



Unidad 10: AMENAZAS Y CIBERATAQUES

BLOQUE III – Redes e
Internet

CONTENIDOS

1. Principales amenazas en la actualidad.
2. Tipos de atacante.
3. Fases de un ataque.
4. Tipos de ataque y patrones.

1. Principales amenazas en la actualidad



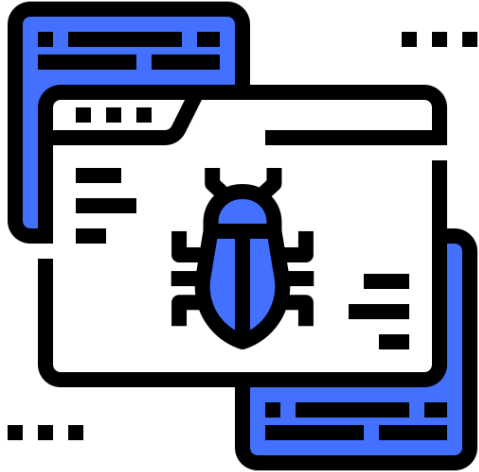
1. Principales amenazas en la actualidad



Asignaturas completas: **Bases de datos, Seguridad en Bases de datos, Redes avanzadas y computación en la nube, Desarrollo web seguro, etc.**

1. Malware

- El software malicioso existe prácticamente desde que existen los computadores (Creeper en ARPANET).
- Se trata de un software o fragmento de código, que se hace pasar por una aplicación “normal” o que de alguna manera se incluye en una de ellas.
 - En algunos casos el malware es independiente y en otros casos necesita de un software que lo aloje o albergue.
- Los objetivos del malware, sus vectores de infección, sus mecanismos de replicación y propagación así como su forma de ocultarse/defenderse son casi infinitos.



Adware
Troyano
LogicBomb Worm
Virus Spyware
Rootkit Backdoor
Gusano

1. Malware

- ¿Por qué existe el malware?

Motivos económicos

Motivos militares/sociopolíticos

Motivos personales
(reputación,
entretenimiento)

Plataforma para
realizar otros ataques y
repetición (anonimato,
botnets, ataques
distribuidos)

1. Malware

- Hoy en día podemos encontrar que la difusión de un malware es completamente aleatoria pero también puede ser dirigida a un individuo o conjunto de individuos muy concretos.
 - Ataques a una infraestructura, a una organización, a un país.
- Hablaremos de las APTs (Advanced Persistent Threats) más adelante.
 - Intentaré que tengáis un seminario específico sobre este tema antes de terminar el cuatrimestre.

1. Malware

Virus

- Fragmento de código que necesita de un software “host” que lo aloje.
- Los vectores de infección son múltiples: ingeniería social, descarga de un fichero, visita a una web, USB, email, etc.
- Tiene capacidad de replicación.
- Necesita de intervención humana para propagarse.

1. Malware

- Virus que infectan ficheros (los más sencillos/tradicionales).
 - Por infección directa cuando se ejecuta el virus.
 - Sobre-escritura.
 - Renombrado.
 - Parasitando.
 - Por residencia en memoria.
 - En este caso los mecanismos de infección son los mismos pero el virus espera residente en memoria y la infección se produce cuando el host se ejecuta.
- Cuidado con el malware “sin ficheros” (file-less).

1. Malware

Worm/gusano

- Software con entidad propia.
- Tiene capacidad de replicación.
- Tiene capacidad de propagación a través de la red sin necesidad de intervención humana, el vector de infección siempre está relacionado con la conexión a la red.
- Casi siempre aprovechan vulnerabilidades de las aplicaciones y/o del SO.

1. Malware

Troyano

- Software autónomo que se camufla en/como aplicaciones o ficheros “normales”.
- En muchos casos se propagan junto con gusanos.
- Su principal objetivo es ocultarse y proporcionar acceso no autorizado al sistema infectado (RAT: Remote Access Trojan), funcionalidad de backdoor.
- Casi siempre incorporan spyware. El troyano bancario es el que más preocupa ahora.

1. Malware

Spyware

- Malware cuya funcionalidad es espiar al usuario/equipo infectado.
- Suelen incorporar keyloggers, grabadores de escritorio, etc.

Adware

- En este caso la funcionalidad es mostrar publicidad.

