The need to protect against file-based attacks

...statistical evidence for the need for greater assurance

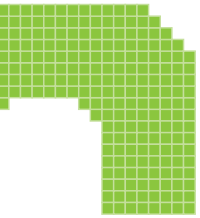
author • Fran Howarth

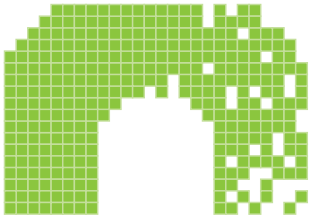
Bloor

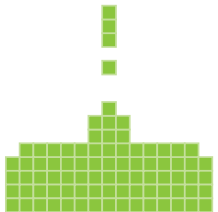
Executive summary

CRIMINALS ARE BECOMING BETTER organised, more sophisticated and have turned their focus from high volume attacks aimed at stealing personal data to lower volume, more targeted attacks that aim to infiltrate networks and steal valuable data such as intellectual property.

In **2012** alone, there was a **42% increase in targeted attacks** and two-thirds of targeted attacks were used only once against one particular target. According to Guidance Software, increasingly precise and sophisticated phishing attacks are being seen that effectively "result in a single person unwittingly handing over the keys to the corporate data kingdom with everything from intellectual property to customer data suddenly up for grabs." According to Vigilant by Deloitte, attackers are also increasingly developing more sophisticated evasion and resilience techniques to bypass defences. This can be seen in the fact that detection rates using traditional techniques for newly created viruses are less than 5%.







However, despite the increasing sophistication of today's attackers, they continue to use the same old attack vectors in many cases, with emails used as bait in the majority of spear phishing campaigns that are the precursor to an advanced threat gaining a foothold on a network. **In 2012, there was a 56% increase in email attacks that successfully penetrated organisations.** The threats are generally contained in documents attached to emails or malicious web links that are included in the body of the email. Another method used is to trick users into downloading files riddled with malware from websites. According to NTT Com Security, users and organisations need to become increasingly sophisticated in their defences, stating that there is a need to change focus from trying to determine what is bad in favour of looking for what is known to be good.

This document aims to provide those interested in better protecting themselves from exploits targeting files and documents in use by and inbound to their organisations with evidence related to those exploits. It discusses the current threat landscape and the part played by files and documents, showing why they continue to be a major point of vulnerability, and why new defences are required as traditional defences are not up to the job of safeguarding organisations from such attacks. It then shows that more vendors are turning to focus on controlling malicious exploits associated with documents and files, with more offerings coming onto the market that attest to the need to expand document security, and discusses their offerings.

Fast facts

Vulnerabilities affecting documents are increasing, spurred by their use as the primary threat vector in spear phishing exploits that are used in targeted attacks. Up to 94% of spear phishing campaigns invite users to open email attachments that are riddled with malware.

Malware exploits embedded in files are becoming increasingly complex in an effort to defeat traditional security defences.

Significant spikes are being seen in new vulnerabilities following security breaches, such as that affecting Adobe recently, which included the theft of source code.

The bottom line

Attacks against networks that aim to gain a foothold and steal valuable information from organisations are growing in sophistication and complexity. A major trend being seen is that attacks are increasingly targeted at specific organisations or individuals in order to increase the chances of locating and stealing the most valuable information, such as intellectual property. Documents are a prime threat vector used in such exploits.

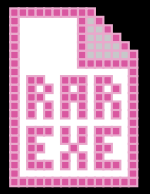
Attackers are also going to great lengths to evade security controls that have traditionally focused on protecting against exploits known to be bad and for which countermeasures have been developed. With increased and fast-growing use of zero-day exploits, that is no longer sufficient. Instead, a new approach is needed that focuses on looking for what is good, sanitising bad exploits from the documents in which they are embedded.

The fact that more vendors are turning to focus on this area attests to the vital need for greater document content assurance and compliance. There is a renewed sense of urgency in defending against document and file-based attacks given their importance in today's threat landscape.

