SOPHOS
Security made simple.

Exploits. Intercepted.

Exploits are one of the main techniques used by cybercriminals to spread malware. They take advantage of weaknesses in legitimate software products like Flash and Microsoft Office to infect computers for their criminal ends. A single exploit can be used by myriad separate pieces of malware, all with different payloads.

Antivirus solutions have traditionally focused on stopping the malware that uses the exploits rather than the exploits themselves. While there are millions of different pieces of malware in existence, hackers only use 10's of different techniques to exploit software vulnerabilities. By blocking these exploit techniques, you can block a massive number of malware samples in one go, before they even enter your system. You can even block exploits that happen over the wire (drive by attacks), or take advantage of vulnerabilities that have never been seen before (zero day vulnerabilities).

Read this paper to learn more about exploits and how to stop them. It explores how exploits work, the exploit industry, what makes a good exploit in the eyes of the cybercriminals, and also how anti-exploit technology is a highly efficient and effective way to secure your organization against advanced and unknown threats.

A Sophos Whitepaper September 2016

Exploits and exploit kits

Exploits

Most cyberattacks involve criminals exploiting some sort of security weakness. That weakness could be down to a poorly chosen password, a user who falls for a fake login link, or an attachment that someone opened without thinking or even just browsing to an infected delivery site and not clicking on anything. The attacks are sophisticated and even the most cautious user is vulnerable to advanced attacks. However, in the field of computer security, the word exploit has a specific meaning: an **exploit** is a way of abusing a software bug to bypass one or more security protections that are in place.

Software bugs that can be exploited in this way are known as **vulnerabilities**, for obvious reasons, and can take many forms. For example, a home router might have a password page with a secret "backdoor code" that a crook can use to login, even if you deliberately set the official password to something unique. Or a software product that you use might have a bug that causes it to crash if you feed it unexpected input such as a super-long username or an unusually-sized image.

Many software bugs cause errors that are annoying but can be detected and handled safely by the operating system. A vulnerability, however, is a bug that can be orchestrated or controlled so that it does something unauthorized and insecure as the program crashes, before the operating system can intervene and protect you.

When attackers exploit a vulnerability of this sort, they usually do so by tricking one of the applications you are using, such as your browser or word processor, into running a small program or program fragment that was sent in from outside. By using what's called a Remote Code Execution exploit, or RCE for short, an attacker can bypass any security popups or "Are you sure" dialogs, preventing you from stopping it.

Zero day exploits are where the hackers take advantage of a vulnerability which is not yet public knowledge and for which no patch is currently available.

As exploits take advantage of often-unknown weaknesses in legitimate software it is often hard to avoid them, even when following best security practices.

Exploit kits

An **exploit kit** is a pre-packaged toolkit of malicious web pages or software that crooks can buy, license or lease for the purpose of distributing malware. In other words, if you have some shiny new malware – ransomware, perhaps, or a Trojan, or a password stealer – you can use an exploit kit to deliver that malware to unsuspecting victims.

Instead of figuring out how to booby-trap your own web pages so that visitors end up infected, you rely on pre-prepared attack code in an exploit kit to try out a series of known security holes, in the hope that one will succeed.

An exploit kit is usually delivered directly into a potential victim's browser in the form of convoluted and hard-to-follow JavaScript, and automatically tries out a series of attacks, typically in the most likely sequence, until one of them works, or they've all failed, something like this:

```
if java installed then
   try java exploit 1
   if exploit worked then install malware end
end
if silverlight installed then
   try silverlight exploit 1
   if exploit worked then install malware end
   try silverlight exploit 2
   if exploit worked then install malware end
end
if flash is installed then
   ...
end
if nothing worked then give up end
```

