elastic security labs

Reporte de amenazas globales 2022

Infografía

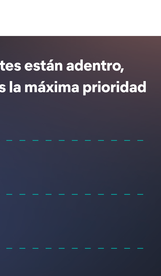
¿De dónde provienen las amenazas?

Sobre la base de la telemetría de soluciones, el Reporte de amenazas globales 2022 de Elastic Security Labs reveló fenómenos, tendencias y recomendaciones relacionadas con amenazas a fin de ayudar a las organizaciones a prepararse para el futuro. Entre los hallazgos se encuentran...

Los clouds en la práctica se vuelven seguros cuando se implementan controles adicionales a los predeterminados

En casi el 41 % de las alertas de acceso a credenciales se intentó robar tokens de acceso a aplicaciones en lugar de otros materiales con credenciales.

Técnicas de acceso a credenciales



Porcentajes de técnicas MITRE ATT&CK para la táctica de acceso a credenciales

Una vez que los atacantes están adentro, el acceso a credenciales es la máxima prioridad

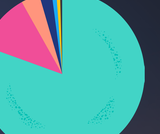
Porcentajes del total de nombres de tácticas MITRE ATT&CK para alertas de detección basadas en el cloud

El software comercial se está usando como arma

El malware diseñado para los equipos rojos se está usando en contra de las organizaciones.

CobaltStrike fue el archivo binario o la carga maliciosa más popular para endpoints de Windows, seguido de AgentTesla y RedLineStealer.

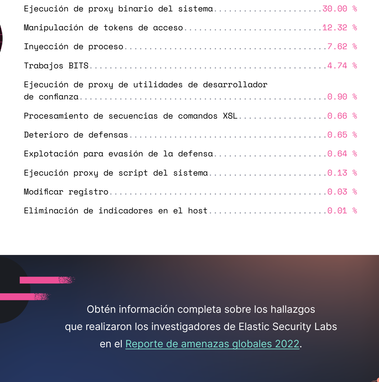
Todas las detecciones



- CobaltStrike..... 35 %
- AgentTesla..... 25 %
- RedLineStealer..... 10 %

El software abierto no es tan seguro como crees

Los 10 principales malware/cargas de Linux



Los 10 principales malware y cargas de Linux que muestran un aumento de la actividad de BPFDoor

Los troyanos siguen siendo una de las formas preferidas para convertir las entregas en armas

Malware por categoría

- Troyano.....80.5 %
- Criptominero...11.3 %
- Ransomware.....3.7 %
- Packer.....2.4 %
- Backdoor.....0.9 %
- Proxy.....0.7 %
- Otros.....0.5 %

Buenas noticias: La seguridad de endpoint está funcionando

Los ataques de endpoint se están diversificando cada vez más con el objetivo de omitir las defensas. Este año observamos 50 técnicas de infiltración de endpoint diferentes que no funcionaron.

Técnica	Porcentaje de la señal
Enmascaramiento	44.29 %
Ejecución de proxy binario del sistema	30.00 %
Manipulación de tokens de acceso	12.32 %
Inyección de proceso	7.62 %
Trabajos BITS	4.74 %
Ejecución de proxy de utilidades de desarrollador de confianza	0.90 %
Procesamiento de secuencias de comandos XSL	0.66 %
Deterioro de defensas	0.65 %
Explotación para evasión de la defensa	0.64 %
Ejecución proxy de script del sistema	0.13 %
Modificar registro	0.03 %
Eliminación de indicadores en el host	0.01 %

Obtén información completa sobre los hallazgos que realizaron los investigadores de Elastic Security Labs en el Reporte de amenazas globales 2022.