Anécdotas de seguridad

–y curriculas detrás de ellas

Ariel Waissbein, Ezequiel Gutesman

CORE SECURITY

El Cíclo Seguro de Desarrollo e Infraestructuras

- Conocimiento de las distintas capas tecnológicas
- Pensar como un atacante
  - Herramientas
  - Intereses
  - Skills / técnicas
  - Experiencia
- Poder diagnosticar problemas de seguridad atacándolos (penetration test)
  - Luego proponer soluciones

"Multics Security Evaluation Vulnerability Analysis," Karger, Schell. HQ Elec. Systs. 1973

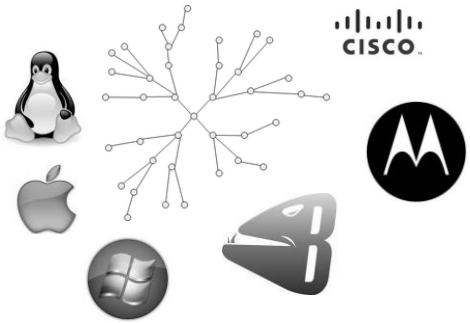
"Protection of Information in Computer Systems," Saltzer, Schroeder. 1975

CORE SECURITY

Algunos conceptos: **Information Gathering (IG)**

Recopilar información sobre el ambiente a atacar:

Red



Aplicaciones

Web

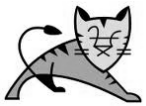
ERP

Desktop

Server

A medida

Genérica (CMS/enlatado)



Servicios

Telefonía

Control de Acceso

Impresión

Dominio

Mail

Backup

Personas

Directivos

Técnicos

Operativos

Tercerizados

CORE SECURITY

Algunos conceptos: **Vulnerabilidades y Exploits**

Una **vulnerabilidad** es un problema en una pieza de software que permite hacer que éste se comporte de maneras imprevistas

Un **exploit** es un programa o proceso que explota una vulnerabilidad

Si la vulnerabilidad no es conocida públicamente, entonces un exploit que la explota se lo llama **0-day (zero day)**

Shellcode es el nombre que se le da generalmente a un programa pequeño (usualmente escrito en assembler) que efectivamente *ejerce la explotación*

HBGary Federal vs. Anonymous

"They think I have nothing but a heirarchy based on IRC aliases!“ […] As 1337 as these guys are supposed to be they don't get it. I have pwned them! :)"

Aaron Barr. – (ex)CEO HBGary Federal

CORE SECURITY

El incidente de HBGary

Brinda, principalmente, servicios y herramientas de seguridad informática a organizaciones gubernamentales de EE.UU.

En 2011, **Aaron Barr**, CEO de HBGary Federal anunció publicamente que había desenmascarado a **Anonymous**…

http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/

"They think I have nothing but a heirarchy based on IRC [Internet Relay Chat] aliases!" he wrote. "As 1337 as these guys are supposed to be they don't get it. I have pwned them! :)" SI?

Aaron Barr.

CORE SECURITY

1. Atacando una aplicación web…

http://hbgaryfederal.com corría un Content Management System (CMS) escrito por **terceros**, especialmente para su site…

1. Un CMS open source (Wordpress, joompla, Drupal, etc) tiene una base de usuarios y programadores enorme, esto inevitablemente trae bugs, pero también patches periódicos…

2. HBGary no ejecutaba (aparentemente) tests de penetración contra su propio site, incluso ofreciendo este servicio a sus clientes

3. El CMS escrito por un tercero, tenía un **SQL injection** trivial…

1. Atacando una aplicación web…

```
http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27
```

1. SQL injection → Base de usuarios

```
http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27
```

```
SELECT title FROM PAGES where id = 27 UNION
SELECT username FROM USERS
UNION
SELECT email FROM USERS
UNION
SELECT pwd FROM USERS --
```

Bob	bob@hbgary.com	0227f7ef5d0cdd9537e38308c9608e3b
Alice	alice@hbgary.com	d41d8cd98f00b204e9800998ecf8427e
Aaron	aaron@hbgary.com	50d36c4f623478dc1cd26e4cfd48b0c6
Ted	ted@hbgary.com	0ad9af03629368a5265cead9f598eb1f

2. Hashes: Mejores prácticas

- Iterative hashing

```
hash = MD5( MD5( MD5("unpassword") ) )
```

- Salting

```
hash = MD5( "unpassword" . "un tringr4ndomd1fic1l" )
```

- Ambas…

Aaron	aaron@hbgary.com	**md5("22cake")**	(CEO)
Ted	ted@hbgary.com	**md5("pony42")**	(COO)

1. Hashes fáciles: rainbow tables

Free Rainbow Tables
Distributed Rainbow Table Project

RainbowCrack Project

```
3fb687203dd64bb8b46698fe23253aa4        21cake
50d36c4f623478dc1cd26e4cfd48b0c6        22cake
8e6b1f209e1516ab87bd4ee8af89c1b9        23cake
. . .
d283adb9606d60019c6413c65e6832f8        pony41
8e6b1f209e1516ab87bd4ee8af89c1b9        pony42
```

De todas maneras solo servirían para comprometer el website...

