Hamza Saleem* and Muhammad Naveed

SoK: Anatomy of Data Breaches

Abstract: We systematize the knowledge on data breaches into concise step-by-step breach workflows and use them to describe the breach methods. We present the most plausible workflows for 10 famous data breaches. We use information from a variety of sources to develop our breach workflows, however, we emphasize that for many data breaches, information about crucial steps was absent. We researched such steps to develop complete breach workflows; as such, our workflows provide descriptions of data breaches that were previously unavailable. For generalizability, we present a general workflow of 50 data breaches from 2015. Based on our data breach analysis, we develop requirements that organizations need to meet to thwart data breaches. We describe what requirements are met by existing security technologies and propose future research directions to thwart data breaches.

Keywords: Data Breach Analysis, Data Privacy, Security Defenses

DOI 10.2478/popets-2020-0067
Received 2020-02-29; revised 2020-06-15; accepted 2020-06-16.

1 Introduction

Data breaches are among the most important computer security and privacy problems. It is routine for the attackers to steal millions or even billions of records. Despite being such a massive problem, data breaches are considered outcomes of other security issues, such as human error and software vulnerabilities. In addition to severe security consequences, data breaches pose dire privacy issues; most data breaches reveal sensitive data to ill-intentioned people who sell it on the dark web and could release it publicly. For example, the attackers publicly posted a subset of the data breached from Ashley Madison, which led to suicides and divorces [1–5]. Yet data breaches have not received due attention from the security and privacy community. In this paper, we systematically study breach workflows, breach methods, and prevention techniques, which we believe will help the reader develop an in-depth understanding of the data breach problem and pave the way for future research on the topic.

We systematize the knowledge on data breaches into concise step-by-step, end-to-end workflows to explain the breach methods. We propose a systematic method to study data breaches and use it to develop the most plausible end-to-end breach workflows from incomplete information. We systematize the knowledge from dozens of sources to develop concise data breach workflows for 10 famous data breaches. To gauge the generalizability of our 10 breach workflows, we also studied a sampling of 50 data breaches from 2015 and found the attack techniques similar to our 10 breach workflows. Based on our breach workflows, we present common breach methods used by the attackers to breach data.

To understand the capabilities of existing security technologies, we developed a set of requirements for different entities of an organization, which need to be met to prevent data breaches. We found that it is extremely challenging to satisfy these requirements, which explains why organizations often suffer from data breaches. While existing security technologies can make the attacker's job harder, they cannot meet many of the requirements needed to prevent data breaches. Using our requirements list, we also present future research directions that could help address some of the requirements that existing technologies cannot address.

Related Work. The current work on data breaches mostly consists of technical reports and white-papers by government bodies and security solution providers. The Microsoft report [6] presents 4 phases of a security breach and briefly discusses 4 anonymized security breaches. The MWR InfoSecurity report [7] presents different phases of a data breach and mitigation strategies. The Symantec report [8] describes common ways in which organizations are breached based on various threat actors and discusses counter-measures. Rashid, et al., provide a model capturing different phases of a data breach [9] and present breach detection and mitigation strategies. Verizon has been publishing their "Verizon Breach Investigation Report" annually since 2008 that provides insights about the past cyber-security incidents. The report highlights common attack patterns, threat actors, attacker motivations, breach discovery methods and timelines, and recent malware trends. The

***Corresponding Author: Hamza Saleem:** University of Southern California, E-mail: hsaleem@usc.edu
Muhammad Naveed: University of Southern California, E-mail: mnaveed@usc.edu

data for the report comes from real-world breaches either investigated by Verizon or by one of the contributing organizations. Verizon also publishes data breach case studies in their "Data Breach Digest". Trustwave publishes its annual Global Security Report [10] that highlights top security threats and attack trends.

Liu, et al., propose a framework to predict the risk of a security breach by using the externally observable features of an organization's network [11]. Bilge, et al., [12] propose RiskTeller, a framework that uses binary file appearance logs to predict the risk of a machine within an organization getting compromised. Gatzlaff, et al., [13] study the effect of data privacy breaches on the company's stock market value. Ponemon Institute publishes its Cost of Data Breach Report that aims to quantify the financial impact of data breaches [14].

2 Systematic Analysis Method

We use the following analysis method to develop end-to-end breach workflows from incomplete information. This is a general method and could be used to study other data breaches.

2.1 Information Analysis

We thoroughly studied all publicly available relevant information to develop breach workflows including investigation reports from victim organizations, government agencies, and security solution providers. We additionally used online articles published by various news, magazines, and blog websites, such as NY Times, Wired, Krebs on security, etc. because in several cases, the victim organizations did not publish the breach investigation reports. The online news articles and blogs we used had news briefings and interviews of the victims, security agency officials [15], security solution provider company management [16], and in some cases even cybercriminals [17]. Moreover, in some cases, the authors of these blogs also performed their independent investigations that were useful in understanding the incident [18]. We list information sources with each workflow. The complete list of such online articles, along-with their authors and websites, is provided in Table 5 in Appendix C.

To gauge the accuracy, reliability, and timeliness of these resources, we present various metrics related to the websites and authors of these articles developed using standard methods [19–22]. Table 4 in Appendix C provides these metrics. We did not use any website or article that has been previously reported as a hoax. We also discarded two relevant articles in cases where we could not verify the author's identity.

2.2 Malware Analysis

The publicly available information on data breaches only mentions the name of malware used in the breach. We studied all the malware in detail, found out their capabilities, and how attackers could have used the malware. We use results from our malware analysis to complete the information that was missing from the publicly available information. We studied Citadel Trojan and BlackPOS malware for the Target breach, Sakula and Mivast malware for Anthem breach, and PlugX malware for OPM breach. For example, the public information on Anthem breach only mentions the names of malware used: Sakula and Mivast. We studied these malware families in detail to understand what functionalities they provide and how each of the malware might have been used by the attacker to steal credentials and escalate privileges. From this analysis, we deduce that the attacker used the credential dumping feature of Mivast to steal credentials to connect with other hosts on the network and Sakula to bypass Windows User Account Control (UAC) to gain elevated privileges.

2.3 Attacker Group Analysis

In some cases, the public information mentions the name of the attacker group behind the data breach. We studied that group's attack methods and previous data breaches to fill the gaps in the breach workflows. For example, in the case of the RUAG breach, the initial attack vector is unknown but while studying the attack methods of the Waterbug attacker group behind the breach, we found that at the time of the breach, the group was widely using watering hole attacks [23] where the attacker infects the websites that the victim is likely to visit and then targets specific users e.g., within a specific IP address range. Therefore, we deduced that the attacker used the watering hole attack as the initial attack vector in the RUAG breach.

2.4 Vulnerable Software/Protocol Analysis

For some data breaches, the public information provides very little detail about the vulnerability the attackers exploited. We studied the vulnerable software in detail to provide a detailed explanation of how the attackers could have exploited the software. For example, in Sony data breach, the public information only mentions that the worm used a brute-force authentication attack to propagate via Windows SMB shares but provides no detail about how the attackers brute-forced the password. We studied the SMB protocol in detail to understand its authentication method and how the password could be brute-forced, to provide a plausible way the attacker may have performed this attack.

2.5 Inferring from other breaches

We also used public information from other data breach incidents to fill the gaps in the breach workflows. For example, in the case of the Yahoo breach, the public information only mentions that attackers escalated privileges, but does not explain how. We studied privilege escalation techniques commonly used in data breaches, such as pass-the-hash attack and use of keyloggers, to understand how exactly attackers could have escalated the privileges. We also studied other breach incidents of the same attacker groups, as mentioned previously, to fill the gaps in the breach workflows.

