A Primer on
File-Borne Malware Threats

OPSWAT®

Introduction

The problem of file-borne malware is a severe one, and it is only growing in scope. More threat actors than ever are concealing malicious code, malicious macros, unsecure hyperlinks, and other malicious content within common files.

This method of delivering malicious software is effective largely for two reasons:

1. Users upload, download, receive, open, and edit many types of files every day and are not used to thinking of them as dangerous. Thus, they may be unaware or dismissive of the threat posed by files from online sources.

2. Users may be tricked into opening files from untrustworthy sources due to social engineering tactics used by attackers.

This paper will examine the ways attackers use files to deliver malware, the reasons these methods are effective, and the steps organizations should take to block these kinds of attacks.

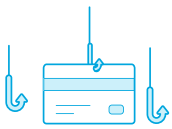
Extent of the Threat: 66% of Malware Installed via Malicious Files

File-borne malware comes in many forms, and the usage of it by attackers is trending upwards. From private users to small businesses to large enterprises, anybody can be a target.

As multiple sources attest, file-borne malware is one of the biggest threats facing companies and users today. An August 2016 post by Ivincea stated that "weaponized documents delivered by phishing remain the single largest threat to the enterprise."[1] Verizon's 2017 Data Breach Investigations Report finds that "66% of malware was installed via malicious email attachments."[2]

Examples of organizations that have been breached through file-borne malware are almost too numerous to list.

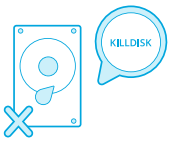
But many well-known malware attacks in recent years have used this attack method, including:



DRIDEX

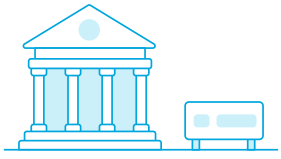
LOCKY

CRYPTOLOCKER



BLACKENERGY

WOLF CREEK NUCLEAR POWER PLANT HACK



CARBANAK BANK ROBBERIES[3]

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER RANSOMWARE INCIDENT

The Top 4 File Attack Methods

Attackers use a number of methods to conceal malicious content and code within common files. They especially use productivity files, such as Microsoft Office files or PDFs, but other file types may be used to deliver malicious payloads as well.

1. Macros: A Conundrum for Enterprises

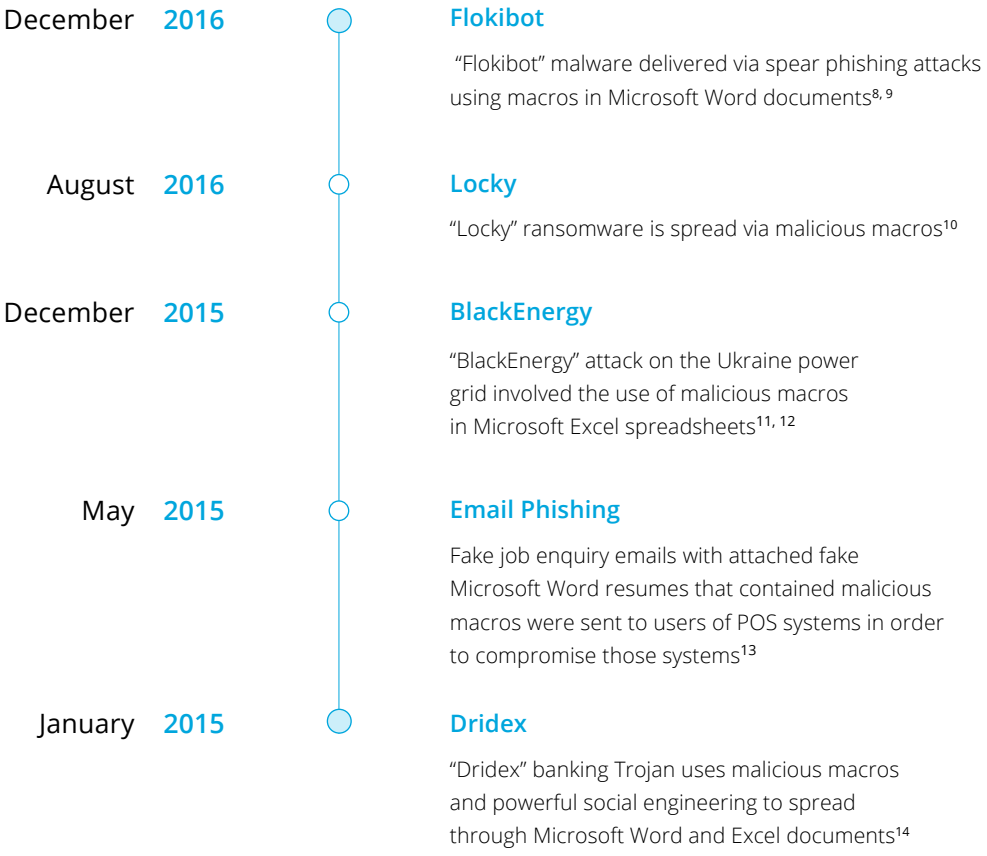
Macros are a feature of Microsoft Office files. They are automated tasks recorded by a user and stored in Visual Basic for Applications. Though macros are extremely useful and often essential within certain organizations, they can also be used for sinister purposes by cyber criminals.