CORE SECURITY

Skills necesarios

Atacante

- Crawling (Information Gathering)
- Fuzzing
- Seguridad Web
  - SQLi
- Cracking de passwords
  - Tools
  - Rainbow Tables

Defensor

- Seguridad Web (mejores prácticas)
  - Sanitización de parámetros (inj)
  - Longitud de passwords y caracteres
  - Configuración (server, DB, etc)
- Autenticación (passwords)

Roles: ADMIN ARQ DEV

Referencias

http://www.freerainbowtables.com/
http://en.wikipedia.org/wiki/Rainbow_table
http://www.openwall.com/john/
https://www.owasp.org/index.php/SQL_Injection
https://www.owasp.org/index.php/Fuzzing
https://www.owasp.org/index.php/Testing:_Information_Gathering
https://www.owasp.org/index.php/Category:OWASP_Guide_Project
https://www.owasp.org/index.php/OWASP_Testing_Project

2. Reutilización de passwords

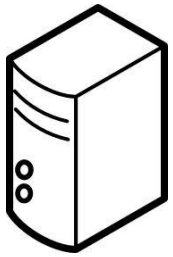
"No utilizarás la misma password para tu mail, linkedin, cajero, etc"

Yo a mi mamá, hace muchos años.

support.hbgary.com

```
ssh ted@support.hbgary.com
password: pony42
```

3. Privilege escalation



support.hbgary.com

backups
research data

```
[ted@support]~$
```

“The GNU C library dynamic linker expands $ORIGIN in setuid library search path” - CVE-2010-3847
http://seclists.org/fulldisclosure/2010/Oct/257

La vulnerabilidad fue reportada en Octubre de 2010, el ataque fue en Febrero de 2011 !

```
[root@support]~$
```

4. Reutilización de passwords, la revancha

Ambas cuentas (Ted y Aaron) también servían para loguearse en los mails de ambos. HBGary utilizaba Google Apps para este servicio y Aaron era **administrador del mail de la compañía**

Ahora podían resetear **cualquier password** de **cualquier cuenta** de mail de HBGary … incluída la de Greg Hoglund

CORE SECURITY

Skills necesarios (cont.)

Atacante

- Exploit DBs
- Exploits
  - Desarrollo de shellcode
  - Nociones de permisos

Defensor

- Reutilización de passwords
- Configuración de SSH
  - Acceso con user+pass vs. public key cryptography
- Patches de vulnerabilidades
  - Bugtraq, Listas de OS, updates
- Permisos de Admin

Roles: ADMIN USER

Referencias

http://www.exploit-db.com/
http://packetstormsecurity.org/
http://seclists.org/fulldisclosure/
http://www.securityfocus.com/
http://www.openssh.org/
http://en.wikipedia.org/wiki/Public-key_cryptography
https://hkn.eecs.berkeley.edu/~dhsu/ssh_public_key_howto.html
http://www.sans.org/security-resources/policies/Password_Policy.pdf

CORE SECURITY

5. Comprometiendo http://rootkit.com

http://rootkit.com era un site administrado por Hoglund, donde se discutía sobre rootkits y cosas relacionadas. Durante años, atacantes de todo tipo intentaron sabotearlo ya que atentaba contra sus creaciones

1. La password de rootkit.com era "88j4bb3rw0cky88" o "88Scr3am3r88“
2. Jussi Jaakonaho (Chief Security Specialist de Nokia) tenía acceso root

6. Un poco de ingeniería social

Por lo general, el acceso remoto como root está restringido, o sea que necesitaban una cuenta de bajos privilegios

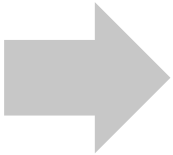
```
From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague? and is
our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
Thanks
---------
From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed
```

http://pastebin.com/kN04jpXu

6. Un poco de ingeniería social

Finalmente, Jussi terminó convencida y:

- Abrió el firewall para cualquier IP con SSH escuchando en el puerto 47152
- Reseteó la contraseña del usuario **hoglund** (el atacante pensó que era **greg**)
- Confirmó la contraseña de root



Y los atacantes:

1. Se robaron las cuentas de mail y hashes de password de rootkit.com (dump DBE + crack con rainbow tables)

2. Hicieron un defacement del site

Skills necesarios (cont.)