3 Case Studies

We thoroughly studied 10 famous data breaches and detail the most plausible step-by-step explanation of how the attackers compromised the organizations and exfiltrated data. We analyzed 10–20 highest risk score breaches for each year from 2013–2017 using breachlevelindex.com risk score and selected the 10 breaches that had the most information available to infer the complete breach workflow. We excluded the 2018–2019 data breaches due to the lack of publicly available information. Table 1 presents the number of records stolen and their type, breach discovery time, attacker type, and techniques used for all 10 breaches. Based on the attack methods used, Table 1 also shows which of the existing security technologies would have helped the organization in thwarting the breach. Below we provide detailed step-by-step workflows for the 10 data breaches.

3.1 Sony Pictures Data Breach, 2014

In 2014, the Lazarus group, a state-sponsored threat group, breached Sony Pictures [24]. They exfiltrated and published unreleased movies, personally identifiable information of Sony employees and their dependents, emails showing behind-the-scenes politics on titles, financial documents, Sony's internal credentials, such as credentials of the Sony's FTP server, and external credentials, such as Sony's YouTube, The Los Angeles Times, and The New York Times accounts. The data were released through torrents and file hosting services, such as MEGA and Rapidgator, with Sony's compromised servers used to upload the data [25]. WikiLeaks later published a searchable database [26] of the leaked data. The attacker also wiped the company machines.

Information sources. We used Novetta [24], DeSimone, et al. [27], and SANS institute investigation [28] reports. The data analytics firm, Novetta, investigated the Sony's breach, in collaboration with Kaspersky Lab, Symantec, AlienVault, Trend Micro, Invincea, PunchCyber, Carbon Black, RiskIQ, Volexity, and ThreatConnect; and published the report [24]. We also used news articles from The New York Times [29], The Intercept [15], ComputerWorld [16], ZDNet [30], and a blog article by Risk Based Security [25]. FBI as well as FireEye investigated the breach but did not publish the reports.

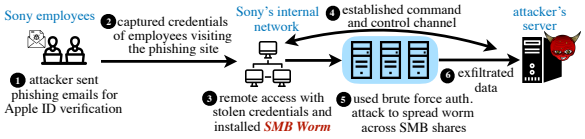

Fig. 1. Sony Pictures Data Breach, 2014

Breach Workflow.

- The attacker found Sony's employees with high network privileges through LinkedIn and sent them spearphishing emails with a link to a clone of the Apple ID verification website. They harvested Apple ID credentials hoping that the same or similar passwords would lead them to remotely access Sony's network. The reuse of passwords equipped the attacker with remote access [16].
- Equipped with remote access, the attacker installed a custom-built worm tool on the infected hosts to exploit vulnerabilities in the Microsoft Server Message Block (SMB) protocol [31]. SMB protocol allows sharing files, printers, and other resources on a network. We describe the important details of the worm and defer a detailed description to Appendix A.1. The worm on the compromised hosts connected to other hosts by brute-forcing SMB authentication password. We studied the Microsoft SMB protocol in detail to understand how the password could be brute-forced [32–36]. The Microsoft SMB protocol supports three authentication protocols to connect to other hosts on the network: (a) LAN Manager (b) New Technology LAN Manager (NTLM) and (c) Kerberos. Microsoft introduced NTLM to replace the weaker LAN Manager protocol but kept on supporting LAN Manager for backward compatibility. LAN Manager, supported by Windows XP and earlier versions, uses a weak hashing algorithm, LM hash, which is crackable in hours using brute-force and in seconds using rainbow tables. LAN Manager has several other weaknesses, such as passwords are not case sensitive, password characters are limited to a subset of 95 characters, password length is limited to 14 characters, and the 14 password characters are divided into two parts and the hashes for each part with 7 characters is calculated separately which makes it exponentially easier to crack. Moreover, for NTLM generated hashes Windows does not employ salting and can thus be cracked using rainbow tables [37]. Kerberos is a network authentication protocol that uses *Kerberos tickets* (proof of identity)

	Data Stolen			Discovery				Techniques										Hiding Malicious Activities																Security Technology Hinders the Breach?													
Organization	Records Stolen	Data Records Type	Exfiltrated Data Availability	Attacker Type	Discovery Time	Discovery Method	Warnings Ignored	Use Data from Past Breaches	Target Third-Party	Spear Phishing	Watering Hole Attacks	Escalate Privileges	Stolen/Default/Weak Credentials	Exploit Password Reuse	Exploit Software Vulnerabilities	Use Open-Source Vulnerability Scanners	Use DDOS Attack for Diversion	Malware Posing as Legitimate Software	Install Malware as System Service	Inject Payload in Benign Processes	Hide Activity During Rush Hours	Obfuscate C&C Server Communication	Obfuscated Malware Payload	Carefully Crafted Domain Names	Obfuscate Data During Exfiltration	Exfiltrate Data Over Extended Period	Clear Activity Logs	Firewalls	Intrusion Detection System	Intrusion Prevention System	Data Leakage Prevention System	Anti-malware	Vulnerability and Patch Management	Security Testing Tools	Multi-factor Authenticators	Threat Intelligence Systems	Data Breach Alert Services	Third-party Risk Assessment Services	Staff Training and Education
Sony	×	■ ☒ □	●	●	○	○				✓			✓	✓	✓							✓	✓	✓	✓		✓								✓					✓
Target	◕	■☒	◑	○	○	●	✓	◑	✓	✓		✓	✓		✓	✓			✓		✓							✓	✓	✓	✓	✓			✓			✓	✓
Yahoo	●	■	◑	●	●	●				✓		✓	✓		×												✓		✓	✓	✓				✓				✓
Anthem	◑	■	○	●	○	○			✓	✓		✓	✓		✓			✓	✓	✓			✓	✓					✓	✓	✓	✓							✓
OPM	◑	■ ☒ ⊟	○	●	◕	○		○	✓	×		✓	✓		✓			✓	✓			✓		✓	✓			✓	✓	✓		✓		✓			✓	
RUAG	×	×	○	●	◔	○			✓		✓	✓			✓	✓		✓		✓		✓			✓	✓			✓	✓		✓							✓
NSA	×	⊞	○	◑	○	●																			✓	✓	✓												
Carphone	◔	■☒	○	○	○	○							✓		✓	✓	✓														✓		✓	✓		✓			
Equifax	◕	■☒	○	○	◔	○	✓					✓	✓		✓										✓			✓	✓	✓		✓	✓		✓			
Zomato	◑	■	◑	○	○	●		●					✓	✓	✓																✓			✓		✓		✓

Table 1. Summary of 10 Data Breach Case Studies

Records Stolen
○ Less than 1 million
◔ 1-10 million
◑ 10-100 million
◕ 100-500 million
● More than 500 million
■ Organization/ employees data stolen
■ Customer data stolen
■ Data includes both customer and employee data

Spear Phishing
✓ Spear phishing emails
■ Spear phishing websites

Data Records Type
■ Personally Identifiable Information
☒ Financial Information
⊟ Protected Health Records
□ Intellectual Property
⊞ Other

Discovery Time
○ Within 3 months
◔ 3-6 months
◕ 6 months-1 year
● 1-2 years

Stolen/Weak/Default Credentials
■ Steal Admin Credentials

Exfiltrated Data Availability
○ Not available online
◑ Sold on dark web
● Released publicly

Discovery Method
○ Internal (Employees or security defenses detected breach)
● External(Media, Banks or FBI informed the company)

Exploit Software Vulnerabilities
■ Unpatched software

Blank cell represents not applicable

Attacker Type
○ Cyber-criminals
◑ Malicious Insider
● State-sponsored

Use Data From Past Breaches
○ Reconnaissance data
◑ Malware source code
● Leaked credentials

× Data unavailable

and provides better security than NTLM. With one-third of businesses running Windows XP in 2019 [38], its safe to assume that many machines at the time of the attack ran old operating systems that supported LAN Manager authentication for SMB connection. The SMB worm was thus able to brute force the password easily and connect with other network hosts through SMB protocol. The worm spread across the network by replicating itself on the newly connected hosts [31].

• The attacker used the listening implant and lightweight backdoor module of the worm to connect with infected hosts and perform reconnaissance [31].

