Módulo 1:
Introducción

Hacking Ético

2023 / 2024

1. Actualidad
2. Principios básicos
3. Ataques y atacantes
4. Principales riesgos

1. Actualidad

2. Principios básicos

3. Ataques y atacantes

4. Principales riesgos

Actualidad

¿Qué habéis escuchado recientemente?

Actualidad

Forbes

FORBES > LIFESTYLE > TRAVEL

2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not

Suzanne Rowan Kelleher Forbes Staff

I write about travel trends and news you can use.

Follow

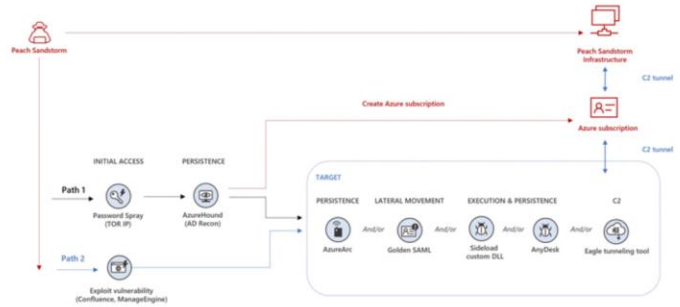
4 Sep 14, 2023, 01:25pm EDT

The House Loses: Caesar's Entertainment paid a ransom after being cyberattacked. GETTY

Within weeks, two of the world's largest casino-hotel companies—MGM Resorts and Caesars—were hit with ransomware attacks. One met the hackers' demands, while the other is resisting.

Iranian Nation-State Actors Employ Password Spray Attacks Targeting Multiple Sectors

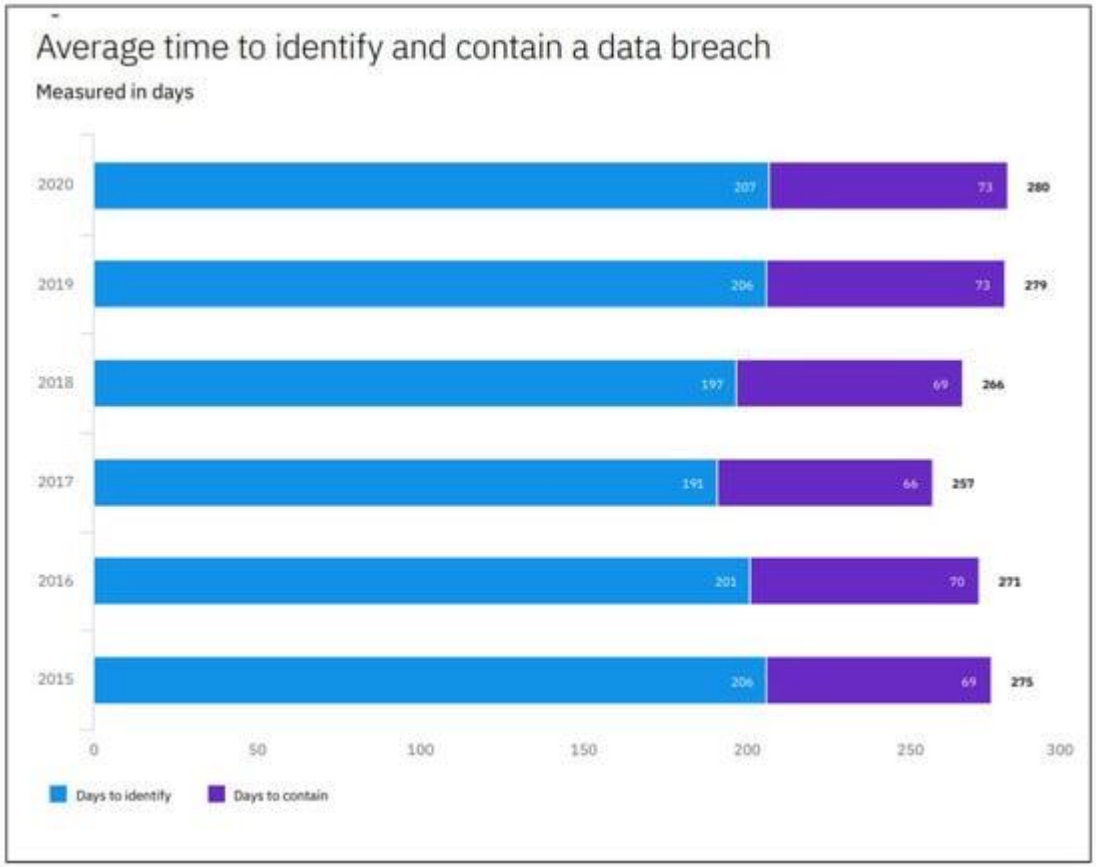
Sep 15, 2023 THN Cyber Attack / Password Security



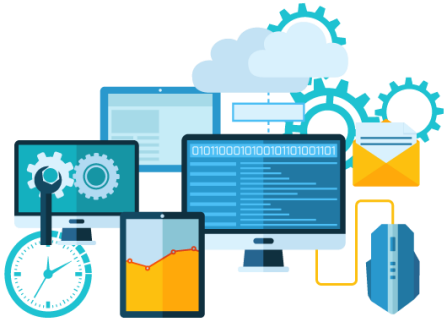
Chinese Redfly Group Compromised a Nation's Critical Grid in 6-Month ShadowPad Campaign

Sep 12, 2023 THN Critical Infrastructure Security

Tiempo medio de intrusión



¿Quiénes pueden ser víctimas?



APTs a la orden del día

Y ahora… ¿Qué pensáis vosotros?

¿Qué técnicas de ataque utilizan?

¿Quién puede estar detrás?

¿Cómo creéis que se realiza un ataque dirigido?

