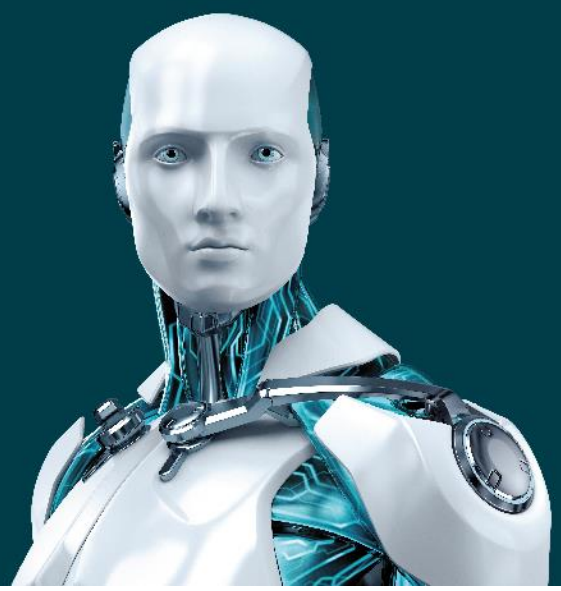
ENJOY SAFER TECHNOLOGY™

EXPLOTACIÓN DE VULNERABILIDADES EN WINDOWS DURANTE 2015



Contenido

Explotación de vulnerabilidades de Windows en 2015

En nuestro informe anterior "Explotación de vulnerabilidades de Windows durante 2014" mencionamos que la tendencia principal en los ciberataques modernos eran los ataques conocidos como 0-day (del día cero, o zero-day). Este término hace referencia a los que aprovechan vulnerabilidades sin reparar para introducirse en un sistema. En el informe del año pasado explicamos con detalle las técnicas empleadas por los atacantes, incluyendo la infección por páginas web y la elevación de privilegios para usuarios locales (del inglés LPE).

En esta nueva versión del informe no queremos repetir lo que ya describimos anteriormente. Por el contrario, nos concentraremos en las novedades de 2015: las nuevas funcionalidades de seguridad de Google Chrome y Microsoft Edge, información sobre exploits de Hacking Team y las nuevas características de EMET de Microsoft.

1. Información general

La siguiente tabla muestra las vulnerabilidades en los navegadores web Internet Explorer y Edge para las que se emitieron revisiones en los últimos doce meses. Las vulnerabilidades de la Tabla 1 que figuran en rojo son las que sabemos que fueron aprovechadas antes de que hubiera un parche disponible.

Componente	Boletín	Tipo	Vulnerabilidad
Internet Explorer	MS15-009, MS15-018, MS15-032, MS15-043, MS15-056, MS15-065, MS15-079, MS15-093, MS15-094, MS15-106, MS15-112, MS15-124	Ejecución remota de código (12)	CVE-2014-8967, CVE-2015-0017, CVE-2015-0018, CVE-2015-0019, CVE-2015-0020, CVE-2015-0021, CVE-2015-0022, CVE-2015-0023, CVE-2015-0025, CVE-2015-0026, CVE-2015-0027, CVE-2015-0028, CVE-2015-0029, CVE-2015-0030, CVE-2015-0031, CVE-2015-0035, CVE-2015-0036, CVE-2015-0037, CVE-2015-0038, CVE-2015-0039, CVE-2015-0040, CVE-2015-0041, CVE-2015-0042, CVE-2015-0043, CVE-2015-0044, CVE-2015-0045, CVE-2015-0046, CVE-2015-0048, CVE-2015-0049, CVE-2015-0050, CVE-2015-0051, CVE-2015-0052, CVE-2015-0053, CVE-2015-0054, CVE-2015-0055, CVE-2015-0066, CVE-2015-0067, CVE-2015-0068, CVE-2015-0069, CVE-2015-0070, CVE-2015-0071, CVE-2015-0032, CVE-2015-0056, CVE-2015-0072, CVE-2015-0099, CVE-2015-0100, CVE-2015-1622, CVE-2015-1623, CVE-2015-1624, CVE-2015-1625, CVE-2015-1626, CVE-2015-1627, CVE-2015-1634, CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1660, CVE-2015-1661, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668, CVE-2015-1658, CVE-2015-1684, CVE-2015-1685, CVE-2015-1686, CVE-2015-1688, CVE-2015-1689, CVE-2015-1691, CVE-2015-1692, CVE-2015-1694, CVE-2015-1703, CVE-2015-1704, CVE-2015-1705, CVE-2015-1706, CVE-2015-1708, CVE-2015-1709, CVE-2015-1710, CVE-2015-1711, CVE-2015-1712, CVE-2015-1713, CVE-2015-1714, CVE-2015-1717, CVE-2015-1718, CVE-2015-1687, CVE-2015-1730, CVE-2015-1731, CVE-2015-1732, CVE-2015-1735, CVE-2015-1736, CVE-2015-1737, CVE-2015-1739, CVE-2015-1740, CVE-2015-1741, CVE-2015-1742, CVE-2015-1743, CVE-2015-1744, CVE-2015-1745, CVE-2015-1747, CVE-2015-1748, CVE-2015-1750, CVE-2015-1751, CVE-2015-1752, CVE-2015-1753, CVE-2015-1754, CVE-2015-1755, CVE-2015-1765, CVE-2015-1766, CVE-2015-1729, CVE-2015-1733, CVE-2015-1738, CVE-2015-1767, CVE-2015-2372, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2388, CVE-2015-2389, CVE-2015-2390, CVE-2015-2391, CVE-2015-2397, CVE-2015-2398, CVE-2015-2401, CVE-2015-2402, CVE-2015-2403, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2410, CVE-2015-2411, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414, CVE-2015-2419, CVE-2015-2421, CVE-2015-2422, CVE-2015-2425, CVE-2015-2423, CVE-2015-2441, CVE-2015-2442, CVE-2015-2443, CVE-2015-2444, CVE-2015-2445, CVE-2015-2446,

