DHS Office of Cybersecurity & Communications

2013 Cybersecurity Review

The 2013 Cybersecurity Review highlights significant cybersecurity stories, attacks, and trends from the past year. The Review represents a survey of significant cybersecurity issues as reported by independent security experts, cybersecurity news sources, cybersecurity service providers, and security research organizations. The Review focuses on issues and events that multiple sources agree were significant to the cybersecurity landscape in 2013. The Review is intended to highlight these topics of discussion and is not intended to prioritize particular issues over others, including issues not discussed in the document. References link to individual sources, but the themes are derived from multiple sources.

Malware

- **Malware grew in number and sophistication.** New strains of malware reached a record 10 million in the third quarter of 2013, and malware incidents increased in frequency.[1] [2] Malware distribution methods grew increasingly diverse to include malicious URLs, spam, compromised websites, and compromised Web servers.[3] [4] [5] Malware in general grew more sophisticated, with some strains of malware using stolen certificates to avoid detection.[6] [7] [8] [9] Continuing a trend observed in recent years, Trojans remained the most popular type of malware.[10] [11]
- **Ransomware attacks were a problem throughout the year.** Ransomware attacks remained a problem and also increased in popularity since 2012.[12] [13] [14] [15] [16] [17] [18] Two broad types of ransomware were common—police-themed ransomware, which threatened to report victims to law enforcement for supposedly having illegal content on their computers, and encryption ransomware, which encrypted victims' files and demanded payment in return for decrypting the files.[19] [20] [21] [22] While ransomware is not a new threat, encryption ransomware in 2013 became more sophisticated, using stronger levels of encryption than before.[23] [24] In the second half of 2013, appearance of CryptoLocker, which threatened to permanently destroy decryption keys if payment was not received, reached an all-time high.[25] [26] [27] 2013 also saw the first instances of mobile ransomware, all of which targeted the Android operating system.[28] [29]
- **Watering hole attacks effectively targeted a variety of organizations.** Watering hole attacks effectively infected specific groups of users with malware by compromising websites that these users would be likely to visit, rather than directly targeting them or their organizations. [30] [31] [32] [33] [34] Watering hole attacks remain

relatively rare compared to other attack methods but the number is rising.[35] The targets of watering hole attacks in 2013 ranged from large technology companies to Tibetan activist groups.[36] [37]

- **Exploit kits continued to be popular among malware developers.** The number of available exploit kits, which are software packages that simplify and manage the installation of a malicious payload on a victim's system, has grown significantly since 2012, and Blackhole is no longer the dominant exploit kit.[38] [39] [40] [41] Exploit kit developers began focusing on zero-day vulnerabilities in 2013 to feed their exploit kits, and the market for zero-day vulnerabilities has grown.[42] [43]

Botnets

- **Botnet attacks delivering malware decreased.** Although botnets remained both a serious problem and the source of many DDoS attacks and malware distribution campaigns, malware infections stemming from botnet attacks decreased.[44] [45] Botmasters improved the resilience of their botnets by moving their command and control servers to the "darknet," using anonymous networks such as Tor.[46] [47] Botmasters also improved their countermeasures against takedowns with faster response times.[48]
- **Botmasters expanded the types of attacks delivered by botnets.** Instead of only enslaving computers for mass spamming campaigns or DDoS attacks, botnets increasingly distributed ransomware, banking malware, and malicious URLs.[49] [50] [51] Mining cryptocurrencies emerged as an easier, faster method of botnet income generation due to botnets combining their computing resources.[52] [53] [54] Mirroring the increase in ransomware infections, botnets increasingly distributed ransomware.[55] [56]