Ataques entre naciones

Ataques más sofisticados

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses

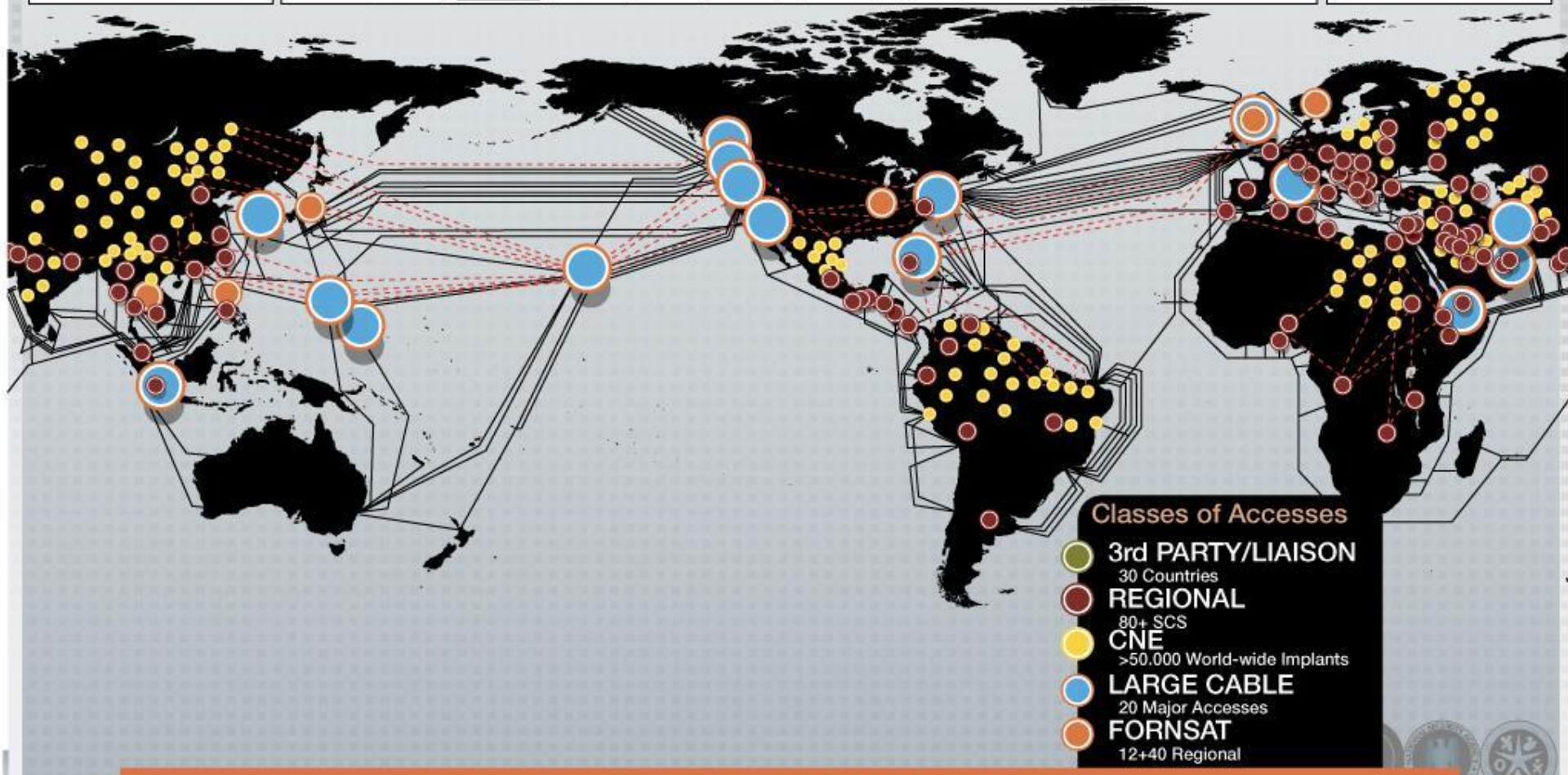
20 Access Programs Worldwide

Regional

[redacted]	Caracas	Havana	[redacted]	Kinshasa	Sofia	[redacted]	Berlin	[redacted]	Pristina	Guatemala City	[redacted]
[redacted]	Tegucigalpa	Panama City	[redacted]	Lusaka	[redacted]	Bangkok	[redacted]	[redacted]	Tirana	[redacted]	RESC
Geneva	Bogota	[redacted]	[redacted]	[redacted]	[redacted]	New Delhi	[redacted]	Phnom Penh	[redacted]	[redacted]	[redacted]
Athens	Mexico City	[redacted]	[redacted]	Budapest	[redacted]	[redacted]	Frankfurt	Sarajevo	[redacted]	[redacted]	Milan
Rome	Brasilia	[redacted]	[redacted]	Prague	[redacted]	Paris	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Quito	Managua	[redacted]	Lagos	Vienna	Rangoon	[redacted]	[redacted]	[redacted]	La Paz	[redacted]	Langley
San Jose	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Zagreb	[redacted]	[redacted]	Vienna Annex	Reston

FORNSAT

STELLAR	INDRA
SOUNDER	IRONSAND
SNICK	JACKKNIFE
MOONPEN	CARBOY
NY	TIMBERLIN
LADYLOVE	E



Ataques más sofisticados

Y ahora… ¿Qué pensáis vosotros?

¿Creéis que se podría desarrollar una guerra en Internet?

¿Necesita el estado capacidades ofensivas?

¿Qué riesgos tenemos como ciudadanos?

¿Sería posible paralizar un país?

1. Actualidad
2. Principios básicos
3. Ataques y atacantes
4. Principales riesgos

¿Hackers?