The same exploit kit can be used to deliver multiple different malware samples; and the same malware sample can be delivered by one or more different exploit kits.

```
<script>var wqncvnhankfhte=(1194000100<780281714?"ie":"rv:1");
var gjxtcjftwwxi=(1149318224+131959385<1122077856+259936926?"gjx":"dk");
var fntzefklgaqvsjy=(1577258313>1944482977?"w":"r");
var wmjsvibonuq=(1293847248>1687638986?"rtr":"\x72\x65\x74\x75\x72\x6e");
wqnctvnankfhte+=(151554506+472333707>363202458?"\x31":"\x68\x74");
var ixgjdotdmfrbi=(160750077+525999200>1876280?"\x5b\x5d":"\x74");
var gfanlterj=(2103263286>2143916270?"czr":"ret");
var wqkbimsjzmmaf=(968162729<189979742?"\x6b":"wq");
var rggshjhsixeofuo=(115809819+1034707353<1078015506+108580141?"\x72":"c");
fntzefklgasjy+=(77641620+817194218<1256743977+344513278?"\x65\x74":"\x71\x6f");
```

Convoluted JavaScript code from an Angler exploit kit web page

In addition to exploit kits that take advantage of web delivery, a number of similar exploit kits are available for email and phishing campaigns where the adversary sends an attachment out to unsuspecting users in the hopes they open the attachment, install the exploit kit, or even just display the images in the email. There are myriad delivery mechanisms and the unsuspecting victims can do little to prevent the most sophisticated attacks other than unplugging their computer, taking the battery out of their phone and walking away.

The exploit industry

Thanks to exploit kits, malware authors don't need to worry about how to find bugs in Java, or Silverlight, or Flash; how to build those bugs into working exploits; how to find insecure web servers to host the exploits; or how to entice prospective victims to the booby-trapped web pages.

Likewise, the exploit kit authors don't have to worry about writing full-blown malware; they don't have to run servers to keep track of infected computers, or to collect money from individual victims; they don't have to get involved in exfiltrating stolen data, or selling that data on, and so forth.

Each group specializes in one or more parts of the threat landscape, in what's become known, satirically, as CaaS, or Crimeware-as-a-Service. And between them stand the exploit brokers.

Exploit brokers buy exploits from the people who discover them and sell them on to any interested parties. These could be government bodies or nefarious hackers in equal measure – however they invariably keep their purposes to themselves. As Kevin Mitnick, founder of Mitnick's Absolute Zero Day Exploit Exchange explained to Wired:

"When we have a client that wants a zero-day vulnerability for whatever reason, we don't ask, and in fact they wouldn't tell us.

Researchers find them, they sell them to us for X, we sell them to clients for Y and make the margin in between."

https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/

It's not illegal to sell exploits, but it is lucrative. Subscriptions for a year of 25 zero-day flaws can sell for as much as US$2.5 million.

The role of patching

As we have seen, exploits take advantage of vulnerabilities in legitimate software products. All reputable software vendors create patches to fix the vulnerabilities once they are aware of them, with probably the most well-known being Microsoft who publishes patches for about 20 to 30 vulnerabilities every second Tuesday of the month (Patch Tuesday). There is almost always a lag time between the discovery of the vulnerability and the creation of the patch, even when it's known to be used for criminal activity, as shown in this Security Advisory issued by Adobe on June 14, 2016:

"A critical vulnerability (CVE-2016-4171) exists in Adobe Flash Player 21.0.0.242 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. Successful exploitation could cause a crash and potentially allow an attacker to take control of the affected system.

Adobe is aware of a report that an exploit for CVE-2016-4171 exists in the wild, and is being used in limited, targeted attacks. Adobe will address this vulnerability in our monthly security update, which will be available as early as June 16."