• The attacker used the worm to exfiltrate large amounts of confidential data to a remote attacker-controlled server. They also used the infected hosts to upload this data to file hosting services, such as MEGA and Rapidgator, etc. [25].

• The attacker then used the destructive hard drive tool and the target cleaning tool to wipe the victim host hard drives to a point beyond recovery and over-write Master Boot Record to make the hosts unbootable. The hosts displayed a message informing employees about the attack [27].

3.2 Target Data Breach, 2013

In 2013, an attacker breached the personal information of 70 million and financial information of 40 million Target customers. The Justice Department alerted Target [39] after the external fraud analysts reported the breach due to a huge increase in the number of stolen cards on the dark web marketplaces from nearly every bank with a common point of purchase: Target [18, 40–42].

Information sources. We used the investigation reports by Aorato Labs [43], Dell SecureWorks Counter Threat Unit [44], and ThreatScape [45]; the testimony of Target's then Executive Vice President, John Mulligan, before the Senate Committee on Commerce, Science, and Transportation [39]; and blog articles by Krebs On Security [46–48], Symantec [49], Malware Bytes [50], InfoSec Institute [51], The Hacker News [52], and Security Intelligence [53]. FBI, Department of Justice, Mandiant, and Verizon investigations were not published.

Breach Workflow.

• The attacker sent phishing emails to Target's HVAC vendor, Fazio Mechanical, infecting an employee with Citadel Trojan. The malware uses web-injects that mod-

ify HTML of targeted websites on the victim's computer to include fake forms asking for personal information and credentials in the context of legitimate websites, captures screenshots, and records screen to steal credentials [49, 50]. Using this malware, the attacker stole the third-party, Fazio Mechanical, employee credentials for Target's vendor-specific web services: Ariba, an electronic billing service, and Partners Online, a project management portal.

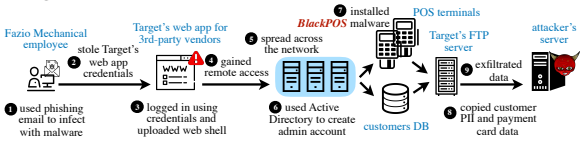

Fig. 2. Target Data Breach, 2013

- The attacker used the stolen credentials to log into the web portal used by Target's third-party vendors. They uploaded a PHP web-shell using the upload functionality meant to upload documents, such as invoices, due to the lack of security checks to validate file types. The web-shell gave the attacker remote access to Target's web server [43].
- The attacker equipped with remote access used Microsoft Active Directory Domain Services [54] to locate critical targets, such as database servers, and point of sale (POS) terminals.
- The attacker used pass-the-hash attack [55], a privilege escalation attack, to connect with network hosts without a password [43]. The attack works because the systems using NTLM [56] or LM authentication are authenticated using password hashes instead of the actual password. The attacker used tools, such as Mimikatz [57], to dump the password hash from the memory and used it to authenticate with other network hosts. Windows generates this hash when a user logs in and it resides in memory for single sign-on (SSO) feature to connect to network hosts and services; the hash only changes when the user resets his password.
- With access to some hosts, the attacker discovered a host with an administrator account, retrieved the administrator's password hash, and used it to authenticate with Active Directory and create another administrator account [43] with the username "best1_user" to imitate the administrator account created by BMC's Bladelogic, a legitimate software [47] used by Target. The attacker used this administrator account to propagate to target hosts such as database server and point of sale (POS) terminals and run remote processes on them using Windows utilities, such as Microsoft's PsExec Utility [58] and Remote Desktop Tool. Although the attacker had access to the password hash of an administrator account, they created this new account to achieve persistence in case the password hash of the previously compromised account changes, and to run remote processes using Windows utilities that require the explicit use of password instead of the password hash.
- Once the attacker had access to the database server containing the personally identifiable information (PII) of Target's 70 million customers, they used Microsoft's SQL tools, such as osql, isql, and bcp to retrieve the data. The database did not have customers' payment card information due to Target's compliance with Payment Card Industry Data Security Standard (PCI-DSS); Section 3.2 of PCI-DSS recommends the organizations not to store any payment card data. Target's security systems detected intruder activity, however, it was ignored by the security team [39].
- The attacker installed a customized version of BlackPOS malware on Target's POS terminals. BlackPOS [45, 48] is a RAM-scraping malware used to retrieve payment card data from the memory of the process interacting with the card reader. The data resides unencrypted in the RAM for a short time before it is encrypted for sending over the network. The malware obtains the payment data during this time and stores it in a local file. We defer further details of the malware to Appendix A.2.
- The attacker created a network file share on an FTP-enabled host inside the network and copied the local files from the database server and the POS terminals to the file share between 10 am and 6 pm to hide the activity during rush hours. The attacker used Windows FTP client to exfiltrate about 11GB [53] of this stolen data to 3 attacker-controlled remote servers. The data consisted of 70 million user records with names, mailing addresses, phone numbers and/or email addresses of the customers, and 40 million payment card records containing names, card numbers, expiration dates, and card verification values (CVV).

3.3 Yahoo Data Breach, 2014

In 2014, state-sponsored actors breached Yahoo stealing account information of over 500 million users [59]. The attacker generated forged authentication cookies to gain access to email accounts of various Russian journalists, the United States and Russian government officials, and private-sector employees. They also diverted Yahoo's search engine traffic to certain websites for monetary profit. They later sold the stolen accounts on a dark web marketplace [17].

Information sources. We used the Yahoo incident report [60] published by the US Department of Justice as well as articles by The New York Times [59, 61], CSO

Online [62], Motherboard Vice [17], Ars Technica [63], and eSecurity Planet [64] to create a probable workflow of the data breach incident. FBI investigated the incident and disclosed details about the attackers' origin and their methods [61], which we used. However, the FBI did not publish the investigation report.

Breach Workflow.

• The attacker sent spear-phishing emails to Yahoo employees to trick them into visiting phishing sites and disclosing credentials [63]. The exact details about the phishing sites are unknown. The attacker used the stolen credentials to remotely access Yahoo's network and installed a backdoor for persistent access.

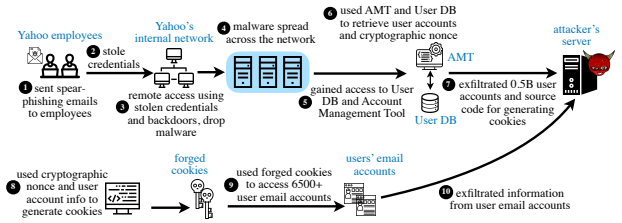

Fig. 3. Yahoo 2014 Data Breach

• The attacker used privilege escalation techniques to authenticate with other hosts and spread across the network. While the exact techniques used are unknown, pass-the-hash [55] attack and using key-loggers to steal credentials are among the common techniques [65, 66].

• The attacker discovered Yahoo's user database and an account management tool used to access and edit the database. The database contained names, email addresses, dates of births, security questions and answers, password recovery emails, hashed passwords, and cryptographic nonces unique to each account [62]. The attacker exfiltrated a backup copy of the database containing over 500 million records using File Transfer Protocol.

• They used the account management tool to identify the accounts of various Russian journalists, United States and Russian government officials, and private-sector employees [64] by using their password recovery email address from the user database; the account management tool did not allow searching the database using victim names. In some cases, the email domain of non-Yahoo account recovery email addresses also gave them hint about the user's organization [62].

• The majority of passwords in the database were hashed using bcrypt [67], a slow password hashing algorithm based on Blowfish cipher that protects against brute-force and rainbow table attacks. The attacker used the cryptographic nonce associated with each account in conjunction with a script available on a Yahoo server to generate web authentication cookies that allowed them to access more than 6,500 victim email accounts without the need for actual passwords [64]. They used this access to steal confidential data from the email accounts including credit and gift card numbers, send spam emails to user contacts, gain information about other accounts of the user, such as user's Gmail account, and use spear-phishing to gain access to those accounts.