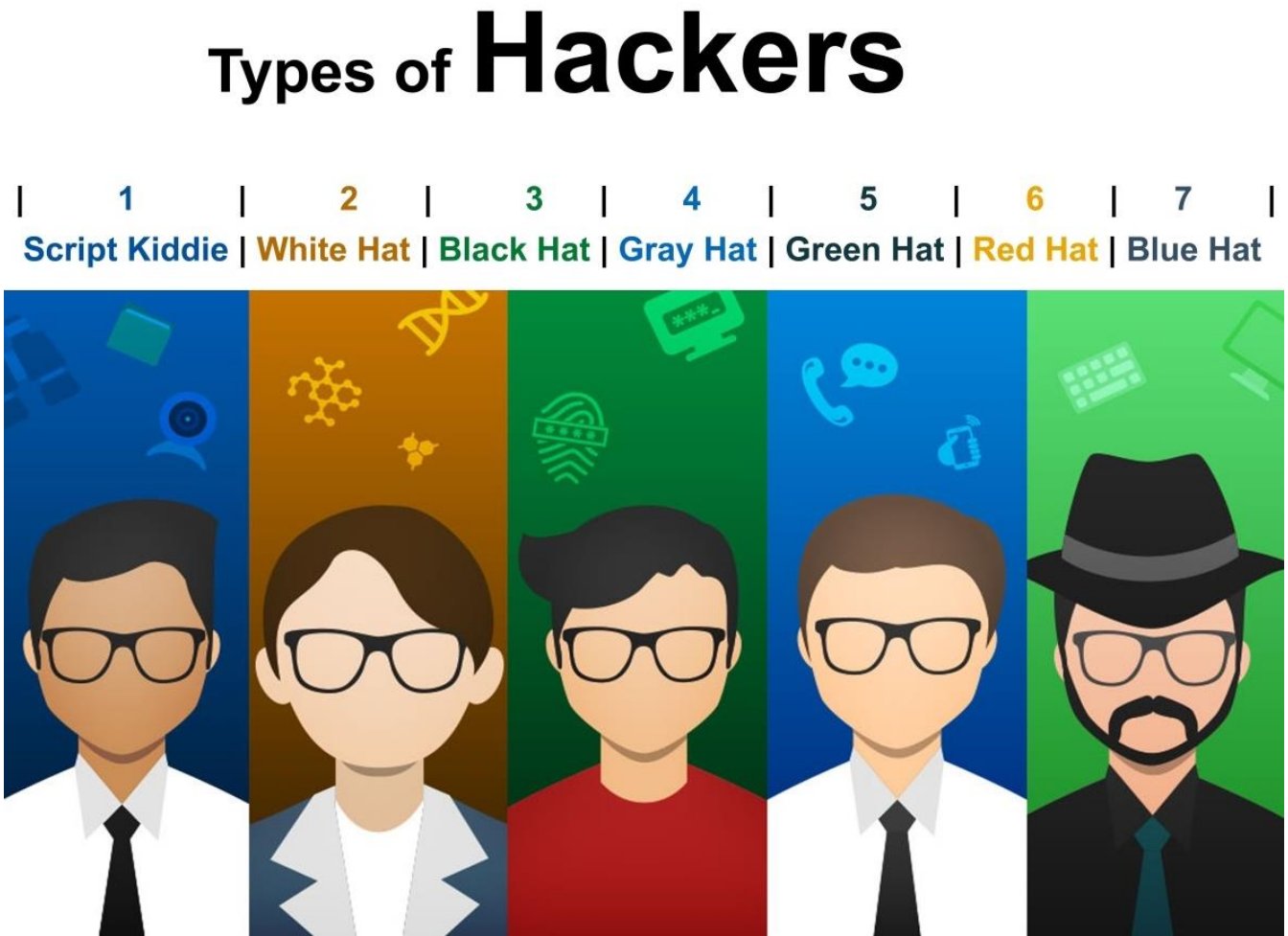
BlackHat

Intrusiones no autorizadas
Incrementar beneficios
Carecen de ética
Cibercriminales

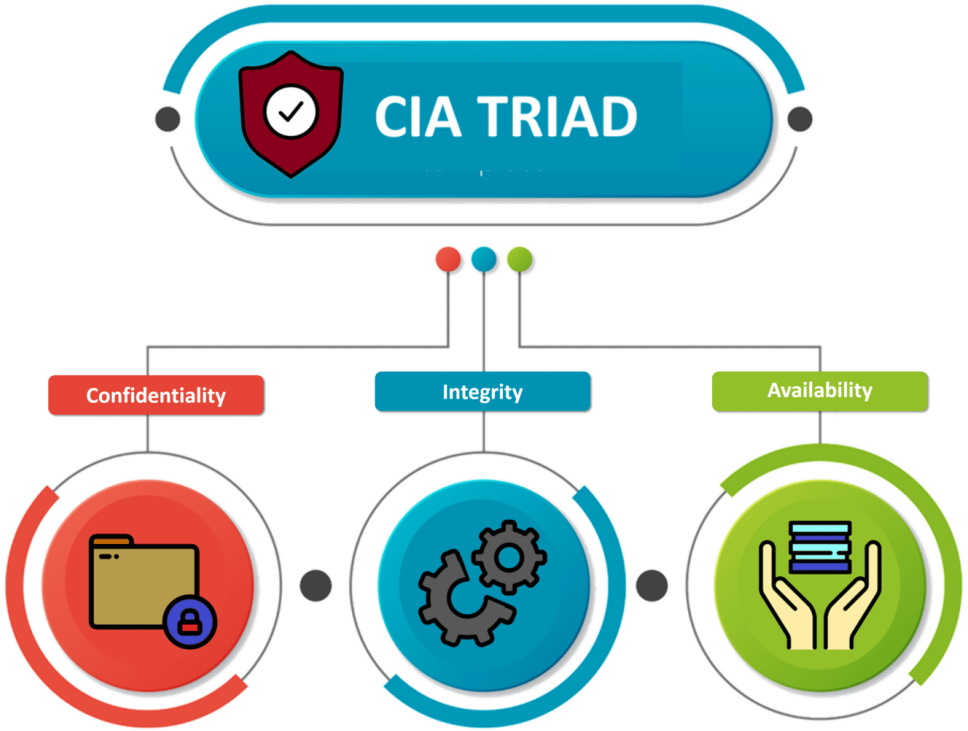
WhiteHat

Intrusiones autorizadas
Incrementar la seguridad
Investigadores de seguridad
Preocupación

¿Hackers?


Types of Hackers
1 | 2 | 3 | 4 | 5 | 6 | 7
Script Kiddie | White Hat | Black Hat | Gray Hat | Green Hat | Red Hat | Blue Hat

Confidencialidad, Integridad y Disponibilidad (CIA)



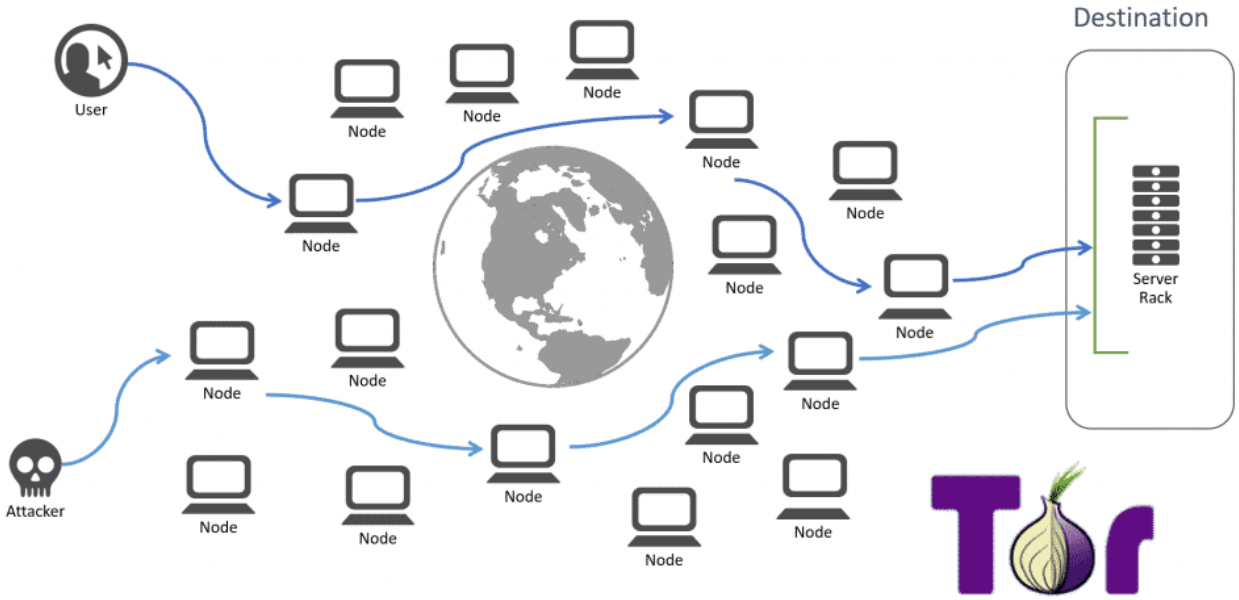
Confidencialidad, Integridad y Disponibilidad (CIA)

El significado de cada uno de estos atributos es el siguiente:

- **Confidencialidad**: Evitar que personas no autorizadas puedan acceder a la información.
- **Integridad**: Guardar la totalidad de la información, cuyo contenido debe permanecer inalterado amenos que sea modificado por personal autorizado.
- **Disponibilidad**: La información y los recursos relacionados estén disponibles para el personal autorizado.

