Microsoft

Malware Protection Center

Overview

Introduction

In our November Threat Intelligence report we looked at advanced persistent threat (APT) attack trends. While APTs often use exploits as part of their attack, exploits are also commonly used to deliver commodity malware onto individual machines.

This report explores recent exploit trends, analyzes prevalent and common exploits, and summarizes current and future mitigation strategies for preventing and recovering from exploit-based attacks.

Exploiting the vulnerable

Exploits provide an entry point for attackers to install malware, to gain persistence and to perform offensive operations. Exploits themselves are not malware – they are the launching pad or beachhead that allows malware to infect a machine.

They use software vulnerabilities to enter a targeted system without the victim's knowledge or consent.

The vulnerabilities are like holes in the software, and the developer of the software might or might not know about them. An exploit seeks to use these holes to provide additional privileges or control of the machine to a file that would otherwise be blocked or not have those privileges.

The best way to prevent most exploit attacks (and therefore, the delivery of malware) is to ensure that software on the machine is fully patched and completely updated.

Exploit analysis looks at specific exploits in detail. See Prevention & mitigation efforts for more information on preventing exploit attacks

Old code means new challenges

As the security industry implements more mitigation techniques and improves its technology, exploiting vulnerable software has become more challenging. Therefore, attackers are adopting a new tactic: they target the legacy components of the software.

Most new software is built on legacy code as it is likely proven to work, reliable, and ready to be used. However, as large parts of this code was written and developed before modern security considerations

were standard practice, defense mechanisms that were once robust don't stand up to modern-day attacks.

This means that despite continuing advances in antimalware and antivirus technology, exploits are still a choice method for delivering malware and attacks. See Trend and prevalence for recent exploit detection data by Microsoft security products.

Kits and caboodles

In the course of an attack, several different vulnerabilities might be targeted by a number of different exploits. Attackers exert such efforts to give them the highest chance of successful penetration into a machine, as illustrated in Figure 1 which shows how Blacole (also known as Blackhole) targets specific vulnerabilities.

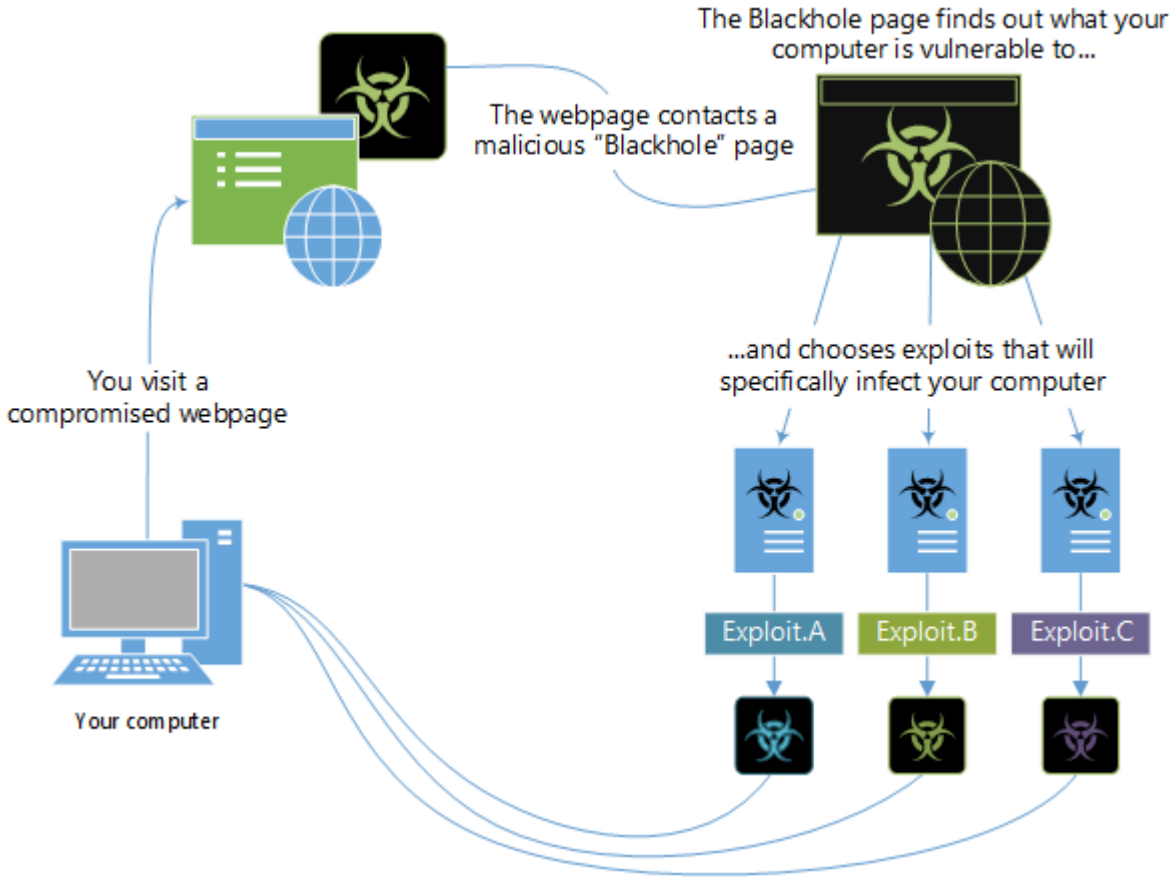
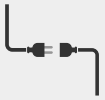