• To gain profit, the attacker also re-directed Yahoo's search engine traffic to an online pharmacy that paid for the traffic [61]. The attacker used log cleaning tools to clear event logs to avoid detection.

3.4 Anthem Data Breach, 2014

Anthem is an American health insurance company. In 2014, a state-sponsored espionage group known as Deep Panda or Black Vine [68] targeted Anthem employees by tricking them into installing malware masquerading as a legitimate VPN software. The attacker gained remote access to the company's data warehouse and exfiltrated 78.8 million customer records.

Information sources. We used the investigation report of the California Department of Insurance [69]; the investigation was conducted by CrowdStrike and Alvarez & Marsal Insurance and Risk Advisory Services. We used the Symantec report [70] that details how the cyber-espionage group behind the Anthem breach operates. We also used articles by MITRE ATT&CK Framework [68, 71], New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) [72], and Symantec [73] to learn about malware used in the breach.

Breach Workflow.

• The attacker sent spear-phishing emails to employees at Amerigroup, Anthem's subsidiary company, with a link to a clone of the official Anthem website, containing instructions about installing VPN software, Citrix and Juniper VPN, used by the company. Before 2014, Anthem was known as Wellpoint Inc.; the attacker registered the domain *we11point.com* to host the phishing site, replacing the two *l* in wellpoint with the numeric character 1 to appear legitimate. The site hosted malware, called Sakula, masquerading as the VPN software.

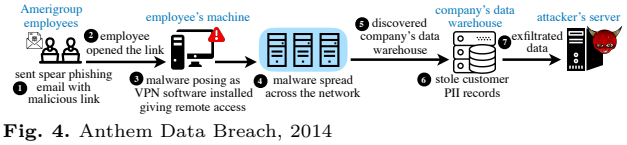

Fig. 4. Anthem Data Breach, 2014

• The employee installed Sakula [71, 72] malware posing as a VPN software, equipping the attacker with remote access to the host. Sakula is a remote access trojan that can execute arbitrary operating system commands, download and execute the payload, and upload files. We defer details of the malware to Appendix A.3.

The attacker also used Mivast backdoor that can dump NTLM password information, run remote commands, and download and execute files. [70, 73].

• We conjecture that the attacker used the credential dumping feature of Mivast malware to steal credentials to connect with other hosts on the network [74] and then used Sakula malware to bypass Windows User Account Control (UAC) to gain elevated privileges [75]. Windows UAC allows the programs to elevate privileges to the administrator level by prompting the user for confirmation. If the UAC protection level is set to other than the highest level, some Windows programs are allowed to elevate their privileges through UAC without prompting for permission. Malware like Sakula can use this weakness to inject themselves into a trusted Windows process and gain elevated privileges without prompting the user for permission. The attacker thus spread across the network infecting more than 50 user accounts and 90 hosts. The command and control server domain names were carefully selected to avoid suspicion, e.g., *extcitrix.we11point.com* [69].

• The attacker discovered the company's enterprise data warehouse containing PII of customers including names, email addresses, medical IDs, social security numbers, and employment information and exfiltrated 78.8 million user records.

3.5 OPM Data Breach, 2014

The attacker targeted the United States Office of Personnel Management (OPM) in two separate but linked attacks in 2014. In the first attack, the attacker stole OPM's network specification documents that they used to understand the network structure and launch another attack. In the second attack, the attacker stole the credentials of a third-party company, KeyPoint: OPM's background investigation contractor, employee to gain access and exfiltrated background investigation data of federal employees.

Information sources. We used the breach investigation report by The Committee on Oversight and Government Reform [76] that provides a detailed account of the incident and the blog article by Wired [77]. We also used the article by The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) that provides information about PlugX malware [78] used in the data breach.

Breach Workflow.

• Network assessments conducted by the U.S. Computer Emergency Readiness Team identified two separate breaches at KeyPoint Government Solutions in 2014 [79]. Although the attack vector used in these breaches is unknown, the attacker, stole PII data of Dept. of Homeland Security employees and remote access credentials of a server at The United States Office of Personnel Management(OPM) [76]. OPM had issued credentials to KeyPoint employees to access a server housing federal employees data, to carry out background investigation tasks.

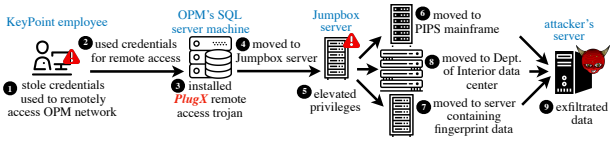

Fig. 5. United States Office of Personnel Management (OPM) Data Breach, 2014

• The attacker accessed OPM's server through a VPN session with the stolen credentials and installed PlugX malware that masqueraded as McAfee Antivirus software [78]. PlugX [78] is a modular remote access trojan used to run arbitrary operating system commands, log keystrokes, capture screenshots and video of user activity, enumerate network resources, and modify files. We defer further details of PlugX to Appendix A.4. The malware command and control server used domain names: *opmlearning.org, opmsecurity.org, wdc-news-post.com*, to avoid suspicion if network traffic was being analyzed.

• The attacker used the key-logging capabilities of the malware to steal credentials and spread across the network gaining access to a jumpbox server: an administrative server used to manage devices in separate network security zones. A security zone is a portion of the network with a specific access control policy implemented by firewalls.

• The attacker used the privileged access on the jumpbox server to connect to the portions of the network otherwise firewalled off from the normal network. The attacker gained access to the Personnel Investigations Processing System (PIPS) used by the OPM to process and store the background investigation data of government employees [76]. The data included government employees Standard Form 86, a 127-page security clearance questionnaire containing sensitive data, such as financial history, past substance abuse, and mental health care information [77]. The attacker also gained access to the employee fingerprint data which can be used to impersonate federal employees to access locations protected by fingerprint authentication.

• The attacker further used their presence on the jumpbox server to access the United States Department of Interior data center and stole OPM's personnel PII records.

• The attacker exfiltrated 21.5 million employee background investigation records, 5.6 million fingerprint records, and 4 million personnel PII records in encrypted compressed files to avoid detection [76].

3.6 RUAG Data Breach, 2014-2015

In 2014, a Russian threat group, Turla, also known as Waterbug, targeted RUAG, a Swiss defense contractor, using watering hole attacks [23, 80]. Using Turla malware and publicly available vulnerability exploitation tools, the attacker exfiltrated 23GB of confidential data over an extended period to avoid detection.

Information sources. We used the breach investigation report by The Computer Emergency Response Team (GovCERT) of the Swiss government [81] and a Symantec report [80] detailing how the cyber-espionage group behind the breach operates.

Breach Workflow.

• The attacker used a watering hole website for fingerprinting i.e. to obtain information about the user's IP address, browser version, browser plugins, and operating system. The watering hole website then redirected the company employees to a malicious website using URL shorteners and Javascript code appearing as Google Analytics scripts.

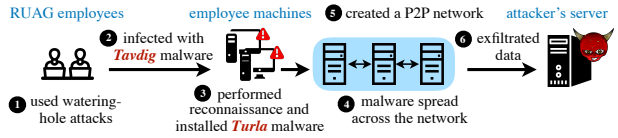

Fig. 6. RUAG Data Breach, 2014-2015

• The attacker used the malicious website to trick the users into downloading Tavdig malware posing as legitimate software, such as Java Installer and Microsoft Security Essentials. The attacker used Tavdig [80], a reconnaissance malware, to collect information about the host operating system and services, login credentials, network, and domain-specific information. The malware injects payload in already running processes [82], such as web browsers, and email clients to thwart firewalls filtering traffic based on the originating process.

• With reconnaissance data on hand, the attacker installed Turla malware [80] on selected hosts. The malware communicates with the command and control server to receive tasks and uses similar process injection techniques described before to run the malicious payload. The attacker used the Mimikatz tool to perform a series of pass-the-hash, pass-the-ticket, and Golden Ticket attacks to escalate privileges and spread across the network infecting other hosts. We detail the description of these attacks in Appendix B.1.