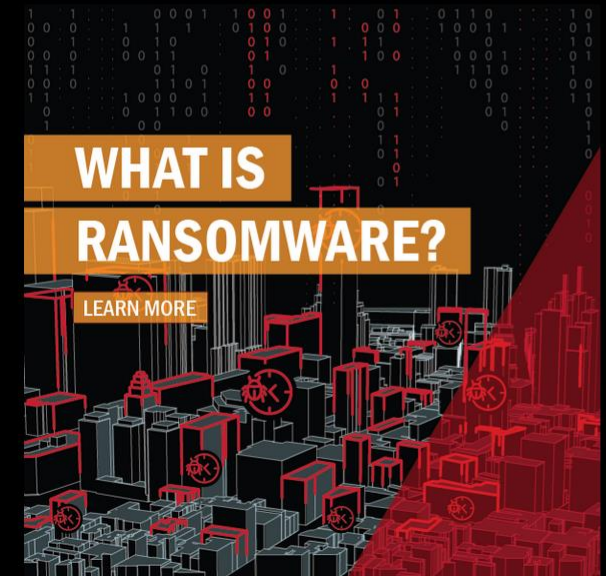
Ransomware

- Malware que cifra los archivos del sistema infectado para chantajear a su propietario si los quiere recuperar.

The State of Ransomware 2021

Sophos' annual ransomware survey delivers fresh new insights into the experiences of mid-sized organizations across the globe. It explores the prevalence of attacks, as well as the impact of those attacks on victims, including year-on-year trends. This year, for the first time, the survey also reveals the actual ransom payments made by victims, as well as the proportion of data victims were able to recover after they had paid.

A Sophos Whitepaper, April 2021



2023

1. Malware

Rootkit

- Conjunto de mecanismos y herramientas que proporcionan el nivel de privilegio máximo a un usuario en un sistema.
- Por lo tanto, control completo desde el hardware y el sistema operativo.
- Es el malware más peligroso por su potencial impacto y por su dificultad de detección.

1. Malware

- El malware también puede clasificarse en función de la comunicación que establece con el atacante y en función del control que éste ejerce sobre los sistemas infectados.



1. Malware

- Un malware que no se puede controlar de forma remota y permanece silencioso suele ser mucho más difícil de detectar.
 - Pero el atacante no puede reaccionar en tiempo real, todo tiene que programarse en el malware y además no se puede utilizar para robar datos.
- Suele ser el malware pensado para destruir de alguna manera.
- El que es silencioso pero se puede controlar (por IRC, P2P o conexión directa) suele utilizarse dentro de botnets.

1. Malware

- Cuando uno de los objetivos del malware sea robar datos o información, no podrá ser silencioso.
- En estos casos que el malware se pueda controlar o no depende de sus objetivos adicionales.
- El malware más sofisticado suele permitir comunicación y control, pero debe estar muy bien programado para que no se pueda detectar.

1. Malware

- Vectores de infección típicos para el malware actual:
 - Vulnerabilidades del SO y del software.
 - Medios físicos (USB, etc.)
 - Email/spam, redes sociales.
 - Compartición de ficheros y redes P2P.
 - Servidores web comprometidos, URLs maliciosas.

1. Malware

- Cada pieza de malware emplea sus propios mecanismos de persistencia, que le permiten ocultarse durante el mayor tiempo posible en el sistema víctima, y de auto-defensa (para evitar que se investigue sobre su código, por ejemplo).
 - Cifrado.
 - Polimorfismo y mutación.
 - Anti-disassembly.
 - Anti-debbug.

1. Principales amenazas en la actualidad

- Del resto de amenazas ya hemos hablado en la asignatura o iremos hablando poco a poco.
- También se investiga acerca de amenazas concretas para entornos muy específicos.
- Por ejemplo, para amenazas web está el Top10 de OWASP.
 - Hay listados equivalente para entornos móviles, cloud, IoT, etc.

T10

OWASP Top 10 Application Security Risks – 2017

6

A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

10, DEBUT 2022-2023

<https://owasp.org/www-project-top-ten/>

2017

2021

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

1. Principales amenazas en la actualidad

- Independientemente del contexto en el que se trabaje, conviene conocer el modelo de amenazas STRIDE propuesto por Microsoft y muy extendido.
 - Spoofing (suplantación de identidad).
 - Tampering (manipulación)
 - Repudiation (repudio).
 - Information disclosure (filtración de información sensible).
 - Denial of service (denegación de servicio).
 - Elevation of privilege (escalado de privilegios).

