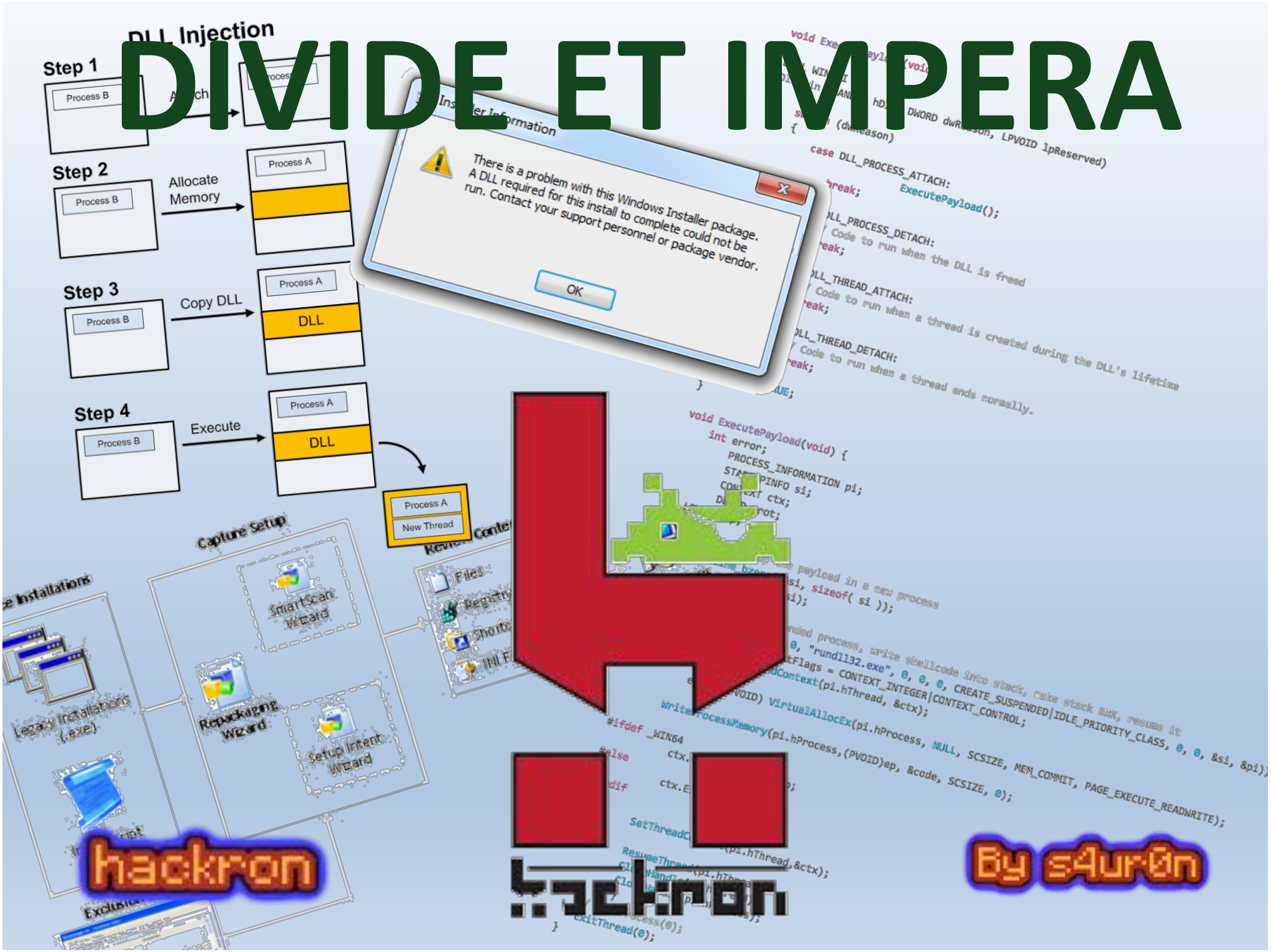

DIVIDE ET IMPERA
DLL Injection
Step 1
Process B
Step 2
Allocate Memory
Process A
Step 3
Copy DLL
DLL
Step 4
Execute
New Thread
There is a problem with this Windows Installer package.
A DLL required for this install to complete could not be run. Contact your support personnel or package vendor.
OK
Capture Setup
SmartScan Wizard
Repackaging Wizard
Setup Intent Wizard
Legacy Installations (.exe)
hackron
By s4ur0n