Attackers have used malicious macros to spread malware since the 1990s, and they continue to be a common, often-effective attack vector. One of the first widespread macro viruses was the 1999 Melissa virus, which was spread via a Microsoft Word document. Once the document was opened, the malware accessed Outlook and emailed the first 50 contacts in the user's contacts list with copies of the document.

After Microsoft began making security updates to Office, macro-based malware attacks declined precipitously and nearly became extinct during the first decade of the 21st century.[4] Then, starting in late 2014, they began to make a comeback as attackers developed more advanced techniques for bypassing security measures and fooling users.[5] According to Proofpoint research, email attachment malware attacks grew over 600% from 2014 to 2015.[6]

A more recent example of a macro-based malware attack would be a series of incidents from February 2017, in which Macintosh users received emails with a Microsoft Word attachment entitled, "U.S. Allies and Rivals Digest Trump's Victory – Carnegie Endowment for International Peace.docm" (an important takeaway from this is that Macs are also susceptible to Microsoft Office macro malware). When a user opened the Word attachment, they would be prompted to enable macros by a dialog box. Once macros were enabled, the malicious payload would try to download malware from a website controlled by the attackers.[7]

Further examples of macro-based attacks:



Even Macintosh computers are now susceptible to macro-based attacks.[15]

In Microsoft Office 2007 and all later versions, macros are disabled by default and have to be enabled by the user in order to run. Attackers often attempt to get around this roadblock through manipulative social engineering techniques. For example, a message may pop up prompting users to enable macros "for security reasons." Mukul Hinge of OPSWAT described another social engineering method:

> *An enterprise employee receives what appears to be a legitimate email with an attachment (such as an invoice). When the attachment is opened, the document encoding appears garbled (full of garbage characters). A message similar to this might be displayed, 'If you see incorrect data encoding, please enable macros.' As soon as the user enables macros, the [malware] is downloaded and the payload is executed.*[16]

One form of social engineering

That these and similar social engineering techniques are effective is borne out by the fact that **98% of Office file attacks use macros.**[17, 18]