			CVE-2015-2447, CVE-2015-2448, CVE-2015-2449, CVE-2015-2450, CVE-2015-2451, CVE-2015-2452, CVE-2015-2502, CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2493, CVE-2015-2494, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-2015-2541, CVE-2015-2542, CVE-2015-2482, CVE-2015-6042, CVE-2015-6044, CVE-2015-6046, CVE-2015-6047, CVE-2015-6048, CVE-2015-6049, CVE-2015-6050, CVE-2015-6051, CVE-2015-6052, CVE-2015-6053, CVE-2015-6055, CVE-2015-6056, CVE-2015-6059, CVE-2015-2427, CVE-2015-6064, CVE-2015-6065, CVE-2015-6066, CVE-2015-6068, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6072, CVE-2015-6073, CVE-2015-6074, CVE-2015-6075, CVE-2015-6076, CVE-2015-6077, CVE-2015-6078, CVE-2015-6079, CVE-2015-6080, CVE-2015-6081, CVE-2015-6082, CVE-2015-6084, CVE-2015-6085, CVE-2015-6086, CVE-2015-6087, CVE-2015-6088, CVE-2015-6089, CVE-2015-6083, CVE-2015-6134, CVE-2015-6135, CVE-2015-6136, CVE-2015-6138, CVE-2015-6139, CVE-2015-6140, CVE-2015-6141, CVE-2015-6142, CVE-2015-6143, CVE-2015-6144, CVE-2015-6145, CVE-2015-6146, CVE-2015-6147, CVE-2015-6148, CVE-2015-6149, CVE-2015-6150, CVE-2015-6151, CVE-2015-6152, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6156, CVE-2015-6157, CVE-2015-6158, CVE-2015-6159, CVE-2015-6160, CVE-2015-6161, CVE-2015-6162, CVE-2015-6164
Edge	MS15-091, MS15-095, MS15-107, MS15-113, MS15-125	Ejecución remota de código (4), Fuga de información (1)	CVE-2015-2441, CVE-2015-2442, CVE-2015-2446, CVE-2015-2449, CVE-2015-2485, CVE-2015-2486, CVE-2015-2494, CVE-2015-2542, CVE-2015-6057, CVE-2015-6058, CVE-2015-6064, CVE-2015-6073, CVE-2015-6078, CVE-2015-6088, CVE-2015-6139, CVE-2015-6140, CVE-2015-6142, CVE-2015-6148, CVE-2015-6151, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6158, CVE-2015-6159, CVE-2015-6161, CVE-2015-6168, CVE-2015-6169, CVE-2015-6170, CVE-2015-6176

Tablas 1: Vulnerabilidades corregidas de Internet Explorer y Edge

En el último año, Microsoft dejó de dar soporte a Internet Explorer (IE) 6 y anunció que el soporte de otras versiones de Internet Explorer, de la versión 7 a la versión 10, cesará el 12 de enero de 2016. Es una buena forma de incentivar a los usuarios para que pasen a una versión más segura: Internet Explorer 11. Por supuesto, Microsoft brindará soporte para las versiones anteriores de IE que funcionen con las correspondientes versiones de Windows (es decir, las versiones para las que estaban destinadas originalmente): por ejemplo, Windows Vista SP2 (IE9) o Windows Server 2012 (IE10).

Componente	Boletín	Tipo	Vulnerabilidad
Windows UMC (telnet service/tlntsess.exe, user profile service/ profsvc.dll, TS WebProxy/ Tswbprxy.exe, group policy, windowscodecs.dll, gdiplus.dll, VBScript, shell32.dll, msctf.dll, Adobe font driver/atmfd.dll, smss, csrsrv.dll, netlogon.dll, Task Scheduler/Ubpm.dll, Wmphoto.dll, RDP, Schannel.dll, Ksecdd.sys, Lsass.exe, Lsasrv.dll, Secur32.dll, Wdigest.dll, Clfsw32.dll, Ntdll.dll, msxml, Hyper-V/ vmms.exe, Journal/jnwdrv.dll, Jnwdui.dll, Jnwmon.dll, Silverlight, SCM/services.exe, Comctl32.dll, media player/	MS15-002, MS15-003, MS15-004, MS15-011, MS15-014, MS15-016, MS15-019, MS15-020, MS15-021, MS15-024, MS15-025, MS15-027, MS15-028, MS15-029, MS15-030, MS15-031, MS15-035, MS15-037, MS15-038, MS15-039, MS15-042, MS15-045, MS15-049, MS15-050, MS15-052, MS15-053, MS15-054, MS15-055, MS15-057, MS15-060, MS15-063, MS15-066, MS15-067, MS15-068, MS15-069, MS15-071, MS15-072, MS15-074, MS15-075, MS15-076, MS15-077, MS15-078, MS15-080, MS15-082, MS15-084, MS15-085, MS15-087, MS15-090, MS15-097, MS15-098, MS15-100, MS15-102, MS15-105, MS15-108, MS15-109,	Ejecución remota de código (28), Elevación de privilegios (19), Bypass de opciones de seguridad (8), Fuga de información (5), Spoofing (2), Denegación de Servicio (3)	CVE-2015-0014, CVE-2015-0004, CVE-2015-0016, CVE-2015-0008, CVE-2015-0009, CVE-2015-0061, CVE-2015-0032, CVE-2015-0081, CVE-2015-0096, CVE-2015-0074, CVE-2015-0087, CVE-2015-0088, CVE-2015-0089, CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, CVE-2015-0093, CVE-2015-0080, CVE-2015-0073, CVE-2015-0075, CVE-2015-0005, CVE-2015-0084, CVE-2015-0076, CVE-2015-0079, CVE-2015-1637, CVE-2015-1645, CVE-2015-0098, CVE-2015-1643, CVE-2015-1644, CVE-2015-1646, CVE-2015-1647, CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, CVE-2015-1699, CVE-2015-1715, CVE-2015-1702, CVE-2015-1674, CVE-2015-1684, CVE-2015-1686, CVE-2015-1681, CVE-2015-1716, CVE-2015-1728, CVE-2015-1756, CVE-2015-1758, CVE-2015-2372, CVE-2015-2373, CVE-2015-2361, CVE-2015-2362, CVE-2015-2368, CVE-2015-2369, CVE-2015-2374, CVE-2015-2364, CVE-2015-2371, CVE-2015-2416, CVE-2015-2417, CVE-2015-2370, CVE-2015-2387, CVE-2015-2426, CVE-2015-2431, CVE-2015-2432, CVE-2015-2435, CVE-2015-2453, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465, CVE-2015-2472, CVE-2015-2473, CVE-2015-2434, CVE-2015-2440, CVE-2015-2471, CVE-2015-1769, CVE-2015-2475, CVE-2015-2428, CVE-2015-2429, CVE-2015-2430, CVE-2015-2506, CVE-2015-2507, CVE-2015-2508, CVE-2015-2512, CVE-2015-2510, CVE-2015-2513, CVE-2015-2514, CVE-2015-