• The attacker created a peer to peer (P2P) network of infected hosts using Turla malware. The network consisted of worker and communication nodes where the worker nodes gathered data for exfiltration while the communication nodes communicated with the command and control servers to receive tasks. On communication nodes, the malware injected its payload in the web browser process and in worker nodes it injected payload in long-living processes, such as explore.exe. The worker and communication nodes communicated through named pipes using CAST128 encryption. The lateral movement took 8 months during which the attacker did not exfiltrate much data [81].

• The attacker exfiltrated 23GB of sensitive data through the communication nodes using HTTP Post requests over an extended period i.e. from September to December 2015. The type of data stolen is unknown as the company had no wiretap in place at the time of the attack.

3.7 NSA Breach, 2013

In 2013, Edward Snowden, a subcontractor for the Central Intelligence Agency (CIA) and the National Security Agency (NSA), exfiltrated and leaked highly classified NSA documents that revealed several global mass surveillance programs run by the NSA and the Five Eyes Intelligence Alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. Snowden, working as a systems administrator at NSA's Office of Information Sharing, used his privileged access to download and exfiltrate sensitive documents over an extended period to avoid detection.

Information sources. We used the autobiography 'Permanent Record' by Edward Snowden published in 2019 [83] and a report by the United States House Permanent Select Committee on Intelligence [84].

Breach Workflow.

• Snowden used his high privileges as a Microsoft SharePoint systems administrator to gain access to Heartbeat server in NSA's network. NSA used SharePoint for intranet document management. Heartbeat was an automated platform designed by Snowden himself in the past to scan and collect documents related to classified intelligence activities from the networks of NSA, CIA, FBI, the Joint Worldwide Intelligence Communications System, and the Department of Defense. Heartbeat presented these documents or news blogs known as 'readboards' to NSA officers based on their clearances, interests, and office affiliations. The Heartbeat server also stored a copy of each document.

• Snowden did not use the Heartbeat server directly to search for the documents of interest or copy them to an external storage device as the server logged all ac-

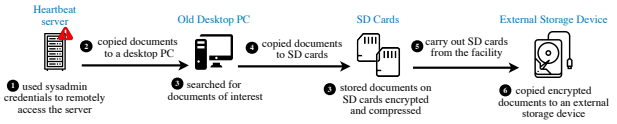

Fig. 7. NSA Data Breach, 2013

tivities and this could raise an alarm. Instead, Snowden connected an old desktop PC, which the agency had wiped and discarded previously when they upgraded to new "thin clients", light-weight machines that depend on their remote connection with the cloud servers to perform computation and data storage. Snowden then copied the documents from the Heartbeat server to the desktop machine, an action that could be justified by asserting that he was performing compatibility testing of Heartbeat with older operating systems.

- Snowden used the desktop PC to search for documents of interest. He then encrypted and copied these documents to mini- and micro-SD cards during his night-time shifts. Although the write-speed of SD-cards was slow taking about 8 hours to fill an SD-card once, it was easier to pass through security checkpoints with an SD-card without getting detected due to their small size.
- Snowden used a variety of methods to carry the SD-cards outside the building each day. He carried them in his socks, at the bottom of his pocket, in his cheek, so he could swallow it if he had to, and in the pried-off square of a Rubik's Cube. Before using Rubik's Cube to hide the SD-card, he would often walk past the guards solving the cube and also handed a few cubes to other employees to avoid raising any suspicion.
- Snowden carried the SD-cards to his home and moved all documents to a larger external storage device using his laptop. He would hide under a blanket to copy these documents due to the fear that the house might be wired by the FBI to detect any malicious activities. He encrypted the documents with multiple layers of encryption using different implementations so that even if one algorithm fails, others can keep the documents safe.

3.8 Carphone Warehouse Breach, 2015

Cyber-criminals breached Carphone Warehouse, a British mobile phone retailer, in 2015, stealing customers' personally identifiable information and historical payment transaction records. The attacker used an automated tool, Nikto Scanner, to discover a company web server running an outdated version of WordPress, which they exploited to gain remote access. The attacker found plain-text database credentials on the server, which they used to access the databases and exfiltrate the data.

Information sources. We used a monetary penalty [85] notice issued by The United Kingdom Information Commissioner's Office (ICO), a news article by The Register [86], and a blog post by Bank Info Security [87].

Breach Workflow.

- The attacker used Nikto scanner [88], an open-source penetration testing tool, to scan for websites running outdated web server software, and discovered the company's web server running a 6 years old version [87] of WordPress [89].

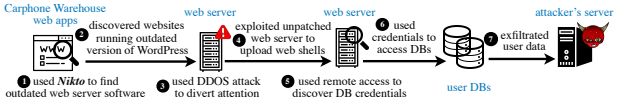

Fig. 8. Carphone Warehouse 2015 Data Breach

- The attacker launched a DDOS attack to divert the attention of the security response staff [86]. Although Carphone initially asserted that the attacker exploited vulnerable WordPress version for compromise, they later maintained that valid WordPress administrator credentials were used to login and install malicious plugins [85]. WordPress plugins are software to extend the functionality of a WordPress website. It is unknown how the attacker stole the administrator credentials.
- The malicious plugins had web shell functionality. A web shell is a script uploaded to a web server that runs in the context of the web server software giving the attacker remote access.
- The attacker used this access for reconnaissance, discovered plain-text database credentials, and used them to access the company's databases containing customer and employee records and historical payment transaction data.
- The attacker exfiltrated 3.3 million customer records containing the name, address, phone number, date of birth, and marital status; 1000 employee records containing the name, phone number, postcode, and car registration number; and historical payment transaction data of about 18,000 customers [85].

3.9 Equifax Data Breach, 2017

In 2017, cyber-criminals breached Equifax by exploiting a remote code execution vulnerability in their web app development framework. They spread across various hosts due to weak network segmentation and discovered an unencrypted data-store containing database credentials. They used these credentials to access the company databases and exfiltrated customers' personally identifiable information and payment card records.

Information sources. We used the breach investigation report [90] published by The United States Government Accountability Office (GAO).

Breach Workflow.

• The attacker exploited a remote code execution vulnerability (CVE-2017-5638) [91] in the Equifax dispute portal server running Apache Struts and gained remote access. The vulnerability allows an adversary to execute arbitrary commands using crafted Content-Type header value in HTTP request [92]. Before the attack, the United States Department of Homeland Security notified Equifax about the vulnerability after Apache disclosed it and released a patch. Equifax scanned their servers but the scan did not detect the vulnerable Equifax dispute portal server since they forgot to use the recursive flag and just scanned the root directory with the tool [90].

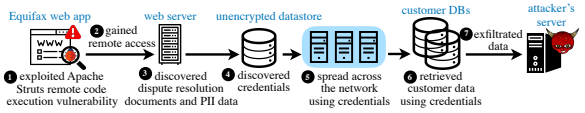

Fig. 9. Equifax 2017 Data Breach

• The attacker discovered 3 databases on the server containing dispute resolution documents and personally identifiable information of 182,000 customers. They also discovered an unencrypted data-store containing credentials to access other servers and company databases.
• The attacker used the stolen credentials to connect with other hosts and spread across a weakly segmented network.
• The attacker discovered 48 databases and used the stolen credentials to extract data in small increments to avoid suspicion; querying the databases 9,000 times over 76 days [90].
• The attacker exfiltrated 148 million customer records containing social security numbers, dates of births, home addresses, and driver's license numbers; 209,000 customers' credit card numbers; and 182,000 dispute resolution documents using standard encryption protocols [90]. Although the company had a traffic inspection tool, a misconfiguration allowed the encrypted traffic to pass without inspection [90].

