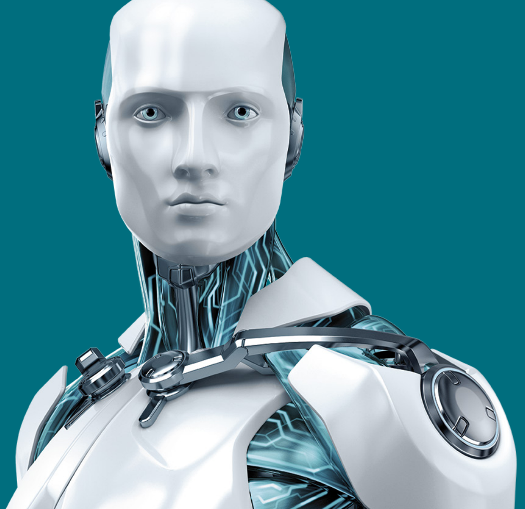
ENJOY SAFER TECHNOLOGY™

WINDOWS EXPLOITATION IN 2015



WINDOWS EXPLOITATION IN 2015

In our previous report "Windows exploitation in 2014", we mentioned a major trend in modern cyberattacks called 0day (or 0-day, or zero-day) attacks. This term refers to attacks that take advantage of unpatched vulnerabilities to penetrate into a system. Last year's report contained comprehensive information about the techniques used by attackers, including drive-by downloads and Local Privilege Escalation (LPE).

In this new version of our report we will not repeat what we have previously described. Instead, we will focus on what was new on the radar in 2015: new security features in Google Chrome and Microsoft Edge, information about Hacking Team exploits, and new features of Microsoft's Enhanced Mitigation Experience Toolkit (EMET).

General information

The table below lists vulnerabilities in the web browsers Internet Explorer and Edge that have been fixed over the past 12 months. Vulnerabilities shown in red in *Table 1* are known to have been exploited in the wild.

Component	Bulletin	Type	Vulnerability
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	Remote Code Execution (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	Remote Code Execution(4), Information Disclosure(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

Table 1: Vulnerabilities Fixed in Internet Explorer and Edge

In the last year, Microsoft has ceased support of Internet Explorer (IE) 6 and announced that support of other versions of Internet Explorer, from version 7 to version 10, will stop from January 12, 2016. This is a good incentive for users to move to the safer Internet Explorer version 11. Of course, Microsoft will support earlier versions of IE to be found in use with corresponding Windows versions (that is, the versions for which they were originally intended): for example, Windows Vista SP2 (IE9) or Windows Server 2012 (IE10).

Component	Bulletin	Type	Vulnerability
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/ WMP.dll, CSRSS/csrss.exe, Msmmsp.dll, wow64.dll, Ehshell.dll, Taskeng.exe, DNS/Dns.exe, Uniscribe)	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, MS15-114, MS15-115, MS15-121, MS15-122, MS15-126, MS15-127, MS15-128, MS15-130, MS15-132, MS15-134	Remote Code Execution(28), Elevation of Privilege(19), Security Feature Bypass(8), Information Disclosure(5), Spoofing(2), Denial of Service(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-2015-2516, 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

Table 2: Vulnerabilities Fixed in Windows User Mode Components

As shown in *Table 2*, in the past year MS has fixed a large number of vulnerabilities in various user mode Windows components (Windows UMC). These vulnerabilities can be used by attackers to implement remote execution of malicious code (Remote Code Execution, RCE) or to achieve maximum SYSTEM privileges on the system through Local Privilege Escalation (LPE). A second class of vulnerability can be used by attackers in conjunction with RCE exploits to gain full access to the system, instead of having to work within the constraints of a restricted user account.

Figure 1 below shows that in 2015 approximately four times more vulnerabilities affecting Windows user mode components were fixed than in 2014.