Figure 1: Typical attack method used by exploits






Exploit kits help to make this 'easier' for an attacker, who might use an exploit kit as part of their attack package. Exploit kits are traded on black markets, and provide somewhat streamlined deployment of a number of exploits in an attack.

Generally, it can be expected that an exploit kit will target several vulnerabilities, and depending on the complexity of the kit, it can determine which specific vulnerabilities to target 'on-the-fly'. The exploit kit will look at the machine, determine the installed software and version numbers, and then select specific vulnerabilities that are only relevant to that specific installed software and version.

Delivery mechanism describes some vulnerability types that are targeted by exploits.

Delivery mechanisms

As attackers look for easier targets, legacy components used in new software are now a major target of exploitation.

While many exploits target vulnerabilities in web code, Adobe Flash, Adobe PDF files, and web browsers like Internet Explorer and Google Chrome, there is a huge variety of targets for exploits.

This section looks at two of the lesser known types of vulnerability that, while not as popular as other exploit delivery mechanisms, are just as harmful.

For a summary of how exploits are tied to vulnerabilities, and how the common vulnerabilities and exposures database and nomenclature work, see the section **How we name exploits** on the MMPC exploits page.

TrueType fonts and OpenType fonts

TrueType fonts (TTF) and OpenType fonts (OTF) are extremely popular and widely used font systems. For many machines, TTF is the default and OTF is becoming more popular, especially as it can be used as an open source format. OTF became publicly available in 1996, and TTF has been in use long before that. The legacy code often used in drivers that support both of these font systems expose vulnerabilities like heap overflow or out-of-bounds errors – both common attack vectors for exploits that lead to malicious privilege execution.

Typically, exploits that target TTF and OTF vulnerabilities target drivers that support the use of these font file types on a computer.

In the case of CVE-2015-2426 (which we detect and block with Exploit:Win32/CVE-2015-2426), the exploit attempted to target a .dll driver file (atmfd.dll) used by the Windows Adobe Type Manager Library in Windows. The vulnerability was resolved with MS15-078.

CVE-2013-3128 (resolved by MS13-081) was a vulnerability in the way that OTF and TTF fonts were parsed by Microsoft programs. In such a case, attackers would embed a malicious or malformed font into a webpage that would then load or target the vulnerability and allow malware to be installed on the machine.

Encapsulated PostScript

Encapsulated PostScript (EPS) files are used to display print previews and provide other functions related to printing. Like TTF, they are ubiquitous.

The .eps file can be embedded in other files, such as a Word .docx file. The .docx file is unpacked or un-zipped, the .eps file is added and referenced as an image, and the .docx file is repacked.

We've seen three versions of this delivery mechanism using CVE-2015-2545, which affected the Post-Script filter used in Microsoft Office:

- The first version attempted to exploit CVE-2015-2545 before it was known publicly, thus making it a zero-day exploit. It used a file called *resume.docx* which was first seen in India. Microsoft released MS15-099 (September release) to fix the vulnerability.
- The second version attempted to bypass MS15-099 (September release) and was observed in Japan. It was mitigated by an update to MS15-099 (November release).
- The third version was observed in Korea with an unknown file name and was also mitigated by an update to MS15-099 (November release).

Trends and prevalence

Categorizing exploits

Our detections for exploits are categorized both into the targeted platform (or file type or programming language), and the name of the actual vulnerability. For some vulnerabilities, we use the CVE identifier as the 'family' name, and for others we use security-industry common names or variants of those names (such as Blacole/Blackhole or Angler/Axpergle).

