

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Deconstruyendo la Estrella Roja: el Linux de Corea del Norte



Simón Roses Femerling

- Licenciado informática (Suffolk University), Postgrado E-Commerce (Harvard University) y Executive MBA (IE Business School)
- Fundador & CEO, VULNEX www.vulnex.com
- Blog: www.simonroses.com
-  @simonroses | @vulnexsl
- Ex: Microsoft, PwC, @Stake
- Beca del DARPA Cyber Fast Track (CFT) para investigar sobre seguridad en el ciclo de desarrollo de software
<http://www.simonroses.com/es/2014/06/mi-visita-al-pentagono/>
- Ponente: Black Hat, RSA, HITB, OWASP, AppSec USA, SOURCE, DeepSec, TECHNET
- CEH, CISSP & CSSLP

Índice

- 1. ESTADO-NACIÓN: ATAQUES Y DEFENSAS**
- 2. UN VISTAZO A LA ESTRELLA ROJA**
- 3. EL OTRO LADO DE LA ESTRELLA ROJA**
- 4. CONCLUSIONES**

AVISO

- Lo expuesto en esta presentación está basado en un análisis al sistema operativo Estrella Roja desarrollado por Corea del Norte (Versión Desktop 3.0). Los resultados no se han validado con nadie de Corea del Norte y son puras conjeturas.



1. ESTADO-NACIÓN: ATAQUES Y DEFENSAS



1. RESPUESTA OFENSIVA

MALWARE	GRUPO DE OPERACIONES
Reign	NSA TAO (EE.UU.)
Flame	PLA UNIT 61398 (China)
Stuxnet	UNIT 8200 (Israel)
Duqu	
OnionDuke	
The Mask / Careto	

1. RESPUESTA DEFENSIVA

Desarrollo de Software Propio: SO y Apps

- Corea del Norte: Estrella Roja
- China:
 - COS (Linux para móviles)
 - Kylin (Ubuntu)
- Rusia:
 - RoMOS (Android)
- Francia: No un SO propio pero ejército se pasa a Ubuntu
- India: Anunciado su propio SO
- EE.UU.:
 - Versión segura de Android por el DISA
 - Plan X: SO para operaciones de ciberguerra en tiempo real



1. BARRERAS

- Conseguir copias del SO / Apps
- Idioma
- Análisis / Escalada de Privilegios (root)



2. UN VISTAZO A LA ESTRELLA ROJA



2. ROMPIENDO LAS BARRERAS

- Conseguir copias del SO / Apps
 - Copias filtradas por Internet
 - Inteligencia
- Idioma
 - Google Traductor
 - Modificación ISO y lenguaje
- Análisis / Escalada de Privilegios (root)
 - Explotación de vulnerabilidades locales / remotas



2. ESTRELLA ROJA HISTORIA

- Comienzo desarrollo en 2002 por el Centro de Computación de Corea (KCC)
- Oficinas KCC: China, Alemania, Siria y Emiratos Árabes
- Estrella Roja:
 - 2010: Versión 2.0
 - 2012: Versión 3.0 (publicada en 2013)
- Fugas en Internet:
 - 2010: Estudiante ruso durante un curso en Pyongyang compró una copia y la publicó (versión 2.0)
 - 2013: Un profesor americano visitante compró una copia y publicó fotos (versión 3.0)
 - 2014: En diciembre se filtran copias de la versión 3.0 en Internet