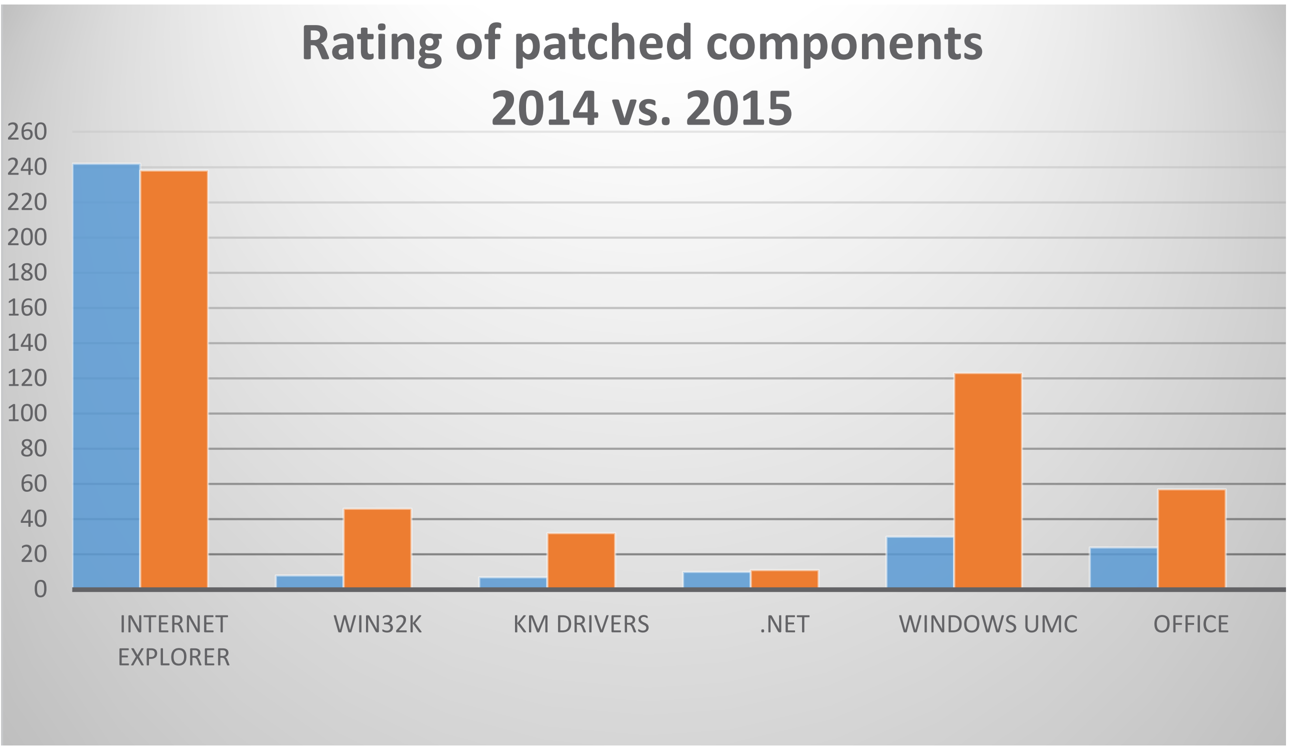


Figure 1: Comparison of components patched 2014-2015

Kernel mode (KM) drivers and the kernel component of the Windows GUI called win32k.sys are typically used by attackers to gain SYSTEM privileges in Windows. The ability of such components to execute code remotely is very dangerous, because an attacker can run malicious code directly in kernel mode. That is, he can gain control of all the PC's resources and the parts of main memory used by system.

Component	Bulletin	Type	Vulnerability
Win32k	MS15-010, MS15-023, MS15-044, MS15-051, MS15-061, MS15-073, MS15-097, MS15-115, MS15-135	Remote Code Execution(3), Elevation of Privilege(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
KM drivers (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	Elevation of Privilege(11), Remote Code Execution(5), Security Feature Bypass(2), Denial of Service(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
.NET Framework	MS15-041, MS15-048, MS15-092, MS15-101, MS15-118	Information Disclosure(1), Elevation of Privilege(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

Table 3: Vulnerabilities in the Kernel and .NET Framework

Figure 2 below shows that Internet Explorer and UMC components were the Windows components most patched in 2015.