WMP.dll, CSRSS/csrss.exe, Msmmsp.dll, wow64.dll, Ehshell.dll, Taskeng.exe, DNS/Dns.exe, Uniscribe)	MS15-114, MS15-115, MS15-121, MS15-122, MS15-126, MS15-127, MS15-128, MS15-130, MS15-132, MS15-134	2516, CVE-2015-2519, CVE-2015-2530, CVE-2015-2509, CVE-2015-2524, CVE-2015-2525, CVE-2015-2528, CVE-2015-2534, CVE-2015-2482, CVE-2015-6052, CVE-2015-6055, CVE-2015-6059, CVE-2015-2515, CVE-2015-2548, CVE-2015-6097, CVE-2015-6103, CVE-2015-6104, CVE-2015-6112, CVE-2015-6095, CVE-2015-6135, CVE-2015-6136, CVE-2015-6125, CVE-2015-6106, CVE-2015-6107, CVE-2015-6108, CVE-2015-6130, CVE-2015-6128, CVE-2015-6132, CVE-2015-6133, CVE-2015-6127, CVE-2015-6131

Tabla 2: Vulnerabilidades corregidas en los componentes de modo de usuario de Windows (UMC)

Como se muestra en la Tabla 2, el año pasado MS corrigió una gran cantidad de vulnerabilidades en los componentes de modo de usuario (UMC, del inglés) de Windows. Estas vulnerabilidades pueden ser utilizadas por atacantes para llevar a cabo la Ejecución remota de código malicioso (RCE, del inglés) o para obtener los privilegios máximos en el sistema a través de una Escala de privilegios para usuarios locales (LPE, del inglés). Los atacantes emplean una segunda clase de vulnerabilidad en conjunto con los exploits RCE para obtener acceso completo al sistema, en lugar de tener que trabajar dentro de las limitaciones de una cuenta de usuario restringido.

La Imagen 1 muestra que en 2015 se corrigieron aproximadamente cuatro veces más vulnerabilidades que afectan a los componentes de modo de usuario (UMC) de Windows que en 2014.

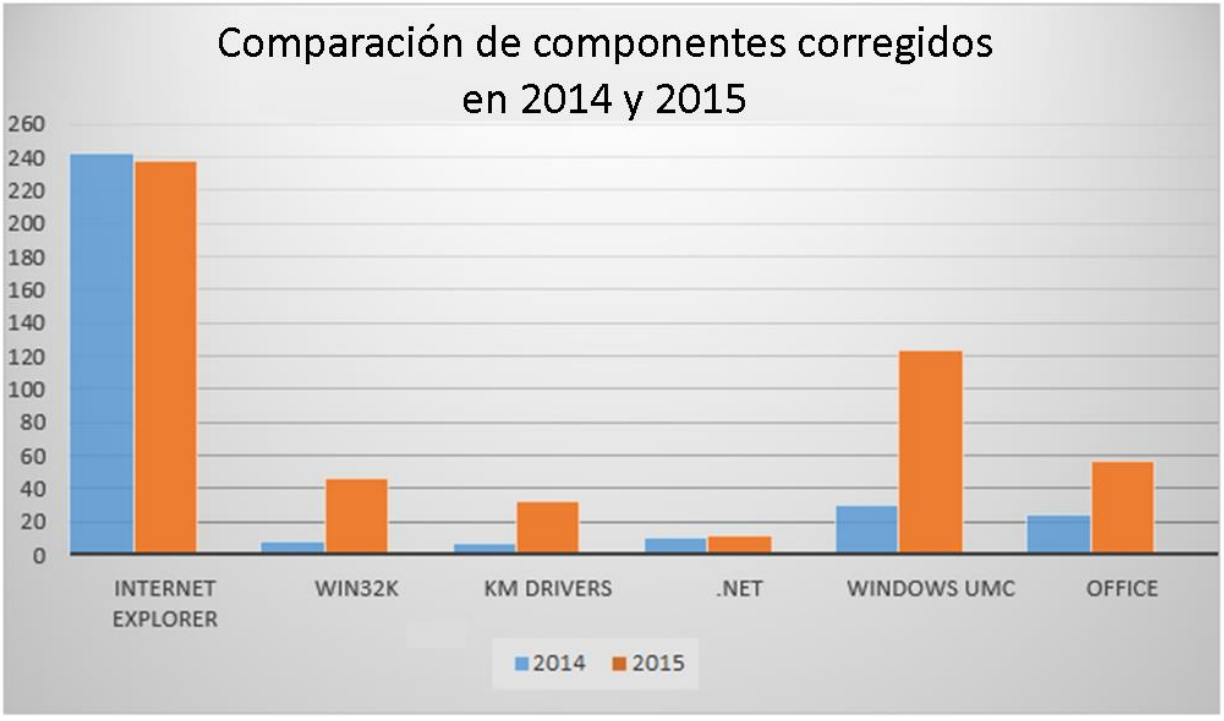


Imagen 1: Comparación de componentes corregidos en 2014 y 2015

Los atacantes suelen usar dos componentes para obtener privilegios de sistema en Windows: los controladores del modo de kernel (KM drivers, del inglés) y el componente de kernel de la interfaz gráfica del usuario de Windows llamado win32k.sys. La capacidad de estos componentes de ejecutar código en forma remota es muy peligrosa, dado que un atacante puede ejecutar código malicioso directamente en modo kernel. Es decir que puede hacerse con el control de todos los recursos de la PC y de las partes de la memoria principal utilizadas por el sistema.