2. ESTRELLA ROJA CARACTERÍSTICAS

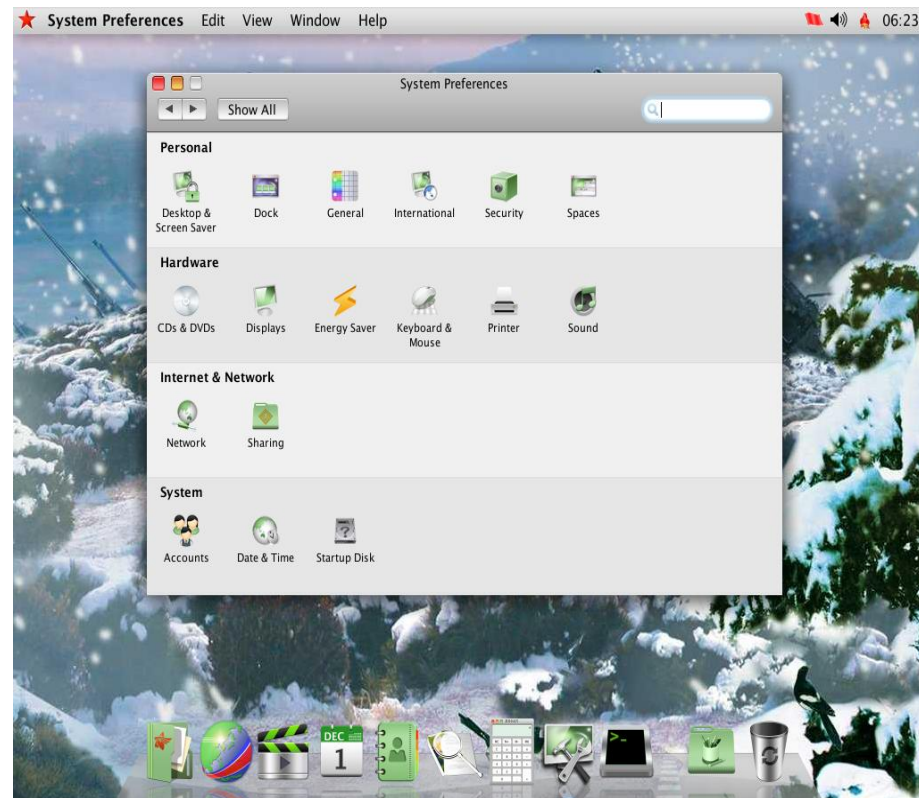
- Sistema Operativo Linux
- Basado en Fedora
- Kernel: 2.6.38.8
- Diseñado para usuarios (versión Escritorio)



2. ESTRELLA ROJA 2.0



2. ESTRELLA ROJA 3.0



2. DEMO: ESCRITORIO ESTRELLA ROJA



2. ¿POR QUÉ EL CAMBIO DE LOOK?



2. CHARLA DE WILL SCOTT EN CCC 2014

- Will Scott: profesor visitante americano impartió dos semestres en el KCC (Pyongyang): programación y SO (Linux y Android)
- <https://www.youtube.com/watch?v=w703MQZcDhY>

3. EL OTRO LADO DE LA ESTRELLA ROJA



3. SEGURIDAD Y VULNERABILIDADES

- Medidas seguridad:
 - Root deshabilitado
 - Snort (2.8.0)

- Lynis: 56 de puntuación

```
Hardening index : [56] [#####          ]
```

```
Hardening strength: System has been hardened, but could use additional hardening
```

- Vulnerabilidades:
 - Configuraciones inseguras
 - Aplicaciones
 - Kernel



3. DEMO: ESCALADA DE PRIVILEGIOS



3. MALWARE

- Applications/MusicScore.app/Contents/Resources/Help/ko_KP/Music Score/score_split.htm
- Exploit:HTML/IframeRef.gen

