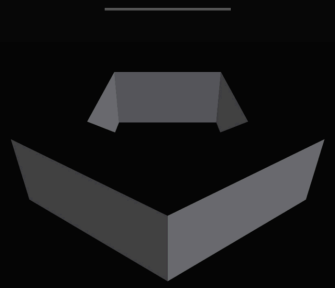


DETECTA

AISLA

IDENTIFICA

REPORTA

Ransomware

NULLSEC

because the NULL value is also insecure

Ransomware

Un ransomware (del inglés ransom, «rescate», y ware, acortamiento de software) o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

> Ocurren más de 4,000 ataques de ransomware por día.

> 75% de las organizaciones infectadas con ransomware tenían protección activa.

> Los daños globales relacionados a ataques de ransomware llegarán a $11.5 billones en el 2019.

> Se estima que habrá un ataque de ransomware cada 14 segundos para el fin del 2019.

> 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones.

*"Ataque del **ransomware** llamado **Sodinokibi** afectó a más de 22 agencias gubernamentales en Texas, E.U."*

*"El gobierno del estado de Luisiana, la ciudad de Baltimore y Pensacola en Florida, E.U. son algunos casos impactados por un ataque de **ransomware.**"*

*"Los ataques de **ransomware** también estuvieron presentes en países de habla hispana: la consultora Everis y la compañía Prosegur en España impactados por **Ryuk**; en México Pemex fue víctima del ransomware **DoppelPaymer**, mientras que en Argentina, el gobierno de la provincia de San Luis declaró la emergencia luego de ser víctima de un ataque de **ransomware**."*

*"Analizando la región Latam en particular, la lista de países en los cuales se registró la mayor cantidad de detecciones de **ransomware** durante el último año la lideró Perú, con poco más del 20% del total de las detecciones, seguido por México y luego Brasil."*

País	Porcentaje de detecciones
Perú	20.93%
México	14.05%
Brasil	12.26%
Colombia	10.85%
Argentina	10.14%
Ecuador	8.18%
Venezuela	6.96%
República Dominicana	3.90%
Guatemala	2.51%
Chile	2.16%
Bolivia	1.75%
Costa Rica	1.72%
Honduras	1.08%
Nicaragua	0.72%
Panamá	0.65%
El Salvador	0.53%
Cuba	0.36%
Paraguay	0.31%
Uruguay	0.29%
Martinica	0.18%

Fuente_ *we live security by eset*

Ransomware	Detecciones
Crysis	27.60%
WannaCryptor	21.36%
ED	11.01%
STOP	9.90%
GandCrab	8.18%
CryptProjectXXX	2.76%
GA	2.70%
Phobos	1.99%
Sodinokibi	1.55%
Philadelphia	1.51%
NHN	1.10%
Buhtrap	0.83%
Otros	9.51%

*"Si analizamos las detecciones de **ransomware** a nivel LATAM el podio está encabezado por distintas variantes de la familia **Crysis**, con poco más del 27%, seguido por **WannaCryptor** y **ED**."*

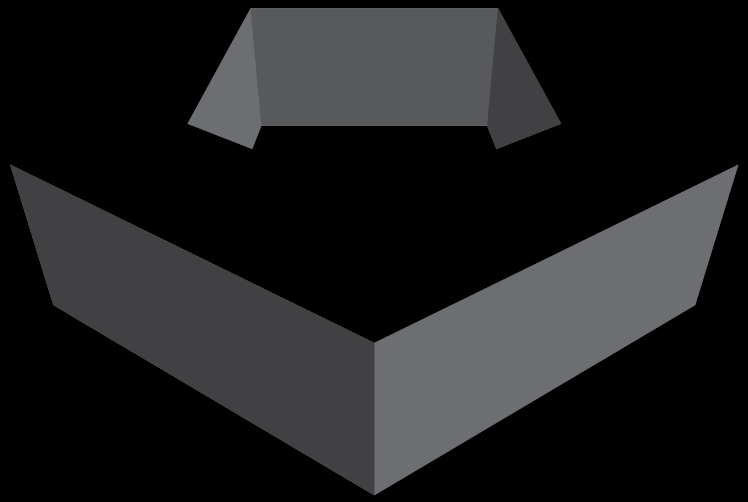
Plataforma	Detecciones
Android	0.02%
BAT	0.06%
HTML	0.01%
Java	0.00%
JS	0.02%
Linux	0.02%
MSIL	1.22%
OSX	0.00%
PHP	0.00%
PowerShell	0.02%
Python	0.03%
VBS	0.02%
Win32	98.04%
Win64	0.53%

*"En cuanto a plataformas, **Windows** es la más afectada (ya que hay varias familias que pueden infectar a equipos multiplataforma) y capta casi el 99% de las variantes."*

Fuente_ *we live security by eset*

Los últimos y recientes ataques de **ransomware** confirman la tendencia que especialistas predijeron para 2019 y los años siguientes, donde era de esperarse ver un giro por parte de los *cibercriminales* con ataques de **ransomware** más sofisticados y dirigidos, buscando mayor rentabilidad, a diferencia de ataques menos específicos y aleatorios que se venían dando años atrás.

N U L L
R A N S O M



¿Qué es?

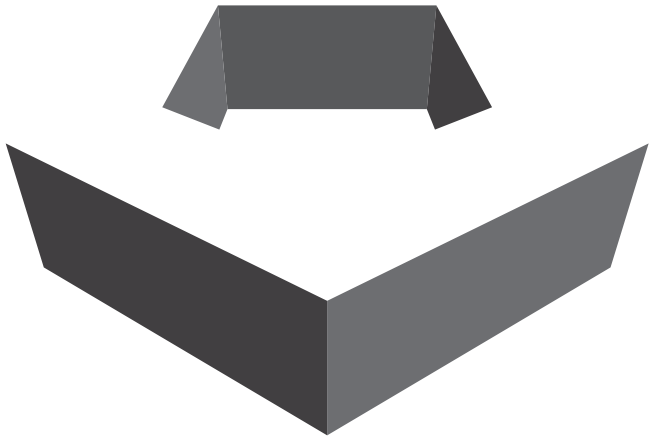
Es un agente de software que verifica el comportamiento en un equipo de computo.

Nuestra propuesta de **solución**

*Prevenir el ataque de software malicioso tipo malware/**ransomware.***

¿Cómo lo hacemos?

N U L L
R A N S O M



Estudiamos el **comportamiento** de un equipo para prevenir ataques

Por medio de un análisis de **inteligencia artificial** determinamos el tipo de ataque malicioso

Presentamos datos y estadística del comportamiento e historial por equipo de computo en un **panel administrativo** con interfaz amigable

Recopilamos información para **predecir** futuros ataques dirigidos

Minimizamos el riesgo de infección distribuido en la red por el **aislamiento y mitigación** de la detección del ataque por equipo de computo

Ejecución segura en segundo plano con **uso optimo** de recursos del equipo

NULLSEC

Ventas y activaciones de licencia:
ventas@nullsec.site
www.nullsec.site