1. Principales amenazas en la actualidad

Amenaza	Pilar de la seguridad
Spoofing	Todos
Tampering	Integridad
Repudio	No repudio
Filtración de información	Confidencialidad
Denegación de servicio	Disponibilidad
Escalado de privilegios	Control de acceso

2. Tipos de atacante

- Ya hemos hablado en la asignatura de la fuerte motivación económica que suele mover a la mayor parte de los atacantes en casi todos los contextos.
 - Sea individual, colectiva (mafias y bandas criminales) o incluso geo-estratégica.
- Pero también existen otras motivaciones reputacionales, políticas, etc.
- En general, intentemos evitar el término “hacker” con la connotación negativa habitual.

2. Tipos de atacante

- Ya hemos hablado en la asignatura de la fuerte motivación económica que suele mover a la mayor parte de los atacantes en casi todos los contextos.
 - Sea individual, colectiva (mafias y bandas criminales) o incluso geo-estratégica.
- Pero también existen otras motivaciones reputacionales, políticas, etc.
- En general, intentemos evitar el término “hacker” con la connotación negativa habitual.

Black Hat hackers, ciber-criminales o delincuentes

- Atacantes que aprovechan las vulnerabilidades de los sistemas con diferentes objetivos, que normalmente vulneran la ley, y que tienen en común sus altos conocimientos y que no revelan las vulnerabilidades descubiertas a los administradores dadas sus malas intenciones.

White Hat hackers, hackers éticos, investigadores o consultores

- Atacantes que informa siempre de las vulnerabilidades descubiertas y que incluso pueden colaborar en su subsanación. Suelen ser profesionales de la "seguridad ofensiva" o expertos interesados en hacer avanzar el conocimiento.

Script kiddies

- Atacantes aficionados sin nivel suficiente de conocimientos técnicos que utilizan herramientas automáticas y recetas cuyo funcionamiento y consecuencias desconocen.

Crackers

- Atacantes que se centran en romper los sistemas criptográficos, por lo tanto, con altos conocimientos en matemáticas y algoritmia.

3. Fases de un ataque

Recogida de información

Construcción

Repetición

Obtención de resultados

Anonimato

3. Fases de un ataque

○ **Recogida de información: Footprinting**

- Se pretende obtener, de manera legal, la huella identificativa o footprint (toda la información posible) de la red, sistema o usuario objetivo del ataque.
- La primera etapa consiste en recuperar información general del objetivo en los medios públicos.
- Para esto, suele recurrirse a consultar en y a investigar los metadatos de la documentación públicamente accesible.
 - Pero también a redes sociales, prensa, el BOE, etc.
- Últimamente se habla de OSINT: Open Source Intelligence.

3. Fases de un ataque

Buscadores

Metadatos

Redes
sociales

Ing. social

Existen buscadores específicos muy útiles para esta fase:

SHODAN - Computer Sea x

www.shodanhq.com

Shodan Exploits Scanhub Maps Blog Anniversary Promotion

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR FREE SIGN UP

Popular Search Queries: Router w/ Default Info - Routers that give their default username/ password as admin/1234 in their banner.

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

Shodan pinpoints shoddy industrial controls.
The Register

It greatly lowers the technical bar needed to canvas the Internet...
threatpost

'Shodan for Penetration Testers' presented at DEF CON 18
DEFCON

It's a reminder to many to know what's on your network...
darkREADING

Shodan is the Google for hackers.
2DNet

Shodan vereinfacht die Suche nach SCADA-Systeme erheblich...
heise online

Firmen öffnen Stuxnet und Co. selbst die Tür.
CIO

Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.
AARGAUER ZEITUNG

Services

HTTP	6,677
HTTP Alternate	5,461
HTTP	366
SNMP	192
SMB	111

Top Countries

United States	1,991
Germany	1,897
Korea, Republic of	1,066
Italy	893
Hungary	605

webcam 7

70.89.172.86
Comcast Business Communications
Added on 25.05.2014

 Denver

70.89.172.86-Busname-
CO.hfc.comcastbusiness.net

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7805
Cache-control: no-cache, must revalidate
Date: Sun, 02 Mar 2014 01:37:08 GMT
Expires: Sun, 02 Mar 2014 01:37:08 GMT
Pragma: no-cache
Server: webcam 7

89.133.255.106

UPC Hungary
Added on 25.05.2014




catv-89-133-255-106.catv.broadband.hu

HTTP/1.0 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002

50.152.101.201

Comcast Cable
Added on 25.05.2014

 Red Lion

c-50-152-101-201.hsd1.pa.comcast.net

HTTP/1.0 401 Authorization Required
Connection: close
Server: Android Webcam Server v0.1
WWW-Authenticate: Basic realm="IP Webcam"
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: -1
Access-Control-Allow-Origin: *
Content-Type: text/html