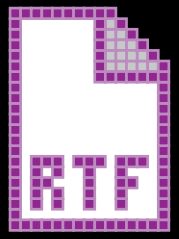
The threat landscape

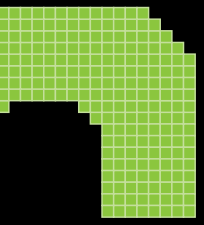
IN RECENT YEARS, hackers and other criminals have become increasingly sophisticated, using a wider range of tools and ever-more complex exploits. They have also turned to targeting their attacks at specific organisations or individuals. According to Symantec, targeted attacks emerged in 2005, when an average of one such attack was seen per week. By 2010, this had reached 60 per day, rising to 80 by the end of 1Q 2011.

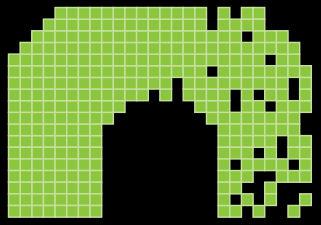
At first, they were mainly targeted at large multi-national organisations and at specific industries; the public sector, defence, energy and pharmaceuticals in particular. Today, attackers have widened their scope to include small and medium organisations—which can often provide a conduit into larger organisations with more valuable information such as intellectual property—and to organisations in any vertical sector. **In 2012, there was a 42% increase in targeted attacks.**

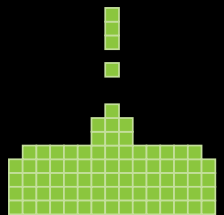


Spear phishing remains the most common method for initiating advanced, targeted malware campaigns, according to FireEye. Generally, such campaigns utilise file-based threats that are downloaded directly by users, either via an exploit or links in emails. Social engineering tactics are used to increase the likelihood of users clicking on malicious links that appear to be interesting to them.









Emails remain the primary channel through which advanced persistent threats (APTs) are initiated—used for Operation Aurora, GhostNet, Night Dragon, the RSA breach, as well as the majority of other APTs that have been publicly documented. **Trend Micro estimates that 91% of APTs are initiated through a spear phishing email.** Advanced targeted attacks increasingly look to mimic tactics used by APTs. Those emails either include attachments containing zero-day vulnerabilities or malicious and dynamic URLs. According to FireEye, **there was a 56% increase in the amount of email-based attacks** that successfully penetrated organisations in 2012.

Whereas it used to be thought that only large enterprises and government agencies were targeted, it is now clear that even small companies are seen as potential targets—sometimes as part of an attack aimed at a larger organisation with which they conduct business. According to research conducted by PwC in association with Infosecurity Europe, **93% of large organisations were breached in 2012, as were 87% of small organisations—up from 76% in 2011** in the latter case. As well as this, organisations suffering breaches experienced on average **50% more incidents in 2012** than the previous year.

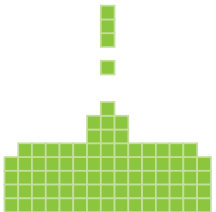
Figures from surveys such as this provide results showing that breaches are more widespread than statistics related to published breaches show. According to estimates from McAfee, just **three out of 10 organisations report all data breaches that they suffer.**

Mobile device usage is also expanding the number and range of threats that organisations face. The International Telecommunications Union estimates that there are 6.8 billion mobile cellular subscriptions globally as of the end of 2013, a growth of 96% in 2013. Cisco estimates that global mobile data traffic grew 70% in 2012 to reach a level that corresponds to almost 12 times total internet traffic in 200.It further estimates that such traffic will grow 13-fold from 2012 to 2017.

According to the Aberdeen Group, **more than 80% of organisations allow employees to use their own devices.** Mobile security vendor Lookout has released research that shows **users are three times more likely to succumb to phishing attacks on their phones than desktop computers** and three in 10 are likely to click on an unsafe link. It found that in the course of 2012, four in ten mobile device users encountered a web threat. This is echoed in the latest mobile threat report from Symantec, which found that **90% of respondents would not open a suspicious file on a PC, whereas only 60% of tablet and 56% of smartphone users would exercise the same caution.** According to Websense, more than 50% of employees access mail from outside of the corporate network, primarily from mobile devices.