Componente	Boletín	Tipo	Vulnerabilidad
Win32k	MS15-010, MS15-023, MS15-044, MS15-051, MS15-061, MS15-073, MS15-097, MS15-115, MS15-135	Ejecución remota de código (3), Elevación de privilegios (6)	CVE-2015-0003, CVE-2015-0057, CVE-2015-0058, CVE-2015-0059, CVE-2015-0060, CVE-2015-0077, CVE-2015-0078, CVE-2015-0094, CVE-2015-0095, CVE-2015-1670, CVE-2015-1671, CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, CVE-2015-1679, CVE-2015-1680, CVE-2015-1701, CVE-2015-1719, CVE-2015-1720, CVE-2015-1721, CVE-2015-1722, CVE-2015-1723, CVE-2015-1724, CVE-2015-1725, CVE-2015-1726, CVE-2015-1727, CVE-2015-1768, CVE-2015-2360, CVE-2015-2363, CVE-2015-2365, CVE-2015-2366, CVE-2015-2367, CVE-2015-2381, CVE-2015-2382, CVE-2015-2511, CVE-2015-2517, CVE-2015-2518, CVE-2015-2546, CVE-2015-2527, CVE-2015-2529, CVE-2015-6103, CVE-2015-6104, CVE-2015-6171, CVE-2015-6173, CVE-2015-6174, CVE-2015-6175
Drivers KM (ahcache.sys, mrxdav.sys, cng.sys, ntoskrnl, dfsc.sys, http.sys, clfs.sys, Fltmgr.sys, Ksecdd.sys, Srvnet.sys, Srv.sys, Ecache.sys, Mountmgr.sys, Ndis.sys, Tdx.sys, Afd.sys, Wfplwfs.sys, Ksecpkg.sys, Rmcast.sys)	MS15-001, MS15-008, MS15-010, MS15-011, MS15-025, MS15-034, MS15-038, MS15-052, MS15-080, MS15-083, MS15-085, MS15-090, MS15-111, MS15-115, MS15-117, MS15-119, MS15-120, MS15-121, MS15-122, MS15-133	Elevación de privilegios (11), Ejecución remota de código (5), Bypass de opciones de seguridad (2), Denegación de Servicio (1), Spoofing (1)	CVE-2015-0002, CVE-2015-0011, CVE-2015-0008, CVE-2015-0073, CVE-2015-0075, CVE-2015-1635, CVE-2015-1643, CVE-2015-1644, CVE-2015-1674, CVE-2015-2454, CVE-2015-2433, CVE-2015-2474, CVE-2015-1769, CVE-2015-2428, CVE-2015-2429, CVE-2015-2430, CVE-2015-2549, CVE-2015-2550, CVE-2015-2552, CVE-2015-2553, CVE-2015-2554, CVE-2015-6100, CVE-2015-6101, CVE-2015-6102, CVE-2015-6109, CVE-2015-6113, CVE-2015-6098, CVE-2015-2478, CVE-2015-6111, CVE-2015-6112, CVE-2015-6095, CVE-2015-6126
Framework .NET	MS15-041, MS15-048, MS15-092, MS15-101, MS15-118	Fuga de información (1), Elevación de privilegios (4)	CVE-2015-1648, CVE-2015-1672, CVE-2015-1673, CVE-2015-2479, CVE-2015-2480, CVE-2015-2481, CVE-2015-2504, CVE-2015-2526, CVE-2015-6096, CVE-2015-6099, CVE-2015-6115

Tabla 3: Vulnerabilidades en el kernel y en .NET Framework

La Imagen 2 demuestra que los componentes de Windows para los que se publicaron más parches en 2015 fueron Internet Explorer y UMC.

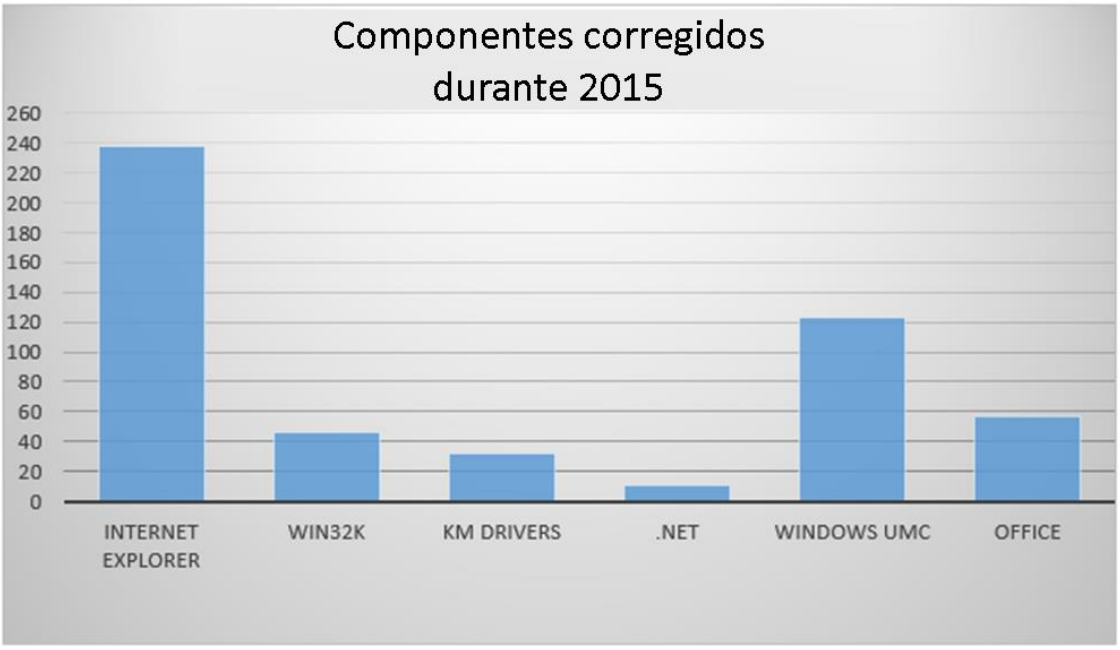


Imagen 2: Componentes corregidos durante 2015

En la Imagen 3 podemos notar que la mayor cantidad de actualizaciones cuya intención principal era solucionar fallas de RCE y LPE se publicaron para componentes UMC de Windows.