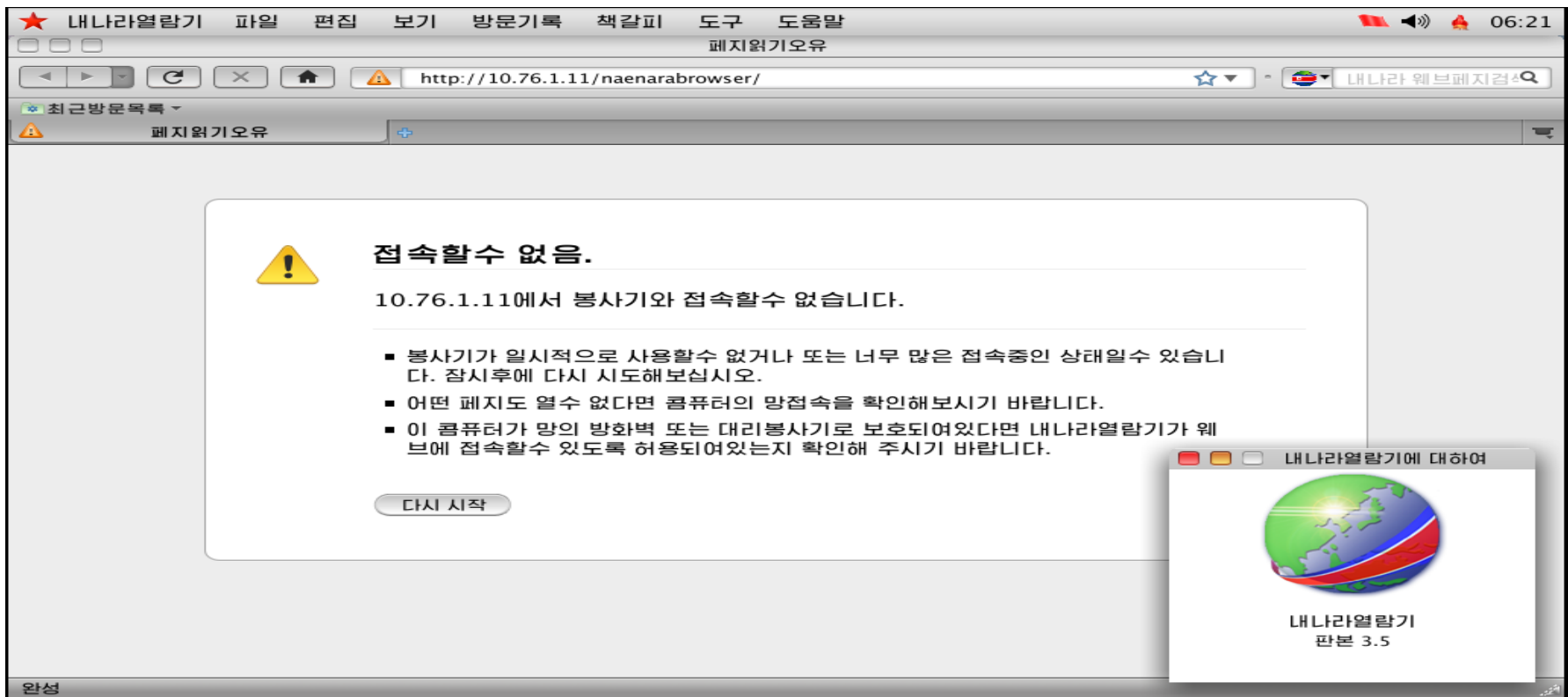


3. NAVEGADOR NAENARA

- Naenara == “mi país”
- Navegador basado en Firefox
- Portal de noticias www.naenara.com.kp (Gestionado por el KCC)
- Configurado para recibir actualizaciones de forma automática



3. NAVEGADOR NAENARA



3. NAVEGADOR NAENARA

- Envía información a un servidor central (10.76.1.11)

- App escrita en PHP

- Links:



- <http://10.76.1.11/naenarabrowser/crash-stats.mozilla.com/report/index/>
- <http://10.76.1.11/se/search/index.php?keyword=TEST2&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:ko-KP:official&client=firefox-a>

3. NAVEGADOR NAENARA

```
GET /test.html HTTP/1.1
NaenaraBrowserHeaderMAC: 192.168.131.134=000C29DFEB25
HardwareSN:
User_AgentSystem: ..... 3.0...
Host: 192.168.131.135
User-Agent: Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv:1.9.1b4) Gecko/20130508
Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ko-kp,ko;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: UTF-8,*
Keep-Alive: 300
Connection: keep-alive
```

3. CONTENTS GUARD

- Demonio que firma ficheros “watermarking” sin que el usuario lo sepa
- Pensado para identificar la procedencia de un fichero
- Compuesto por diferentes ficheros, incluye medidas de defensa