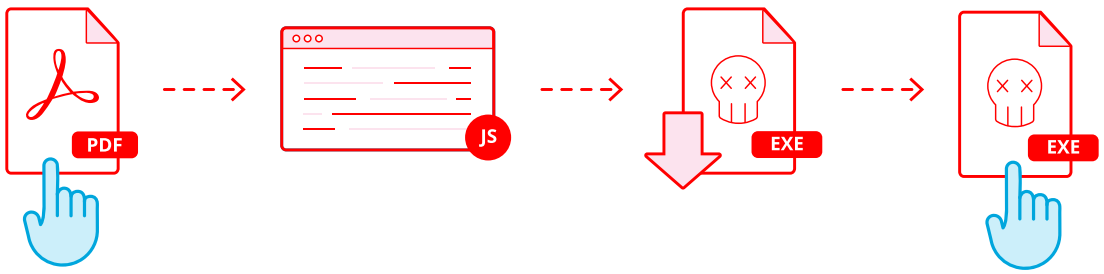
In March 2016, Microsoft added an additional security feature to Office in order to block malicious macros. Administrators are able to block macros from running altogether in Office files downloaded from online sources. However, even this feature does not completely protect users from malicious macros – system administrators may choose to leave macros enabled if macros are necessary for productivity, or they may just be unaware of this option.[19]

Additionally, macros are just one of many attack methods that involve commonly used productivity files.

2. Scripts: JavaScript Powers the Internet, But Shouldn't Be in Documents

Adobe PDFs support complex content such as scripts, and malicious JavaScript is often inserted within PDF files. A common attack vector is to take advantage of an Adobe buffer overflow vulnerability, crash the program, and inject malicious code into an operating system's stack. (You can see an example of such a vulnerability being exploited by ransomware in the OPSWAT blog post "Ransomware Exploits: Detecting and Exploiting CVE-2008-2992 in Adobe Acrobat Reader" by engineer Vinh Lam.[20])

Another common attack method using PDFs is to embed malicious JavaScript that accesses online malware and executes it when the PDF is opened. It is relatively simple for an attacker to insert JavaScript within a PDF, and several malware researchers have described the methods used.[21, 22]



A PDF becomes malicious

Cyber criminals can also deliver malicious JavaScript to victims by hiding them within archive files, such as ZIP folders. Malwarebytes Labs described this method of attack in their 2017 "State of Malware" report:

> *One of the biggest changes in distribution in 2016 was the use of attached scripts to phishing emails. These scripts usually reside inside of a ZIP file and, once opened and launched, reach out to a remote server to download and install malicious software on the system.*[23]

Since Windows operating systems often hide the extensions of files when displaying them in a folder, users may be unsure what kinds of files they are looking at when they open a ZIP folder. If the files have deceptive names, users may just open the JavaScript files, which will then execute and download the malware payload.

Attackers will also add fake extensions to JavaScript file names – for example, the true name of a malicious JavaScript file could be "Invoice.pdf.js," but when Windows hides the file extension, the file name will appear to be "Invoice.pdf." Thinking that the file is just a PDF, the user could then open it.

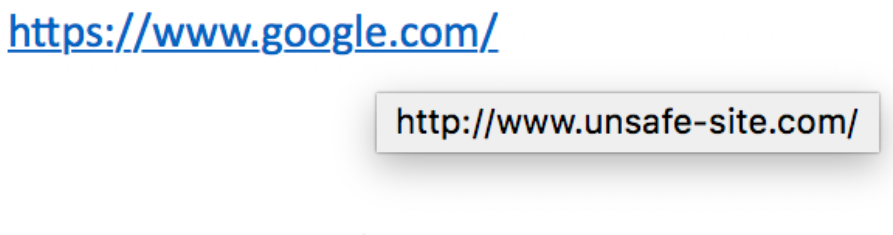
Only one user has to fall for such a ruse for an endpoint, and possibly an entire network, to be compromised.

Further reading: Selvaraj, Karthik and Gutierrez, Nino Fred. "The Rise of PDF Malware," Symantec.

3. Hyperlinks: Redirection Is Key in This Form of Attack

Hyperlinks to malicious websites are another well-known method of delivering malware to victims. Users may be tricked into visiting phishing websites or unsafe websites that trigger drive-by downloads.

Phishers may type out a legitimate-looking URL and embed a hyperlink within it that links to a different, malicious URL. Or they may use a domain that looks very similar to a legitimate domain that users are used to visiting.