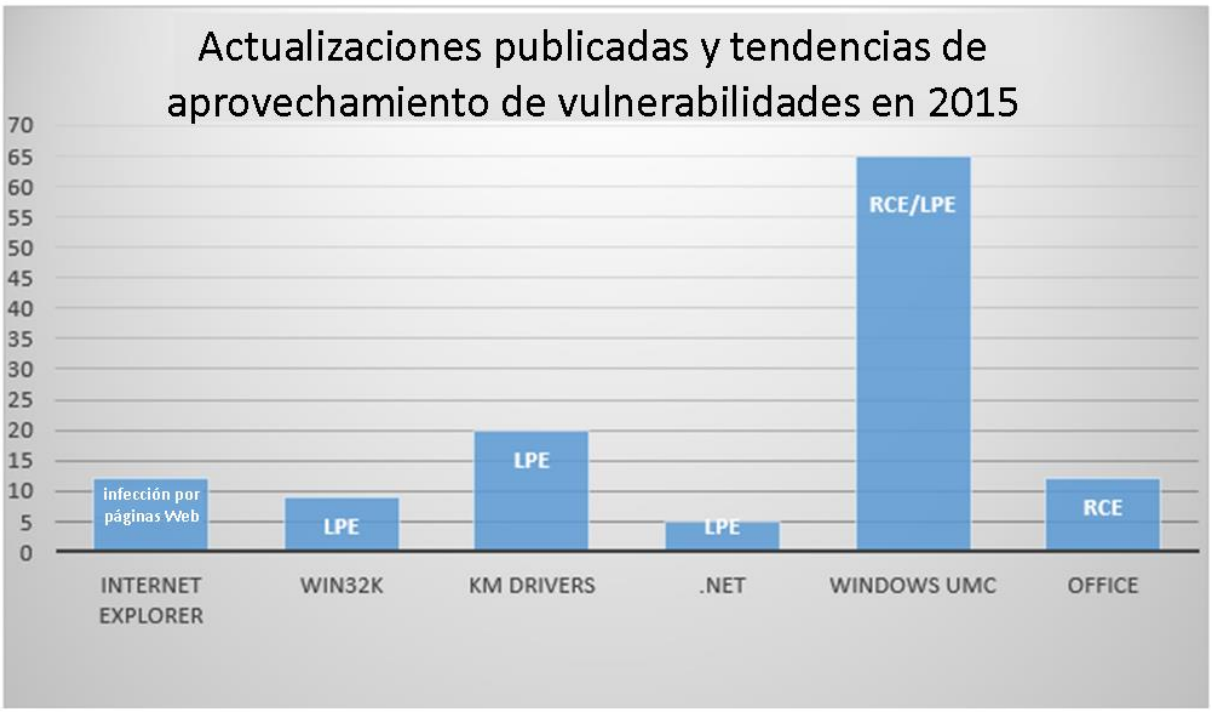


Imagen 3: Actualizaciones publicadas y tendencias de explotación de vulnerabilidades en 2015

En comparación con 2014, se solucionaron más errores en este último año en casi todas las categorías, con la excepción del navegador Web Internet Explorer, como se muestra en la Imagen 1.

2. Explotación de vulnerabilidades

En la versión 2014 de nuestro informe ya analizamos en detalle dos tipos de ataque prevalentes: la infección por páginas Web y la Escala de privilegios para usuarios locales. Los atacantes suelen incorporar el segundo tipo de ataque en el malware para conseguir privilegios de sistema. También se emplea en exploits RCE para eludir el modo sandbox de los navegadores y lograr ejecutar el payload ya sea desde el navegador o directamente en modo kernel.

La Tabla 4 muestra los detalles de las vulnerabilidades que fueron utilizadas por exploits in the wild, detectadas por los productos antimalware de ESET.

Vulnerabilidad in-the-wild	Detección de ESET	Mes	Ataque dirigido*
CVE-2015-0310	SWF/Exploit.CVE-2015-0310	Enero	No
CVE-2015-0311	SWF/Exploit.CVE-2015-0311	Enero	No
CVE-2015-0313	SWF/Exploit.CVE-2015-0313	Febrero	Sí
CVE-2015-3113	SWF/Exploit.CVE-2015-3113	Junio	Sí
CVE-2015-5119	SWF/Exploit.Agent.IG; SWF/Exploit.ExKit.AX; SWF/Exploit.CVE2015-5119	Julio	No
CVE-2015-5122	SWF/Exploit.Agent.IG; SWF/Exploit.CVE-2015-5122	Julio	No
CVE-2015-5123	SWF/Exploit.Agent.IR; SWF/Exploit.CVE-2015-5123	Julio	No
CVE-2015-4495	JS/Exploit.CVE-2015-4495	Agosto	Sí

Tabla 4: Detección de vulnerabilidades in the wild por ESET

Una de las vulnerabilidades LPE más memorables del último año fue CVE-2015-1769 (una vulnerabilidad de elevación de privilegios en el Mount Manager), que fue corregida por una actualización muy importante: MS15-085. Se trataba de una vulnerabilidad ubicada en el subsistema Mount Manager de Windows que afectaba a las ediciones cliente y servidor de Windows, desde la versión Vista en adelante. Les permitía a los atacantes ejecutar código arbitrario desde una unidad extraíble USB con privilegios de sistema mediante archivos con vínculos simbólicos especialmente diseñados, ubicados en la carpeta raíz.

Aunque decimos que esta vulnerabilidad es similar a Stuxnet, en realidad es menos peligrosa que la falla Stuxnet original (que se reparó con la actualización MS10-046) porque la vulnerabilidad CVE-2015-1769 no está ubicada en el Shell de Windows y solo se acciona cuando se inserta una unidad USB en uno de los puertos USB de la PC. En otras palabras, antes que nada, el atacante debe tener acceso físico a la PC. La actualización MS15-085 corrige el controlador *mountmgr.sys* y dos de los archivos kernel de Windows: *ntdll.dll* y *ntoskrnl.exe*.