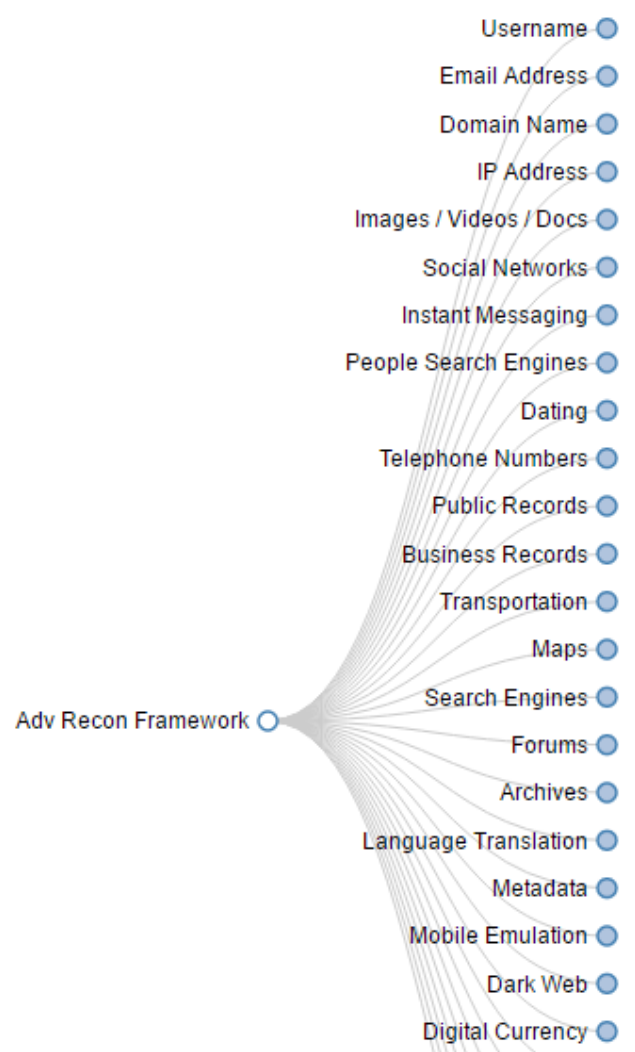
121.100.70.204

Gyounggidongbu cable tv co., Ltd.
Added on 25.05.2014

 Hanam

HTTP/1.0 401 Authorization Required
Connection: close
Server: Android Webcam Server v0.1
WWW-Authenticate: Basic realm="IP Webcam"
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: -1
Access-Control-Allow-Origin: *
Content-Type: text/html

Advanced Reconnaissance Framework



3. Fases de un ataque

- **Recogida de información: Fingerprinting**
 - Se trata de una recogida de datos más específicos que permiten recopilar información sobre toda la pila TCP/IP de una red o sistema concreto. Es decir:
 - Topologías, direcciones y nombres a diferentes niveles, estado de puertos, versiones y estado de actualización de software y parches de SO, listados de vulnerabilidades, contraseñas, etc.
 - En este caso, la información no es pública y se suele conseguir utilizando técnicas y herramientas específicas.
 - Alegales o ilegales en muchos casos.

3. Fases de un ataque

Ingeniería
social y
phishing

Sniffing

Mapping

Scanning

3. Fases de un ataque

- **Construcción, repetición y obtención de resultados**
 - Estudiaremos los diferentes tipos de ataque que se conocen en la actualidad y discutiremos algunos patrones en la siguiente sección de esta unidad.
 - La repetición no siempre es necesaria, se busca la persistencia cuando se desea mantener el ataque en el tiempo, pero esto depende mucho del patrón empleado y de los objetivos del atacante.

3. Fases de un ataque

- Anonimato

Anonimato físico

Anonimato por uso de bouncer

Anonimato por uso de proxy

3. Fases de un ataque

- Los atacantes buscan el anonimato para evitar consecuencias legales, para dificultar la atribución y para que las víctimas no puedan aprender sobre sus técnicas.
- En el primer caso, anonimato físico, se consigue proteger la identidad del atacante porque éste accede a la red desde un lugar público, desde un cibercafé, etc.