The real URL pops up as a cursor hovers over it

Hyperlink attacks are especially pernicious because productivity documents and intra-office emails often contain hyperlinks. Cyber criminals specialize in tricking unwitting users into thinking an unsafe or deceptive link is legitimate.

Examples of hyperlink-based attacks abound. Cyber security journalist Brian Krebs reported on one such example in May 2017. After hackers stole a list of customer email addresses from electronic signature company DocuSign, they sent phishing emails to these customers:

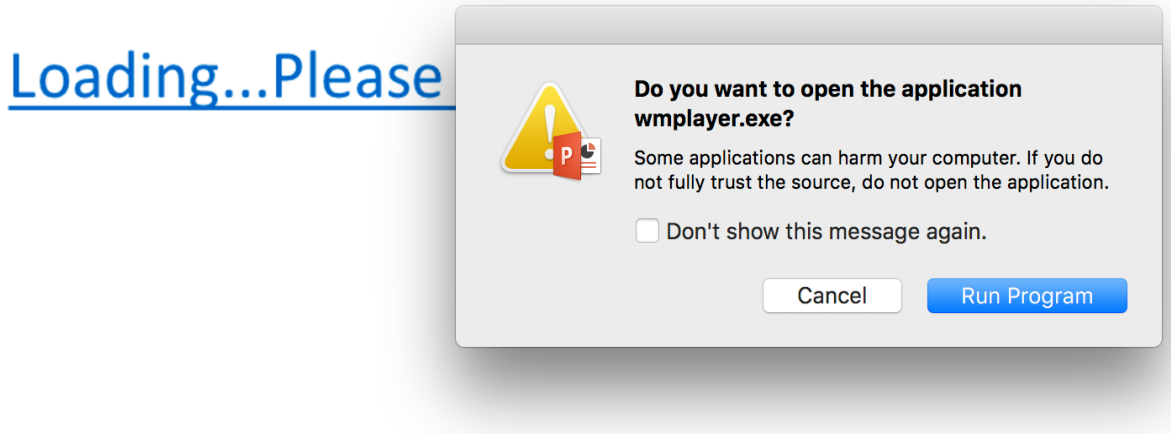
> *San Francisco-based DocuSign warned on May 9 that it was tracking a malicious email campaign where the subject line reads, 'Completed: docusign.com – Wire Transfer Instructions for recipient-name Document Ready for Signature.' The missives contained a link to a downloadable Microsoft Word document that harbored malware.*[24]

Once users clicked on a link labeled "View Documents," they were compromised.[24]

However, links to insecure websites are far from the only attack method, and in some file types, users may not even need to click on the link in order to trigger malicious actions that lead to the download of a malware payload.

In one example from 2017, attackers sent malicious PowerPoint (PPSX) attachments to their targets. The PowerPoint presentations contained a hyperlink that read simply, "Loading...Please Wait." When a user's cursor passed over the hyperlink, without clicking on it, PowerPoint was triggered to access an external application that performed malicious actions eventually resulting in the download and execution of a Trojan virus. Such an attack takes advantage of a legitimate, useful feature of an Office program. It is very simple to set up an attack like this in Microsoft PowerPoint and in several other Microsoft Office programs.[25, 26, 27]

Users who have been trained not to enable macros or scripts could still be highly susceptible to this kind of attack.



A PowerPoint hyperlink tries to access an external program

4. Image-Borne Malware: A Highly Stealthy Form of Attack

"Steganography" refers to concealing hidden information in text or an image. Steganography is an information concealment technique that predates the invention of computers.

In the digital age, attackers have been able to take this old practice and apply it to digital images. Malicious code can be concealed within an image's pixel data, or it can be masked or distorted within an image.