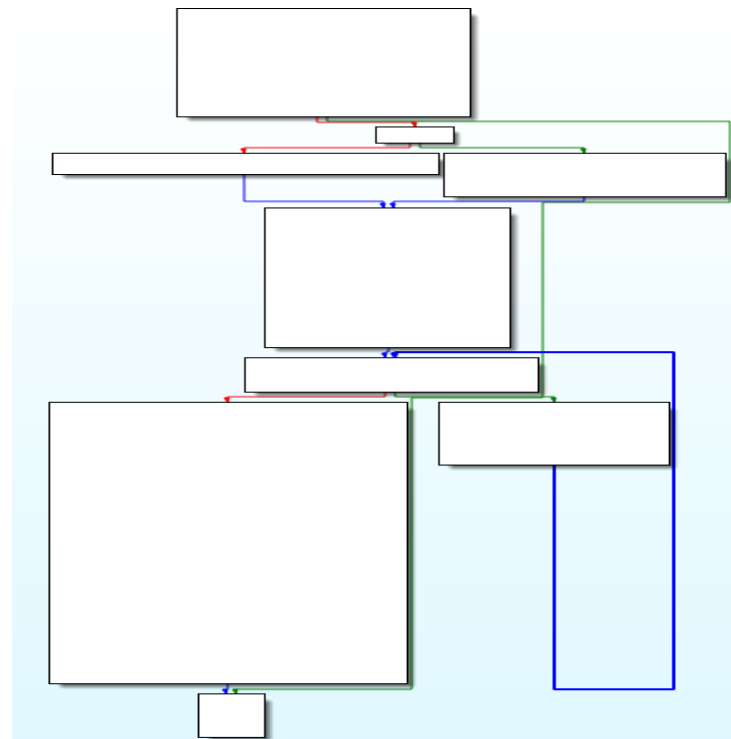
3. CONTENTS GUARD

opprc

```

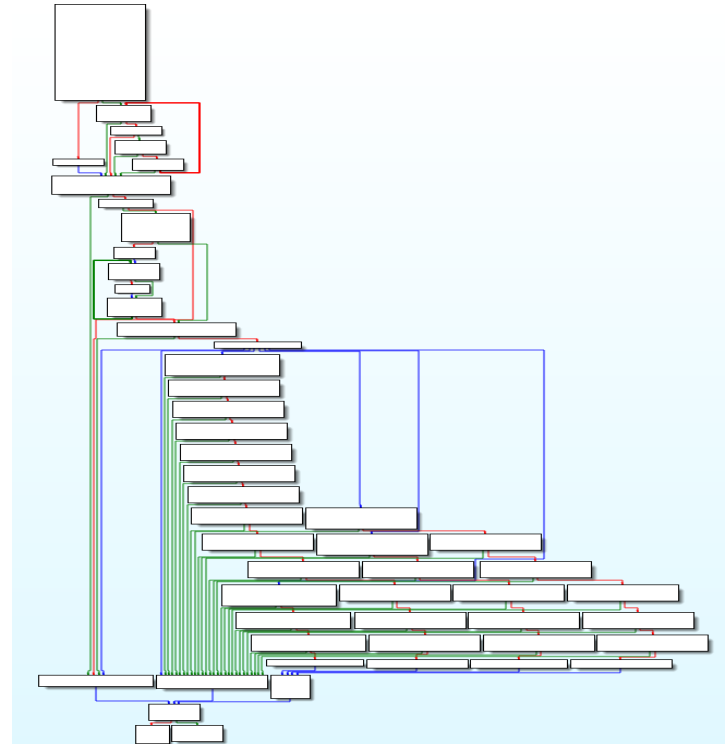
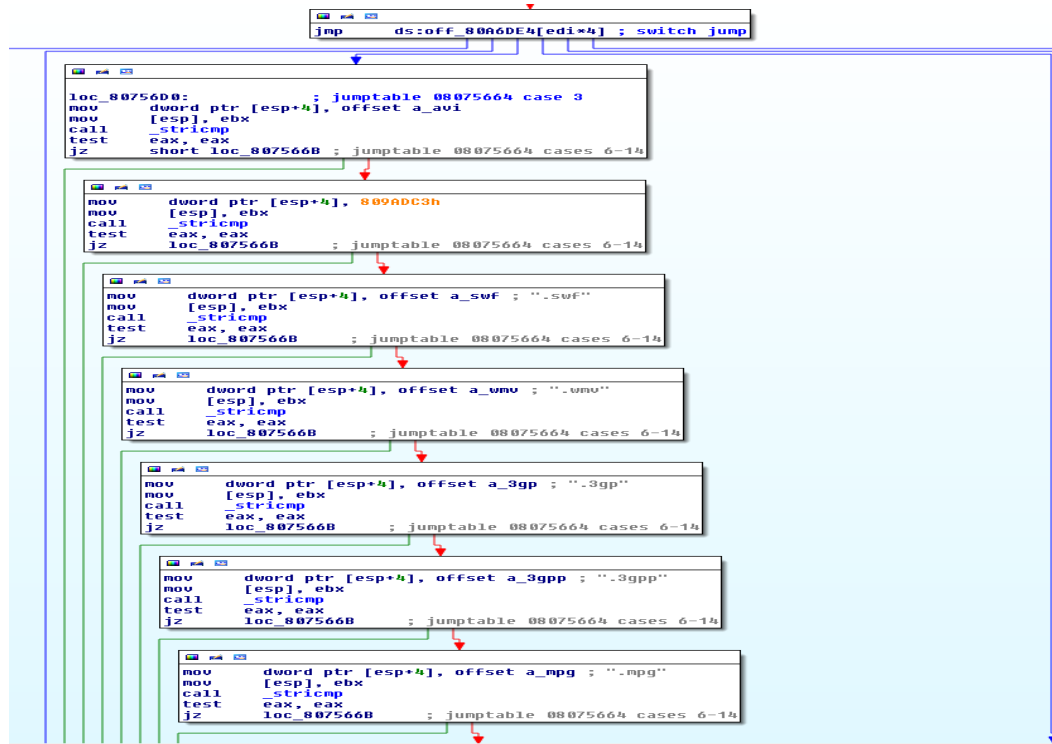
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrBin0pprc ; "/usr/bin/opprc"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrBinScnprc ; "/usr/bin/scnprc"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrLibAudiosig ; "/usr/lib/AudioSignal.dat"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset gsZDBFile ; "/tmp/AnGae.dat"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset gsZDictFileName ; "FileName.bin"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrShareAutost ; "/usr/share/autostart/scnprc.desktop"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aEtcInitCtguard ; "/etc/init/ctguard.conf"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrLibLibigl_s ; "/usr/lib/libigl.so.0"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrLibLibmg1_s ; "/usr/lib/libmg1.so.0"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset magicFile ; "/usr/lib/magiccb"
mov     [esp+4], esi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset aUusrLibAudiosig ; "/usr/lib/AudioSignal.dat"
mov     [esp+4], edi ; request
mov     [esp], eax ; fd
call    _ioctl
mov     eax, gfd
mov     dword ptr [esp+8], offset gsZDBFile ; "/tmp/AnGae.dat"
mov     [esp+4], edi ; request
mov     [esp], eax ; fd
call    _ioctl

