Panda
MalwareRadar

Informe técnico

Roberto Peña González

Auditoría: North Secure

Fecha de comienzo: 27/05/2013 15:22:33 **Fecha de fin:** 28/05/2013 21:17:02

Informe técnico de análisis de los siguientes equipos

BT-ORD-57
BT-ORD-43

Información complementaria

Anexo I - Descripción de códigos maliciosos
Anexo II - Descripción de vulnerabilidades

Detalles de análisis de BT-ORD-57

Equipo: BT-ORD-57

IP: 192.168.3.71	Sistema Operativo: Windows XP Professional
Dominio: TXORIERRI	Service Pack: Service Pack 3
Nombre del usuario: TXORIERRI\Bizkargi1	Versión IE: 8.0.6001.18702
Grupo: Administradores,Usuarios	Versión Outlook: No detectado
	Versión Outlook Express: 6.0.2900.5512
	Navegador por defecto: Internet Explorer
	Cliente de correo por defecto: Outlook Express

Comienzo del análisis:	27/05/2013 15:20:15	**Fin del análisis:**	27/05/2013 16:19:01
Tipo del análisis:	Completo	**Elementos analizados:**	278611
		Archivos:	278610
		Mensajes:	1

No se ha encontrado código malicioso en su equipo.

Software de protección detectado:

- *ESET NOD32 Antivirus 3.0 3.0*

Protección	Activada	Actualizada
Antivirus	✓	✗

- *Windows Firewall*

Protección	Activada	Actualizada
Firewall	✗	

Códigos maliciosos:

No se han encontrado códigos maliciosos en este equipo

Cookies y Jokes:

Ubicación	Tipo	Detectados
C:\Documents and Settings\457Proiektua\Cookies	Cookie	5
C:\Documents and Settings\Administrador.TXORIERRI\Cookies	Cookie	2
C:\Documents and Settings\ana\Cookies	Cookie	4
C:\Documents and Settings\BERDINTASUNA\Cookies	Cookie	10
C:\Documents and Settings\Proyecto418\Cookies	Cookie	3
C:\Documents and Settings\usulocal\Cookies	Cookie	10

Vulnerabilidades:

No se han encontrado vulnerabilidades en este equipo

Detalles de análisis de BT-ORD-43

Equipo: BT-ORD-43

IP: 192.168.3.206	Sistema Operativo: Windows XP Professional
Dominio: TXORIERRI	Service Pack: Service Pack 3
Nombre del usuario: TXORIERRI\Bizkargi1	Versión IE: 8.0.6001.18702
Grupo: Administradores,Usuarios	Versión Outlook: No detectado
	Versión Outlook Express: 6.0.2900.5512
	Navegador por defecto: Internet Explorer
	Cliente de correo por defecto: OUTLOOK.EXE

Comienzo del análisis:	27/05/2013 15:22:46	**Fin del análisis:**	27/05/2013 17:05:38
Tipo del análisis:	Completo	**Elementos analizados:**	191053
		Archivos:	191052
		Mensajes:	1

No se ha encontrado código malicioso en su equipo.

Software de protección detectado:

- *ESET NOD32 Antivirus 4.0 4.0*

Protección	Activada	Actualizada
Antivirus	✓	✓

- *Windows Firewall*

Protección	Activada	Actualizada
Firewall	✓	

Códigos maliciosos:

No se han encontrado códigos maliciosos en este equipo

Cookies y Jokes:

Ubicación	Tipo	Detectados
C:\Documents and Settings\ADMINISTRADOR\Cookies	Cookie	3
C:\Documents and Settings\alejandro\Cookies	Cookie	3
C:\Documents and Settings\bizkargi1\Cookies	Cookie	21
C:\Documents and Settings\Bizkargi12\Cookies	Cookie	3
C:\Documents and Settings\elena\Cookies	Cookie	2
C:\Documents and Settings\eneko\Cookies	Cookie	2
C:\Documents and Settings\selekpro\Cookies	Cookie	3
C:\Documents and Settings\susana\Cookies	Cookie	3
C:\Documents and Settings\USULOCAL\Cookies	Cookie	6

Vulnerabilidades:

Identificador	Fecha de aparición	Criticidad
MS10-034	09/06/2010	Baja
MS10-032	09/06/2010	Baja
MS10-021	14/04/2010	Baja
MS10-020	14/04/2010	Baja
MS10-015	10/02/2010	Baja
MS10-012	10/02/2010	Baja
MS10-011	10/02/2010	Baja
MS10-008	10/02/2010	Baja
MS10-006	10/02/2010	Baja
MS09-065	11/11/2009	Baja
MS09-058	#Error	#Error
MS09-055	14/10/2009	Baja
MS09-032	15/07/2009	Baja
MS09-026	10/06/2009	Baja
MS09-025	10/06/2009	Baja
MS09-007	11/03/2009	Baja
MS09-006	11/03/2009	Baja
MS09-001	14/01/2009	Baja
MS08-068	12/11/2008	Baja
MS08-066	15/10/2008	Baja
MS08-063	15/10/2008	Baja
MS08-061	15/10/2008	Baja
MS08-037	09/07/2008	Baja
MS08-032	11/06/2008	Baja

Anexo I - Descripción de códigos maliciosos

No se ha encontrado código malicioso.