In 2015, cyber security researcher Saumil Shah described a method of concealing malicious code within an image. Shah got a browser to process a malicious image's pixel data as JavaScript by taking advantage of the HTML 5 <canvas> tag. Once the image was loaded by the browser, the JavaScript was read and executed, resulting in the download of a malicious payload.[28, 29, 30]

In their June 2017 quarterly threats report, McAfee described an exploit kit called "Sundown" that first began using steganography to conceal malicious code within images in 2016:

> *A Sundown attack begins when a victim visits a compromised website or a clean website with malicious ads. ... [V]ictims were redirected toward the Sundown landing page. The page retrieved and downloaded PNG images. The Sundown kit landing page contains a decoding routine that unlocks the PNG file and extracts the malicious content. The landing page is heavily obfuscated.*[31]

Image-borne malware is not just carried by JPEG and PNG files. In February 2017, researchers described attacks that used malicious SVG files. Similar to the other attacks described above, these SVG images contained malicious JavaScript. When the files were opened by a browser, the JavaScript would execute.[32]

GIF and BMP files can also conceal malicious scripts.[33]

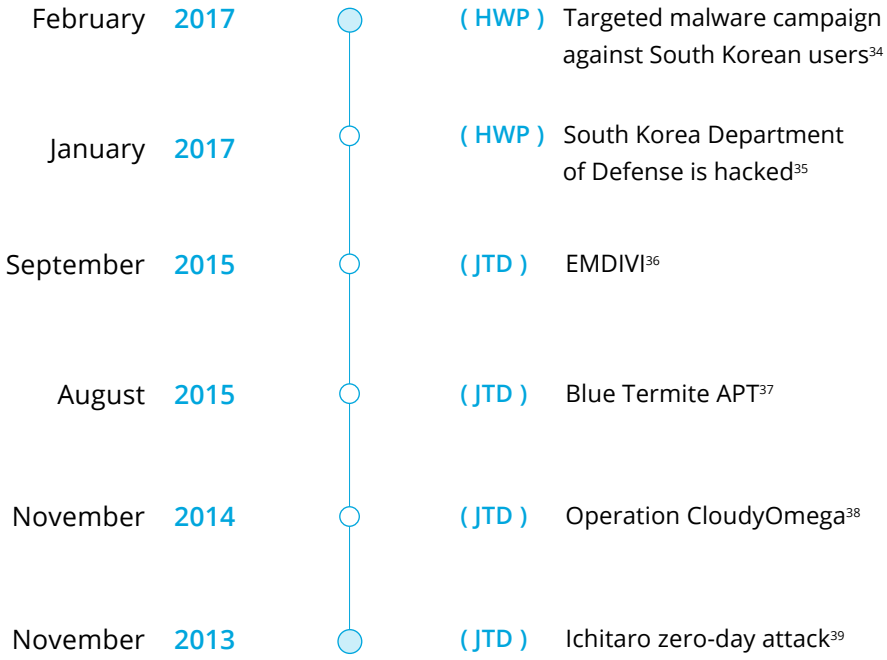
Image-borne malware is especially hazardous because opening an image is not typically considered risky – much like the average user may not consider Word documents or PDFs to be risky.

The List Goes On: Other File Types Attackers Use

Naturally, productivity files encompass far more than Microsoft Office files, PDFs, and images. **If a file type is regularly used by a business or industry, it is likely that cyber criminals have already begun using those file types to carry out their attacks.**

In many countries in Asia, **JTD** and **HWP** files are commonly used instead of Microsoft Office documents. Attackers have found ways to use these file types to deliver malware as well.

Examples of malware attacks that used either JTD or HWP files include:



XML documents are highly flexible and widely used, including within Microsoft Office documents and SOAP messages. Unfortunately, XML documents also have many security vulnerabilities, and attackers are well aware of this fact. For example, in 2015 cyber criminals used XML documents containing malicious macros to spread the Dridex banking Trojan, in addition to using regular Microsoft Excel and Word files.[40]

LNK files are shortcuts to executables. They are not widely used by most users, but when they are attached to targeted phishing emails, users may open them anyway. In 2017, Microsoft Malware Protection Center researchers discovered malicious LNK files hidden within ZIP archives that were attached to phishing emails.[41]

Conclusion

The list of organizations that have been compromised by files with malicious content is ever-growing. This, in and of itself, is proof that typical security measures are failing to block such attacks.