```



3. CONTENTS GUARD

scnprc



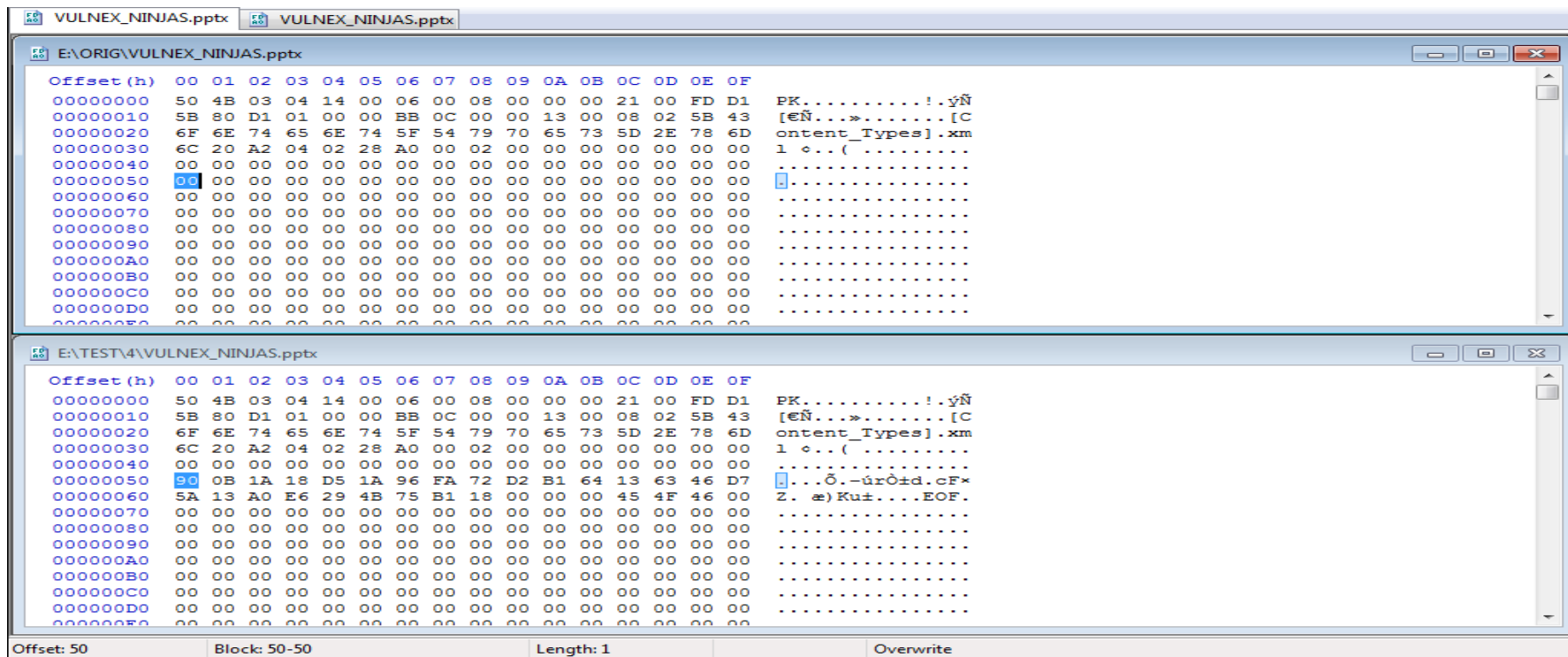
3. CONTENTS GUARD

BMP



3. CONTENTS GUARD

PPTX



The screenshot displays a hex editor with two open files. The top file is 'E:\ORIG\VULNEX_NINJAS.pptx' and the bottom file is 'E:\TEST\4\VULNEX_NINJAS.pptx'. Both files show a hex dump on the left and an ASCII view on the right. The top file's ASCII view shows a standard PKZIP signature and XML content. The bottom file's ASCII view shows a modified signature and content, with the word 'Z.' appearing in the ASCII view.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000	50	4B	03	04	14	00	06	00	08	00	00	21	00	FD	D1	PK.....!.yN	
00000010	5B	80	D1	01	00	00	BB	0C	00	00	13	00	08	02	5B	43	[eN...».....[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
00000030	6C	20	A2	04	02	28	A0	00	02	00	00	00	00	00	00	00	l e... (.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Offset: 50 Block: 50-50 Length: 1 Overwrite

3. DEMO: CONTENTS GUARD



3. SOFTWARE ADICIONAL

- Antivirus
- “Canción de Pyongyang”
- Paquetes ofimáticos



3. INTELIGENCIA

- Es posible recabar información de la Estrella Roja:
 - Nombres de programadores
 - Ri Yong Kel
 - Kim Yong Gwang
 - Direcciones de correo
 - ryk659@osd.inf.kp
 - glory@osandok.inf.kp
 - kyg1024@osd.inf.kp
 - IP
 - Dominios
 - Librería de cifrado



4. CONCLUSIONES



4. CONCLUSIONES

- Diseñado para el usuario
- Incorpora diferentes mecanismos de vigilancia
- Se desconoce su cuota de implantación
- Posiblemente exista una versión más moderna



4. CONTRAINTELIGENCIA

- Publicar SO / Apps falsos
 - Consumo de recursos para su obtención / análisis
- Malware



Q&A

- ¡Gracias!
-  @simonroses
-  @vulnexasl
- www.vulnex.com
- www.simonroses.com



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in