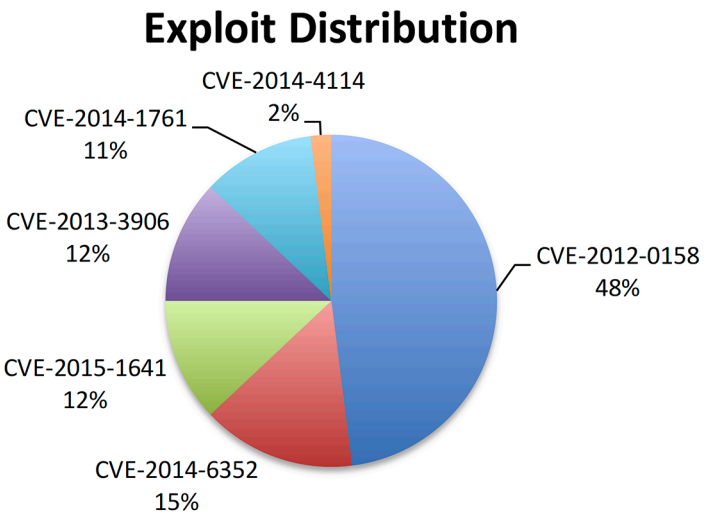
Generally, once a vulnerability has been patched its effectiveness as an attack vector should be short lived, because as more users update their software, fewer remain susceptible to the exploit. However, this all depends on how quickly and effectively organizations patch the vulnerabilities. Lax patching leaves the door wide open to the cyber crooks, as CVE-2012-0158 shows.

Anatomy of a prolific exploit: Introducing CVE-2012-0158

Arguably one of the most exploited vulnerabilities of the last decade, the story behind CVE-2012-0158's longevity is one of constant adaptation; somewhat a modern day embodiment of Charles Darwin's "On the Origin of Species".

Publicly, CVE-2012-0158 has gained notoriety as in a number of well documented targeted attacks such as Red October, FakeM and the Rotten Tomato campaign. The targeted victims in these cases ranged from logistics and leather companies right through to diplomatic and governmental organizations, suggesting the vulnerability is not only very popular but also used by diverse groups of criminals with contrasting intentions.

CVE-2012-0158 which was disclosed and patched by Microsoft (MS12-027) all the way back in 2012, has proved perennially popular amongst cybercriminals. Indeed, despite a patch being available for over three years, CVE-2012-0158 still topped the *SophosLabs* exploit statistics for the last quarter of 2015, making up a whopping 48% of all recorded Word-based exploit attacks.



Exploit Distribution, October – December 2015
Source: SophosLabs

It's not unheard of for the crooks to favor a specific vulnerability, but it is unusual for them to do so for so long. Patching a vulnerability normally signals the beginning of the end of its usefulness to the crooks: the more people who apply the patch, the weaker the vulnerability becomes. Given that April 2016 marked the fourth anniversary of Microsoft patching CVE-2012-0158, it's astonishing that cybercriminals are still able to exploit it.

What's next for CVE-2012-0158?

Realistically, until Office Exploit Kits cut their ties with it, it seems very unlikely that we will see the back of CVE-2012-0158 anytime soon. Its continued usage in the wild lends more weight to the theory that it's still having some success; even though it's had to change its game from spam campaigns to more concentrated attacks. If there are still vulnerable computers in the world, it seems doubtful that exploit kit authors will discard it.

Whilst its existence might not be in jeopardy, one thing much more at risk is its position at the top of the exploit charts. Newer and sexier vulnerabilities have emerged in the last year that have already been inducted into exploit kits and found favor amongst malware groups. The two most likely contenders to CVE-2012-0158's crown are CVE-2015-1641, an RTF vulnerability that exploits the way Office processes embedded content, and CVE-2015-2545, which exploits the code Office uses to parse Postscript files.

What makes a 'good' vulnerability

CVE-2012-0158's initial popularity was understandable given that it meets a lot of the criteria malware authors look for when selecting a dropper for their spam campaigns. Spam campaigns are typically sent to a large number of random recipients so when choosing an attack technique there can be no assumptions as to what software the intended victim has installed. As a result, the bad guys must "play the percentages" and choose an attack technique likely to work in the majority of common setups. There are four key questions in ascertaining how fit for purpose a vulnerability is:

1. **Is the file format unsuspicious as an email attachment?**

   One of the first lines of defense in a company's security solution is the ability to stipulate exactly which attachment types are allowed to enter the network from external email addresses.

   The code that CVE-2012-0158 exploits is housed within the Microsoft Windows Common Control Library. CVE-2012-0158 is concerned specifically with the ListView and TreeView ActiveX controls. Both of these controls can be exploited in Word documents and Excel spreadsheets, and neither of which would appear out of place in emails between acquaintances or customers.