Otra vulnerabilidad peligrosa que aprovecharon los atacantes fue CVE-2015-1635. Estaba ubicada en el controlador del sistema *http.sys* en Windows 7 y versiones posteriores, y les permitía a los atacantes ejecutar códigos maliciosos en forma remota con privilegios de sistema, para luego llevar a cabo ataques de denegación de servicio o infectar el sistema deseado con la Pantalla azul de la muerte (BSoD, del inglés). Una vulnerabilidad más relevante para Windows Server, que sirve conexiones HTTP, puede ser aprovechada con mucha facilidad mediante el establecimiento de un valor especial en el parámetro de la cabecera HTTP Rango ("Range") para activar un error de desbordamiento de enteros. El exploit para la vulnerabilidad CVE-2015-1635 se veía así:

```
GET /%7Bwelcome.png HTTP/1.1
User-Agent: Wget/1.13.4 (linux-gnu)
Accept: */*
Host: [server-ip]
Connection: Keep-Alive
Range: bytes=18-18446744073709551615
```

3. Hacking Team

El ataque informático del grupo cibernético Hacking Team (HT) seguramente es la historia más esclarecedora no solo de este año sino de los últimos años (por no decir de todos los tiempos). Desde el punto de vista legal y ético, es un ejemplo de los temas abordados por el tan discutido Acuerdo de Wassenaar, ya que algunos de los documentos que se filtraron demuestran que HT se especializaba en la venta de sus herramientas ofensivas a varios países legalmente inapropiados.

Los exploits 0-day que se filtraron para Windows, Flash Player e Internet Explorer se utilizaron (o podrían haberse utilizado) por los clientes de HT como instrumentos perfectos para organizar un poderoso ataque dirigido mediante infecciones por páginas web. El análisis del código fuente demostró que los exploits para Flash Player funcionaban en varios navegadores, como Microsoft Internet Explorer y Edge, Google Chrome, Mozilla Firefox y Opera. Por otra parte, algunos no solo funcionaban en Windows, sino también en Linux y Apple OS X.

CVE	Componente	Tipo	Corregido	Detección de ESET
CVE-2015-5119	Adobe Flash Player	RCE	APSB15-16	SWF/Exploit.CVE-2015-5119
CVE-2015-5122	Adobe Flash Player	RCE	APSB15-18	SWF/Exploit.CVE-2015-5122
CVE-2015-5123	Adobe Flash Player	RCE	APSB15-18	SWF/Exploit.CVE-2015-5123
CVE-2015-2387	MS Windows Vista – Win 8.1	LPE	MS15-077	Win32/Exploit.Agent.NCB; Win32/Exploit.CVE-2015-2387
CVE-2015-2425	MS Internet Explorer 11	RCE	MS15-065	
CVE-2015-2426	MS Windows Vista – Win 8.1	LPE	MS15-078	Win32/Exploit.CVE-2015-2426

Tabla 5: Detecciones de exploits del Hacking Team que se filtraron

Es difícil decidir qué es mejor: que los exploits 0-day fueran desconocidos e inaccesibles para el público o que estuvieran disponibles, pero solo para el uso privado de los clientes de HT. El primer caso es peligroso porque muchos ciberdelincuentes adaptaron rápidamente los exploits 0-day para utilizarlos en exploit kits comerciales. Esta situación es bastante alarmante para los usuarios, ya que las infecciones por páginas web afectan incluso las máquinas Windows con todas las actualizaciones y revisiones correspondientes (hasta a la fecha). El Equipo de ESET de Respuesta ante Malware agrega las firmas de exploits lo antes posible.

La Tabla 5 muestra información sobre los exploits de HT que se filtraron y los nombres de detección correspondientes de ESET.

Hacking Team ofreció a sus clientes la posibilidad de implementar herramientas de vigilancia (backdoors) en todas las plataformas principales para equipos de escritorio y dispositivos móviles: Windows, Linux, Android, OS X e iOS.

La Tabla 6 muestra un resumen con las detecciones de las familias de backdoors del HT. Los diversos backdoors para Windows se detectan como parte de la misma familia *Win32/Agent*.

Plataforma	Nombre de detección
Microsoft Windows	Win32/TrojanDropper.Morcut
Linux	Linux/Spy.Morcut
Google Android	Android/Morcut
Apple OS X	OSX/Morcut; OSX/Morcut.X.Gen; OSX/TrojanDropper.Morcut
Apple iOS	iOS/TrojanDropper.Morcut; iOS/Spy.Morcut
CVE-2015-2426	MS Windows Vista – Win 8.1

Tabla 6: Nombres de detección de las familias de backdoors del HT por plataforma

4. Google Chrome

Los desarrolladores del navegador web Google Chrome están haciendo todo lo posible para dificultarles la vida a los atacantes y así aumentar significativamente el costo para desarrollar exploits estables. En el último año, Google introdujo métodos útiles para mitigar los ataques de exploits.

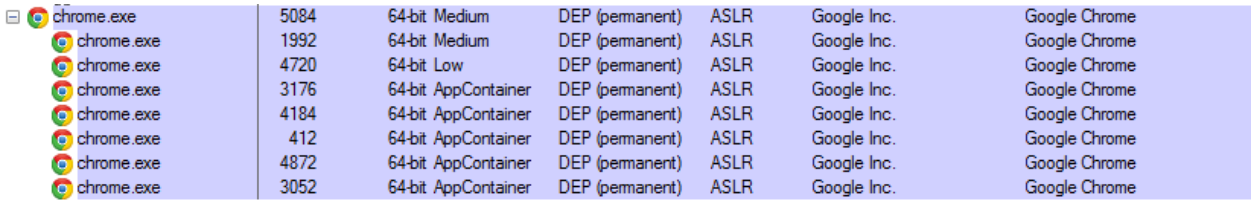
En primer lugar, analizamos los métodos de mitigación para exploits LPE que se basan en deshabilitar el controlador *win32k.sys*, una fuente notable de varias fallas en el kernel de Windows. Esta restricción se llama "bloqueo del renderizador win32k" y se aplica a los procesos que se llevan a cabo en modo sandbox, también conocidos como procesos de renderización. Esta funcionalidad está disponible para los usuarios de Windows 8 y versiones posteriores (*SetProcessMitigationPolicy*). La medida de seguridad tiene como objetivo principal reducir las oportunidades de los atacantes de eludir el modo sandbox de Chrome y ejecutar códigos maliciosos con el nivel más alto de privilegios.