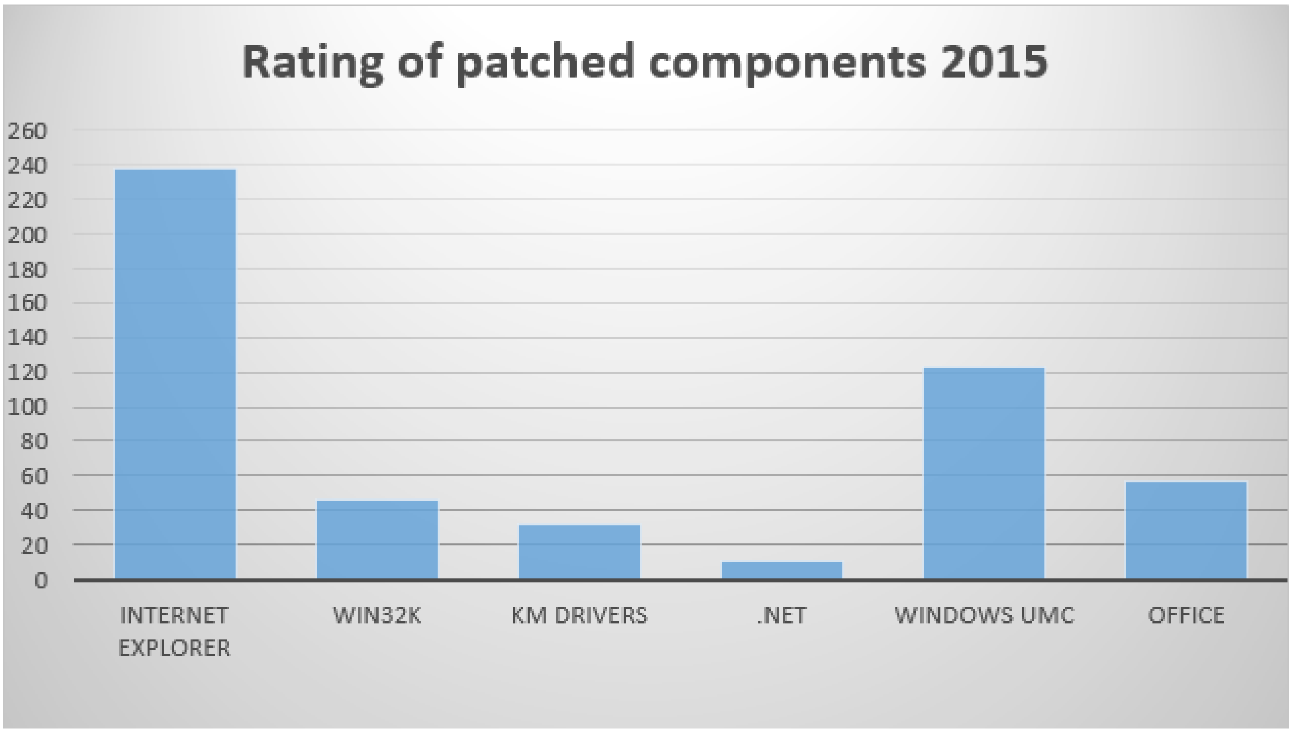


Figure 2: Proportions of patched components 2015

From *Figure 3* we can see that the largest number of updates intended predominantly to fix RCE and LPE flaws was issued for Windows UMC .