Anexo II - Descripción de vulnerabilidades

Identificador	**MS10-034**
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades críticas en varios controles ActiveX en ordenadores con Windows 2008/7/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	09/06/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-034.mspx

Identificador	**MS10-032**
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en los controladores modo kernel de Windows en ordenadores con Windows Server 2008/7/Vista/XP/2003/2000, que permite conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	09/06/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-032.mspx

Identificador	MS10-021
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en el Núcleo de Windows en ordenadores con Windows 2008/7/Vista/XP/2003/2000, que permite conseguir elevación local de privilegios y lanzar ataques de denegación de servicio.
Criticidad:	Baja
Fecha de aparición:	14/04/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/Bulletin/MS10-021.mspx

Identificador	MS10-020
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades críticas en el cliente SMB sobre ordenadores con Windows 2008/7/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión y lanzar ataques de denegación de servicio.
Criticidad:	Baja
Fecha de aparición:	14/04/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx

Identificador	MS10-015
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en el Núcleo de Windows en ordenadores con Windows 2008/7/Vista/XP/2003/2000, que permite conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/02/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-015.mspx

Identificador	MS10-012
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en el servidor SMB sobre ordenadores con Windows 2008/7/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión, lanzar ataques de denegación de servicio y conseguir elevación de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/02/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-012.mspx

Identificador	MS10-011
Descripción/Posibles efectos:	Es una vulnerabilidad importante en el subsistema de tiempo de ejecución de cliente-servidor de Windows (CSRSS) sobre ordenadores con Windows 2003/XP/2000, que permite conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/02/2010
Sistemas afectados:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-011.mspx

Identificador	MS10-008
Descripción/Posibles efectos:	Es una vulnerabilidad crítica en el control ActiveX de Data Analyzer en ordenadores con Windows 2008/7/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	10/02/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-008.mspx

Identificador	MS10-006
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades críticas en el cliente SMB sobre ordenadores con Windows 2008/7/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión, lanzar ataques de denegación de servicio y conseguir elevación de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/02/2010
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS10-006.mspx

Identificador	MS09-065
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades críticas en los controladores modo kernel de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión y conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	11/11/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms09-065.mspx

Identificador	MS09-058
Descripción/Posibles efectos:	#Error
Criticidad:	#Error
Fecha de aparición:	#Error
Sistemas afectados:	#Error
Amenazas que lo explotan:	#Error
Solucionable:	#Error
Link a Solución:	#Error

Identificador	MS09-055
Descripción/Posibles efectos:	Es una vulnerabilidad crítica en varios controles ActiveX, en ordenadores con Windows 7/2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	14/10/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms09-055.mspx

Identificador	MS09-032
Descripción/Posibles efectos:	Es una vulnerabilidad crítica en el control ActiveX Video, msvidctl.dll, en ordenadores con Windows 2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	15/07/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS09-032.mspx

Identificador	MS09-026
Descripción/Posibles efectos:	Es una vulnerabilidad importante en en la función de llamada a procedimiento remoto (RPC) de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/06/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms09-026.mspx

Identificador	MS09-025
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en el Núcleo de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	10/06/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms09-025.mspx

Identificador	MS09-007
Descripción/Posibles efectos:	Es una vulnerabilidad importante en el SChannel de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite la suplantación de identidad.
Criticidad:	Baja
Fecha de aparición:	11/03/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS09-007.mspx

Identificador	MS09-006
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades críticas en el Núcleo de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión y conseguir elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	11/03/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/MS09-006.mspx

Identificador	MS09-001
Descripción/Posibles efectos:	Se trata de un grupo de vulnerabilidades, calificadas como críticas, en el protocolo de bloque de mensajes del servidor (SMB) en ordenadores con Windows 2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión y lanzar ataques de denegación de servicio.
Criticidad:	Baja
Fecha de aparición:	14/01/2009
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Identificador	MS08-068
Descripción/Posibles efectos:	Se trata de una vulnerabilidad, calificada como importante, en el protocolo SMB en ordenadores con Windows 2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	12/11/2008
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-068.mspx

Identificador	MS08-066
Descripción/Posibles efectos:	Es una vulnerabilidad importante en el controlador de función auxiliar en Windows 2003/XP, que permite elevación local de privilegios en el sistema vulnerable.
Criticidad:	Baja
Fecha de aparición:	15/10/2008
Sistemas afectados:	WINDOWS2003, WINDOWSXP
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-066.mspx

Identificador	MS08-063
Descripción/Posibles efectos:	Se trata de una vulnerabilidad, calificada como importante, en el protocolo de bloque de mensajes del servidor (SMB) en ordenadores con Windows 2008/Vista/2003/XP/2000, que permite ejecutar remotamente código arbitrario con los mismos privilegios que el usuario que haya iniciado la sesión.
Criticidad:	Baja
Fecha de aparición:	15/10/2008
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-063.mspx

Identificador	MS08-061
Descripción/Posibles efectos:	Es un grupo de vulnerabilidades importantes en el Núcleo de Windows en ordenadores con Windows Server 2008/Vista/XP/2003/2000, que permite elevación local de privilegios.
Criticidad:	Baja
Fecha de aparición:	15/10/2008
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-061.mspx

Identificador	MS08-037
Descripción/Posibles efectos:	[AUTO]
Criticidad:	Baja
Fecha de aparición:	09/07/2008
Sistemas afectados:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-037.mspx

Identificador	MS08-032
Descripción/Posibles efectos:	[AUTO]
Criticidad:	Baja
Fecha de aparición:	11/06/2008
Sistemas afectados:	WINDOWSVISTA, WINDOWS2003, WINDOWSXP, WINDOWS2000
Amenazas que lo explotan:	
Solucionable:	Sí
Link a Solución:	http://www.microsoft.com/technet/security/bulletin/ms08-032.mspx