Mobile

- **Although mobile malware comprised a small percentage of malware overall, mobile malware threats became increasingly advanced and carried out targeted attacks.** Attack patterns and tools that target desktop operating systems are now present on mobile platforms.[57] [58] First sighted in the wild in 2012, mobile botnets continue to mature.[59] [60] [61] Several samples of mobile malware successfully gained root device access and exposed online banking information.[62] [63] [64] [65] During the second quarter of 2013, one source said that exploits harvesting personal banking information are one of the most prevalent forms of mobile malware, and another source said that mobile banking toolkits increased.[66] [67] Researchers observed multiple instances of SMS forwarding Trojans designed to overcome two-factor authentication by stealing mobile Transaction Authentication Numbers from SMS messages (i.e. man-in-the-mobile).[68] [69] [70]
- **Android remained the most targeted mobile operating system as mobile malware continues to evolve.** The rapid growth of Android malware samples that occurred in 2012 continued in 2013.[71] [72] Several researchers found that Android malware comprised over 98 percent of mobile malware encounters in 2013.[73] [74] In September, researchers discovered Obad, a multifunctional Android Trojan distributed by a mobile botnet, which has the ability to send premium SMS messages, install other malware, and infect other devices via Bluetooth.[75]

DDoS

- **As botnets increased in sophistication, distributed denial of service (DDoS) attacks were observed on a massive scale.** Experts reported multiple DDoS attacks exceeding 300 Gbps in 2013, which were larger than previously observed highs of

about 100 Gbps.[76] [77] DDoS retained its 2012 designation as the primary tool for politically motivated attacks, known as digital activism or hacktivism.[78] [79] [80] In March 2013, a major DDoS attack was launched against Spamhaus, an organization that tracks and documents the sources of spam-related activity.[81] [82] [83] [84] [85] Researchers estimate that, at its peak, the attack reached a throughput over 300Gbps.[86] [87] [88] The assault made use of DNS amplification to increase malicious traffic, a strategy that gained traction this year.[89] [90] [91]

Organizational Security

- **The shift toward bring your own device (BYOD) highlighted device security and device policy development.** Research suggested that the proportion of organizations allowing employees to use their own devices continued to increase, while few organizations had policies to secure and govern these devices.[92] [93] [94] While BYOD policies have distinct business advantages, they created new challenges for IT staff, placed additional responsibility on users, and are recognized as valuable targets by cybercriminals.[95] [96] [97] One study found that, while only 13 percent of respondents reported a security breach related to BYOD, 40 percent of respondents were unsure if they had experienced a breach.[98]

Third-Party Applications

- **Java continued to be the most exploited third-party application.** Researchers determined that an overwhelming percentage of attacks and discovered vulnerabilities were Java-based.[99] [100] [101] [102] [103] Researchers attributed this focus to Java's large user base, which provides a large pool of potential victims for cybercriminals' tailored attacks.[104] [105] [106] Exploit kits increasingly included multiple Java vulnerabilities as attack vectors.[107] [108] [109] [110] Java's popularity among developers led to a Java vulnerability forming the core of a major watering hole attack that affected major organizations such as Facebook, Twitter, Apple Corp. and Microsoft in February 2013.[111] [112] Java's consistent use in malicious attacks led to a significant number of security organizations recommending that it be uninstalled from systems that do not critically require the software.[113] [114] [115]
- **Other third-party applications experienced attacks, albeit much less commonly than Java.** Researchers calculated that in terms of percentage of attacks and discovered vulnerabilities, Java dwarfed other applications like Acrobat Reader and Flash Player.[116] [117] [118] [119]
- **Developers of major third-party applications responded to security threats.** A Java update in 2013 raised the default security level from "medium" to "high" and Adobe transitioned to more frequent and automatic updates.[120] [121]

Spam

- **Spam evolved and grew.** Experts agreed that in 2013 spam evolved with new tactics and capabilities from the spam seen in previous years.[122] [123] [124] After a decrease in spam volume in 2012, most sources indicate that spam volume increased again in 2013 for unknown reasons.[125] [126] [127] [128]
- **The content of spam messages varied from previous years.** Spam messages most commonly included content on buying pharmaceuticals and news about current events, such as the Boston Marathon bombing, to lure recipients into opening the messages.[129] [130] [131] [132] Sources indicated that pump-and-dump stock spam, which had previously died off after aggressive policing by the U.S. Securities and Exchange Commission, made a comeback in 2013.[133] [134]