Today, society and productivity center around the exchange of information, and digital files are foundational to this transfer of information. It is not feasible to simply close off these threat vectors by blocking all files from external sources, as many file types are necessary for organizational productivity. But as long as human error is part of the equation, malicious files will continue to slip through and be opened by victims.

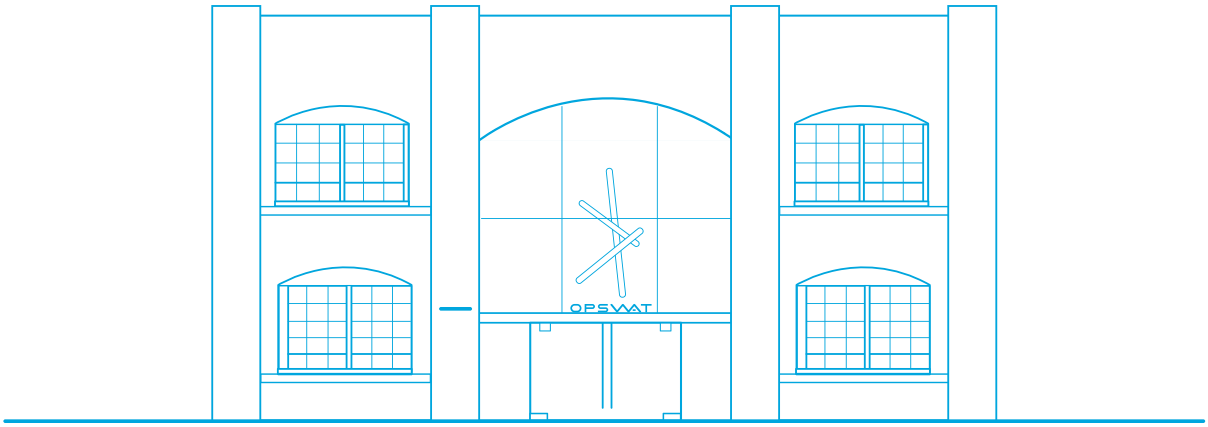
While our overview has focused on the most popular file types used in organizations today, all kinds of files can be used by attackers as a transport vehicle for malware.

As a leading provider of and authority on cyber security solutions to counter the threat from file-based malware, OPSWAT offers several strategies within its portfolio to prevent these attacks and data breaches stemming from them. If we define traditional anti-malware approaches as endpoint antivirus suites, web and email security gateways, and firewalls, we believe it is clear that these approaches in and of themselves do not work against file-borne malware attacks.

Newer approaches must focus on ways to detect and prevent unknown and zero-day attacks that emanate from the file-based vector.

About OPSWAT

OPSWAT is a global cyber security company providing solutions for enterprises since 2002 to identify, detect, and remediate advanced security threats from data and devices coming into and out of their networks. Trusted by over 1,000 organizations worldwide for this secure data flow, OPSWAT prevents advanced security threats across multiple channels of file transfer and data flow with flexible options of Metadefender solutions and API-based development and threat intelligence platforms. With over 30 anti-malware engines, 100+ data sanitization engines, and more than 25 technology integration partners, OPSWAT is a pioneer and leader in data sanitization (Content Disarm and Reconstruction), vulnerability detection, multi-scanning, device compliance, and cloud access control. To learn more about OPSWAT, please visit **www.OPSWAT.com**.