3.10 Zomato Data Breach, 2017

In 2017, cyber-criminals accessed GitHub account of a developer at Zomato, a restaurant search and discovery service, using credentials leaked in a data breach at 000webhost. They analyzed Zomato's web app source code repository and discovered a vulnerability that gave them remote access to Zomato's server. The attacker stole a database containing 17 million customer account records. The company became aware of the breach when the attacker posted an ad for selling the data on a dark web marketplace.

Information sources. We used the blog posts by Zomato [93–95] that describe the incident.

Breach Workflow.

• The attacker targeted *000webhost*, a web hosting service, by exploiting a web app vulnerability in an old version of PHP. They stole a database containing emails and unencrypted passwords of about 13 million users which were leaked afterward.

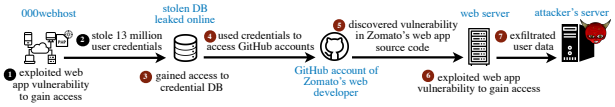

Fig. 10. Zomato 2017 Data Breach

• In a separate incident, an attacker used the leaked user credentials to log into other websites, hoping that some users might have reused their passwords, gaining access to a GitHub account of a Zomato employee because of the password reuse.
• The attacker used this access to review Zomato's web app source code repository and discovered a remote code execution vulnerability. The attacker exploited the vulnerability to gain remote access to Zomato's server.
• The attacker discovered a database containing names, user-names, email addresses, and password hashes of 17 million customers, which was then exfiltrated.

4 Breach Workflow and Methods

While the above 10 case studies contain detailed step-by-step breach workflows, in order to systematize breach methods, it is important to understand if these case studies paint a comprehensive picture of the techniques used by the attackers. Therefore, we studied 50 data breaches from 2015 to develop a more general data breach workflow. We extracted all the data breaches of 2015 from Breach Level Index [102]: a website that maintains a database of breaches, containing basic information, such as the number of records stolen, industry, country, and year. We studied data breaches from 2015 because many later breaches did not have enough publicly available information. Breach Level Index has a total of 1866 data breaches for the year 2015. We filtered out the breaches with records less than 10,000 leaving us with 248 incidents. Since not all of them had enough public information, we randomly chose 100 incidents from the 248 and kept on adding more incidents to end up with 50 cases with enough public information. Thus by analyzing 110 random incidents we found 50 breaches as shown in Table 6 in Appendix C, that had enough publicly available information for us to infer the details. Figure 11 shows the general breach workflow for all 60 data breaches we studied including the 10 cases presented in Section 3. We found that almost all the techniques used by the attackers in these 50 breaches are covered in our 10 case-studies; exceptions include ac-

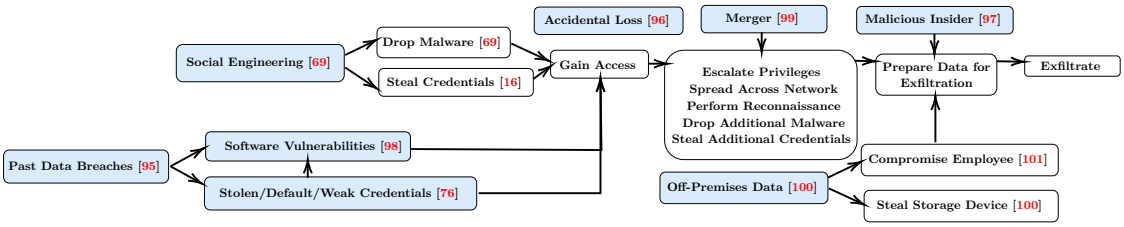

Fig. 11. General breach workflow for all 60 data breaches we studied along with an example for each breach method

cidental loss, off-premises data, and organization mergers. The reason for this difference is that we selected the 10 cases to include targeted attacks that are technically more interesting to analyze as opposed to the cases that involve e.g. accidental loss, making the workflow straightforward.

The following are the exceptions in our 2015 breach study that we did not observe in the 10 case-studies:

Accidental Loss. In some cases, the employees inadvertently disclosed the company data, e.g., by making the database publicly available on the internet or sending data to the wrong email address. For example, in Patreon breach attackers gained access through a debug version of the website [96]. 8% of 2015 breaches were due to accidental loss as shown in Table 2.

Mergers. We also found cases where one of the companies in a merger was already compromised and the breach was discovered only afterward. For example, Vivanuncios, a Mexican classified ad website, was compromised before eBay acquired it but the breach was discovered after the acquisition [99]. Such incidents constitute 4% of the breach incidents we studied.

Off-premises data. Employees often take data off-premises for work. We found that in 22% of 2015 breaches the attackers compromised employees off-premises and stole data. For example, an unencrypted laptop was stolen from the car of an employee at North East Medical Services [100]. The laptop contained Protected Health Information of almost 70,000 patients.

Based on our analysis of the 10 case studies and the 50 data breaches from 2015, we now systematize the breach methods used by the attackers.

4.1 Human Error

We found that human error is the main method attackers employ to compromise organizations and breach data; following key human errors lead to breaches:

Social Engineering. Phishing, spear-phishing, and watering hole attacks are prevalent initial attack vectors in the data breaches we studied. The attacker needs to fool only a single employee with access to the company network, which eventually leads to data leakage. Bursztein et al. [103] also found phishing to be the main attack vector used by hijackers for credential theft.

Reusing Passwords. We found that password reuse by a single employee can lead to serious breaches as seen in the Zomato breach 3.10. Previous work [104] shows that the majority of users tend to reuse passwords with slight or no modifications for various online accounts.

Storing Plain-text Passwords. In some breaches, the employees stored plain-text credentials, which helped the attackers to connect with other hosts and access company databases as seen in the Equifax breach. Multi-factor authentication could lessen the impact of storing plain-text credentials.

Ignoring Intrusion Warnings. In some cases, the intrusion detection systems detected the intrusion that later led to the breach, but the warning was ignored by the company as seen in Target breach. Timely response in these cases could have limited the damage [39]. However, one reason for ignoring these warnings is the high false-positive rate of these systems. Previous research has shown that in many cases, a high false alarm rate is inevitable for intrusion detection [105] which may cause the users to ignore these warnings [106].

Failing to Update Software. We found cases where despite explicit warnings the organizations failed to update their software, enabling the attackers to steal data as seen in the Equifax breach. However given the sheer number of vulnerabilities disclosed each month, it is non-trivial for an organization to prioritize the patches based on their relevance and importance as the attackers may only exploit vulnerabilities that cost less yet provide useful functionality during the attack. These patches also need to be tested first before application in the production environment which costs both time and money [107]. The system may also require a reboot and this downtime is costly for critical systems. Moreover, the majority of remote code execution vulnerabilities are either zero-days or exploited within 30 days of the announcement [108] which makes it even harder for the organizations to patch their systems in time.

Off-Premises Data. We found that employees often export data off-premises in their computers or upload sensitive data to the cloud. We found breaches, where

Records Stolen	<0.1 million	62%
	0.1 - 1 million	18%
	1 - 10 million	12%
	>10 million	8%
Data Records Type	Personally Identifiable Information	68%
	Financial Information	4%
	User Accounts	16%
	Other	12%
Attacker Type	Cyber-criminals	90%
	State-sponsored	8%
	Other	2%
Industry	Healthcare	28%
	Government	14%
	Technology	10%
	Retail	10%
	Education	8%
	Financial	8%
	Other	22%
Techniques Used	Exploit Software Vulnerabilities	28%
	Target Third-Party	26%
	Data Storage Device Stolen Off-premises	18%
	Social Engineering to Steal Credentials	8%
	Malicious Insiders	8%
	Accidental Loss	8%
	Social Engineering to Drop Malware	6%
	Stolen/Default/Weak Credentials	4%
	Employees Compromised Off-premises	4%
	Company Mergers and Acquisitions	4%
	Use Customers' Access to Breach the Company	2%

Table 2. Breach patterns observed in 50 breaches from 2015. Some incidents include multiple patterns. The complete list of organizations is provided in Appendix C.

the attackers compromised employees' laptops, email accounts, or cloud storage to exfiltrate data. For example, an attacker used phishing to steal credentials and hijack an email account of an employee at Oakland Family Services. The employee had uploaded the client's data to the email account [101]. Past research [109] confirms that the account hijacking problem is widespread where 30% of users reported having at least one of their email or social networking accounts compromised. In several breaches, employees lost their devices containing sensitive data, for example, the laptop of an employee at SterlingBackcheck [110], a company that provides employment background checks, was stolen from his car containing background check data of 100,000 users.