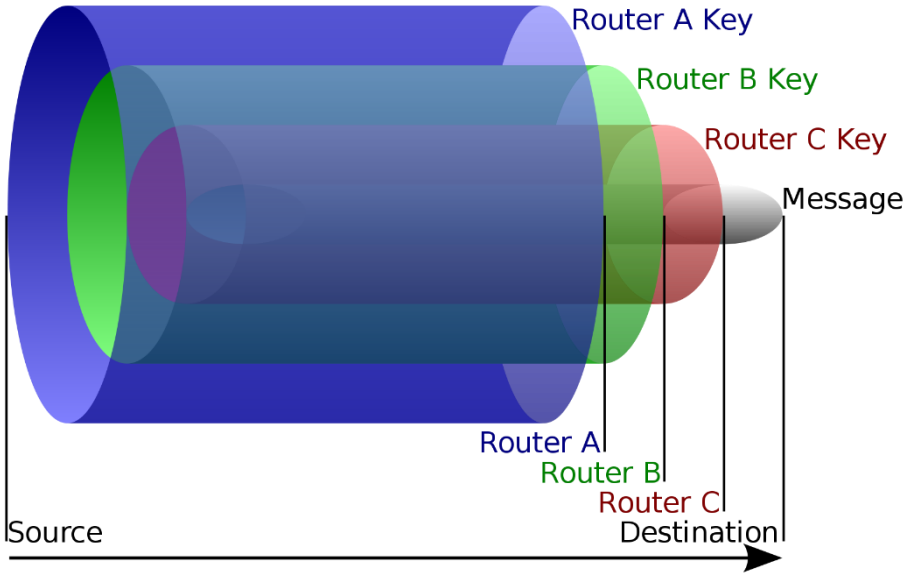
Anonimato en la red

En la actualidad existen multitud de proyecto que permiten mantener el anonimato en la red (‘no siempre se es tan anónimo como se piensa…’). Una de las mas conocidas es la red TOR.



Anonimato en la red

Para mantener la seguridad dentro de la red TOR, por cada equipo se aplica una capa de cifrado. De esta forma únicamente el ultimo nodo (Nodo de salida) conoce el texto en claro.



1. Actualidad
2. Principios básicos
3. Ataques y atacantes
4. Principales riesgos

Ataque dirigido

Se da cuando el atacante sigue un proceso especifico para lograr acceso a la entidad, buscando para ello los vectores de acceso necesarios.

Ataque no dirigido

Consiste en un ataque desarrollado sin un objetivo fijo, y que normalmente busca afectar al mayor número posible de víctimas. Un ejemplo podría ser el despliegue de una botnet.

Tipología de atacantes

Aunque las tipologías son genéricas se podrían definir en:

- Estados
- Cibercriminales
- Hacktivistas
- Ciberterroristas

- Organizaciones privadas
- Empleados internos
- Investigadores
- Script kiddies

- Ataque dirigido: Control de infraestructuras, Sabotaje, Espionaje, …
- Ataque no dirigido: Robo de dinero, control de sistemas, …

1. Actualidad
2. Principios básicos
3. Ataques y atacantes
4. Principales riesgos

Principales riesgos según ENISA

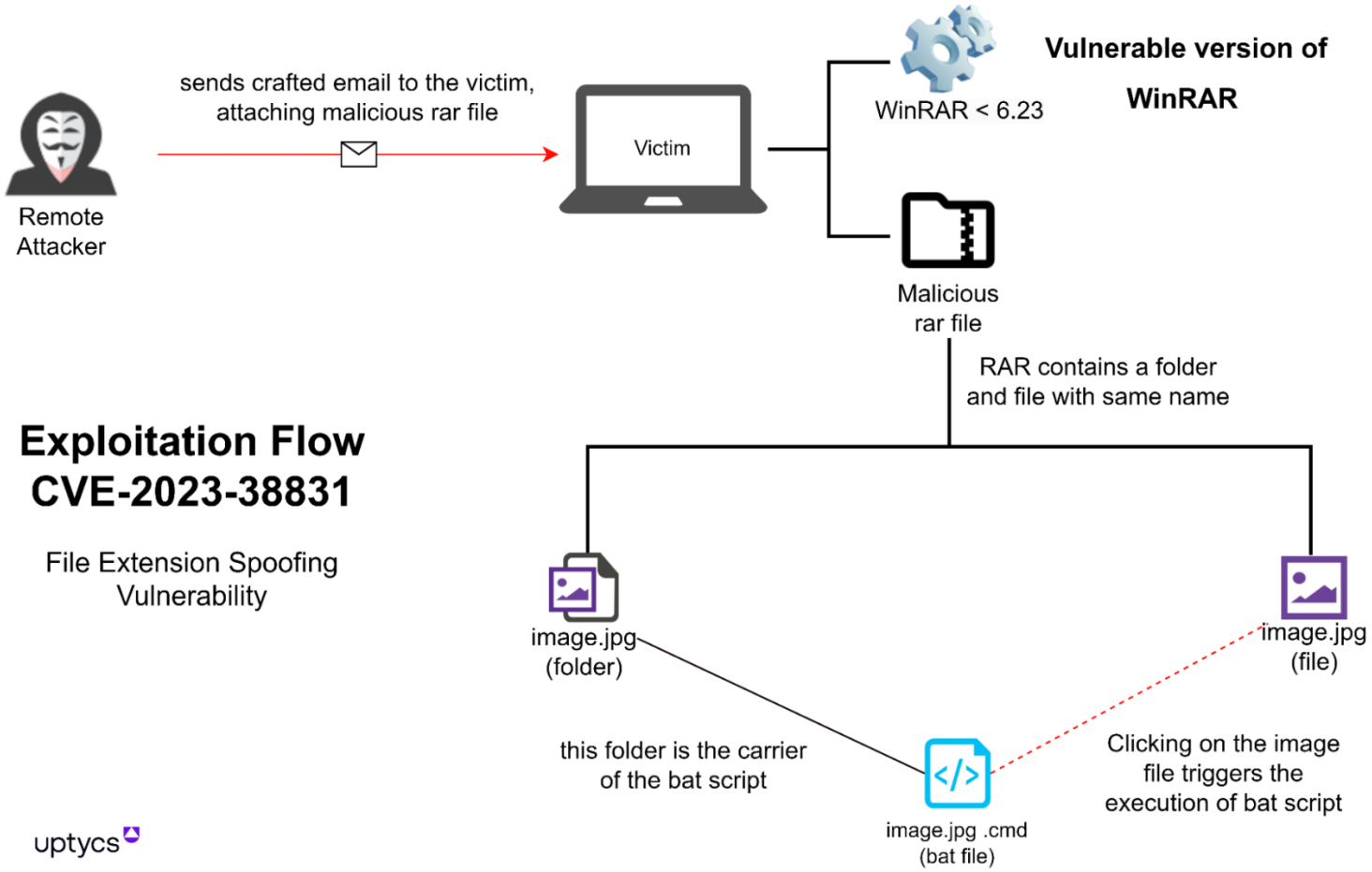
Exploits

Fragmento de software, de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema.