- **Variations in spam were based on geography.** Two experts discussed how spam adjusted its marketing focus based on geography, e.g. drug spam was popular in the United Kingdom, while "lonely women" spam was popular in India, Italy, Poland, and Spain.[135] [136]

Phishing

- **Experts observed differing phishing trends.** One source said that phishing increased, while another source said that malicious phishing URLs decreased from January through June 2013, and then began to rise again from July through September 2013.[137] [138] One source recorded nearly a 50 percent increase in spear phishing attacks on organizations, with 45 percent of spear phishing attacks used as the entry point for advanced persistent threat (APT) attacks.[139]
- **Phishing emails were launched against a diverse set of targets.** One source stated that most new attacks targeted financial websites or online auctions; others agreed that financial and online auction credentials were some of the most desired credentials, but also added that e-mail, storage, media, social networking, online services, online dating, e-commerce, and gaming targets were also quite popular among attackers.[140] [141] [142] [143] [144]

Country-Linked Attacks

- **Country-linked activist groups primarily targeted media outlets with some attacks on government entities.** In May 2013, a phishing attack on Twitter resulted in an activist-generated tweet that U.S. President Barack Obama was hurt in an explosion, causing stocks to drop.[145] [146] [147] In August 2013, several webpages on the *Washington Post's* website were rerouted to the activist group's website.[148] [149] [150] In August, the *New York Times* and Twitter were attacked with domain name system cache poisoning.[151] [152] Other victims of activist attacks include the Agence France-Presse, *Al-Jazeera,* Associated Press, CBS News, Channel 4 (UK), CNN, Fox News, *The Guardian, The Huffington Post,* Human Rights Watch, Mashable, National Public Radio, NBC News, *NY Post*, Outbrain, ShareThis.com, *Slate,* ThomsonReuters, TrueCaller, Government of Turkey, and *U.S. Weekly*—mostly news media or political websites, or in the case of Outbrain, a third-party content provider for news media.[153] [154] [155] [156] [157]
- **Attacks on governments and militaries organizations continued.** In March 2013, almost 50,000 systems of financial institutions and television broadcasters in South Korea were infected with malware as part of what security researchers estimated to be a larger campaign targeting South Korea's military.[158] [159] In June 2013, on the anniversary of a significant event of the Korean War, North Korean and South Korean government websites were attacked.[160] [161] Additionally, a foreign government's hardware and software became a supply chain concern for the U.S. Government, resulting in new restrictions in 2013 on products manufactured in the country used by the U.S. Department of Defense (DOD), as well as DOD employment restrictions of personnel from the country.[162]

Targeted Attacks

- **APTs increasingly affected organizations' networks**. Attackers targeted specific companies and organizations seeking specific financial, sensitive, and proprietary information.[163] [164] Surveys support this finding; one security organization found that 40% of respondents had encountered APTs while another saw growth in the percentage of respondents encountering APTs from 20% to 30% in the last year.[165] [166]

APT attacks were also increasingly executed by attackers with significant resources, potentially groups with links to country governments.[167] [168] [169]