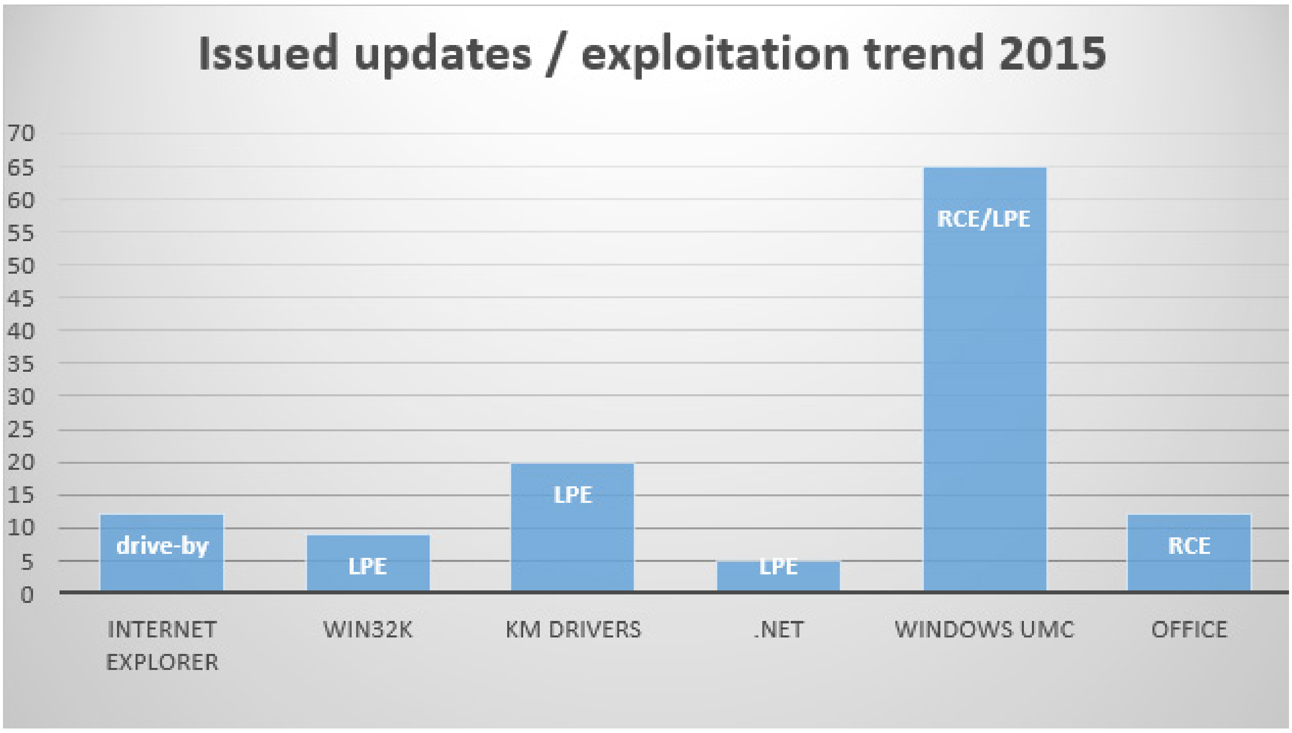


Figure 3: Updates and Exploitation Trends 2015

In comparison with 2014, more bugs in the past year were closed in almost all categories, the exception being the Internet Explorer web browser, as shown in *Figure 1*.

Exploitation

We have considered in detail two major types of attack in the 2014 version of our report: drive-by download and Local Privilege Escalation (LPE). The second type of attack can be incorporated by attackers into malware to achieve SYSTEM privileges into the system as well as being used for RCE-exploits to bypass a browser's sandbox to run the payload there or directly in kernel mode.

Table 4 below gives details of detection by ESET antimalware products for vulnerabilities known to have been used by exploits In the Wild (ItW).

Vulnerability in-the-wild	ESET detection	Month	Targeted attack*
CVE-2015-0310	SWF/Exploit.CVE-2015-0310	January	No
CVE-2015-0311	SWF/Exploit.CVE-2015-0311	January	No
CVE-2015-0313	SWF/Exploit.CVE-2015-0313	February	Yes
CVE-2015-3113	SWF/Exploit.CVE-2015-3113	June	Yes
CVE-2015-5119	SWF/Exploit.Agent.IG; SWF/Exploit.ExKit.AX; SWF/Exploit.CVE-2015-5119	July	No
CVE-2015-5122	SWF/Exploit.Agent.IG; SWF/Exploit.CVE-2015-5122	July	No
CVE-2015-5123	SWF/Exploit.Agent.IR; SWF/Exploit.CVE-2015-5123	July	No
CVE-2015-4495	JS/Exploit.CVE-2015-4495	August	Yes

Table 4: ESET Detection of Vulnerabilities In the Wild

One of the most memorable LPE vulnerabilities in the past year was *CVE-2015-1769* (Mount Manager Elevation of Privilege Vulnerability): the vulnerability was fixed by the important update *MS15-085*. A vulnerability was located in the Windows Mount Manager subsystem and affected both client and server editions of Windows from Vista onwards. It allowed attackers to run arbitrary code from a removable USB drive with SYSTEM privileges via specially-crafted symbolic link files in the root folder. We call this vulnerability *Stuxnet-like*, but it is less dangerous than original Stuxnet flaw – which was fixed by the MS10-046 update – because the CVE-2015-1769 is not located in Windows Shell and is triggered only when a USB drive is inserted into one of a PC's USB ports. In other words, an attacker needs physical access to the PC. The MS15-085 update patched the *mountmgr.sys* driver and two Windows kernel files – *ntdll.dll* and *ntoskrnl.exe*.