Exploits Públicos

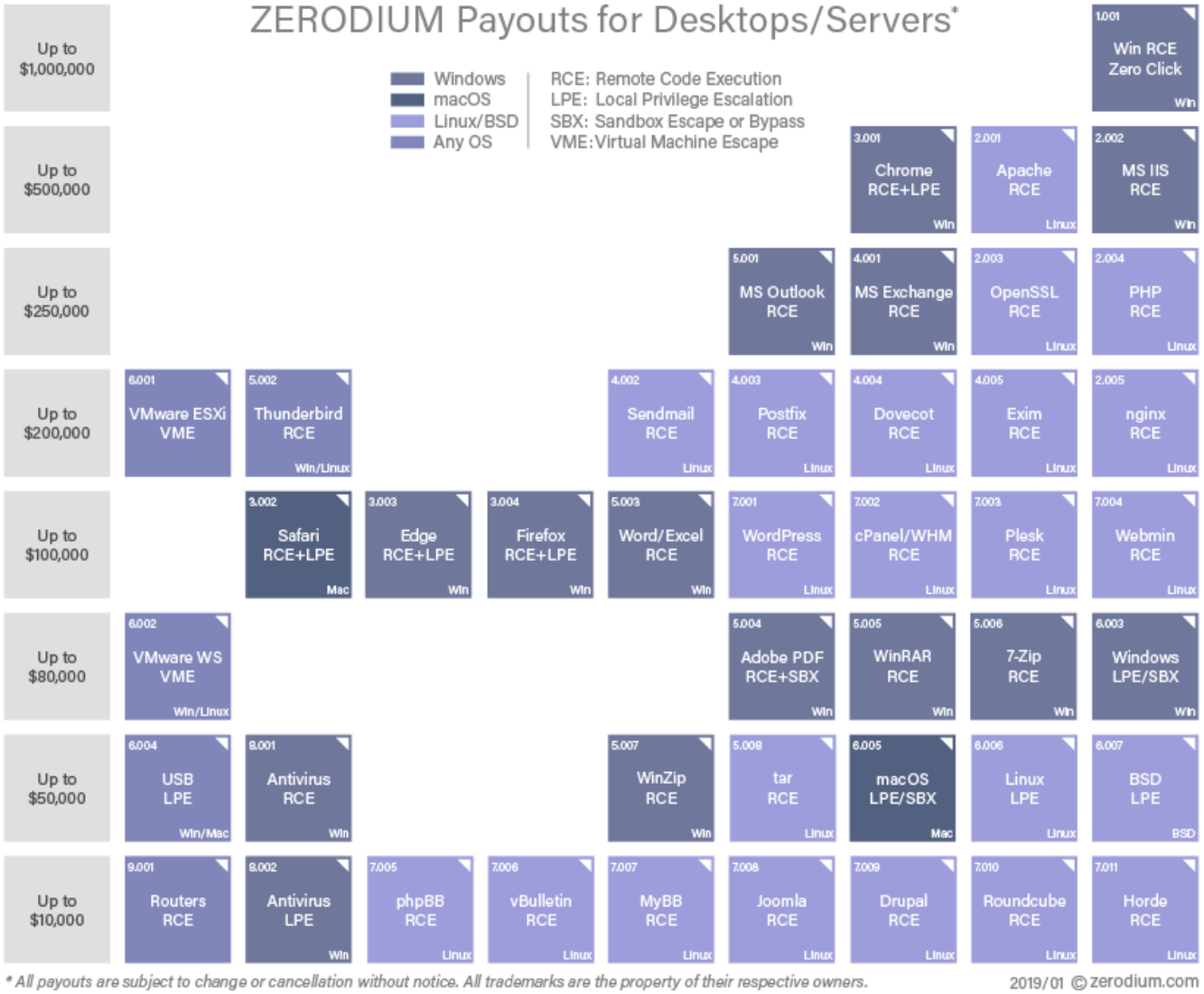
Exploits Privados

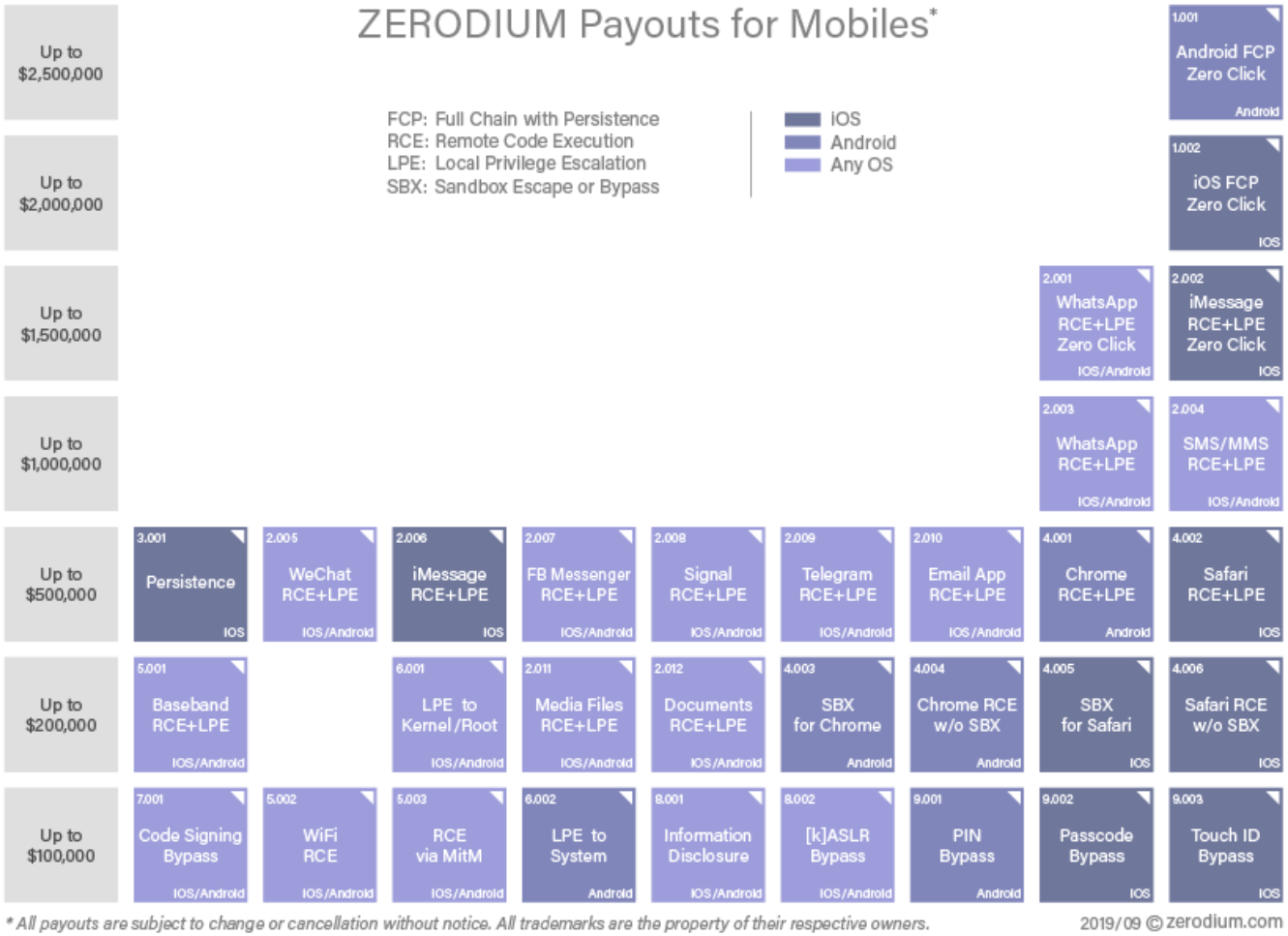
Ejemplo de exploit (WinRAR – CVE-2023-38831)