Data Breaches

- **Organizations using differing methodologies disagree over whether the number of data breach incidents increased in 2013, though the number of exposed records appears to have increased significantly.**
    - The number of reported global data breaches, as logged by the Open Security Foundation (OSF), was 2,164 in 2013.[170] This is about a 31 percent decrease from 3,140 breaches in 2012, which was the highest figure recorded since reporting began in 2004. The number of records exposed, however, increased over 300 percent from 267 million to 822 million, surpassing the previous annual record of 412 million records in 2011.
        - Malicious hacking caused 59.8 percent of incidents recorded and caused the loss of 72 percent of the lost records.
        - OSF sorts victim organizations into four industries and one unknown category. The breakdown of breaches by industry is:
            - Business (including financial): 53.4 percent
            - Government: 19.3 percent
            - Medical: 11.5 percent
            - Education: 8.2 percent
            - Unknown: 7.2 percent
        - OSF included all global breaches of personally identifiable information (PII), including encrypted data. Of these global numbers, the U.S. experienced 48.7 percent of the incidents and 66.5 percent of the lost records.
        - Information about previous breaches continues to become public months and even years after initial reporting, so OSF's numbers for 2012 and 2013 represent information available before the publication of its report in February 2014.
    - The number of reported U.S. data breaches, as logged by the Identity Theft Resource Center (ITRC), increased by 30 percent to 614 in 2013 from 447 in 2012.[171] The ITRC does not consider the number of unique records exposed, as a significant number of publicly reported U.S. data breaches do not supply this information.[172]
        - The ITRC sorts victim organizations into five industry categories. The breakdown of breaches by industry is:
            - Medical/Healthcare: 43.8 percent (9.6 percent of records)
            - Business: 34.4 percent (84 percent of records)
            - Government/Military: 9.1 percent (2 percent of records)
            - Education: 9.0 percent (3.5 percent of records)
            - Banking/Credit/Financial: 3.7 percent (0.9 percent of records)
        - The ITRC generally defines a breach of PII as when "an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk."[173] The ITRC does not generally include the number of records exposed in its statistics if the data is encrypted.
        - Information about previous breaches continues to become public months and even years after initial reporting, so ITRC's numbers for 2013 represent information available before the publication of its

updated report on February 20, 2014.

- **Several large, high-profile data breaches occurred this year.** OSF records four of the largest breaches on record as occurring in 2013. These four breaches account for nearly 470 million lost records, which may explain the large increase in exposed records from 2012 to 2013.[174] For example, in October 2013, attackers compromised account credentials from over 150 million Adobe users, which were then posted to the Internet.[175] [176] The sheer size of this dataset makes it invaluable for other illicit activities, including brute-force password cracking and targeted attacks.[177] OSF currently ranks this incident as the largest data breach on record.[178]

[1] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 4, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[2] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 5, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[3] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 58, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[4] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 17, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[5] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 13, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[6] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 18, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[7] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 8, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[8] "Security Threat Report 2014," Sophos, 2013, p. 18, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[9] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 28, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[10] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 38, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[11] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 4, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[12] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 59, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[13] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 8, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[14] "Security Threat Report 2014," Sophos, 2013, p. 16, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[15] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 20, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[16] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[17] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, p. 19, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[18] "Threat Report H1 2013," F-Secure, 2013, p. 26, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[19] "Threat Report H1 2013," F-Secure, 2013, p. 26, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[20] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 10, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[21] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 59, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[22] "Security Threat Report 2014," Sophos, 2013, p. 5, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

[23] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 28, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[24] "Security Threat Report 2014," Sophos, 2013, p. 3, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[25] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 59, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[26] "Security Threat Report 2014," Sophos, 2013, p. 5, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[27] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 7, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[28] "Security Threat Report 2014," Sophos, 2013, p. 8, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[29] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 11, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[30] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, pp. 41-42, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[31] "Threat Report H1 2013," F-Secure, 2013, p. 11, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[32] "Security Threat Report 2014," Sophos, 2013, p. 12, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[33] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 13, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[34] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 32, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[35] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 32, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[36] "Threat Report H1 2013," F-Secure, 2013, p. 11, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[37] "Security Threat Report 2014," Sophos, 2013, p. 12, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[38] "Threat Report H1 2013," F-Secure, 2013, p. 34, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[39] "Security Threat Report 2014," Sophos, 2013, p. 15, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[40] "A Year of Spam: The Notable Trends of 2013," TrendLabs, 7 January 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/
[41] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 59, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[42] "Threat Report H1 2013," F-Secure, 2013, p. 35, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[43] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 20, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[44] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 21, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[45] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 5, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf

[46] "Security Threat Report 2014," Sophos, 2013, p. 6, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[47] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 20, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[48] "Security Threat Report 2014," Sophos, 2013, p. 4, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[49] "Security Threat Report 2014," Sophos, 2013, p. 5, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[50] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 21, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[51] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 58, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[52] "Security Threat Report 2014," Sophos, 2013, p. 6, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[53] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 19, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[54] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 20, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[55] "Security Threat Report 2014," Sophos, 2013, p. 5, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[56] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 58, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[57] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 45, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[58] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 33, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[59] "Threat Report H1 2013," F-Secure, 2013, pp. 14, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[60] "Security Threat Report 2014," Sophos, 2013, p. 8, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[61] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 33, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[62] "Threat Report H1 2013," F-Secure, 2013, pp. 21, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[63] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 37, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[64] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 5 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[65] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, p. 14 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[66] "Threat Report H1 2013," F-Secure, 2013, pp. 8, 19, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[67] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[68] "Threat Report H1 2013," F-Secure, 2013, pp. 14, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[69] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 6 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf

[70] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 23, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[71] "Security Threat Report 2014," Sophos, 2013, pp. 7-8, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[72] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, pp. 11-12, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[73] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 11, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[74] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 33, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[75] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 12, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[76] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 18, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[77] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[78] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 17, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[79] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[80] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, pp. 3, 19, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[81] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 24, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[82] "Threat Report H1 2013," F-Secure, 2013, pp. 6, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[83] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 55, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[84] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 60, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[85] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[86] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 9, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[87] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 55, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[88] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[89] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 51, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[90] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 24, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[91] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 24, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[92] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 79, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[93] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 32, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[94] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 7, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[95] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 79, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[96] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 7, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[97] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 5, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[98] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 39, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
[99] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 17, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[100] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 28, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[101] "Symantec Intelligence Report December 2013," Symantec, December 2013, p. 17, https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf
[102] "Threat Report H1 2013," F-Secure, 2013, pp. 7, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[103] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 17, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[104] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 17, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[105] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 30, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[106] "Threat Report H1 2013," F-Secure, 2013, pp. 7, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[107] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 37, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[108] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[109] "Security Threat Report 2014," Sophos, 2013, p. 16, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[110] "Threat Report H1 2013," F-Secure, 2013, pp. 34, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[111] "Security Threat Report 2014," Sophos, 2013, p. 12, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[112] "Threat Report H1 2013," F-Secure, 2013, pp. 36, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[113] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 30, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[114] "Security Threat Report 2014," Sophos, 2013, p. 13, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[115] "Threat Report H1 2013," F-Secure, 2013, pp. 39, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[116] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 37, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[117] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 28, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[118] "Symantec Intelligence Report December 2013," Symantec, December 2013, p. 17, https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf
[119] "Security Threat Report 2014," Sophos, 2013, p. 17, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[120] "Threat Report H1 2013," F-Secure, 2013, pp. 35, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[121] "Kaspersky Security Bulletin 2013," Kaspersky Lab, 10 December 2013, p. 17, http://media.kaspersky.com/pdf/KSB_2013_EN.pdf
[122] "Security Threat Report 2014," Sophos, 2013, p. 22, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[123] "A Year of Spam: The Notable Trends of 2013," TrendLabs, 7 January 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/
[124] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, pp. 26-27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[125] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, pp. 3, 19, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[126] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p.3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[127] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 1 October 2013, p.3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[128] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 26-27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[129] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, p. 27, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[130] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 25 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[131] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 26-27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[132] "Cisco 2014 Annual Security Report," Cisco, 16 January 2014, p. 24, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[133] "Security Threat Report 2014," Sophos, 2013, p. 22, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[134] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, p.27, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[135] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, p.27, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[136] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 26-27, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[137] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 25-26, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[138] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, p. 25 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[139] *2014 State of Endpoint Risk,* Ponemon Institute, p. 8, https://www.lumension.com/2013
[140] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, p. 3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[141] "McAfee Threats Report: Secibd Quarter 2013," McAfee Labs, 2013, McAfee Labs, p. 3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf

[142] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, pp. 3, 25, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[143] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, pp. 25-26, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[144] "Threat Report H1 2013," F-Secure, 2013, pp. 44-46, http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf
[145] Steve Ragan, "The 8 Hottest Security Stories of 2013, *CSO*," 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[146] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 6, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[147] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, pp. 9-12, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[148] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 6, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[149] Scott Simkin, "Examining the Worst Data Breaches of 2013: Part 2," *Palo Alto,* 13 December 2013, http://researchcenter.paloaltonetworks.com/2013/12/examining-worst-data-breaches-2013-part-2/
[150] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, pp. 9-12, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[151] "Quarterly Report PandaLabs July-September 2013," Panda Labs, 26 November 2013, p. 6, http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q3-2013/
[152] Scott Simkin, "Examining the Worst Data Breaches of 2013: Part 2," *Palo Alto,* 13 December 2013, http://researchcenter.paloaltonetworks.com/2013/12/examining-worst-data-breaches-2013-part-2/
[153] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[154] Scott Simkin, "Examining the Worst Data Breaches of 2013: Part 2," *Palo Alto,* 13 December 2013, http://researchcenter.paloaltonetworks.com/2013/12/examining-worst-data-breaches-2013-part-2/
[155] "McAfee Threats Report: First Quarter 2013," McAfee Labs, 2013, p. 3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf
[156] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, McAfee Labs, p. 35, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[157] "McAfee Threats Report: Third Quarter 2013," McAfee Labs, 2013, McAfee Labs, pp. 9-12, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf
[158] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[159] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 3, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[160] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[161] "McAfee Threats Report: Second Quarter 2013," McAfee Labs, 2013, p. 33, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf
[162] William Jackson, "Scoring Cybersecurity Hits and Misses for 2013," *GCN,* 20 December 2013, http://gcn.com/blogs/cybereye/2013/12/hits-and-misses.aspx
[163] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 31, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[164] "Security Threat Report 2014," Sophos, 2013, p. 18, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[165] "2014 State of Endpoint Risk," Ponemon Institute, December 2013, p. 7, https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf
[166] "Worldwide Infrastructure Security Report Volume IX," Arbor Networks, 2013, p. 34, http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf

[167] "ENISA Threat Landscape 2013," European Union Agency for Network and Information Security, 11 December 2013, p. 31, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[168] "Security Threat Report 2014," Sophos, 2013, p. 18, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
[169] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[170] "Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends," Open Security Foundation, February 2014, https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf
[171] "2013 Data Breach Stats," Identity Theft Resource Center, 1 January 2014, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf
.[172] "2013 Data Breach Stats," Identity Theft Resource Center, 1 January 2014, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf
[173] "2013 Data Breach Stats," Identity Theft Resource Center, 1 January 2014, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf
[174] "Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends," Open Security Foundation, February 2014, https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf
[175] Scott Simkin, "Examining the Worst Data Breaches of 2013: Part 2," *Palo Alto,* 13 December 2013, http://researchcenter.paloaltonetworks.com/2013/12/examining-worst-data-breaches-2013-part-2/
[176] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[177] Steve Ragan, "The 8 Hottest Security Stories of 2013," *CSO*, 18 December 2013, http://www.csoonline.com/article/744850/the-8-hottest-security-stories-of-2013
[178] "Data Breach QuickView: An Executive's Guide to 2013 Data Breach Trends," Open Security Foundation, February 2014, https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf