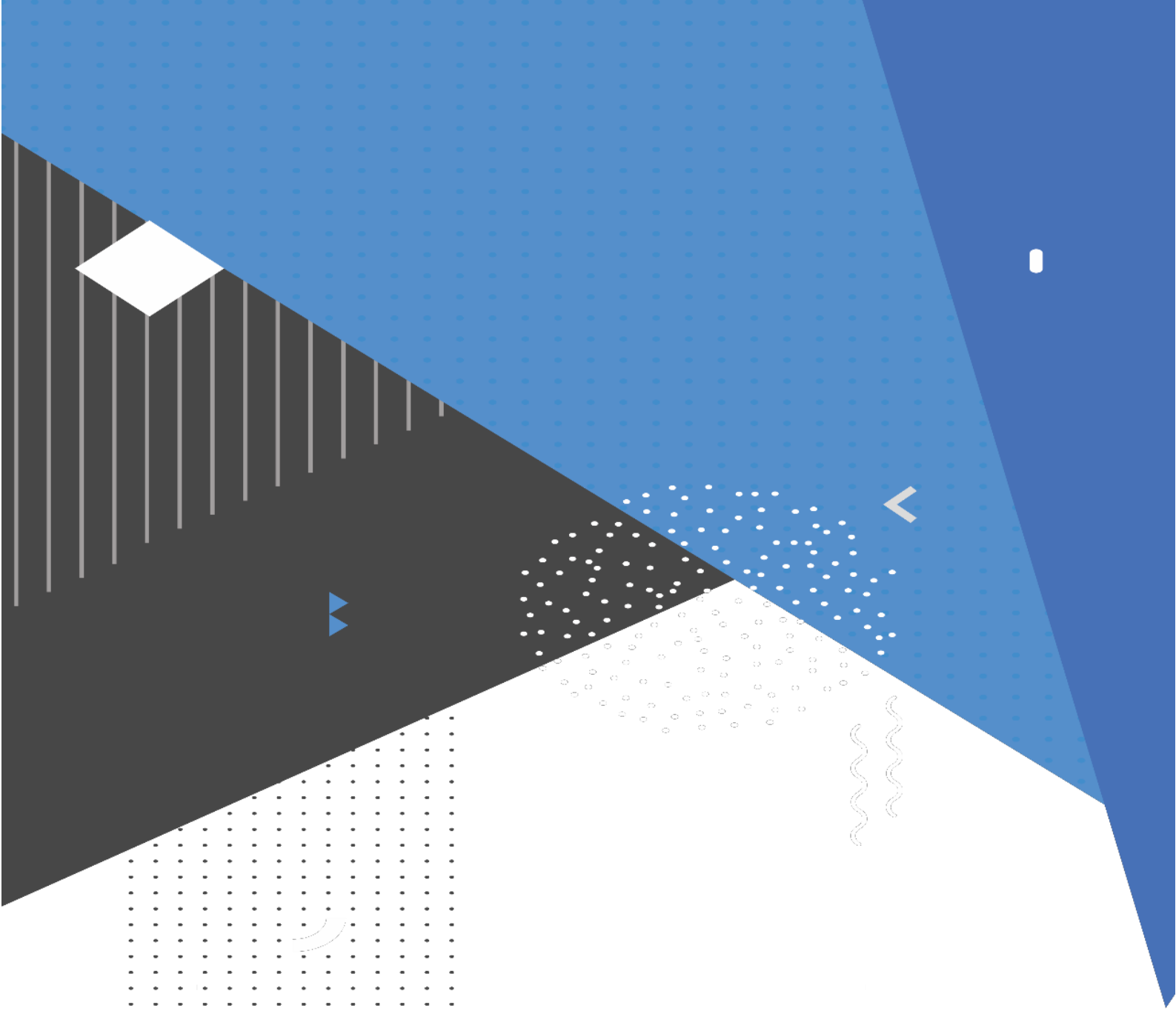
- Correos fraudulentos /phishing.
- Exploit Kits.
- A través de páginas web dañinas.

¿Y el objetivo del ataque?

- Internet de las Cosas (IoT).
- Dispositivos móviles.
- Servidores.

Buenas prácticas para evitar este tipo de malwares:

- ✓ Uso de bloqueadores y ventanas emergentes.
- ✓ Tener actualizado el antivirus.
- ✓ Mantener actualizado el sistema operativo.
- ✓ Usar navegadores seguros.
- ✓ Mostrar las extensiones de los archivos.



centro criptológico nacional