3. Fases de un ataque

- Para las técnicas más frecuentes son las de bouncer y proxy.
- En el primer caso el atacante toma el control sobre un sistema y lo utiliza como “puerta” de entrada para su conexión, de manera que se vea siempre como el origen de los ataques.
 - Como tiene control total sobre este sistema, puede editar todos sus registros para borrar sus huellas y hacer el rastreo imposible.
- Para convertir a una víctima en un bouncer se explota alguna de sus vulnerabilidades, normalmente con algún software malicioso como un troyano.

3. Fases de un ataque

- Un proxy es una máquina, que normalmente mediante NAT, realiza funciones de intermediación, ocultando el origen de las comunicaciones.
- La víctima del ataque verá como origen de las comunicaciones al proxy, no al atacante.



3. Fases de un ataque

- Los servidores proxy tradicionales suelen trabajar con http:
 - Si se desea lograr anonimato usando un servicio diferente al http (ftp, irc, telnet, ssh) es posible localizar un servidor proxy que cree un socket para intercambiar la información de estos servicios a través suyo.
 - Estos proxies sock, por tanto, no sólo ocultan la dirección IP del origen, sino también puertos, servicios y aplicaciones origen.
- Existen aplicaciones que manejan matrices de proxies y que permiten cambiar de servidor cada cierto tiempo construyendo complejas rutas muy difíciles de rastrear.

3. Fases de un ataque

- Muchos servidores proxy requieren de autenticación para evitar un uso malicioso.
 - Pero no siempre están protegidos adecuadamente.
 - De todas formas, los proxies corporativos mantienen un registro de todas las peticiones atendidas, lo que no permite el anonimato deseado.
- El problema es la falta de consenso en jurisdicción internacional y el vacío legal que permite que estos proxies se instalen en ciertos países sin ninguna repercusión.

3. Fases de un ataque

○ Proyecto Tor

I2P
FreeNet

Tor Project: Anonymity O x
← → ↻ <https://www.torproject.org>

Tor Home About Tor Documentation Press Blog Contact

Download Volunteer Donate

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor ↓

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

[Learn more about Tor »](#)

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

[Get involved with Tor »](#)

Recent Blog Posts

Tor Weekly News — October 1st, 2014
Wed, 01 Oct 2014 Posted by: *harmony*

Tor Browser 4.0-alpha-3 is released
Fri, 26 Sep 2014 Posted by: *mikeperry*

Tor Browser 3.6.6 is released
Thu, 25 Sep 2014 Posted by: *mikeperry*

Tails 1.1.2 is out
Thu, 25 Sep 2014 Posted by: *tails*

Tor Weekly News — September 24th...
Wed, 24 Sep 2014 Posted by: *harmony*

[View all blog posts »](#)

Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Businesses

Businesses use Tor to research

3. Repaso: Fases de un ataque

Objetivo del ataque: robo de propiedad intelectual accediendo a las copias de seguridad de la competencia

Recogida de información

Construcción

Repetición

Obtención de resultados

Anonimato

3. Repaso: Fases de un ataque

- La empresa víctima del ataque se dedica al diseño de moda y tiene externalizadas todas las funciones asociadas a las TIC.
- Mediante footprinting y fingerprinting se recopila información sobre nombres de usuario, servidores, topología de red, etc.
- A continuación se utiliza la ingeniería social para obtener información sobre las copias de seguridad de los diseños con los que se está trabajando.
 - El atacante se hace pasar por teléfono y por email por uno de los técnicos de la empresa que gestiona las TIC.
 - Mediante habilidades sociales descubre que las copias se almacenan en la nube, se tiene contratado un servicio del proveedor Amazon en un determinado centro de datos.

3. Repaso: Fases de un ataque

- Sabiendo el proveedor y el centro de datos concreto, el atacante contrata el mismo servicio que su víctima y fuerza la co-residencia de sus instancias virtuales en el mismo host físico que las de su víctima.
- A continuación aprovecha una vulnerabilidad conocida del hipervisor utilizado por este proveedor para robar la información deseada.

3. Repaso: Fases de un ataque

- El atacante realiza el ataque desde un cibercafé sin cámaras de video-vigilancia dentro del local ni un sistema de registro adecuado.
- Además aprovecha un bouncer que había conseguido previamente para lanzar el ataque.

Anonimato










4. Tipos de ataque y patrones

- **Tipos de ataque (en función de acción/objetivo)**
 - **Intercepción:** Espionaje y/o redirección de comunicaciones para tener acceso a datos a los que no se está autorizado a acceder.
 - **Fabricación:** Creación de un activo falso para engañar a un usuario.
 - **Interrupción:** Bloqueo del normal funcionamiento de un activo o de una comunicación.
 - **Modificación:** Alteración no autorizada de un activo.