Atacante

- Social Engineering
  - Revisar mails
  - Utilizar la información encontrada para convencer al admin

Defensor

- Best Practices
- SSH con public key cryptography!
- Admin 101

Roles: ADMIN

Referencias

http://en.wikipedia.org/wiki/Social_engineering_(security)
https://hkn.eecs.berkeley.edu/~dhsu/ssh_public_key_howto.html

Skills necesarios (resúmen)

Atacante

- Crawling/Fuzzing
- Seguridad Web
- Cracking de passwords
- Exploit DBs
- Exploits / Shellcode
- Social Engineering

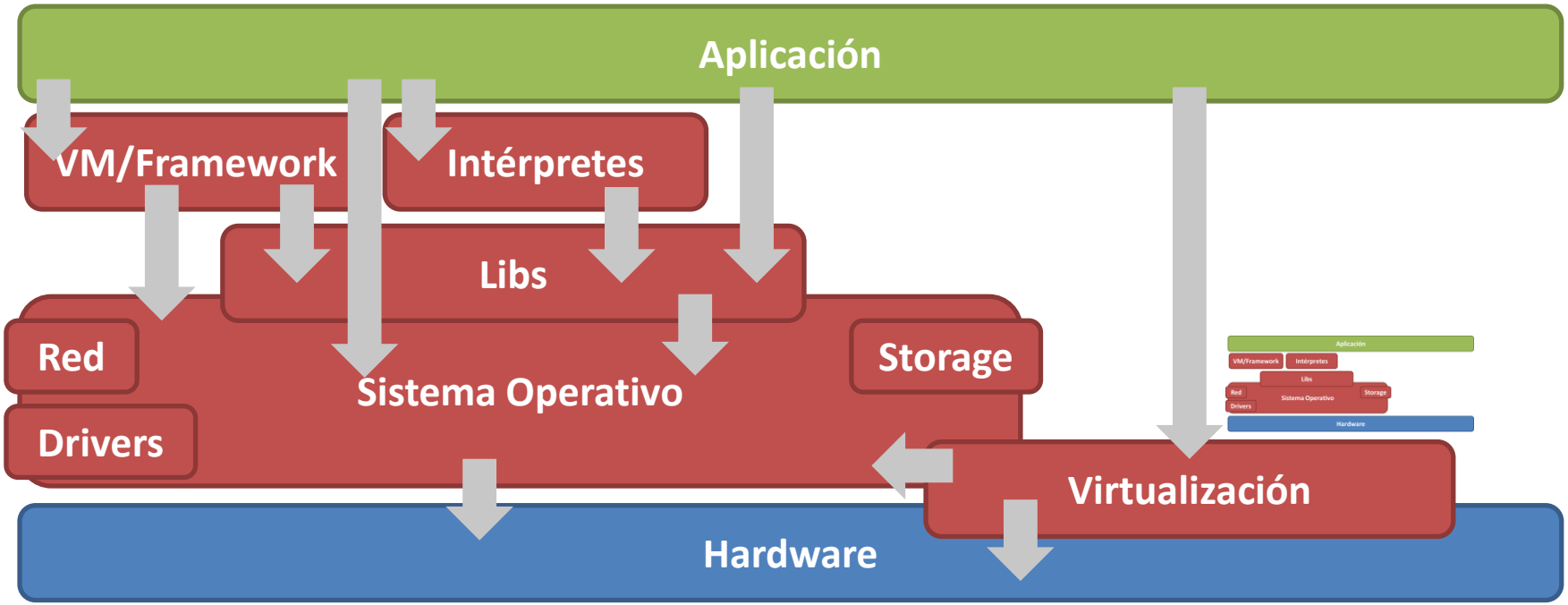
Defensores

ADMIN ARQ DEV

- Reutilización de passwords
- Configuración de SSH
- Patches de vulnerabilidades
- Permisos de Admin
- Best Practices
  - De desarrollo web
  - De aministración de redes / servers
  - De autenticación
- Sentido común

Recopilando

Vectores de ataque: **Bugs “binarios”**

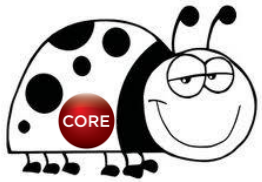


CORE SECURITY

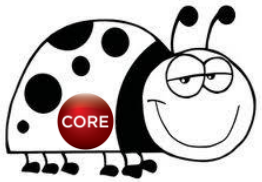
Recopilando

Vectores de ataque: **Bugs “binarios”**

Aplicación



Corel Paint Shop Pro Photo X2 FPX Heap Overflow (CORE-2009-1126)



Internet Explorer Dynamic OBJECT tag and URLMON sniffing vulnerabilities (CVE-2010-0255)

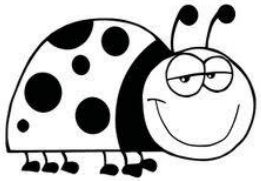
CORE SECURITY

Recopilando

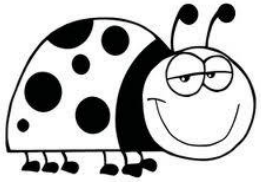
Vectores de ataque: **Bugs “binarios”**

Aplicación

VM/Framework | **Intérpretes**



ASP.NET Padding Oracle Vulnerability (CVE-2010-3332)