A more detailed description of how we name our detections (including a list of the targeted file types, programming languages, and platforms we use in our names, and how they map to a detection) can be found at the Naming malware page.

Most exploited vulnerability types

Overall, Win32, Java, and JavaScript (JS) exploits are the most often detected. There are occasional spikes and troughs, but overall the ratio of these exploits to any other target is high.

For the last six months, we've seen a consistent number of detections, shown in Chart 1.

Win32, Java, and JavaScript-targeting exploits are all equally high, followed by HTML. Interesting, after the top four, the remainder of the types are all equally low in comparison.

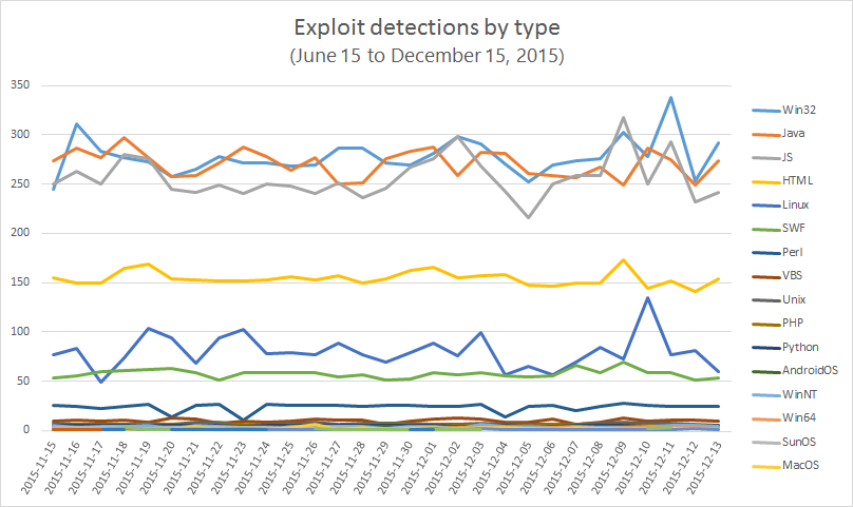


Chart 1: Exploit detections by type – June to December 2015

Zooming to the past 30 days, however, we see finer granularity in the peaks and troughs (shown in Chart 2). The overall average number of detections is consistent with the six months period, although we can see a peak in both Win32 and Linux detections in the second week of December.