2. **What is the likelihood of the victim's computer being compatible with the attack?**

   Another consideration regarding file format is whether or not the victim will have the right software installed in order for the attack to be successful if opened. The likelihood of a successful infection with, say, an AutoCAD dropper is likely much lower than, say, that of a PowerPoint presentation dropper.

   The CVE-2012-0158 vulnerability affects Office 2003, 2007 and 2010, with the latter being the latest Microsoft offering at the time of the vulnerability's disclosure. Despite alternatives to Microsoft Office making inroads recently, it is still the dominant player in the market which makes CVE-2012-0158 a perfect candidate.

3. **What functionality does the attack allow?**

   Being in an inconspicuous, well-supported file format is all well and good, but unless the attack method grants the bad guys the functionality they need, the technique is useless.

   CVE-2012-0158 is classified as an "Arbitrary Code Execution" vulnerability. This type of vulnerability is considered one of the most severe as, if exploited, it allows the bad guys to hijack the program (in this case Microsoft Word/Excel) and force it to do its bidding.

4. **How flexible is the attack method in evading AV detection?**

   A key factor in deciding in how prolific an attack method will be is how adaptable it is. Once the AV industry discovers an attack method, it becomes a constant game of cat and mouse in which the malware continuously changes form to appear different and elude detection.

   Unfortunately, it didn't take the malware authors long to find a number of ingenious ways of concealing the presence of CVE-2012-0158, including:

   - Default password encryption
   - Use of Rich Text File Format
   - Whitespace and embedded group obfuscation
   - Intermixing binary data

How to secure against exploits

Anti-exploit technology

While there are millions of different pieces of malware in existence, hackers only use 10's of different techniques to exploit software vulnerabilities. Blocking these exploit techniques is a highly efficient and effective way to stop a massive number of malware samples in one go.

Sophos Intercept X is a next-gen endpoint solution that delivers powerful anti-exploit capabilities. It detects and blocks exploit techniques, stopping the myriad pieces of malware that use them. It doesn't matter if the malware is a known strain or not: Intercept X simply recognizes the exploit techniques and prevents them from being leveraged. Unlike traditional anti-malware technology, Sophos Intercept X stops the threats before they enter your system, reducing the impact on your infrastructure.

Security best practices

To boost your defences against exploit kits we recommend you:

Deploy Sophos Intercept X. It runs alongside Sophos Central Endpoint Protection Advanced as well as endpoint solutions from other antivirus and next-generation vendors to bolster your protection. When deployed with Sophos Endpoint it integrates into a single protection agent controlled through one central management platform.

Patch early, patch often. If you have already closed the holes that an exploit kit is programmed to try, all its alternatives will fail and the exploit kit will be useless.

Keep your security software up to date. A good anti-virus can block document attacks at many points, including getting rid of dangerous email attachments before you open them, filtering out booby-trapped web sites so you can't reach them, and blocking booby-trapped files so you can't launch them.

Consider using a stripped-down document viewer. Microsoft's own Word Viewer, for example, is usually much less vulnerable than Word itself. Also, it doesn't support macros, another Word-based malware trick commonly used by ransomware.

Remove unused browser plugins. If you don't need Java (or Silverlight, or Flash) in your browser, uninstall the plugin. An exploit kit can't attack a browser component that isn't there.

Conclusion

Exploits are incredibly powerful tools that are widely used by today's cybercriminals, with a single exploit used to distribute millions of malware variants. The good news is that by stopping these exploits, you can block the vast majority of malware before it even enters your system.

The proven anti-exploit technology in Sophos Intercept X enables you to stop exploits in their tracks. This next-gen endpoint solution complements your existing antivirus protection, enabling you to secure your organization with minimal effort.

Further reading

For more information on CVE-2012-0158, read the detailed technical report from SophosLabs.

Try Sophos Intercept X for free:
www.sophos.com/intercept-x

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

16-09-13 WPNA (RP)

SOPHOS