PHP ext/session Session Cookie Parameter Injection Vulnerability (month of php bugs: PMOPB-46-2007)

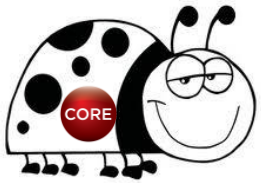
Recopilando

Vectores de ataque: **Bugs “binarios”**

Aplicación

VM/Framework | Intérpretes

Libs

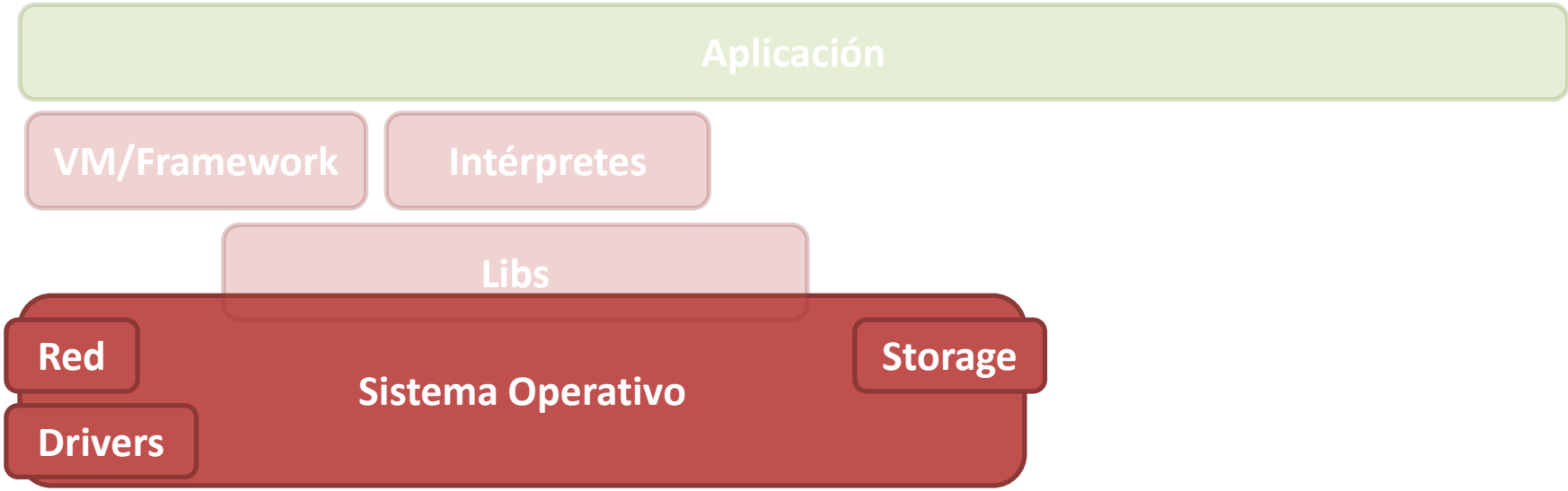


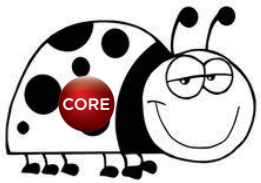
DCE RPC Vulnerabilities New Attack Vectors Analysis (CORE-2003-1205)

CORE SECURITY

Recopilando

Vectores de ataque: **Bugs “binarios”**





Windows Kernel ReadLayoutFile Heap Overflow (CORE-CVE-2012-1890)

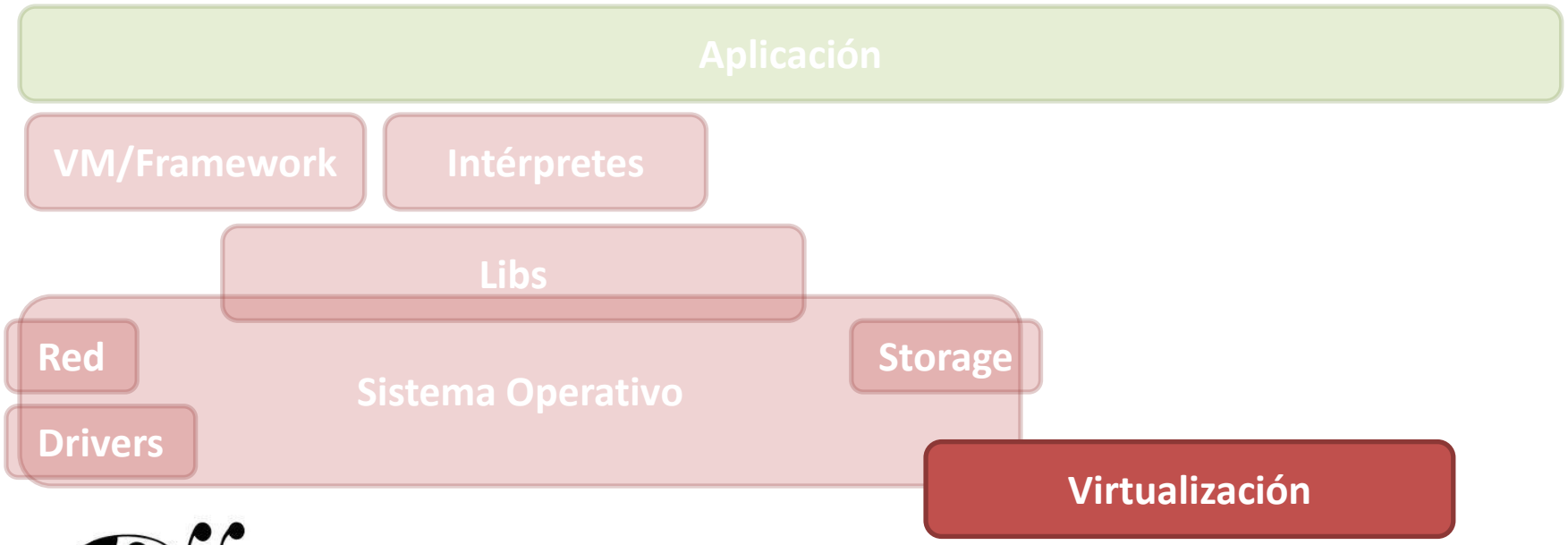
OpenBSD's IPv6 mbufs remote kernel buffer overflow (CORE-CVE-2007-1365)