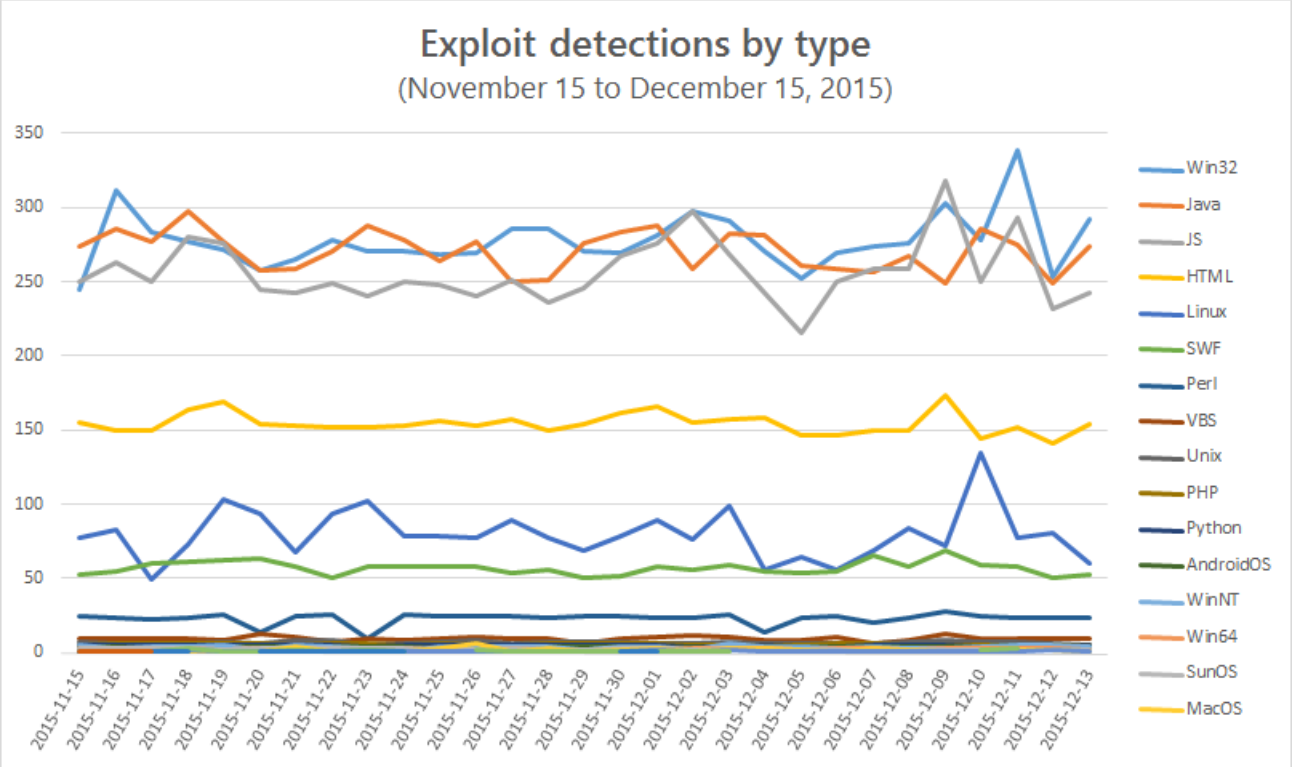


Chart 2: Exploit detections by type – November to December 2015

The United States received the majority of all exploit detections over the past 6 months. Chart 3 lists the top 10 countries based on detections.

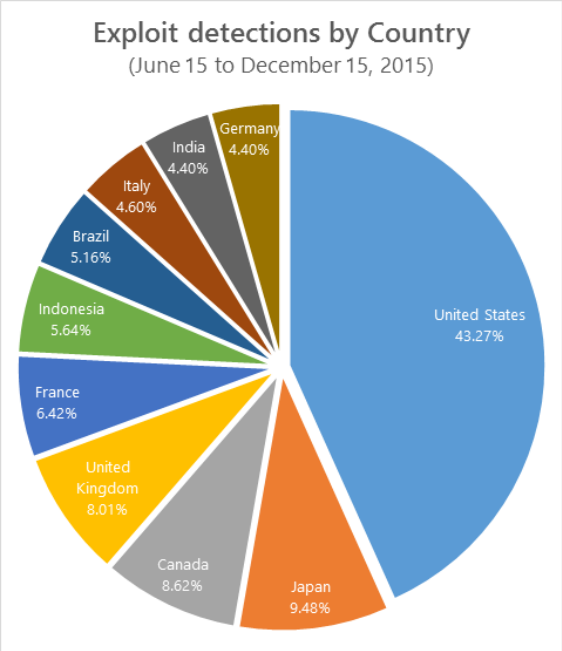


Chart 3: Exploit detections by country – June to December 2015

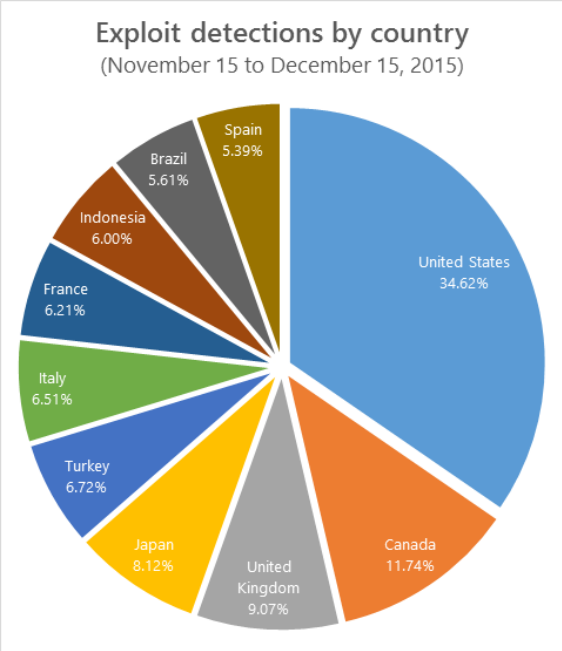


Chart 4: Exploit detections by country – November to December 2015

Over a 30-day period (between November 15, 2015, and December 15, 2015) the data changes only slightly. As seen in Chart 4, Spain replaces Germany with a similar percentage share. However, Turkey appears as fifth highest. The detections are slightly more spread out amongst all the countries, with just over one third (instead of nearly half) of the distribution amongst the top ten seen in the United States.