INSECURE INSTALLERS

Whoami

Deloitte. CyberSOC Academy

```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email = 'pcandel@cybersoc.deloitte.es'
        self.nickname = '@NN2ed_s4ur0n'
        self.role = 'Security Researcher'
        self.interest = [ 'Reversing', 'Malware', 'Offensive Security' ]
        self.member_of = [ 'NavajaNegra', 'mlw.re', 'OWASP', 'FAQin' ]
```

mlw.re hunting Malware like a sir

NAVAJA NEGRA CONFERENCE #nn4ed ALBACETE

OWASP Open Web Application Security Project Madrid Chapter

FAQin Congress

INSECURE INSTALLERS

Motivación

INSECURE INSTALLERS

Motivación

- Evitar las **protecciones** de los antivirus
- Querer lograr **persistencia** en el sistema
- **Elevar** privilegios en el sistema
- **Tomar** el control total del equipo
- ¿Es un **APT**? Advance Persistent Threat (Amenaza Persistente y Avanzada)

INSECURE INSTALLERS

Instaladores
Ejecutables
considerados
“maliciosos”

INSECURE INSTALLERS

Breve historia

- Georgi Guninski security advisory #21, **2000**
- **Double clicking on MS Office documents from Windows Explorer may execute arbitrary programs in some cases**
- http://www.guninski.com/officedll.html

INSECURE INSTALLERS

Brow

-
-

FRIDAY, FEBRUARY 17, 2012

Downloads Folder: A Binary Planting Minefield

Browser-Aided Remote Binary Planting, Part Deux

This article reveals a bit of our research and provides an advance notification of a largely unknown remote exploit technique on Windows. More importantly, it provides instructions for protecting your computers from this technique while waiting for the affected software to correct its behavior.

Two weeks from now I'll be holding a presentation at RSA Conference US called "Advanced (Persistent) Binary Planting" (Thursday, March 1, 9:30 AM Room 104). The presentation will include demonstrations of "two-step" binary planting exploits where in the first step the attacker silently deploys a malicious executable to user's computer, and the second step gets this executable launched. For those familiar with our past research on binary planting, this removes the need for remote shared folders as well as the need to get the user to double-click on a document in Windows Explorer.

Obviously, the idea is not new: If the attacker manages to somehow get her executable onto user's computer, getting it executed may be just a step away. But in order to deploy the file without heavy-duty social engineering (which invariably works in practice but is frowned upon among security folks) or physical access (which may include an overseas round trip), what is she left with? One ally she may find is the web browser - which lets the user download all sorts of files from all sorts of web sites. Directly to the Downloads folder.

ABOUT ACROS SECURITY

ACROS Security is specialized in providing advanced security analyses of products and systems. Our innovative security research pushes the boundaries of global knowledge, keeps our customers ahead of competitors and users safe from attackers.

We're also the authors of 0patch, a microscopic cure for BIG security problems.

FOLLOW US ON twitter

...to learn details from our research projects as soon as we disclose them.

BLOG ARCHIVE

- ▶ 2016 (2)
- ▶ 2013 (1)
- ▼ 2012 (7)
  - ▶ May (2)
  - ▶ April (1)

INSECURE INSTALLERS

¿Qué tenemos en Downloads?

- Es un auténtico "**repositorio**" de versiones de todo tipo de programas, DLLs, OCXs, etc.
- Los navegadores **no suelen eliminar** los ficheros descargados (IE, Firefox, Safari, Chrome, Opera…) a no ser que al usuario le falte espacio en disco...

INSECURE INSTALLERS

¿Qué tenemos en Downloads?

- ¿Qué ocurre al descargar una DLL?
- El navegador no suele advertir al usuario para que pueda ejecutarla al contrario que un binario
- Por tanto, **permanece** en dicho directorio
- Hasta su "**limpieza**" o incluso formateo
- Técnicas de **clickjacking**

INSECURE INSTALLERS

Descargada, pero no ejecutada…

- Se encuentra "**latente**" en el sistema a la espera de ser ejecutada o invocada
- El usuario descarga un **instalador** para ejecutar e instalar un binario
- O incluso de llama a **CreateProcess("msiexec.exe")** sin especificar su ruta de acceso

INSECURE INSTALLERS

Descargada, pero no ejecutada…

- Se podría incluso crear un bogus/fake **msiexec.exe** en dicho directorio
- Posteriormente, se tratará de localizar y cargar e inicializar las **DLLs necesarias** desde el mismo directorio
- Y todo ello, supone un **problema**…

INSECURE INSTALLERS

Instaladores “inseguros”

- Listas como **Full Disclosure** o **BugTraq** con **Stefan Kanthak** y diferentes casos
- Timelines:

Not a vulnerability

- ¿Usuarios?

Stay tunned

INSECURE INSTALLERS

Instaladores “inseguros”

- Todos los instaladores ejecutables y autodescompresores (SFXs) **presentan un problema** a los usuarios
- Deben ser considerados como **potencialmente peligrosos**
- Incluso como **malware** en casos de Organizaciones

INSECURE INSTALLERS

Instaladores “inseguros”

- El usuario ejecuta **directamente** el instalador desde **downloads** u otros directorios como **%TEMP%, %APPDATA%**
- Dichos ejecutables pueden **cargar y ejecutar** DLLs y/o programas que un atacante podría haber dejado para su ejecución en dichos directorios

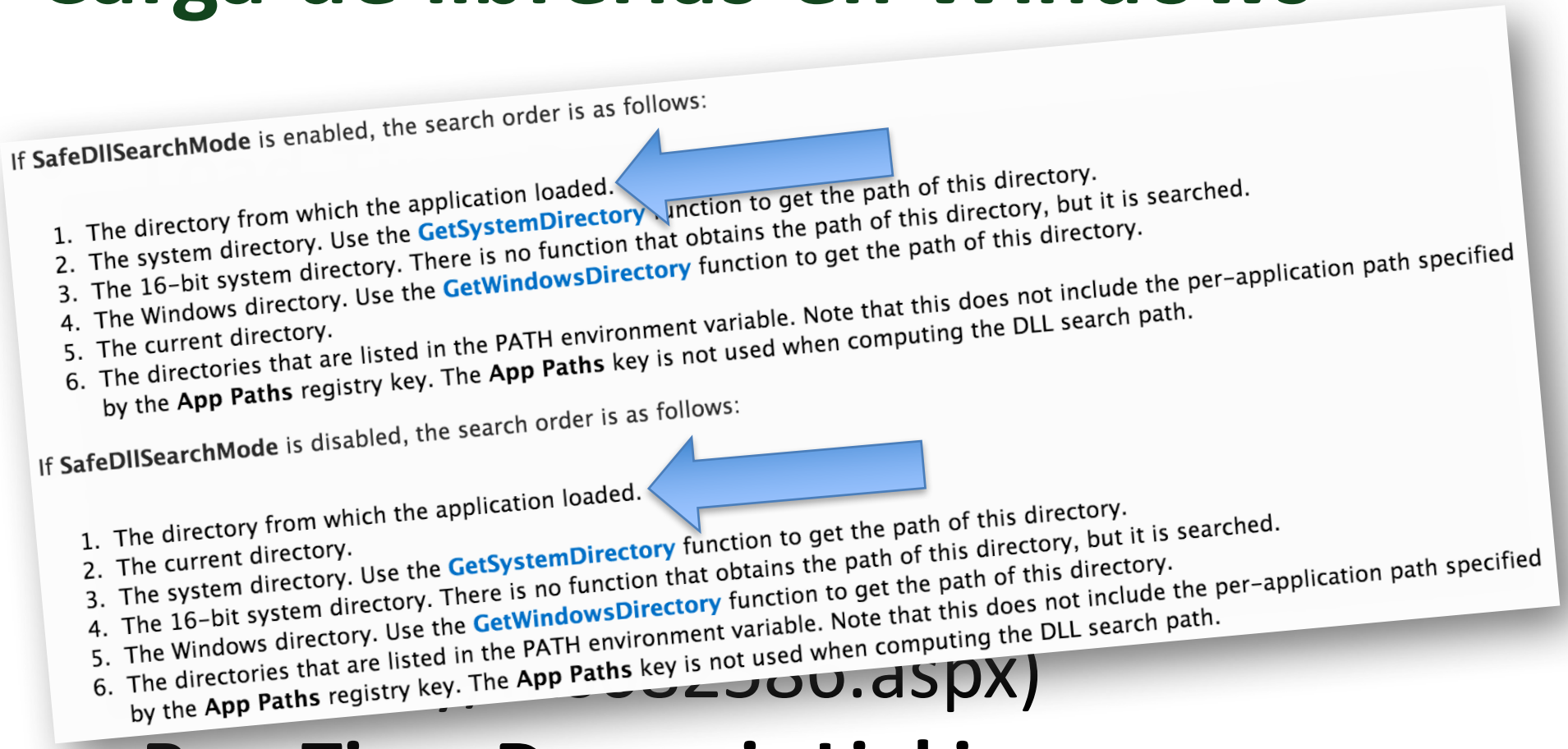
INSECURE INSTALLERS

Instaladores “inseguros”

- Riesgo de “**Arbitrary Code Execution**”
- Riesgo de “**Privilege Escalation**”

INSECURE INSTALLERS

Carga de librerías en Windows



If **SafeDllSearchMode** is enabled, the search order is as follows:

1. The directory from which the application loaded.
2. The system directory. Use the **GetSystemDirectory** function to get the path of this directory.
3. The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched.
4. The Windows directory. Use the **GetWindowsDirectory** function to get the path of this directory.
5. The current directory.
6. The directories that are listed in the PATH environment variable. Note that this does not include the per-application path specified by the **App Paths** registry key. The **App Paths** key is not used when computing the DLL search path.

If **SafeDllSearchMode** is disabled, the search order is as follows:

1. The directory from which the application loaded.
2. The current directory.
3. The system directory. Use the **GetSystemDirectory** function to get the path of this directory.
4. The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched.
5. The Windows directory. Use the **GetWindowsDirectory** function to get the path of this directory.
6. The directories that are listed in the PATH environment variable. Note that this does not include the per-application path specified by the **App Paths** registry key. The **App Paths** key is not used when computing the DLL search path.

- **Run-Time Dynamic Linking**

INSECURE INSTALLERS

Vulnerabilidades: Rutas no absolutas

- **CWE-426: Untrusted Search Path** (https://cwe.mitre.org/data/definitions/426.html)
- **CWE-427: Uncontrolled Search Path Element** (https://cwe.mitre.org/data/definitions/427.html)

INSECURE INSTALLERS

Vulnerabilidades: Descomprimir en directorios no seguros

- Muchos instaladores **descomprimen** los ficheros en **directorios no seguros**
- **Posteriormente** ejecutan los binarios **desde los mismos**

INSECURE INSTALLERS

Vulnerabilidades: Descomprimir en directorios no seguros

- **CWE-377: Insecure Temporary File** (https://cwe.mitre.org/data/definitions/377.html)
- **CWE-379: Creation of Temporary File in Directory with Incorrect Permissions** (https://cwe.mitre.org/data/definitions/379.html)

INSECURE INSTALLERS

Vulnerabilidades: Permisos

- Los instaladores suelen requerir **elevación de privilegios** para contar con permisos **administrativos**
- Suelen incluirse en la **detección de tecnología de instalación** e ir embebidos en el propio instalador

INSECURE INSTALLERS

INSECURE INSTALLERS

WinImage

- http://www.winimage.com/download.htm
- **http://home.arcor.de/skanthak/download/SENTINEL.DLL**
- Copiar a UXTheme.dll, RichEd32.dll, WindowsCodecs.dll, MPR.dll

INSECURE INSTALLERS

Python 3.5.1

- https://www.python.org/downloads/
- **http://home.arcor.de/skanthak/download/SENTINEL.DLL**
- Copiar a FEClient.dll, ClbCatQ.dll (Windows NT 5.x) o ProfAPI.dll (Windows NT 6.x)
- Copiar a MSI.dll y Version.dll (Repwned)

INSECURE INSTALLERS

Microsoft Antimalware Definition Updates

- https://support.microsoft.com/en-us/kb/935934
- **http://home.arcor.de/skanthak/download/SENTINEL.DLL**
- Copiar a FEClient.dll

INSECURE INSTALLERS

Microsoft (Otros)

- Malicious Removal Tool
- Root Certificate Updater
- Root Certificate Revocation List Updater
- **Todos** los instaladores de .NET Framework
- Windows Defender Offline

INSECURE INSTALLERS

Microsoft (Otros)

- **Todos** los Visual C++ Runtime 20xx Redistributable Packages
- **Todos** los hotfixes y updates para Windows 2000, Windows XP, Windows Embedded POSReady 2009, Windows Server 2003 (Windows*-KB*-*.exe)

INSECURE INSTALLERS

Panda

- http://acs.pandasoftware.com/Panda2016/AP/181164/AP16.exe
- **http://home.arcor.de/skanthak/download/SENTINEL.DLL**
- Copiar a UXTheme.dll, RichEd20.dll y RichEd32.dll

INSECURE INSTALLERS

Avira

- https://www.avira.com/en/download/product/avira-registry-cleaner
- **http://home.arcor.de/skanthak/download/SENTINEL.DLL**
- Copiar a WTSAPI32.dll, UXTheme.dll, RichEd20.dll

Demo 2
Divide et Impera

INSECURE INSTALLERS

Universal

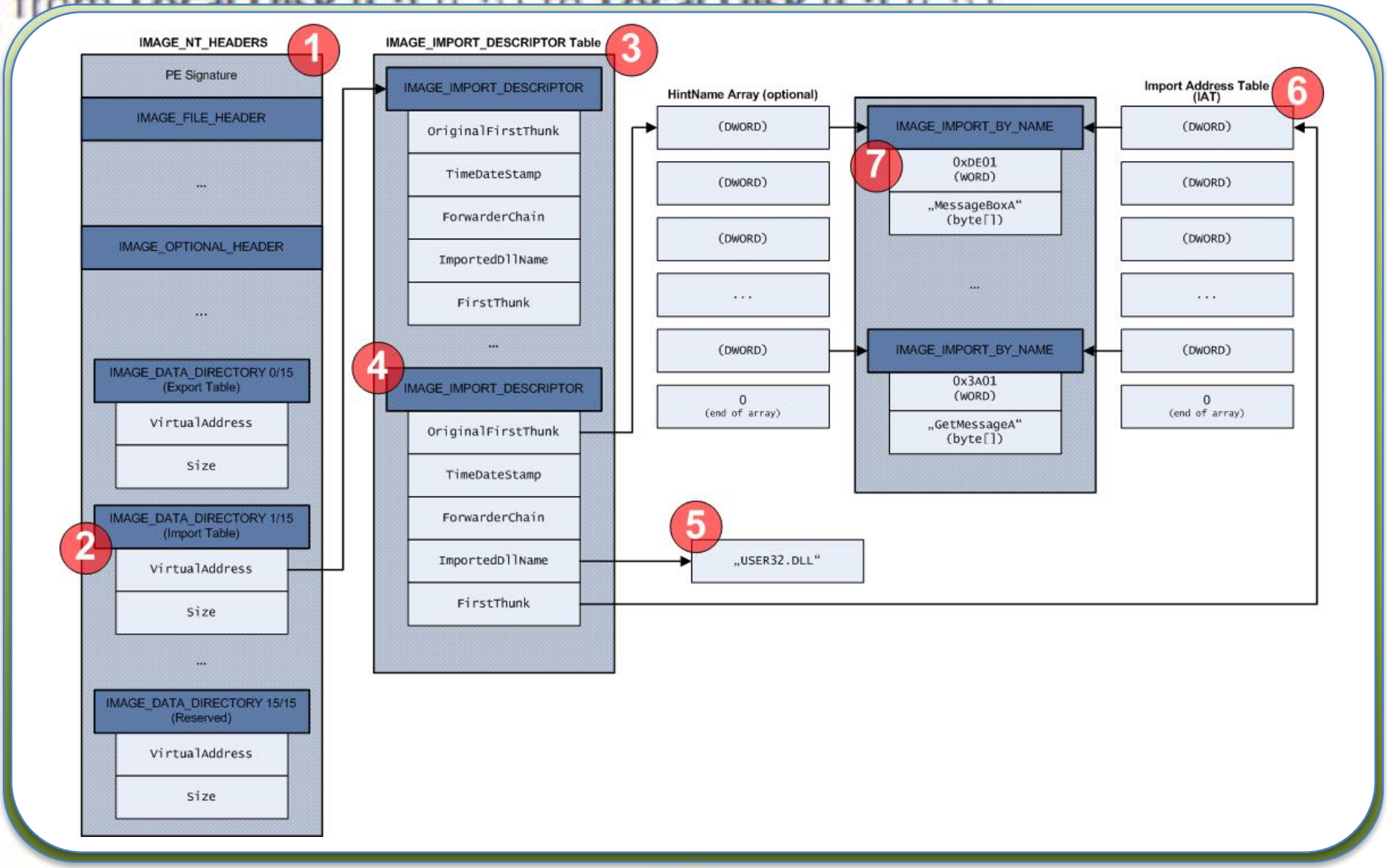
- dll
- M
- h
- fr /master/data/templates
- /src/pe/dll/template.c

```
#include <windows.h>

BOOL WINAPI DllMain (HANDLE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    switch (fdwReason)
    {
        case DLL_PROCESS_ATTACH:
        dll_m11();
        case DLL_THREAD_ATTACH:
        case DLL_THREAD_DETACH:
        case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}

int dll_m11()
{
    MessageBox(0, "DLL Hijacked!", "DLL Message", MB_OK);
}
```

INSECURE INSTALLERS



INSECURE INSTALLERS

Contramedidas

INSECURE INSTALLERS

Contramedidas: generales

- **No ejecutar** instaladores ejecutables
- Jamás desde **download** o **%TEMP%**
- Si las aplicaciones **no son distribuidas en el formato de paquete del instalador** nativo del Sistema Operativo (tipo MSI, CAB), solicitar al fabricante o desarrollador su empaquetado con dicho formato o depurar proceso instalación

INSECURE INSTALLERS

Contramedidas: usuarios

- Deshabilitar la **elevación de privilegios** para usuarios estandard y la **detección de instalación** para todos los usuarios
- https://technet.microsoft.com/en-us/library/dd835564.aspx#BKMK_RegistryKeys

INSECURE INSTALLERS

Registry Key	Group Policy setting	Registry settings
FilterAdministratorToken	User Account Control: Admin Approval Mode for the built-in Administrator account	0 (Default) = Disabled 1 = Enabled
EnableUIADesktopToggle	User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	0 (Default) = Disabled 1 = Enabled
ConsentPromptBehaviorAdmin	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	0 = Elevate without prompting 1 = Prompt for credentials on the secure desktop 2 = Prompt for consent on the secure desktop 3 = Prompt for credentials 4 = Prompt for consent 5 (Default) = Prompt for consent for non-Windows binaries
ConsentPromptBehaviorUser	User Account Control: Behavior of the elevation prompt for standard users	0 = Automatically deny elevation requests 1 = Prompt for credentials on the secure desktop 3 (Default) = Prompt for credentials
EnableInstallerDetection	User Account Control: Detect application installations and prompt for elevation	1 = Enabled (default for home) 0 = Disabled (default for enterprise)
ValidateAdminCodeSignatures	User Account Control: Only elevate executables that are signed and validated	0 (Default) = Disabled 1 = Enabled
EnableSecureUIAPaths	User Account Control: Only elevate UIAccess applications that are installed in secure locations	0 = Disabled 1 (Default) = Enabled
EnableLUA	User Account Control: Run all administrators in Admin Approval Mode	0 = Disabled 1 (Default) = Enabled
PromptOnSecureDesktop	User Account Control: Switch to the secure desktop when prompting for elevation	0 = Disabled 1 (Default) = Enabled
EnableVirtualization	User Account Control: Virtualize file and registry write failures to per-user locations	0 = Disabled 1 (Default) = Enabled

INSECURE INSTALLERS

Contramedidas: sysadmins

- No permitir la ejecución de binarios en **downloads**, **%TEMP%** y subdirectorios
- NTFS ACL (**D;OIIO;WP;;;WD**) Ver https://msdn.microsoft.com/en-us/library/aa374928.aspx
- **Software Restriction Policies**
- **AppLocker**

INSECURE INSTALLERS

Contramedidas: developers

- No hay **ninguna razón** para construir, distribuir, desplegar o emplear ejecutables para instalar software o descomprimir ficheros
- Los SS.OO. tienen sus **propios instaladores** o **gestores de paquetes** que incluyen todo

INSECURE INSTALLERS

¿Preguntas?

Muchas gracias

@NN2ed_s4ur0n

s4ur0n@navajanegra.com