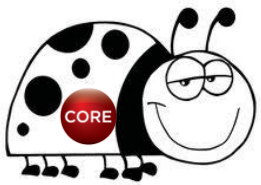
Windows SMTP Service DNS query Id vulnerabilities (CORE-CVE-2010-1689, CVE-2010-1690)

CORE SECURITY

Recopilando

Vectores de ataque: **Bugs “binarios”**



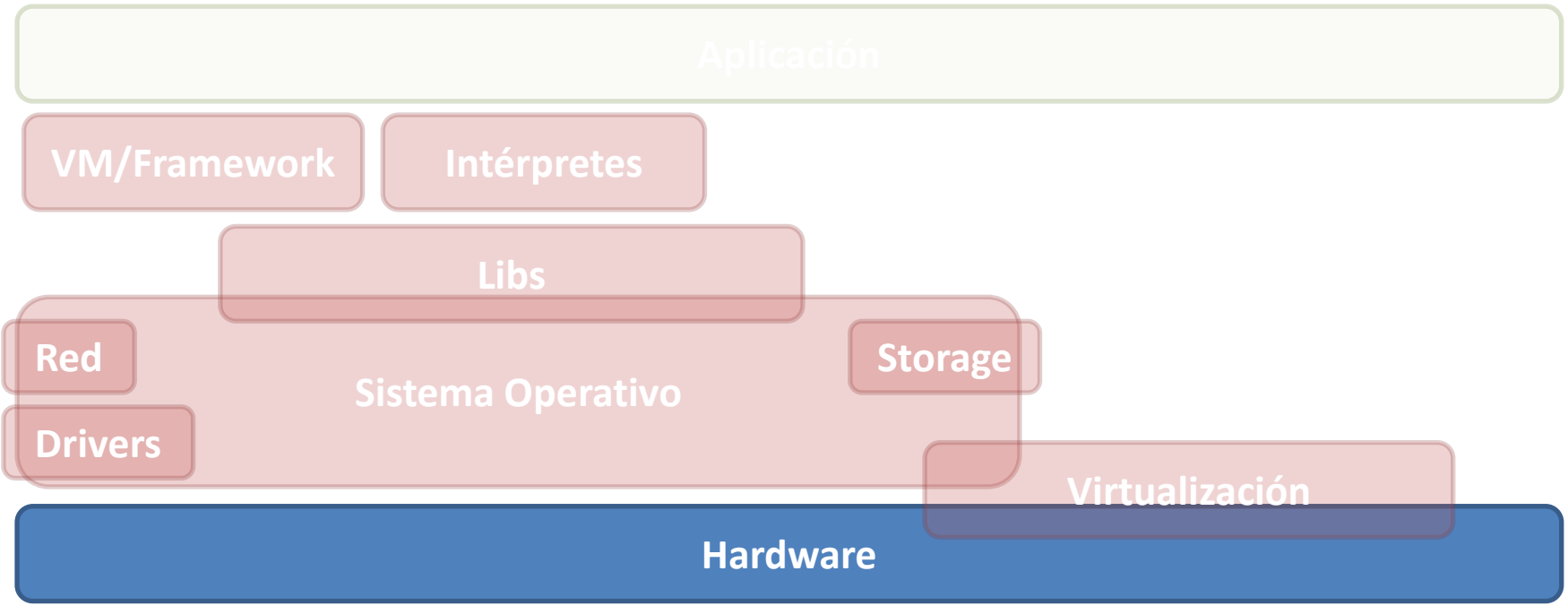


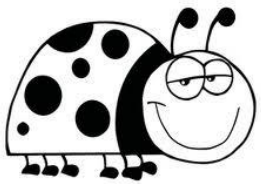
Virtual PC Hypervisor Memory Protection Vulnerability (CORE-2009-0803)

CORE SECURITY

Recopilando

Vectores de ataque: **Bugs “binarios”**



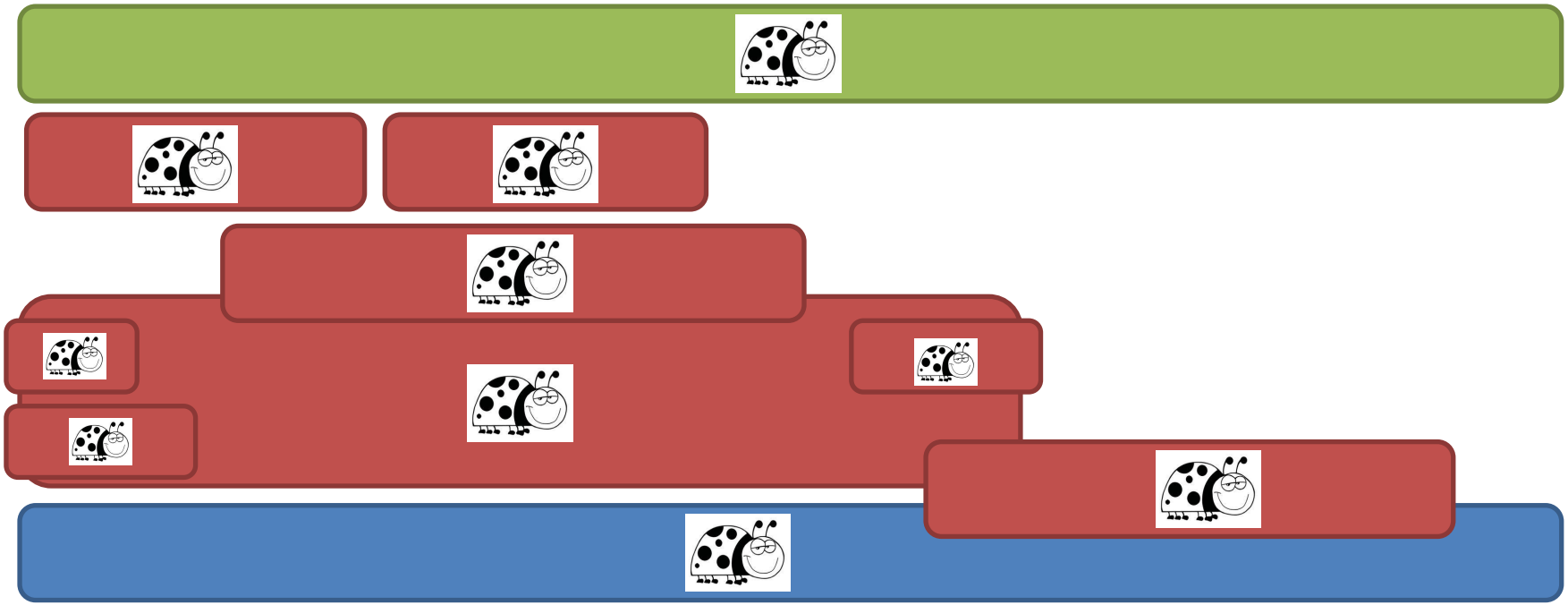


The Intel SYSRET privilege escalation
http://blog.xen.org/index.php/2012/06/13/the-intel-sysret-privilege-escalation/
Deactivate the Rootkit @Ekoparty 2009

CORE SECURITY

Recopilando

Vectores de ataque: **Bugs “binarios”**



CORE SECURITY

Recopilando

Vectores de ataque: **El vector Web**

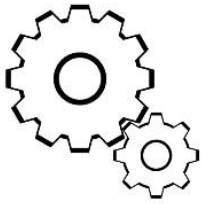
Web Server

- Tecnología del server
- Lenguaje de programación
- Recursos

BD

- Ubicación del server
- Tipo de base

HTTP



Infraestructura

- Cloud providers (SaaS, PaaS, IaaS)
- Accelerators
- CDN
- Streaming services

Cliente

- Browser
- Lenguajes de scripting
- Objetos embebidos

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CORE SECURITY

Gauss

"It seems a lot of stuff is attributed to Gauss –either he was really smart or had a great press agent.

--*"Concrete Mathematics," DE Knuth, Graham Patashnik*

CORE SECURITY

Gauss botnet - intro

- Las Botnets que atacan libaneses
  - Ataque a Libaneses
  - En especial, Clientes de bancos libaneses

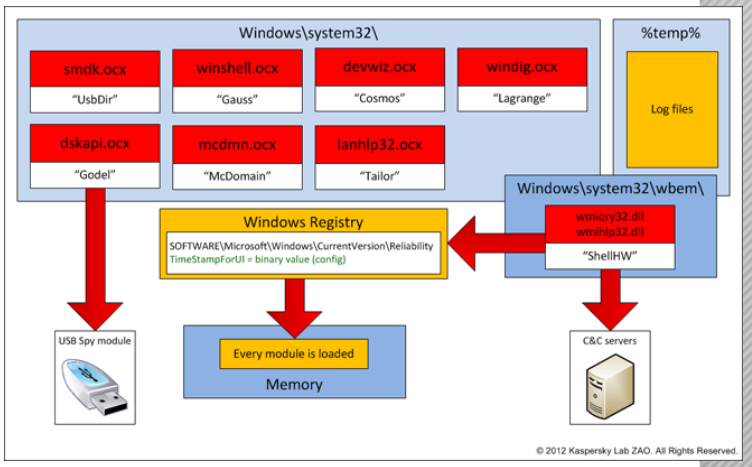
BYBLOS BANK

BANK OF BEIRUT s.a.l.

FRANSABANK

- Detectado por Kaspersky Labs
  - Ven ~2500 casos (1700 en Libano)

- Payload de 200k (shellHW)
  - Mas [20M de plugins]
  - Usa con técnicas de rootkit para esconderse
  - Busca información y se la pasa al C&C
  - Desarrollado en C++



CORE SECURITY

ShellHW: loader y comm

%system32%\wbem\wmihlp32.ocx

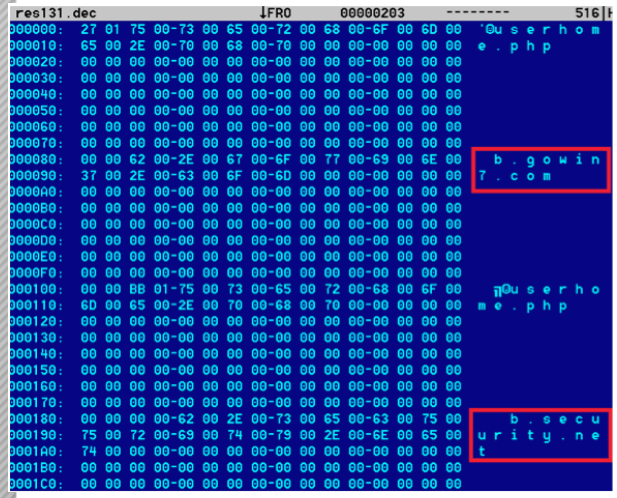
- Dropper no detectado
- El loader escribe el codigo a una DLL

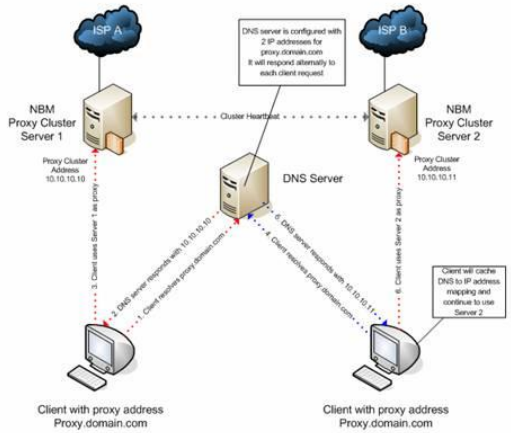
y modifica la registry pq las carge

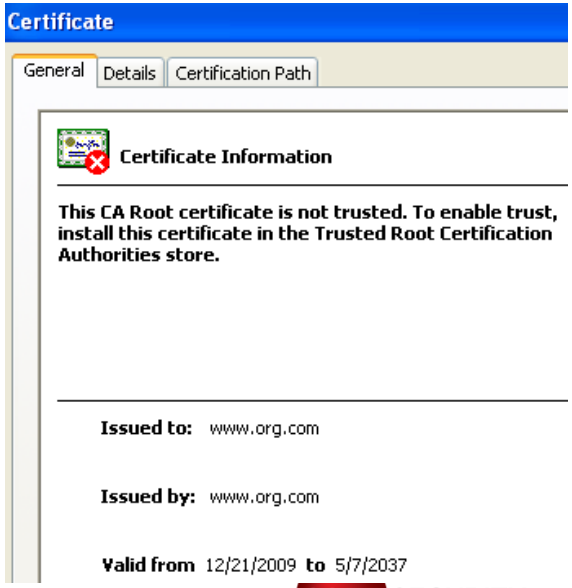
- Lee la config encriptada de la registry
  - XOR w ACDC
  - Nombres de archivos, ubicacion, nombres de las *export functions*
- Borra evidencias
  - privilegios de explorer.exe , TTL sin conexiones
- Loadea esos módulos

ShellHW (dll)

- Logea a un file temp encriptando todo (%temp%\~shw.tmp)
  - Contenedor universal (de logs)
- Comunicación con el C&C
  - Round-robin DNS
  - Hace un GET con un magic no. y recibe un update
  - Hace un POST con la data