Looking deeper, we can see the families that make up over 75% of all exploit detections for each of the top 10 countries over the past 30 days in Chart 5.

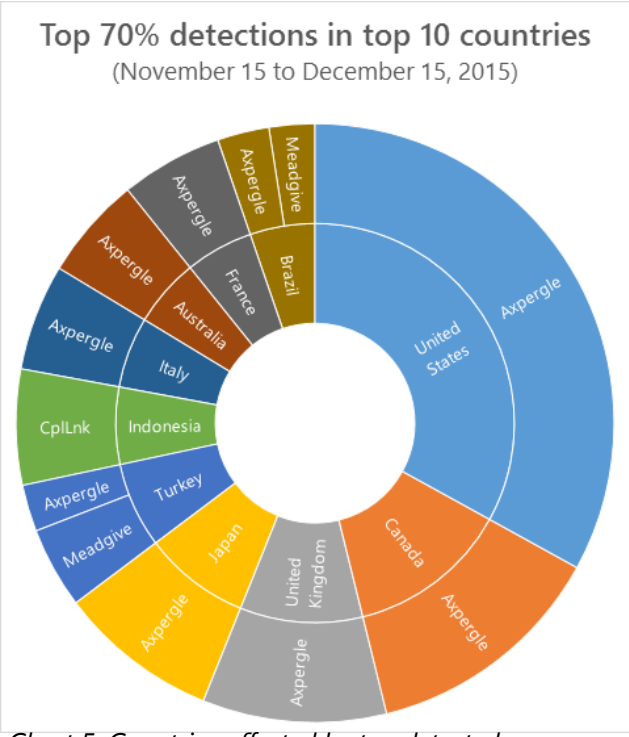


Chart 5: Countries affected by top detected exploit families

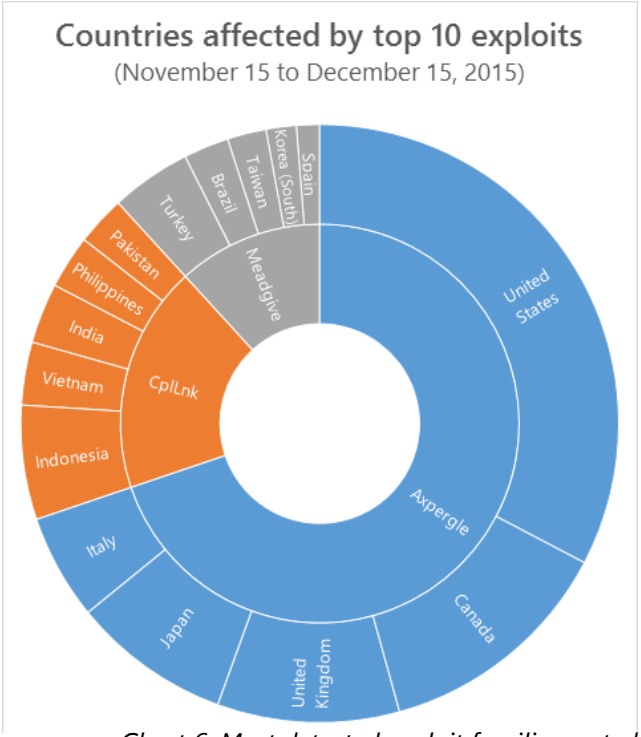


Chart 6: Most detected exploit families sorted by country

We can see that Axpergle is nearly always the culprit and takes the largest share of detections for most countries. Meadgive is also highly represented.

We can flip this data around in Chart 6 to see the countries affected by the most detected exploits.

This shows us that Axpergle is far and away the highest or most detected exploit, followed by CplLnk. Meadgive is not as highly detected as Chart 5 suggested, although it is still prominent.

Prevalent exploits and analysis

Top detected exploits

The most detected exploits, both individual variants (where we've created an individual detection based on unique behavior exhibited by an exploit as compared to other exploits within that 'family') and overall families, are in Table 1 and Table 2.