4.2 Well-Known Vulnerabilities

A common pattern observed in the data breaches we studied is that they are all caused by well-known fixable vulnerabilities, such as outdated software, password reuse, and opening a malicious email.

4.3 Third Parties

Another problem we observed during our analysis is the attackers stealing the organization's data by targeting third-party companies [43, 76]. We define *third parties* as the entities, the company does business with and may include vendors, partners, software, and hardware solution providers. If the third parties lack adequate security infrastructure they can be easier targets for the attackers. Moreover, third-party service providers, such as payment processing, credit-reporting companies, and health insurance providers have access to the data of a large number of organizations, and therefore are more lucrative for the attackers. The Ponemon Institute [111] estimates third-party risks as the highest-rated cybersecurity concern for 2019. The annual 2018 Ponemon Institute report [112] notes that 59% of the companies interviewed have experienced a third-party data breach, with the average number of third parties with access to an organization data being 471. Our analysis of data breaches of 2015 shows that in 26% of cases, adversaries targeted third parties with access to the organization's data. The companies provide data access to third parties in two ways: (*a*) direct access, e.g., providing customer credit card details for payment processing or (*b*) providing physical or remote access to the company's infrastructure, e.g., to carry out maintenance tasks. The Experian breach of 2015 exposed the data of T-mobile customers because T-Mobile had provided Experian with direct access to their customer's data for credit checking [113]. We also found attackers targeting third-party vendors with weak security posture and exploiting them to access the target organization's network as seen in the Target and OPM breaches.

4.4 Lack of Multi-factor Authentication

Companies often allow employees as well as third parties to access the company network remotely using various remote desktop tools. Such tools require valid credentials for connection and many of them allow multi-factor authentication. We found that in several breaches, attackers stole these credentials through phishing, third-party entity compromise, and past credential leaks, and gained access to the company machines remotely due to lack of multi-factor authentication e.g. OPM breach, and Zomato breach 3.10.

4.5 Hiding Malicious Activities

The attackers used various techniques to hide their activities during lateral movement and data exfiltration. In some cases, they installed malware posing as legitimate software as seen in the Anthem and OPM breaches. In RUAG breach, malicious code was injected in benign applications. The attackers also used binary obfuscation to hide malware from anti-malware tools as seen in the Sony Pictures breach. The command and control server domain names were carefully selected to prevent detection by someone analyzing network traffic,

e.g., in the case of Anthem and OPM breaches. Similarly, the attackers created new domain accounts with user-names selected carefully to appear legitimate accounts in the Target breach.

The communication of the malware with the command and control server, and between malware installed on various hosts was also hidden using different obfuscation techniques as seen in Sony, Target, and RUAG breaches. Moreover, the attackers used tactics like encrypting, compressing, and exfiltrating data over an extended period of time to prevent detection. They also hid their activities in the normal traffic during rush hours as seen in the Target breach.

4.6 Breach Discovery Through Dark Web

In financially motivated breaches, the stolen data is often sold on the dark web marketplaces. We observed that some companies such as Target and Zomato discovered the data breach after a third-party entity notified them of their stolen data being sold on the dark web.

4.7 Concurrent Attacks

We also noticed attackers using concurrent attacks, where an attacker diverted the attention of the company by launching an attack and while the security team was busy responding to it, the attacker launched a second attack to exfiltrate the data. Examples include breach incidents involving Carphone Warehouse, and OPM.

5 Thwarting Data Breaches

In sections 3 and 4, we systematized the breach workflows and methods. In this section, we address the following three questions to systematically explain how to thwart data breaches. (a) What are the requirements for an organization to prevent data breaches? (b) What requirements can be addressed with existing security technologies? and (c) What are the promising research directions that could address the requirements not being currently satisfied.

5.1 Requirements

Based on our analysis of the data breaches, we develop a set of requirements an organization needs to meet for thwarting data breaches. First, we identify all the entities related to an organization such as employees, third-parties, network devices, etc. that an attacker can exploit in any stage of a data breach. Then we develop a total of 57 security requirements for these entities as shown in Table 3. We color code the requirements to show the relevant breach stage: red shows initial compromise, yellow represents lateral movement, and blue represents data exfiltration. While meeting these requirements will significantly reduce data breaches, we do not intend these requirements to be exhaustive. In fact, some of the requirements listed in Table 3 are extremely difficult or even impossible for many organizations to meet. Nonetheless, we believe that the requirements in Table 3 are adequate to systematically understand the capabilities of existing security technologies and identify future research directions.

5.2 Current Security Technologies

To understand the capabilities of the existing security technologies in preventing data breaches, we studied 84 security tools: 13 common open-source systems listed by sectools.org and 71 proprietary systems by RSA Security, McAfee, and Symantec. Table 7 in Appendix C provides the complete list of these tools. We used the tools' data-sheets to understand their protection capabilities, the techniques they use, and their efficacy. Table 3 sheds light on the insufficiency of the existing security technologies to meet the identified requirements and thwart data breaches. With the existing technology, 2 requirements can be fully addressed, represented by filled circles, and the remaining 55 can only be partially addressed, represented by half-filled circles. Therefore, it is unsurprising that attackers often succeed in breaching huge amounts of data from all types of organizations. Table 3 also presents information about various types of deployment difficulties associated with each security technology. Below we discuss these security technologies and their efficacy in thwarting data breaches. For our 10 breach workflows, Table 1 shows if these technologies would have helped thwart the breaches.

Firewalls can protect an organization's boundary and segment the network to limit the attacker's lateral movement. We found attackers exploiting weak network segmentation to reach their targets as seen in the Target breach. Firewalls can also be used to block unwanted network traffic e.g. employees accessing malicious websites or uploading sensitive data to the internet, as shown in Table 3.

Intrusion Detection and Prevention Systems (IDS/IPS) monitor an organization's endpoints, network, cloud infrastructure, web access, and emails for security policy violations. We found attackers using social engineering techniques, common privilege escalation techniques, communicating with command and control servers, and installing malware. Such attempts can be detected by an IDS and blocked by an IPS. However, as discussed earlier, various obfuscation techniques used by the attackers and high false alarm rates reduce the efficacy of IDS/IPS which is why we rate them as partially