Another dangerous vulnerability to be exploited by attackers was *CVE-2015-1635*. This was located in the system driver *http.sys* on Windows 7 and later, and allowed attackers to execute malicious code remotely with SYSTEM privileges, to launch DoS-attacks, or to bring down a targeted system with a Blue Screen of Death (BSoD). A vulnerability more relevant to Windows Server, which serves http connections, it can be exploited very easily by setting a special value in the "Range" HTTP header parameter to trigger an integer overflow flaw. The exploit for CVE-2015-1635 looked like this:

```
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
```

Hacking Team

The hacking of the Hacking Team (HT) cybergroup was the most enlightening story not only of last year, but of the last several years (or maybe ever). From the legal and ethical point of view, it exemplifies the issues addressed by the much-discussed Wassenaar Arrangement, because leaked documents show that HT specialized in selling their offensive tools to various legally inappropriate countries.

Leaked 0day exploits for Windows, Flash Player and Internet Explorer were used (or could be used) by HT's customers as perfect instruments for organizing a powerful targeted attack using drive-by downloads. It was discovered in source code that exploits for Flash Player worked for several browsers, including Microsoft Internet Explorer and Edge, Google Chrome, Mozilla Firefox, and Opera: moreover, some exploits were capable of working not only on Windows but also on Linux and Apple OS X.

CVE	Component	Type	Fixed	ESET detection
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 – Win8.1	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 – Win8.1	LPE	MS15-078	Win32/Exploit.CVE-2015-2426

Table 5: Detections of Leaked Hacking Team Exploits.

It's difficult to say which was better: for 0day exploits to be unknown and inaccessible to the public or for them to be still available but only for the private use of HT's customers. The first case is dangerous because many cybercriminals implemented a *quick adaptation of* 0day exploits to use them in commercial exploit kits. This situation is really scary for users, because drive-by attacks affect fully patched (up-to-date) Windows machines. ESET's Malware Response Team added signatures of the aforementioned exploits as quickly as possible. In *Table* 5 above you can see information about HT's leaked exploits and ESET's corresponding detection names.

Hacking Team offered its customers the ability to deploy surveillance tools (backdoors) on all major desktop and mobile platforms: Windows, Linux, Android, OS X, and iOS. In *Table* 6 summarized families of detections for HT backdoors. We detect the various backdoors for Windows as part of the Win32/Agent family.

Platform	Detection name
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

Table 6: Detection Names for HT's Backdoor Families by Platform

Google Chrome

The developers of the Google Chrome web browser are doing everything possible to make life for attackers more difficult and thus to significantly increase the cost of developing a stable exploit. In the past year, Google has introduced useful methods of exploit mitigation. First of all, we consider LPE exploit mitigation methods based on disabling the use of the win32k.sys driver, which is notorious as a source of various Windows kernel flaws. This restriction is called "win32k renderer lockdown" and applies to processes working within sandboxed tabs and are also called *"render processes"*. This feature is available for users of Windows 8+ (*SetProcessMitigationPolicy*). The main goal of this security measure is to reduce the opportunities for attackers to bypass the Chrome sandbox and run malicious code at the highest privilege level.

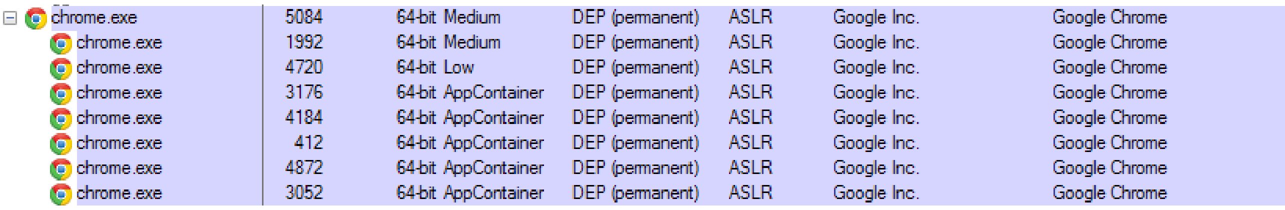
We already *wrote* about the Chrome sandbox in 2013: it relies on such Windows mechanisms as low integrity level, Deny SID, special restricted job objects, and removal of privileges from the token of a sandboxed process. But these measures are useful only for RCE-exploits and for exploits that rely on exploitation of user mode code. Attackers who aim to do a complete penetration with the intention of getting maximum privileges in the target system use an RCE-exploit in conjunction with another LPE-exploit that is usually intended to exploit the win32k.sys driver and can help attackers to run their code directly in kernel mode.