Table 1: Top 20 detected exploit variants

Exploit	Detections	% 30 days	% 6 months
Exploit:HTML/Axpergle.O	591039	22.03%	40.36%
Exploit:JS/Axpergle.BW	319167	11.90%	14.78%
Exploit:JS/Axpergle.BM	315809	11.77%	5.54%
Exploit:Win32/CplLnk.A	293258	10.93%	5.33%
Exploit:JS/Axpergle.CF	207545	7.74%	4.89%
Exploit:HTML/Meadgive.K	173948	6.48%	4.09%
Exploit:JS/Axpergle.BO	154872	5.77%	3.43%
Exploit:JS/Axpergle.CB	124715	4.65%	2.64%
Exploit:JS/Axpergle	100152	3.73%	1.99%
Exploit:JS/Axpergle.CD	91402	3.41%	1.95%
Exploit:HTML/Neutri-noEK.G	90501	3.37%	1.94%
Exploit:JS/Axpergle.BP	47641	1.78%	1.90%
Exploit:JS/Axpergle.BY	36471	1.36%	1.81%
Exploit:HTML/IframeRef.gen	35882	1.34%	1.51%
Exploit:SWF/Ckieam.B	29259	1.09%	1.50%
Exploit:Win32/CplLnk.B	22991	0.86%	1.49%
Exploit:Java/CVE-2012-1723	14027	0.52%	1.48%
Exploit:Java/Anogre.E	12090	0.45%	1.30%

Exploit:Java/CVE-2010-0840	11536	0.43%	1.03%
Exploit:Win32/Sdbby	10763	0.40%	1.03%
		100.00%	100.00%

Table 2: Top 20 detected exploit families

Exploit	Detections	% 30 days	% 6 months
Axpergle	1169273	58.52%	54.66%
CplLnk	308665	15.45%	16.36%
Meadgive	189781	9.50%	7.53%
NeutrinoEK	91335	4.57%	3.44%
IframeRef	55444	2.77%	2.42%
Ckieam	29260	1.46%	2.19%
ShellCode	18296	0.92%	1.56%
CVE-2012-1723	15850	0.79%	1.42%
Anogre	12742	0.64%	1.25%
Obfuscator	12583	0.63%	1.23%
Pdfjsc	11910	0.60%	1.08%
CVE-2010-0840	11859	0.59%	0.98%
CVE-2012-0507	11308	0.57%	0.89%
Blacole	11150	0.56%	0.86%
Sdbby	10763	0.54%	0.78%
CVE-2013-0422	10183	0.51%	0.78%
CVE-2011-3544	7768	0.39%	0.77%
CVE-2015-5119	6997	0.35%	0.61%
Neclu	6645	0.33%	0.60%
CVE-2013-1493	6202	0.31%	0.58%
		100.00%	100.00%

These tables only show actual numbers from the past 30 days, but when comparing the percentage share of each detection across the top 20, we see that Exploit:HTML/Axpergle.O has a higher detection ratio over a period of 6 months than the past 30 days. The "family' detections for Axpergle, however, is consistent between a 30-day period and a 6 month period.

Axpergle - analysis

The top 10 Axpergle detections for the past 30 days (13 November to 13 December, 2015) indicate that Exploit:HTML/Axpergle.O was highly detected, along with Exploit:JS/Axpergle.BW, during the end of November, as seen in Chart 7.