Venta de exploits

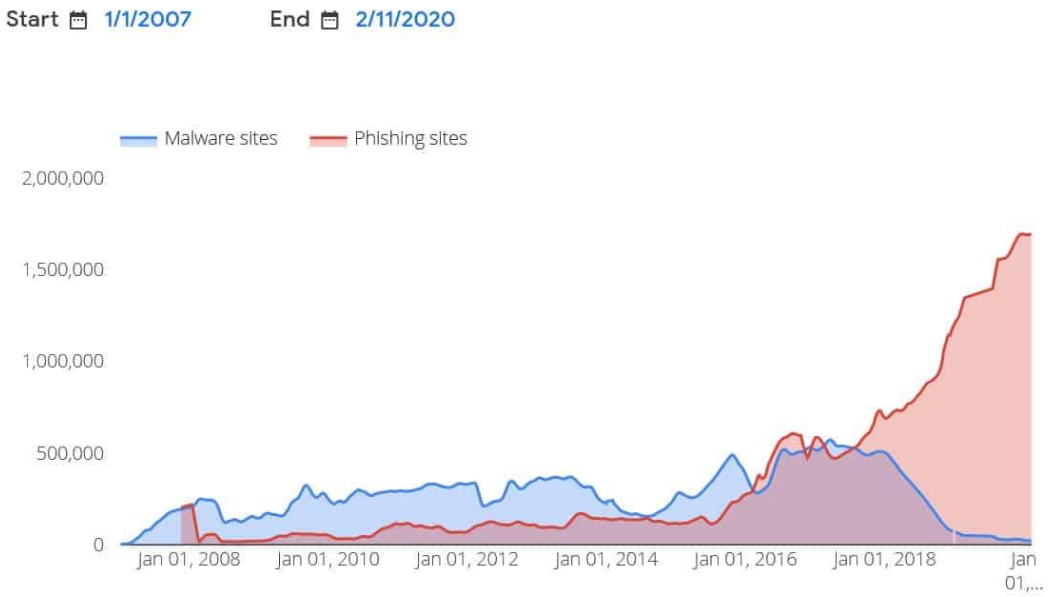
Organizaciones como Zerodium hacen de intermediarios en la compra/venta de exploits, sin importar quien compra o vende.


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com


ZERODIUM Payouts for Mobiles*
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $2,500,000
Up to $2,000,000
Up to $1,500,000
Up to $1,000,000
Up to $500,000
Up to $200,000
Up to $100,000
1.001 Android FCP Zero Click Android
1.002 iOS FCP Zero Click iOS
2.001 WhatsApp RCE+LPE Zero Click iOS/Android
2.002 iMessage RCE+LPE Zero Click iOS
2.003 WhatsApp RCE+LPE iOS/Android
2.004 SMS/MMS RCE+LPE iOS/Android
3.001 Persistence iOS
2.005 WeChat RCE+LPE iOS/Android
2.006 iMessage RCE+LPE iOS
2.007 FB Messenger RCE+LPE iOS/Android
2.008 Signal RCE+LPE iOS/Android
2.009 Telegram RCE+LPE iOS/Android
2.010 Email App RCE+LPE iOS/Android
4.001 Chrome RCE+LPE Android
4.002 Safari RCE+LPE iOS
5.001 Baseband RCE+LPE iOS/Android
6.001 LPE to Kernel/Root iOS/Android
2.011 Media Files RCE+LPE iOS/Android
2.012 Documents RCE+LPE iOS/Android
4.003 SBX for Chrome Android
4.004 Chrome RCE w/o SBX Android
4.005 SBX for Safari iOS
4.006 Safari RCE w/o SBX iOS
7.001 Code Signing Bypass iOS/Android
5.002 WiFi RCE iOS/Android
5.003 RCE via MitM iOS/Android
6.002 LPE to System Android
8.001 Information Disclosure iOS/Android
8.002 [k]ASLR Bypass iOS/Android
9.001 PIN Bypass Android
9.002 Passcode Bypass iOS
9.003 Touch ID Bypass iOS
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/09 © zerodium.com

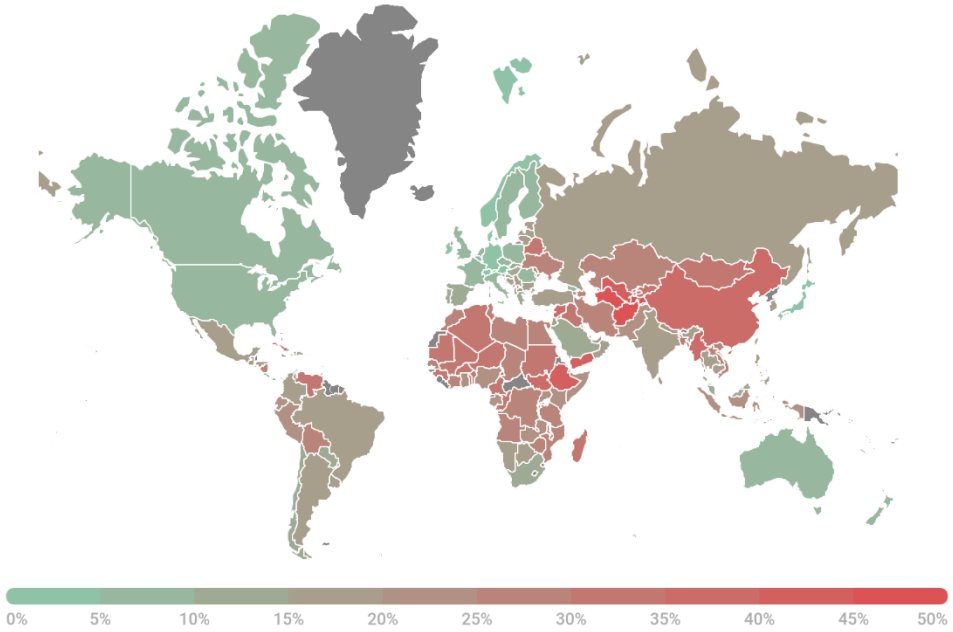
Malware

Aunque cada vez existe mas malware, realmente el número de muestras nuevas va disminuyendo. Cada vez se reutiliza más código y malware desarrollado previamente, asi como aumenta el número de ataques mediante el uso de phishing.