4. Tipos de ataque y patrones

Según el CAPEC:

1000 - Mechanisms of Attack

- +  Engage in Deceptive Interactions - (156)
- +  Abuse Existing Functionality - (210)
- +  Manipulate Data Structures - (255)
- +  Manipulate System Resources - (262)
- +  Inject Unexpected Items - (152)
- +  Employ Probabilistic Techniques - (223)
- +  Manipulate Timing and State - (172)
- +  Collect and Analyze Information - (118)
- +  Subvert Access Control - (225)

3000 - Domains of Attack

- +  Software - (513)
- +  Hardware - (515)
- +  Communications - (512)
- +  Supply Chain - (437)
- +  Social Engineering - (403)
- +  Physical Security - (514)

Concepto de TTP: Tactics, Techniques and procedures

<https://attack.mitre.org/>

ATT&CK Matrix for Enterprise

layouts show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 18 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (2)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (3)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	Access Token Manipulation (5)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (9)	Boot or Logon Autostart Execution (12)	BITS Jobs	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (9)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Replication Through Removable Media	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (4)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Boot or Logon Initialization Scripts (9)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Encrypted Channel (2)	Endpoint Denial of Service (4)	Disk Wipe (2)
Search Closed Sources (2)	Supply Chain Compromise (3)	Software Deployment Tools	System Services (2)	Create Account (2)	Create or Modify System Process (4)	Domain Policy Modification (2)	Man-in-the-Middle (2)	Domain Trust Discovery	Taint Shared Content	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Technical Databases (3)	Trusted Relationship	System Services (2)	User Execution (2)	Create or Modify System Process (4)	Domain Policy Modification (2)	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (4)	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)	Valid Accounts (4)	Windows Management Instrumentation	Event Triggered Execution (13)	Event Triggered Execution (13)	Event Triggered Execution (13)	File and Directory Permissions Modification (2)	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
Search Victim-Owned Websites			External Remote Services	External Remote Services	Event Triggered Execution (13)	Hide Artifacts (7)	DS Credential Dumping (3)	Network Stiffing		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
			Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Password Policy Discovery		Data Staged (2)	Non-Standard Port	System Shutdown/Reboot	
			Implant Container Image	Process Injection (11)	Process Injection (11)	Indicator Removal on Host (4)	Steal or Forge Kerberos Tickets (4)	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling		
			Office Application Startup (4)	Scheduled Task/Job (6)	Scheduled Task/Job (6)	Indirect Command Execution	Steal Web Session Cookie	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)		
			Pre-OS Boot (3)	Valid Accounts (4)	Valid Accounts (4)	Masquerading (4)	Two Factor Authentication Interception	Process Discovery		Man in the browser	Remote Access Software		
			Scheduled Task/Job (4)			Modify Authentication Process (4)	Unsecured Credentials (3)	Query Registry		Man-in-the-Middle (2)	Traffic Signaling (1)		
			Server Software Component (3)			Modify Cloud Compute Infrastructure (4)		Remots System Discovery		Screen Capture	Web Service (3)		
			Traffic Signaling (1)			Modify Registry		Software Discovery (1)		Video Capture			
			Valid Accounts (4)			Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
						Obfuscated Files or Information (3)		System Network Connections Discovery					
						Pre-OS Boot (3)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (4)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							



Para practicar un poco

1. ¿Sabes usar dorks de búsqueda en Google? Por ejemplo, ¿cómo buscas ficheros con una extensión concreta?
2. Créate una cuenta en Shodan y comienza a realizar búsquedas sencillas con este buscador.
3. ¿Sabes averiguar con qué dirección IP estás navegando por Internet? ¿Sabes configurar un proxy para cambiarla/ocultarla? Prueba la web <http://www.cualesmiip.com/> y busca como es la configuración de un proxy con tu navegador (prueba con uno de la lista que hemos visto en clase).
4. ¿Cómo funciona Tor? Busca información e intenta explicarlo de manera sencilla.

Referencias

- Fotografías
 - <https://unsplash.com>
- Iconos
 - <https://www.flaticon.es/>



**Reconocimiento-CompartirIgual 3.0
España (CC BY-SA 3.0 ES)**

©2019-2022 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.

Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en
<https://creativecommons.org/licenses/by-sa/3.0/es/>