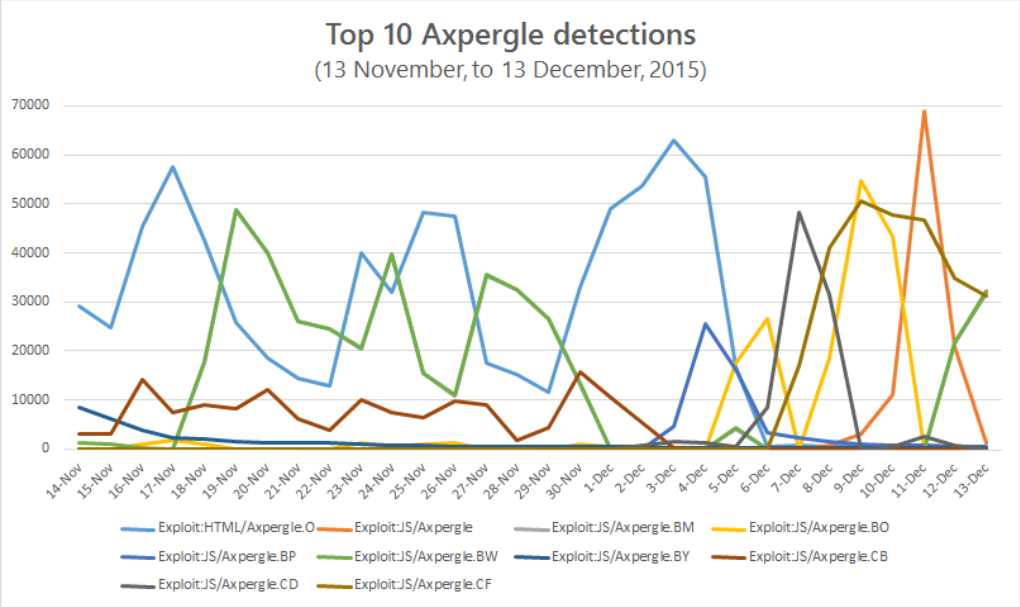


Chart 7: Top 10 Axpergle detections

However, as December began, the detections for Exploit:HTML/Axpergle.O dropped greatly, and instead previously low-detected exploits were instead rising in prevalence. This correlates with the data of detections for the past 6 months versus 30 days (in Table 1 and Table 2).

Individual exploits do vary in popularity, and exploits are constantly tweaked by their authors; it's likely we're seeing that here. The detection for Exploit:JS/Axpergle.CF was published on December 7, 2015, which explains why we saw no detections until around that date.

What's interesting is that Exploit:HTML/Axpergle.O is a HTML-targeting exploit, whereas Exploit:JS/Axperlge.BO and Exploit:JS/Axpergle.CF target JavaScript vulnerabilities. The fact that two JavaScript exploits rose to prominence over the last two weeks, and a previously highly detected HTML exploit dropped off also explains why the overall family detection for Exploit:JS/Axpergle rose.

Prevention and mitigation efforts

Microsoft uses several built-in web browser technologies to help keep your PC safe from malware.

Microsoft Edge

Microsoft Edge is designed to provide protection from sophisticated and prevalent online attacks. It includes sandboxing, compiler, and memory management techniques to help keep you safe online.

- Microsoft Edge: Building a safer browser

Internet Explorer

SmartScreen Filter

The SmartScreen Filter can help you avoid exploits by warning you about known malicious, phishing, or malware-downloading websites before you visit them.

- What is the SmartScreen Filter and how can it help protect me?

Protected mode

Protected mode in Internet Explorer uses security settings to make it more difficult for malicious software to be installed on your PC. In protected mode, Internet Explorer will warn you when a website tries to install software or run certain programs.

- What does Internet Explorer protected mode do?

IExtensionValidation interface

Windows Internet Explorer 11 includes added protection from exploits through the IExtensionValidation interface (IEV).

This feature scans content asking for access to ActiveX controls for malicious activity - checking the website is safe before it can run any malicious code. This can help avoid malware successfully exploiting a vulnerability from a malicious or compromised webpage.

Learn more about safer browsing with Internet Explorer:

- Security in Internet Explorer

General security tips

Following a few general security tips can help reduce the chance of a malware infection through software exploits.

Keep your software up-to-date

Software vendors regularly patch known vulnerabilities in their products. That's why it's essential to keep all your software up-to-date.

- Update your software

Microsoft regularly releases security patches through Windows Update.

- Choose how updates are installed in Windows 10

Run up-to-date security software

You should run an up-to-date, real-time security product, such as Windows Defender. Definitions for Microsoft security products are updated regularly.

- Updating your Microsoft antimalware and antispyware software

Read more about how Windows Defender for Windows 10 can help protect you from malware and exploits.

- Threat intelligence report - Windows Defender

Use cloud protection

The Microsoft Active Protection Service (MAPS) uses cloud protection to help guard against the latest malware threats. It's turned on by default for Microsoft Security Essentials and Windows Defender.

- Check if MAPS is enabled on your PC

Microsoft

Malware Protection Center

Top detections for the past 30 days

The tables in this section show top detections for all malware categories for the past 30 days.
"Dist." is the percentage share of each detection amongs the top 10 detections in that category.