Other threat vectors can also allow malicious files to enter an organisation, including the use of USB memory sticks and downloads from cloud-based services such as SaaS applications.

Metadata related to documents poses a further threat to organisations as it can provide a view of corporate network users, including email addresses, software versions and internal network locations—all of which provide useful information for those looking to attack organisations. According to a recent survey by KPMG of FTSE 350 organisations, **attackers were able to gain an average of 41 internal user names, 44 email addresses and five sensitive internal file locations from each company from metadata related to documents.** It therefore recommends that organisations should strip metadata from documents before they are published or sent out of an organisation.



Frequency of compromise

On average, an organisation sees a malware threat every three minutes from a malicious email attachment or web link, as well as a callback communication to a command and control server

98.5% see at least 10 incidents per week

Median is about **643** incidents per month

20% of organisations have thousands of incidents per week

95% of organisations are compromised with malicious infections inside their networks

Almost **80%** of organisations averaged an infection rate of more than **75 per week**

Growth in malware infections from 2H 2011 to 1H 2012 was **225%**, and from 1H 2011 to 1H 2012, **392%**.

Source: FireEye

Vulnerabilities with files and documents

Why documents are vulnerable: the case of PDF

According to a report released by Sandia National Laboratories, the PDF file type, on its release in 1993, was seen as a secure file format and was to be preferred over other document formats such as Microsoft Word that use macros and can contain vulnerabilities. **The first malware to affect the Adobe Acrobat family was discovered in 2001**, although it did not affect Reader. However, it did pave the way for other malicious exploits being developed for PDF. Many of these have been made possible by extensions made to the PDF format since 2001, including additional compression and encryption algorithms, scripting support, and multimedia support such as embedded Flash—all of which can be used to embed malware into a PDF file or to hide the presence of embedded malware.

Because **a PDF file is easy to edit and manipulate because it is written in PostScript, a text format, it is easy to write malware exploits for**. However, it is considered to be difficult to analyse PDF files for malware because of the complexity of the formatting language, the parsing idiosyncrasies in Reader and undocumented correction techniques used by Reader. At the CARO 2011 Workshop in the Czech Republic, a security researcher, **JM Esparza, demonstrated that PDF malware could be hidden from 42 out of 43 antivirus packages** tested by combining multiple obfuscation techniques.

According to Cisco, **all Microsoft Office documents can also contain embedded objects such as Flash files that make them similarly vulnerable**.

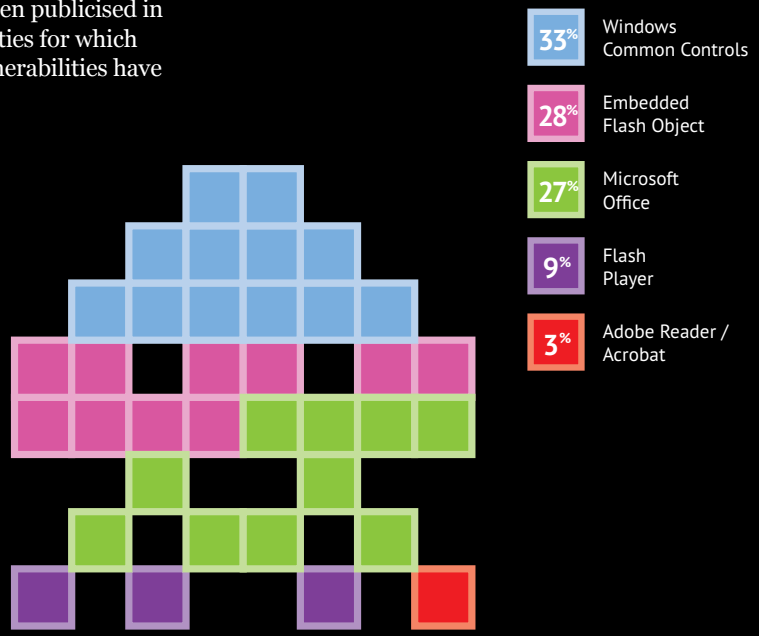
Exploiting vulnerabilities in documents

According to Microsoft's Security Intelligence Report **of June 2012, 39% users fail to install a Microsoft Word update one year after its release** and **70% have not installed an Adobe Flash Player update within a month of its release.**

Deploying patches is critical for protecting endpoints but, according to Trusteer, failure to keep up with software patches is identified by security and IT professionals as one of the most common challenges that organisations face—in the main part because of the sheer volume of patches that are released.

Some of the major attacks that have been publicised in recent years have exploited vulnerabilities for which patches existed and many of those vulnerabilities have been known about for years.

Chart 1: Vulnerabilities used in targeted attacks



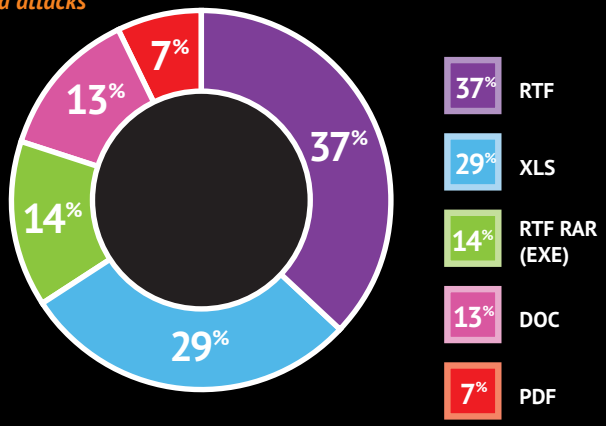
Source: Based on targeted attacks monitored by Trend Micro in 2012

However, **many advanced attacks deploy zero-day vulnerabilities**, which are software vulnerabilities that have not been seen before and for which no countermeasures have been developed. In many cases, they use variants of malware strains that have previously been seen, but that can evade signature-based defences because the existing malware strain has been modified in some way. As a result, the number of new malware strains, including variants, that is being seen is increasing dramatically.

Increasingly, malware is being custom written for a specific target and is used on only one occasion. According to FireEye, **68% of all malware seen in August 2012 was seen only the once.**

According to research from FireEye, **malware is delivered in Zip format in 92% of attacks. Of the remainder, 4% use PDF, 1% .exe and 3% others.**

Chart 3: Email attachment types used in targeted attacks



However, in a separate report, it states that the range of file types being used is growing more diverse. The use of Zip files is common among hackers since the majority of organisations do not block this type of file extension and **Zip files are often undetected by scanners**. Executables are less commonly used as most organisations already block or quarantine such attachments, according to Microsoft. According to Gartner, attackers generally look to exploit vulnerabilities in the reader application of Word or Adobe Reader, exploit the powerful scripting capabilities within the reader, or use containers such as Zip or RAR to camouflage malicious files.

Growing complexity of embedded malware

Many sources point to the growing complexity of malware that is being embedded in files. Trustwave likens this to a Russian nesting doll—every time an attachment is opened, there is another one hiding inside. This not only makes it extremely difficult to detect with traditional security controls, but also exploits the functionality of each file format, making it harder to control what cannot be executed. For example, **a Flash file embedded within a PDF does not require Flash Player to be installed in order to load. MP4 files can be loaded directly from within Flash Player and most PDFs will execute JavaScript.**

Chart 2: Growth in number of malware variants

Source: AV-Test.org Last Update: 12/01/2013

Email attachments versus web links

THE USE OF EMAIL ATTACHMENTS versus malicious links fluctuates. According to FireEye, malicious links represented about 15% of the volume of malicious emails in January 2012, whilst the volume of malicious links outnumbered malicious attachments in May and June 2012.

Symantec research shows similar fluctuations, as emails with malware URLs dropped significantly in 2012 to half of the corresponding rate per month in 2011 in some cases. It states that, **in 2012, around 23% of email malware contained a URL rather than an attachment, compared to 39% in 2011.** However, research from Trend Micro puts the use of email attachments higher, stating that 94% of spear phishing campaigns invite users to open an email attachment, compared with just 6% that ask the user to click on a link.

The use of links versus attachments varies for the following reasons:

Exploits that attackers have at hand – if a zero-day exploit is discovered in Adobe Acrobat, for example, organisations will see a spike in malware distributed via PDFs, whereas if a browser exploit is uncovered, more attacks will be waged via the web.

As zero-day application vulnerabilities are patched, file attachments used in attacks wane and attackers return to web-based vectors. However, they return to attachment-based attacks as new zero-day application vulnerabilities are discovered.

Preference for specific targets – sometimes fluctuations are determined by the predilections of a specific attack group, such as in a specific industry.

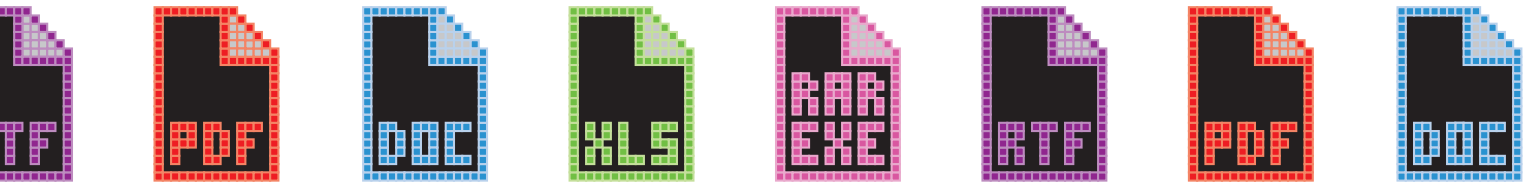
Season – web-based attacks are often seasonal, such as peaking around the end of year holiday season.

In October 2013, it was announced that information related to 38 million Adobe customers had been illegally accessed by hackers, as well as source code, which included Adobe Acrobat, which itself includes Reader. Such an event gives hackers the opportunity to examine the source code for new unknown vulnerabilities that can be exploited and for which zero-day exploits can be created. This is exactly the sort of event that tends to lead to a new stream of zero-day exploits being used in attachments using the application affected. Once vulnerabilities have been discovered, there is a vibrant and growing black market for the zero-day exploits that are developed as a result.

Table 1: Black market value of various zero-day exploits

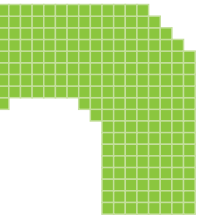
Adobe Reader	$5,000 to $30,000
Mac OSX	$20,000 to $50,000
Android	$30,000 to $60,000
Flash or Java browser plugin	$40,000 to $100,000
Microsoft Word	$60,000 to $100,000
Windows	$60,000 to $120,000
Firefox or Safari	$60,000 to $150,000
Chrome or Internet Explorer	$80,000 to $200,000
ISO	$100,000 to $250,000

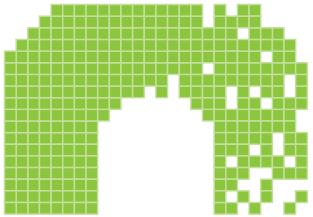
Source: Trusteer

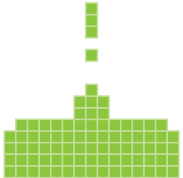


Exploits bypassing defences

TRADTIONAL ANTI-MALWARE CONTROLS can only defend against threats that have previously been defined. Imperva recently ran 82 new malware files through the VirusTotal system that checks files against up to 48 different antivirus engines, finding the detection rate to be zero. This is echoed by further research from Imperva that studied more than 80 malware samples to assess the effectiveness of antivirus controls, finding initial detection rates for a newly created virus to be less than 5%. It also found that it could take up to four weeks to detect a new virus from the time of the initial scan.







Vendors of such controls have moved to use newer techniques that include heuristic examination and sandboxing to try to isolate threats from the network. However, malware writers are increasingly focused on evading such techniques. For example, they incorporate virtual machine detection to bypass sandboxes. They also avoid using .exe file types that are most commonly picked up by antivirus engines. To avoid traditional defences such as reputation and signature-based filters, many attackers use a particular domain just a limited number of times and the number of 'throw-away' domains has increased dramatically. **In 2H 2011, domains seen just once amounted to 38% of the total malicious domains used for spear phishing, rising to 46% in 1H 2012**.

When new exploits are seen, they are also not always reported to antivirus vendors so that a countermeasure can be developed. In some cases, this is because organisations do not publish the fact that they have been breached. However, in many cases, the organisation is not even aware that it has been breached. According to the 2013 data breach investigations report from Verizon Business, **66% of breaches took months or more to discover and 69% were discovered by external parties to the organisation involved.** According to the forensics department at PwC, it is now very common for advanced criminal groups to be in networks and systems for a year or longer without being detected.

Increased use of mobile devices is also making the task of defending against malware harder, especially where the device is owned by users themselves. In such cases, users may not be inclined to install or use security controls such as antivirus on their devices owing to the performance drain that this leads to, or may disable controls that have been installed.

Another method that can be used for defending against malware is email sender and URL reputation filtering, which compare emails and links against a database of those known to be malicious. The weakness of this method is that threats are constantly changing and evolving, meaning that such lists may not be up to date, allowing threats to pass unchecked. Some vendors deploy real time checks in their email and web security gateways to ascertain if malicious activity has been detected, although this adds latency to services and the quality of the service depends on the techniques deployed to look for nefarious activity.

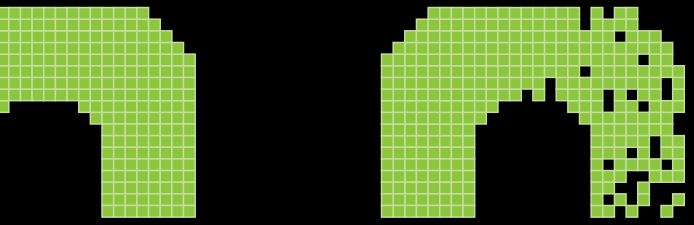
According to a survey undertaken by Gartner **in 2012, 65% of respondents stated that advanced encryption is a very important or critical capability of an email security gateway product.** However, it cautions that the use of encryption is also an incomplete solution. Many email gateway security vendors license their encryption capabilities from specialised vendors, which can mean that access to the full management capabilities of the encryption solution is often lacking. It also points to potential operational problems with email encryption, such as the requirement for client readers or browsers to be deployed on every endpoint, which can be an issue where users own their own equipment. It also states that encrypted emails can look 'phishy' to users, who will ignore them, or will end up in spam quarantines, where they are not always noticed.

Summary

DOCUMENTS ARE VITAL in the conduct of any business and have an enormous part to play in effectively communicating and collaborating both within organisations and with business partners and customers. They often contain some of the most important information generated by organisations, causing users to be less than cautious in opening documents that could be considered to be suspicious.

The underlying structure of many document types makes it a relatively easy task to embed malicious exploits within such documents, downloading malware onto the machines and devices of those users. This, along with their widespread use, makes them a favoured threat vector for attackers, who are using increasingly complex exploits to bypass traditional defences.

The growing number of vendors turning to focus on defending against document and file-based threats attests to the severity and scale of the problem. These days, every organisation is vulnerable to targeted attacks using exploits tailored especially for them. Therefore, every organisation needs to take the threat seriously and close the window of opportunity presented to attackers through lax controls over the malicious content that can be embedded into such documents that can cause serious harm to their business.



Where next?

Bloor maintains a Technology page on their website with further information regarding Advanced Threat Protection.

The author of this eBook is Fran Howarth, Senior Analyst for Bloor's security area.

Fran's website page has a rundown of her experience and you can discover other papers and articles she has written.

Copyright & disclaimer

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com