Starting from Chrome version 47, all users of this browser have a special option called "*PPAPI* win32k lockdown" that they can find at the address chrome://flags and can use it to enable win32k lockdown mode either for all render processes or just for Flash or PDF plugins.

Another exploit mitigation *method* introduced for Chrome refers to Flash Player and is called "*vector.<uint> exploit hardening*". This security measure introduced special checks and a new type of heap allocation to protect Flash Player process from infamous potential vulnerabilities like buffer overflows (BufferOv).

As of the Chrome M48 beta, Google developers introduced the AppContainer sandbox for render processes. This security feature is similar to the sandbox in MS Internet Explorer 11 with Enhanced

Protected Mode (EPM) and Edge. By default this feature is turned off: in order to turn it on, the user should set option "Enable AppContainer Lockdown" at 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

Figure 4: AppContainer Lockdown

The Google M48 beta contains the option to turn on the AppContainer sandbox, along with already-existing security techniques like Deny SID, removal of privileges from access token, and restrictive job object.

To improve the safety of users and encourage them to move on from old (insecure) Windows versions, Google also promised to end support of the browser for Windows XP and Windows Vista from April 2016. This means that users on those platforms will not receive security updates and other browser updates.

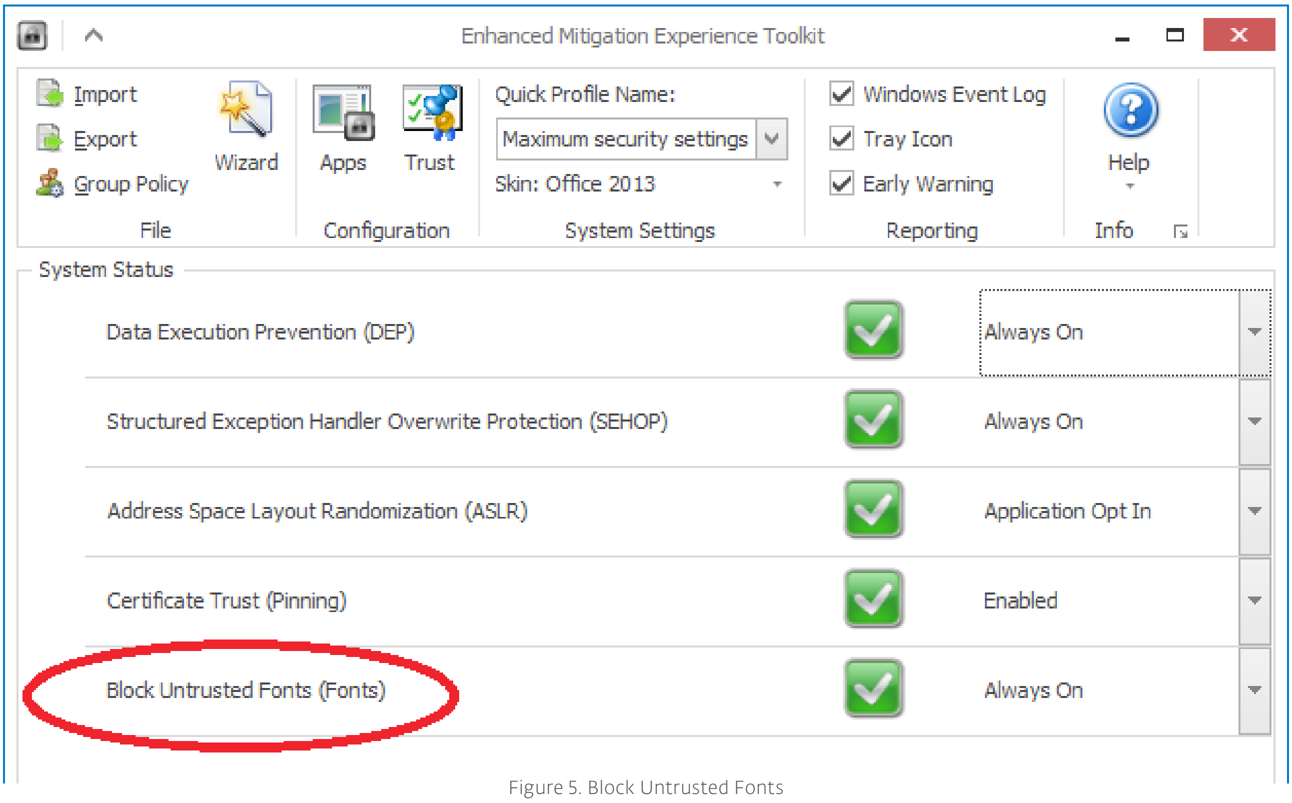
Edge