Enterprise detections	
Threat name	**Dist.**
BrowserModifier:Win32/Diplugem	20%
SoftwareBundler:Win32/OutBrowse	16%
BrowserModifier:Win32/SupTab	14%
JS/Axpergle	10%
Trojan:Win32/Dorv.A!rfn	8%
Win32/Gamarue	7%
Win32/Sventore	7%
Trojan:Win32/Peals	5%
Trojan:Win32/Skeeyah.A!plock	6%
Trojan:JS/Iframeinject.A	6%

Families	
Threat name	**Dist.**
HackTool:Win32/AutoKMS	28%
BrowserModifier:Win32/SupTab	15%
HackTool:Win32/Keygen	13%
Win32/Gamarue	10%
BrowserModifier:Win32/Diplugem	8%
Win32/Dynamer	6%
Trojan:Win32/Peals	5%
Win32/Obfuscator	5%
JS/Axpergle	5%
Program:Win32/Hadsruda!bit	5%

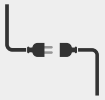
Top detections (all types)	
Threat name	**Dist.**
HackTool:Win32/AutoKMS	30%
BrowserModifier:Win32/SupTab	16%
HackTool:Win32/Keygen	13%
Worm:Win32/Gamarue.gen!lnk	9%
BrowserModifier:Win32/Diplugem	9%
Trojan:Win32/Dynamer!ac	6%
Program:Win32/Hadsruda!bit	5%
SoftwareBundler:Win32/Mizenota	5%
SoftwareBundler:Win32/OutBrowse	4%
Trojan:Win32/Skeeyah.A!bit	4%

Top rogue detections	
Threat name	**Dist.**
Rogue:JS/FakeCall.D	91%
Rogue:JS/FakeCall.B	6%
Rogue:Win32/Winwebsec	1%
Rogue:Win32/Quamatix	1%
Rogue:Win32/FakeRean	1%
Rogue:VBS/FakePAV	0%
Rogue:Win32/FakePAV	0%
Rogue:VBS/Trapwot	0%
Rogue:Win32/Onescan	0%
Rogue:MSIL/Rustliver	0%

Microsoft

Malware Protection Center






Top ransomware detections	
Threat name	Dist.
Ransom:JS/FakeBsod.A	26%
Ransom:Win32/Crowti.A	18%
Ransom:HTML/Tescrypt.D	16%
Ransom:HTML/Crowti.A	16%
Ransom:JS/Brolo.C	10%
Ransom:Win32/Crowti	4%
Ransom:HTML/Teerac.C	3%
Ransom:Win32/Tescrypt.A	3%
Ransom:HTML/Tescrypt.B	3%
Ransom:Win32/Critroni	2%

Top expoit detections	
Threat name	Dist.
Exploit:JS/Axpergle.CF	16%
Exploit:HTML/Axpergle.O	15%
Exploit:JS/Axpergle.BW	13%
Exploit:JS/Axpergle.BM	13%
Exploit:Win32/CplLnk.A	10%
Exploit:JS/Axpergle.BO	10%
Exploit:HTML/Meadgive.K	7%
Exploit:HTML/Axpergle.AH	7%
Exploit:JS/Axpergle	6%
Exploit:HTML/NeutrinoEK.G	4%

Top unwanted software detections	
Threat name	Dist.
BrowserModifier:Win32/SupTab	34%
BrowserModifier:Win32/Diplugem	18%
SoftwareBundler:Win32/Mizenota	10%
SoftwareBundler:Win32/OutBrowse	9%
Adware:Win32/EoRezo	6%
BrowserModifier:Win32/KipodToolsCby	6%
BrowserModifier:Win32/Yoursearching!blnk	5%
SoftwareBundler:Win32/InstallMonetizer	5%
BrowserModifier:Win32/Istartpageing!blnk	4%
BrowserModifier:Win32/Smudplu	4%

Top password stealer detections	
Threat name	Dist.
PWS:HTML/Phish.GK	19%
PWS:Win32/Fareit	17%
PWS:Win32/VB.CU	15%
PWS:Win32/Prast!rts	13%
PWS:MSIL/Stimilini.M	7%
PWS:Win32/QQpass.CI	7%
PWS:MSIL/Mintluks.A	6%
PWS:Win32/Kegotip.C	6%
PWS:Win32/Zbot	6%
PWS:HTML/Phish.GD	4%

Microsoft

Malware Protection Center

Top spyware detections	
Threat name	**Dist.**
TrojanSpy:Win32/Banker	44%
TrojanSpy:Win32/Banker!rfn	19%
TrojanSpy:MSIL/Omaneat.B	9%
TrojanSpy:MSIL/Hakey.A	7%
TrojanSpy:Win32/Ursnif.HP	5%
TrojanSpy:Win32/Mafod!rts	4%
TrojanSpy:Win32/Ursnif.HN	4%
TrojanSpy:Win32/Usteal.D	3%
TrojanSpy:JS/Phish.D	3%
TrojanSpy:Win32/Banker.ANX	3%