Endnotes

1. Belcher, Pat. Ivincea, "Invincea Data Breach Prevention Series: August 2016": https://www.invincea.com/2016/09/invincea-data-breach-prevention-series-august-2016/

2. Verizon, "Verizon 2017 Data Breach Investigations Report"

3. Gilbert, David. International Business Times, "The Billion Dollar Bank Job: How hackers stole $1bn from 100 banks in 30 countries": http://www.ibtimes.co.uk/billion-dollar-bank-job-how-hackers-stole-1bn-100-banks-30-countries-1488148

4. Szappanos, Gabor. Virus Bulletin, "VBA Is Not Dead!": https://www.virusbulletin.com/uploads/pdf/magazine/2014/vb201407-VBA.pdf h/t https://nakedsecurity.sophos.com/2014/07/07/remember-macro-viruses-infected-word-and-excel-files-theyre-back/

5. Donohue, Brian. Threatpost, "Microsoft Reports Massive Increase in Macros-Enabled Threats": https://threatpost.com/microsoft-reports-massive-increase-in-macros-enabled-threats/110204/

6. Proofpoint, via Clearswift, "10 Shocking Malware and Ransomware Statistics": https://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

7. Mimoso, Michael. Threatpost, "Macro Malware Comes to macOS": https://threatpost.com/macro-malware-comes-to-macos/123640/h/thttp://business.financialpost.com/technology/cio/mac-users-receiving-malware-spam-hacker-hits-160000-printers-security-news-it-leaders-need-to-know/wcm/504c85a3-459b-4178-8480-28243b1f3df6

8. Sjouwerman, Stu. KnowBe4 Security Awareness Training Blog, "VISA warns for Flokibot Spear Phishing Infections": https://blog.knowbe4.com/visa-warns-for-flokibot-spear-phishing-infections

9. Spring, Tom. Threatpost, "Zeus Variant 'Floki Bot' Targets PoS Data": https://threatpost.com/zeus-variant-floki-bot-targets-pos-data/122310/

10. SecurityWeek, "Locky Ransomware Reverts to Malicious Macros": http://www.securityweek.com/locky-ransomware-reverts-malicious-macros

11. U.S. Department of Homeland Security, "Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure": https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

12. Higgins, Kelly Jackson. Dark Reading, "Macros, Network Sniffers, But Still No 'Smoking Gun' In Ukraine Blackout": http://www.darkreading.com/threat-intelligence/macros-network-sniffers-but-still-no-smoking-gun-in-ukraine-blackout/d/d-id/1324076

13. Constantin, Lucian. PCWorld, "Attackers use email spam to infect point-of-sale terminals with new malware": http://www.pcworld.com/article/2926352/attackers-use-email-spam-to-infect-pointofsale-terminals-with-new-malware.html

14. Mimoso, Michael. Threatpost, "Dridex Banking Trojan Spreading Via Office Macros": https://threatpost.com/dridex-banking-trojan-spreading-via-office-macros/110255/

15. Cimpanu, Catalin. Bleeping Computer, "Word Document Spreads Macro Malware Targeting Both Windows and macOS": https://www.bleepingcomputer.com/news/security/word-document-spreads-macro-malware-targeting-both-windows-and-macos/

16. Hinge, Mukul. OPSWAT Blog, "Ransomware Is Now an Enterprise Threat: How OPSWAT Can Help": https://www.opswat.com/blog/ransomware-now-enterprise-threat-how-opswat-can-help

17. Microsoft TechNet, "New feature in Office 2016 can block macros and help prevent infection": https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

18. Higgins, Kelly Jackson. Dark Reading, "Why Microsoft's New Office 2016 Macro Control Feature Matters": http://www.darkreading.com/vulnerabilities---threats/why-microsofts-new-office-2016-macro-control-feature-matters/d/d-id/1325632

19. Constantin, Lucian. PCWorld, "Microsoft adds macros lockdown feature in Office 2016 in response to increasing attacks": http://www.pcworld.com/article/3047480/security/microsoft-adds-macros-lockdown-feature-in-office-

20. Lam, Vinh. OPSWAT Blog, "Ransomware Exploits: Detecting and Exploiting CVE-2008-2992 in Adobe Acrobat Reader": https://www.opswat.com/blog/ransomware-exploits-detecting-and-exploiting-cve-2008-2992-adobe-acrobat-reader