CORE SECURITY

USB Payload (plugin)

- Infecta pendrives USB con un módulo que roba datos.
  - CVE-2010-2568: Microsoft Windows Shortcut 'LNK/PIF' Files **Automatic** File Execution Vulnerability [BID], [MSFT]
- Loader (mismo truco que shellHW)
- Se auto-borra si encuentra ve un AV de una lista
- Copia info a `%temp%`
  - Magic number
  - La appendea al file `.thumbs.db` en el pendrive
- Mecanismo de desinfección TTL=30

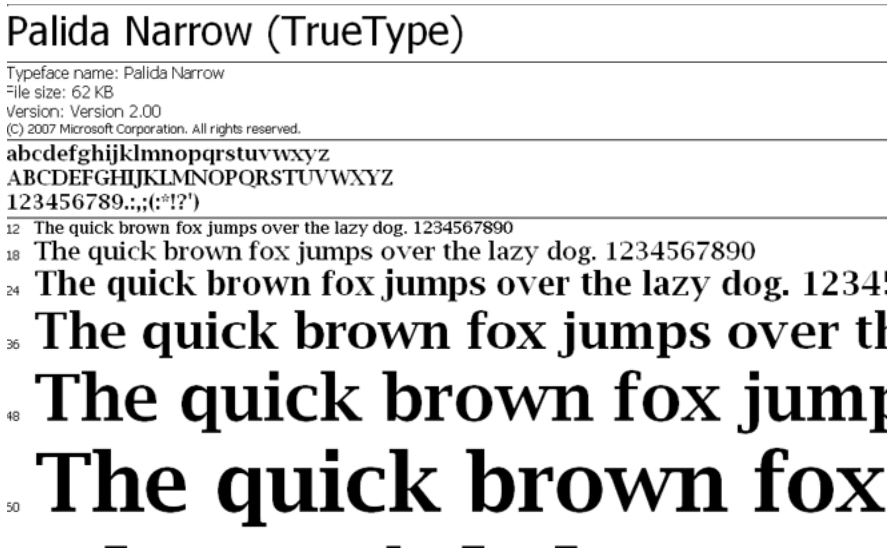
Info que sacan los plugins

- Version of the Windows OS
- Workstation info
  - Procesos
  - Environment variables and disk information
  - URL cache, cookies (IE)
- Firefox plugin
  - Browsing history
  - Passwords
  - Cookies (de los bancos!)
- Networking
  - Network adapter information
  - WIFI: SSIDs y calves, SSIDs visbles, etc
  - Tabla de routeo
- Red
  - List of visible network shares
  - Network proxy information
- MS SQL servers

Dos misterios:

- El worm instala este font.

Porque?



- `Triggers(%PATH%,%PROGRAMFILES%)`

  Para todo para de entradas en PATH y PROGRAMFILES:

  - Concatenarlos
  - Hashearlos 10,000 veces MD5(MD5(…(x)))…) y
  - Comparar el resultado con un string.
  - Si mathcea, usa eso como key para desencriptar un payload

- Cómo podemos deencriptarlo?

Skills necesarios (cont.)

Atacante

- C++, Arquitectura
- Exploits
  - Desarrollo de shellcode portable
  - AV evasion
- Firefox plugins (y stealth)
- Windows internals
- Crypto
- Networking/ Webapp deployment
  - Secure C&C install

Defensor

- Setup de AVs,
- Patches de vulnerabilidades
- Configuración de IDS y analisis de logs
- Forensics

Roles: ADMIN USER

Referencias

The C++ Programming Language: Special Edition by Bjarne Stroustrup

"DNS Complexity – Although it contains just a few simple rules, DNS has grown into an enormously complex system," Paul Vixie. ACM Queue 2007.

http://rdist.root.org/

"Strong payload obfuscation," AW, Futo, Gera. PacSec 2006.

"Reversing: Secrets of Reverse Engineering," Eldad Eilam. Wiley, 2005

"Virtual Honeypots," Neils Provos y Thorsten Holz. Addison-Wesley, 2007

"Strong payload obfuscation," AW, Futo, Gera. PacSec 2006.

Cyberattacks on Iran – Stuxnet and Flame. New York Times. Aug. 9, 2012

Gracias!

Skills necesarios (corelabs.coresecurity.com)

Atacante

- Crawling/Fuzzing
- Seguridad Web
- Cracking de passwords
- Exploit DBs
- Exploits / Shellcode
- Social Engineering
- C++, Arquitectura
- Firefox plugins (y stealth)
- Windows internals
- Crypto
- Networking/ Webapp deployment

Defensores

ADMIN ARQ DEV

- Reutilización de passwords
- Configuración de SSH
- Patches de vulnerabilidades
- Permisos de Admin
- Best Practices
  - De desarrollo web
  - De aministración de redes / servers
  - De autenticación
- Setup de AVs,
- IDS y analisis de logs
- Forensics
- Sentido común