Ya escribimos sobre el modo sandbox de Chrome en 2013: se basa en mecanismos propios de Windows como el bajo nivel de integridad, la denegación del SID, la restricción de objetos JOB especiales y la eliminación de los privilegios del token de procesos en modo sandbox. Pero estas medidas son útiles solamente para exploits RCE y exploits basados en la explotación de código en modo usuario. Los atacantes cuyo objetivo es penetrar en forma completa en el sistema de destino para conseguir los privilegios máximos utilizan un exploit RCE junto con otro exploit LPE que suele estar destinado para aprovecharse del controlador *win32k.sys* y que puede ayudar a los atacantes a ejecutar su código malicioso directamente en modo kernel.

A partir de la versión 47 de Chrome, todos los usuarios de este navegador tienen una opción especial llamada "PPAPI win32k lockdown" que pueden encontrar en la dirección `chrome://flags` y que se usa para activar el modo de bloqueo de win32k, ya sea para todos los procesos de renderización o simplemente para los complementos Flash o PDF.

Otro método para mitigar el ataque de exploits que introdujo Chrome tiene que ver con el programa Flash Player y se llama "*vector.<uint> exploit hardening*". Esta medida de seguridad incorporó controles especiales de verificación y un nuevo tipo de asignación de bloques de memoria para proteger los procesos de Flash Player ante vulnerabilidades potenciales, como los desbordamientos de búfer (BufferOv).

A partir de la versión M48 beta de Chrome, los desarrolladores de Google introdujeron el modo sandbox AppContainer para los procesos de renderización. Esta funcionalidad de seguridad es similar al modo sandbox de MS Internet Explorer 11 con el Modo protegido mejorado (EPM, por sus siglas en inglés) y de Edge. La función se encuentra desactivada por defecto: para activarla, el usuario debe configurar la opción "Habilitar AppContainer Lockdown" en `chrome://flags`.



chrome.exe	5084	64-bit Medium	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	1992	64-bit Medium	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	4720	64-bit Low	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	3176	64-bit AppContainer	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	4184	64-bit AppContainer	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	412	64-bit AppContainer	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	4872	64-bit AppContainer	DEP (permanent)	ASLR	Google Inc.	Google Chrome
chrome.exe	3052	64-bit AppContainer	DEP (permanent)	ASLR	Google Inc.	Google Chrome

Imagen 4: Bloqueo de AppContainer

La versión M48 beta de Google contiene la opción de activar el modo sandbox AppContainer, además de las técnicas de seguridad ya existentes como la denegación del SID, la eliminación de los privilegios del token de acceso y la restricción de objetos JOB.

Para mejorar la seguridad de los usuarios y motivarlos a pasar de las versiones viejas (e inseguras) a las versiones más nuevas de Windows, Google también comunicó que finalizaría el soporte de su navegador para las versiones Windows XP y Windows Vista a partir de abril de 2016. Esto significa que los usuarios de estas plataformas no recibirán actualizaciones de seguridad y otras actualizaciones para el navegador.

5. Edge

Edge es un navegador web desarrollado por Microsoft especialmente para Windows 10. Contiene fuertes opciones de seguridad que, a diferencia de Internet Explorer 11, están activadas en forma predeterminada. Las pestañas de Edge se ejecutan por defecto como procesos de 64 bits en el modo AppContainer. Edge es un navegador completamente nuevo, que no fue creado para ofrecer compatibilidad con los viejos complementos. Por otra parte, no es compatible con varias tecnologías antiguas y heredadas, como ActiveX, BHO y VBScript. Estas tecnologías a menudo son utilizadas por el malware y los exploits para penetrar en un sistema a través de un navegador web, incluyendo vulnerabilidades en el motor VBScript: *vbscript.dll*.

En la primera actualización principal de Windows 10, Microsoft sacó una nueva funcionalidad de seguridad para Edge: se trata de una opción que protege el navegador de la inyección binaria. Ahora, para cargar correctamente un archivo DLL en un navegador, la biblioteca debe estar firmada con un certificado digital de Microsoft o debe estar aprobada y certificada por Microsoft Windows Hardware Quality Lab (WHQL). La medida de seguridad bloquea la carga de todas las demás bibliotecas en el contexto de los procesos del navegador que no cumplan con dichas condiciones. Sin embargo, aún permite que se carguen los controladores de video para la aceleración en 3D, por lo que estos controladores podrían ser vistos como una manera de entrar en el sistema y pueden resultar objeto de amenazas en el futuro (aunque aun así necesitarán pasar por alto los mecanismos de defensa de Edge).

6. EMET

Microsoft viene mejorando su herramienta Enhanced Mitigation Experience Toolkit (EMET) año tras año. Esta herramienta cubre una amplia variedad de exploits y técnicas RCE. Su última versión de EMET incorporó un nuevo mecanismo que ayuda a proteger a los usuarios ante los exploits LPE que aprovechan vulnerabilidades en *win32k.sys* mediante el uso de archivos de fuentes especialmente creados con dicho propósito. Esta funcionalidad, denominada *Bloqueo de fuentes que no son de confianza*, está disponible para usuarios de Windows 10. La funcionalidad es similar a la función llamada *SetProcessMitigationPolicy* con el argumento no documentado *ProcessFontDisablePolicy*. Esta versión de EMET es compatible con Windows 10.