Edge is a web browser that Microsoft developed specially for Windows 10. It contains strong security options that, unlike Internet Explorer 11, are turned on by default. Edge tabs run by default as 64-bit processes in AppContainer mode. Edge is a completely new web browser and it should not focus on backwards compatibility with old add-ons and plugins. Moreover, it does not support various old and legacy technologies such as ActiveX, BHO and VBScript. These technologies are often used by malware and exploits to penetrate into a system via a web browser, including vulnerabilities in the VBScript engine – vbscript.dll.

With the first major update for Windows 10, Microsoft brought out a new security *feature* for Edge: An option that protects the web browser against binary injection. Now, in order to successfully load a DLL into a browser, the library should be signed with a Microsoft digital certificate or should be approved and signed with a Windows Hardware Quality Lab (WHQL) certificate from Microsoft. The loading of all other libraries in the context of the browser's process will be blocked by this security measure. However, this still allows video drivers to be loaded for purposes of 3-D acceleration, so those might be targeted for exploitation in the future as a way of getting into a system. (Of course, Edge's defense mechanisms still have to be bypassed as well.)

EMET

Microsoft has improved its Enhanced Mitigation Experience Toolkit (EMET) from year to year. This tool covers a wide range of RCE-exploits and techniques. The latest EMET 5.5 beta introduced a new mechanism, which helps to protect users from LPE exploits that use vulnerabilities in *win32k.sys* by exploiting specially-crafted font files. This feature is called *Block Untrusted Fonts* and is available to users of Windows 10. This feature is similar to the function call *SetProcessMitigationPolicy* with the undocumented argument *ProcessFontDisablePolicy*. This version of EMET is compatible with Windows 10.