21. Lakhani, Aamir. Doctor Chaos, "Distributing malware inside Adobe PDF documents": http://www.drchaos.com/distributing-malware-inside-adobe-pdf-documents/

22. InfoSec Institute, "Analyzing Malicious PDFs": http://resources.infosecinstitute.com/analyzing-malicious-pdf/

23. Malwarebytes Labs, "2017 State of Malware Report": https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdfh/t https://www.forbes.com/sites/kevinmurnane/2017/01/31/the-malwarebytes-report-the-2016-malware-threat-landscape/

24. Krebs, Brian. Krebs on Security, "Breach at DocuSign Led to Targeted Email Malware Campaign": https://krebsonsecurity.com/2017/05/breach-at-docusign-led-to-targeted-email-malware-campaign/

25. Kovacs, Eduard. SecurityWeek, "New Method Used to Deliver Malware via PowerPoint Files": http://www.securityweek.com/new-method-used-deliver-malware-powerpoint-files

26. Fenton, Caleb and Liba, Itai. SentinelOne Labs, ""Zusy" PowerPoint Malware Spreads Without Needing Macros": https://sentinelone.com/blogs/zusy-powerpoint-malware-spreads-without-needing-macros/

27. Dodge This Security, "New PowerPoint Mouseover Based Downloader – Analysis Results": https://www.dodgethissecurity.com/2017/06/02/new-powerpoint-mouseover-based-downloader-analysis-results/

28. Khandelwal, Swati. The Hacker News, "How to Hack a Computer Using Just An Image": http://thehackernews.com/2015/06/Stegosploit-malware.html

29. Shah, Saumil. SyScan '15 Singapore, "Hacking With Pictures": https://www.youtube.com/watch?v=np0mPy-EHII

30. Qiao, Chris. OPSWAT Blog, "Image-Borne Malware: How Viewing an Image Can Infect a Device": https://www.opswat.com/blog/image-borne-malware-how-viewing-image-can-infect-device

31. Beek, Christiaan et al. McAfee Labs, "McAfee Labs Threats Report June 2017": https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

32. Thomson, Victor. iTech Post, "Malware To Be Found On Less Suspicious File Types": http://www.itechpost.com/articles/81761/20170208/malware-found-less-suspicious-file-types.htm

33. "Stegosploit": http://stegosploit.info/

34. Arghire, Ionut. SecurityWeek, "Targeted Malware Campaign Uses HWP Documents": http://www.securityweek.com/targeted-malware-campaign-uses-hwp-documents

35. Min-Ji, Choi. Digital Daily, "국방부 사칭 해킹메일, PC 내 파일 탈취 시도 발견 (English translation via Google: Hacking of the Department of Defense)": http://www.ddaily.co.kr/news/article.html?no=151613

36. Sy, Benson. Trend Micro, TrendLabs Security Intelligence Blog, "Attackers Target Organizations in Japan; Transform Local Sites into C&C Servers for EMDIVI Backdoor": http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/

37. Kovacs, Eduard. SecurityWeek, "Blue Termite APT Targets Japanese Organizations": http://www.securityweek.com/blue-termite-apt-targets-japanese-organizations

38. Symantec Official Blog, "Operation CloudyOmega: Ichitaro zero-day and ongoing cyberespionage campaign targeting Japan": https://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

39. Kumar, Mohit. The Hacker News, "Japanese word processor 'Ichitaro' zero-day attack discovered in the wild": http://thehackernews.com/2013/11/Japanese-Ichitaro-zero-day-vulnerability-CVE-2013-5990.html

40. Trustwave, via Threatpost, "Dridex Banking Trojan Spreading Via Macros in XML Files": https://threatpost.com/dridex-banking-trojan-spreading-via-macros-in-xml-files/111503/

41. Constantin, Lucian. CSO Online, "Malware distributors are switching to less suspicious file types": http://www.csoonline.com/article/3166152/security/malware-distributors-are-switching-to-less-suspicious-file-types.html