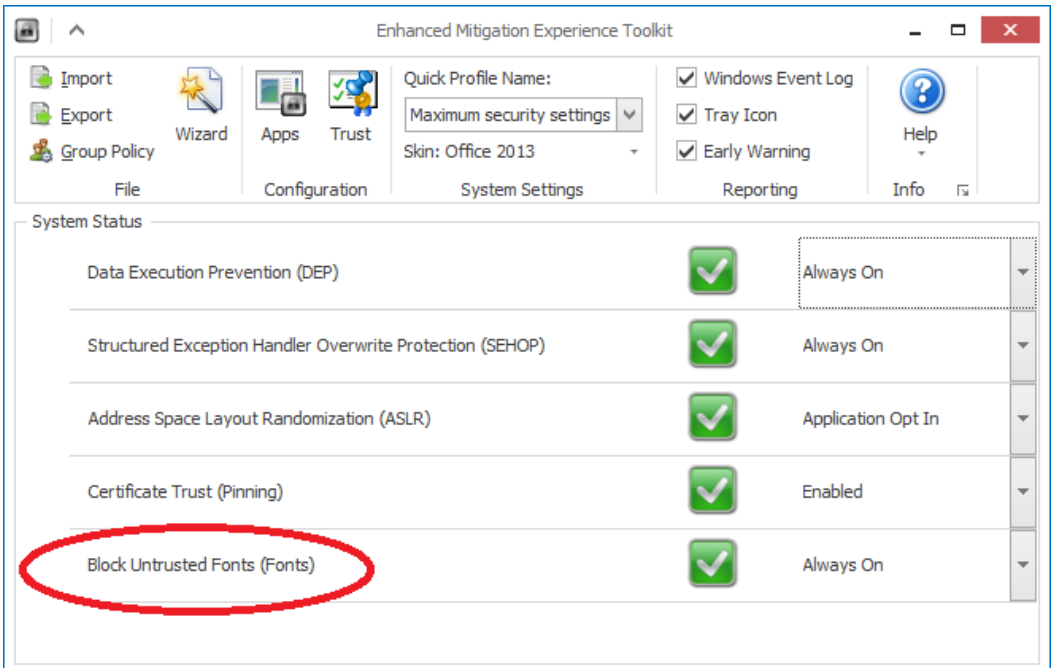


Imagen 5: Bloqueo de fuentes que no son de confianza

La versión 5.5 beta de EMET les permite a los usuarios habilitar opciones especiales de mitigación para contrarrestar la actividad de los exploits LPE, que activan vulnerabilidades (la mayoría en *win32k.sys*) mediante el uso de los llamados archivos de fuentes que no son de confianza. Microsoft los define como fuentes que se instalan fuera del directorio de fuentes %windir%/fonts.

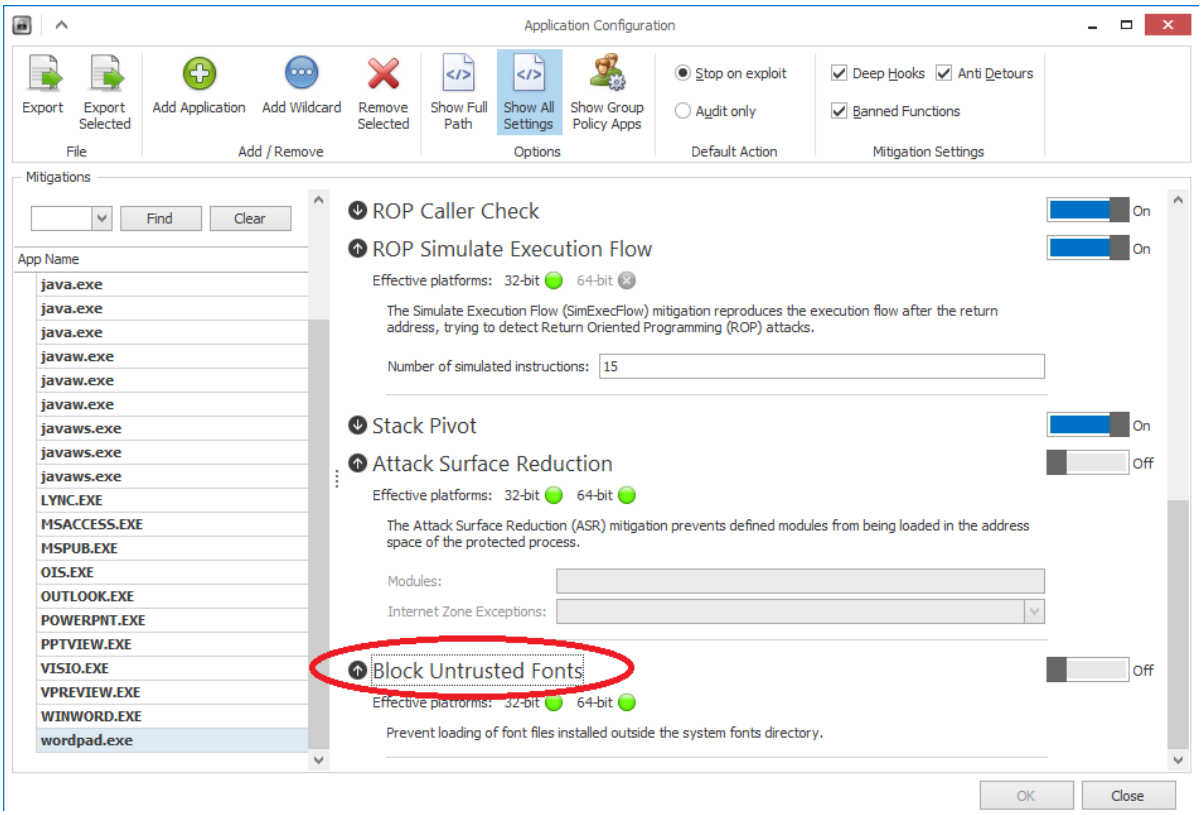


Imagen 6: Fuentes que no son de confianza

En el informe "Explotación de vulnerabilidades en Windows durante 2014" se detalla información sobre otras de las funcionalidades de seguridad de EMET.

7. Conclusión

En este informe exploramos varias medidas de seguridad para los navegadores web y para EMET incorporadas en el transcurso del último año. También presentamos información estadística acerca de las vulnerabilidades corregidas de los productos de Microsoft. Los componentes más peligrosos para los usuarios fueron los de modo usuario de Windows, dado que se incorporaron en ataques que efectivamente se estaban implementando.