Quick Profile Name: Maximum security settings

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

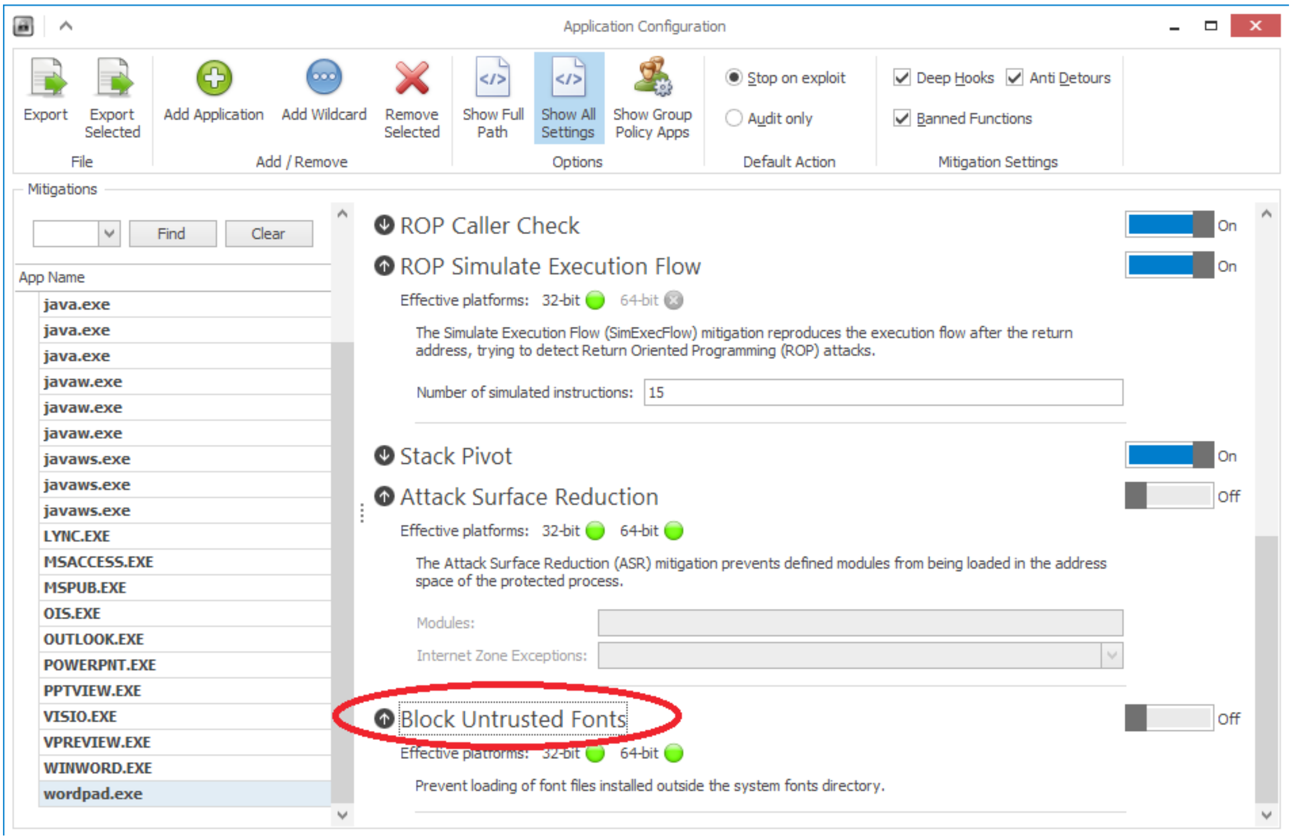
☑ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Always On
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Always On
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled
Block Untrusted Fonts (Fonts)	✓	Always On

Figure 5. Block Untrusted Fonts

The EMET 5.5 beta allows users to turn on special mitigation options for countering LPE exploits, which trigger vulnerabilities – mostly in *win32k.sys* – through so-called untrusted font files. Microsoft defines these as font files installed outside the %windir%/fonts directory.



● Stop on exploit

○ Audit only

☑ Deep Hooks ☑ Anti Detours

☑ Banned Functions

App Name

java.exe
java.exe
java.exe
javaw.exe
javaw.exe
javaw.exe
javaws.exe
javaws.exe
javaws.exe
LYNC.EXE
MSACCESS.EXE
MSPUB.EXE
OIS.EXE
OUTLOOK.EXE
POWERPNT.EXE
PPTVIEW.EXE
VISIO.EXE
VPREVIEW.EXE
WINWORD.EXE
wordpad.exe

ROP Caller Check — On

ROP Simulate Execution Flow — On

Effective platforms: 32-bit ● 64-bit ☒

The Simulate Execution Flow (SimExecFlow) mitigation reproduces the execution flow after the return address, trying to detect Return Oriented Programming (ROP) attacks.

Number of simulated instructions: 15

Stack Pivot — On

Attack Surface Reduction — Off

Effective platforms: 32-bit ● 64-bit ●

The Attack Surface Reduction (ASR) mitigation prevents defined modules from being loaded in the address space of the protected process.

Modules:

Internet Zone Exceptions:

Block Untrusted Fonts — Off

Effective platforms: 32-bit ● 64-bit ●

Prevent loading of font files installed outside the system fonts directory.

Figure 6. Untrusted Fonts

Detailed information about other EMET security features can be found in "Windows exploitation in 2014".

Conclusion

In this report we have looked at various security measures for web browsers and Enhanced Mitigation Experience Toolkit (EMET) introduced in the past year. We have also presented statistical information about repaired vulnerabilities in Microsoft products. Various Windows user-mode components were the most dangerous for users in terms of their being incorporated into attacks actually being implemented.