Distribución de malware

También cabe destacar las diferencias respecto de dispositivos comprometidos de media por país. Se muestra a continuación un gráfico de la marca de Antivirus Kaspersky.



Tipos de malware

Rootkit

ADware

Spyware

Bot

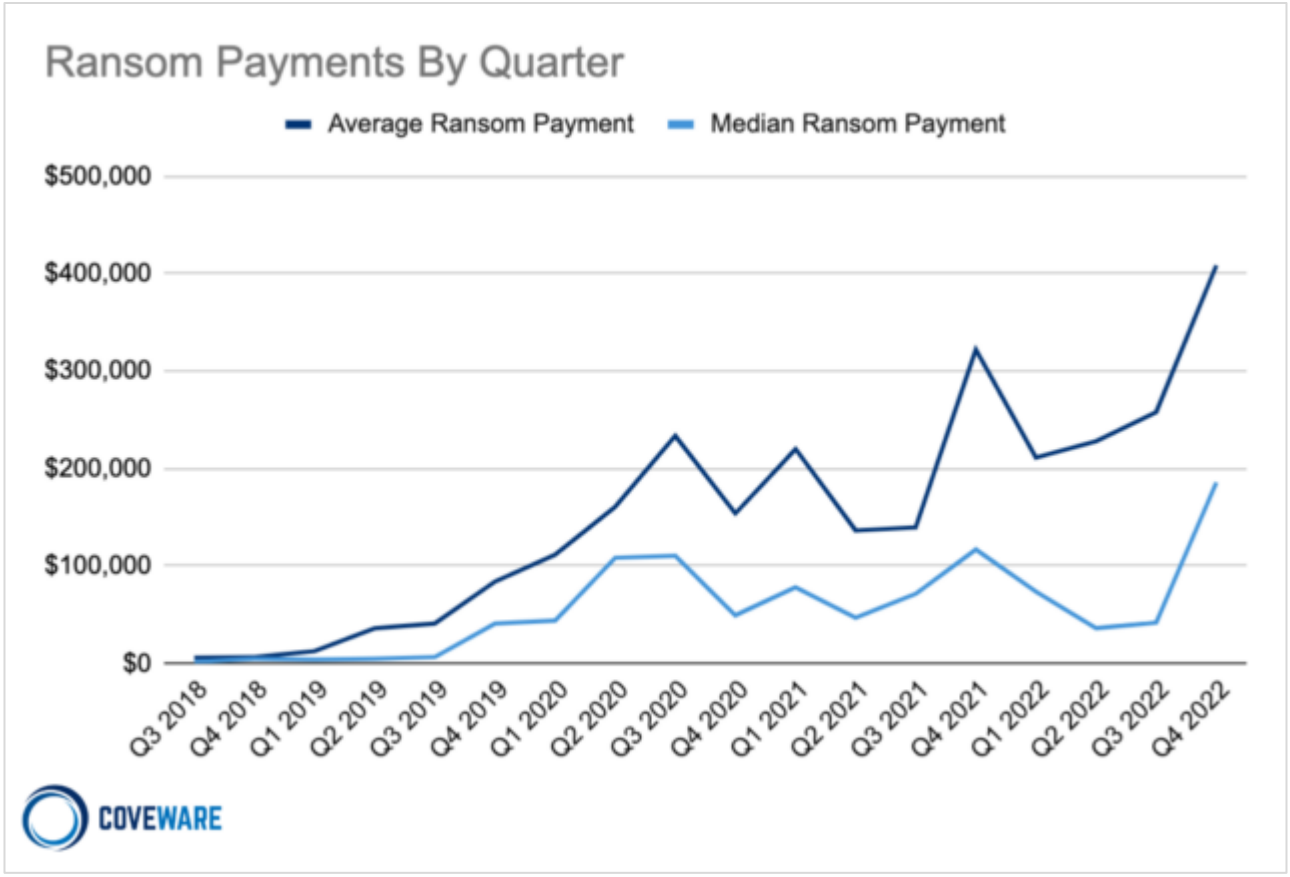
Troyano

Ransomware

Virus

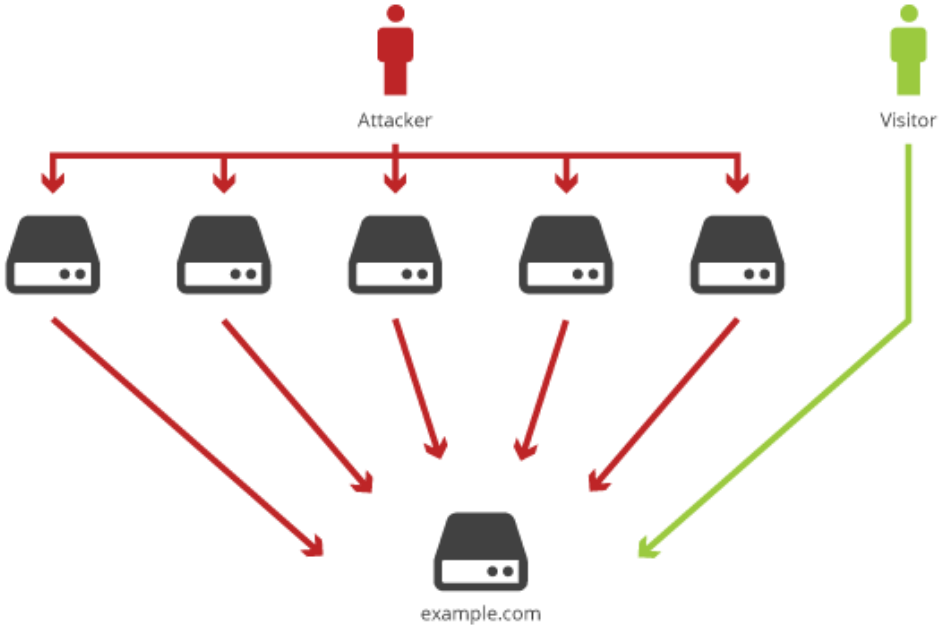
Gusano

Cifras del ransomware

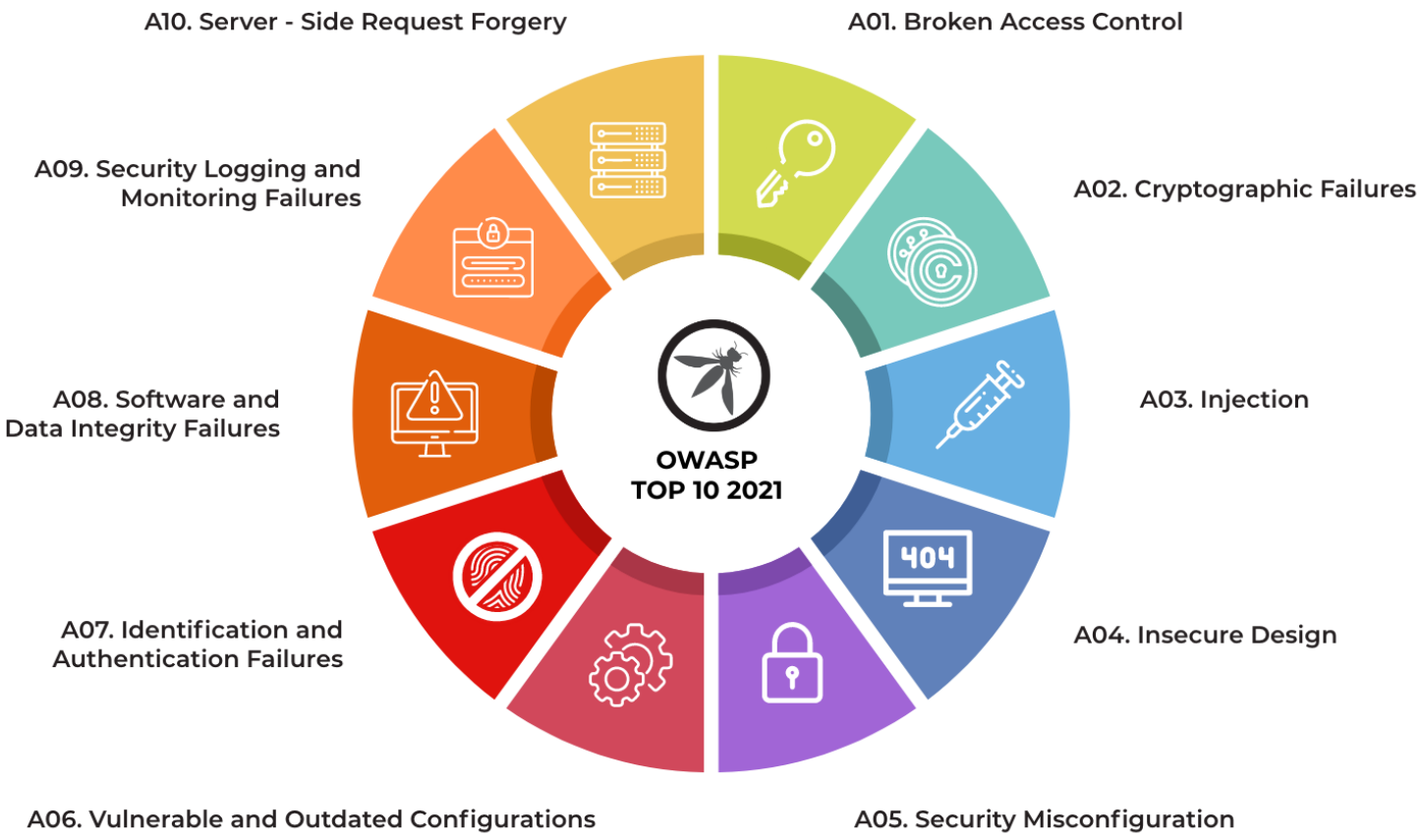


Ataques de denegación de servicio

Uso de gran cantidad de equipos para saturar los recursos de determinados servidores a través de la realización a múltiples conexiones.

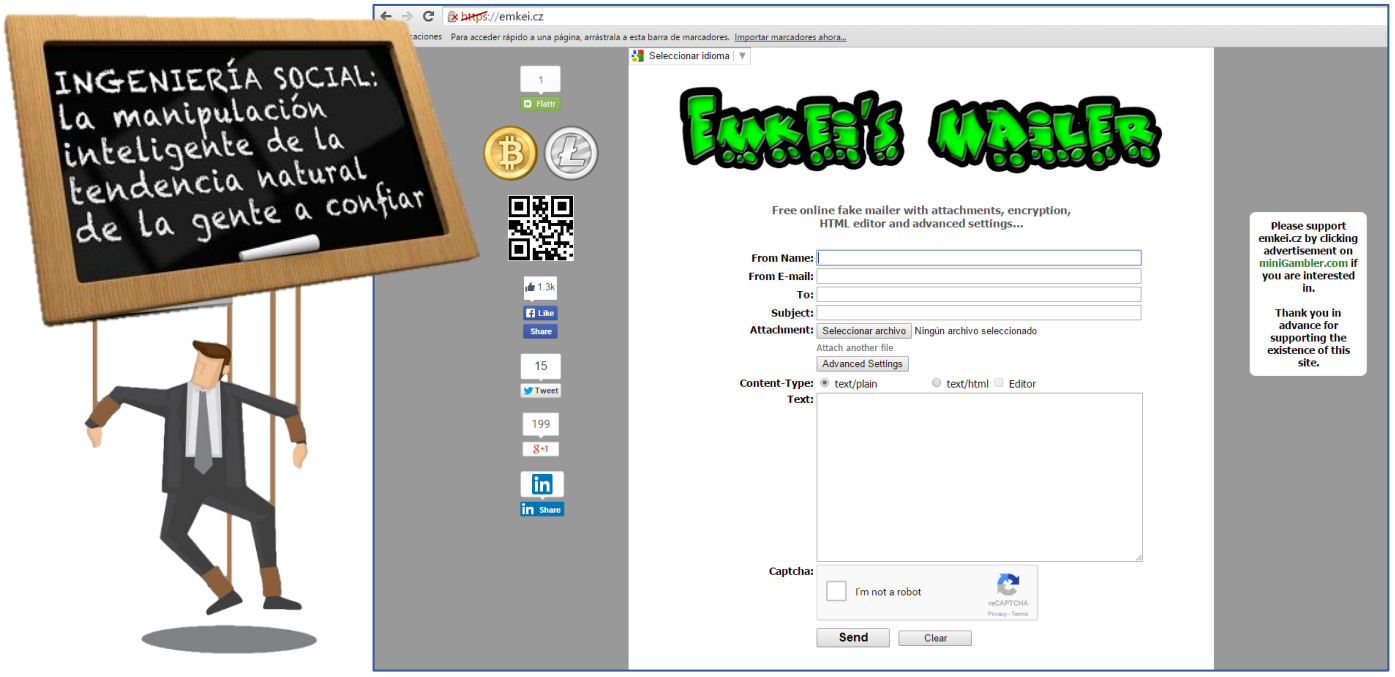


Ataques en aplicaciones Web



Phishing

Envío de correo electrónico con el objetivo de forzar a la victima a realizar una determinada acción a través del uso de ingeniería social.



Vishing

Consiste en la suplantación de un tercero en una llamada con el objetivo de lograr información sensible o lograr acceso a un sistema mediante la ayuda de la víctima.

IA en Ingeniería Social (DeepFake)

Gracias al uso de Inteligencia Artificial, hoy en día están siendo automatizados escenarios de Ingeniería social tales como llamadas telefónicas, video conferencias, etcétera.

Uso de IA para el desarrollo de intrusiones