		Current Security Technologies														Non-technical Solutions					Future Directions						
		Firewalls	Intrusion Detection System	Intrusion Prevention System	Data Leakage Prevention System	Anti-malware	Vulnerability and Patch Management	Security Testing Tools	Multi-factor Authenticators	Security Management Tools	Threat Intelligence Systems	Security Incident Investigation Tools	Data Breach Alert Services	Third-party Risk Assessment Services	Staff Training and Education	Security Policies	Laws & Regulations	Diplomacy	Least Data Retention	Robust Anti-Phishing	Secure Multiparty Computation	Trusted Hardware	Usability	Automatic Non-Disruptive Updates	Detecting Malicious Insiders	Detecting Obfuscated Malware
Security Solution Deployment Difficulty	Deployment Cost	●	●	●	●	◑	◑	○	◑	◑	◑	◑	◑	◑	–	–	–	–	–	–	–	–	–	–	–	–	–
	Technical Difficulty in Deploying and Managing	◑	●	●	●	○	○	○	○	◑	○	●	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–
	May Disrupt the Organization Workflow			✓	✓										–	–	–	–	–	–	–	–	–	–	–	–	–
	May Affect Usability of the System for Employees								✓						–	–	–	–	–	–	–	–	–	–	–	–	–
Requirements for an Organization to be Secure Against Data Breaches																											
Organization boundary																											
Can detect phishing attempts			◑																		✓						
Can block phishing attempts				◑																✓							
Can detect employees accessing malicious websites		◑	◑								◑																✓
Can block employees accessing malicious websites		◑		◑							◑																✓
Can prevent employees from uploading data to the internet					◑														◑		✓					✓	
Can detect malicious network requests from the internet		◑	◑																								
Can block malicious network requests from the internet		◑		◑																							
Can detect malicious use of remote access credentials			◑						◑													✓					
Can block malicious use of remote access credentials				◑																			✓				
Can detect data exfiltration attempts			◑		◑																						
Can block data exfiltration attempts				◑	◑																						
Employee																											
Employee is not a malicious insider																		◑							✓		
No online information about the employee to aid the attacker during their research															◑												
Does not upload sensitive data to the internet except to trusted sites					◑										◑	◑			◑		✓	✓					
Can detect phishing attempts															◑					✓							
Can detect malicious websites											◑				◑												✓
Does not install malware			◑			◑				◑	◑				◑	◑											✓
Uses strong credentials to connect with the local network										◑					◑	◑											
Credentials have not been reused															◑	◑											
No direct access to sensitive data (may request administrator for access)		◑			◑					◑						◑			◑		✓	✓					
Does not copy data to external storage devices e.g. hard drives					◑					◑					◑	◑			◑		✓					✓	
Does not take any sensitive data off-premise					◑										◑	◑			◑		✓					✓	
Administrator (Include all requirements from Employee)																											
Performs security risk assessment					◑											◑	◑									✓	
Performs vulnerability and penetration tests to gauge the security posture							◑	◑															✓	✓			
Analyzes current security policies and makes suggestions for improvements																◑	◑										
Conducts employee security training															◑												
Manages access privileges of other employees properly		◑			◑				◑	◑																	
Updates unpatched software as soon as a vulnerability is disclosed							◑				◑													✓			
Administers security systems properly		◑	◑	◑	◑	◑			◑	◑													✓				
Analyzes all security warnings to detect breaches										◑		◑											✓				
Performs post-breach investigations												◑											✓			✓	
Employee machine(corporate owned)/ Employee device(personally owned)																											
No software vulnerabilities to allow remote code execution or privilege escalation							◑	◑			◑													✓			
Domain account has low network privileges										◑						◑											
Does not allow unwanted network connections		◑																									
Does not connect with attacker's C2 server to receive commands		◑	◑								◑																✓
Sensitive data not stored on the machine					◑										◑	◑			◑		✓						
Does not connect with attacker's C2 server and exfiltrate data		◑	◑		◑						◑										✓						✓
Physical security to prevent unauthorized physical access																◑					✓	✓				✓	
Other network devices (printers, POS terminals, IOT devices)																											
Do not have vulnerabilities							◑				◑													✓			
Do not allow unwanted network connections		◑																									
Malware is not installed on these devices		◑	◑			◑					◑																✓
Are configured properly								◑		◑						◑							✓				
Internal network																											
Strong network segmentation to hinder attacker's lateral movement		●								●						●											
Analyze network traffic and block unwanted data movement					◑																						
Block unwanted connections between network machines and devices		●								●						●						✓					
Servers (web server, database server, email server, file server, Active Directory)																											
No software vulnerabilities present							◑	◑			◑													✓			
Access control implemented with strong credentials										◑						◑						✓					
Email server can detect phishing emails			◑																		✓		✓				
Email server can block phishing emails				◑																	✓		✓				
Active Directory can block malicious requests for network reconnaissance			◑							◑						◑											
Active Directory can block malicious requests for creating new admin accounts			◑							◑						◑											
Email server can prevent sensitive data leakage through emails					◑														◑		✓						
Physical security to prevent unauthorized physical access																◑					✓	✓				✓	
Dark web																											
Organization can detect presence of data that can aid the attacker													◑														
Organization can remove such data (leaked credentials) from dark web																	◑										
Third-party(Include all security requirements of the victim organization)																											
Prevents malicious use of credentials allocated for remote access									◑				◑										✓			✓	
Protects sensitive data provided for processing		◑	◑	◑	◑	◑	◑	◑	◑	◑	◑			◑	◑	◑	◑		◑		✓					✓	✓

Table 3. The table presents requirements for an organization to be secure and role of existing security technologies in implementing these requirements. We also provides metrics to gauge the difficulty of deploying these security technologies in an organization. Moreover, we show how the proposed future directions can help the organizations in implementing the security requirements.

Deployment Cost
○ Low (open-source)
◑ Medium (software-based)
● High (requires dedicated hardware)

Technical Difficulty in Deploying and Managing
○ Low
◑ Medium (updates to security policy required)
● High (updates to security policy and constant monitoring required)

Requirements
◑ Defense is partially effective
● Defense is fully effective
initial compromise, lateral movement, data exfiltration

Blank cell represents not applicable

effective in detecting various security policy violations in Table 3.

Data Leakage Prevention Systems (DLP) identify, monitor, and protect data at rest, in use by the applications, or in transit. Although DLP systems can raise the bar for attackers [114], they are still insufficient if the attackers use sophisticated techniques for hiding their activities as discussed in Section 4, which renders them partially effective at detecting data leakage as shown in Table 3. Moreover, as Table 3 shows DLP systems may also disrupt or block normal organizational workflow due to false positives.

Anti-malware Software. Attackers often use malware in data breaches, yet due to various obfuscation techniques described in Section 4 and Appendix A, existing anti-malware are only partially effective in detecting such obfuscated malware [115]. Table 3 shows that these systems usually have low deployment costs and require lesser technical proficiency for deployment and management as compared to other tools.

Vulnerability and Patch Management. Data breaches involving known software vulnerabilities, such as Equifax and Carphone breach, could have been prevented by using these systems. However, configuring these tools properly is equally important as evident by the Equifax breach. We also found attackers using vulnerability scanners to discover vulnerabilities and compromise the organizations.

Security Testing Tools. The attackers use tools, such as network scanning and packet crafting tools, penetration testing tools, and password auditing tools, to identify security weaknesses. These tools could help the organizations identify the same weaknesses before the attackers could exploit them.

Multi-factor Authenticators can improve the security of organizations against opportunistic attacks, e.g., the Zomato breach. However, they may also affect the usability of the system, as shown in Table 3, and add costs to the organization both in terms of the employee time lost during authentication and cost incurred to replace lost hardware-based authenticators [116–118].

Security Management Tools are used to specify and monitor security policies consistently across an organization and manage other security tools. In the event of a security breach, these tools provide a holistic view allowing security teams to analyze various events and take remediation actions accordingly reducing the cost of investigation by an average of $200,000 [14].

Threat Intelligence Systems collect and share both global and internal threat intelligence feeds, such as malware signatures, malicious IP addresses, software vulnerabilities, and latest attack patterns, to allow the organizations to identify the latest threats, as seen in Table 3. When critical zero-day vulnerabilities are discovered or new malicious tools surface, the attackers start using them to target a large number of organizations [119, 120]; these systems can prevent such threats.

Security Incident Investigation Tools collect and store system logs and events, allowing organizations to comply with standards and to investigate security breaches. These tools can be useful for detecting malicious behavior on the enterprise-scale and reduce the cost of post-breach investigations [14], as shown in Table 3. We found attackers deleting system logs after the breach to prevent detection. These tools can take regular remote backups of the event logs for later analysis.

Staff Training and Education. Since human error is a prevalent attack vector, organizations can train their employees to detect common threats such as phishing emails and malicious websites.

Data Breach Alert Services continuously monitor Surface Web, such as paste sites, code repositories, file-sharing platforms, social media, and dark web marketplaces and forums to detect data leaks and alert the organization. As Table 3 shows, such services can help the organizations detect any information that could be useful for the attacker during an attack.

To summarize, our analysis shows that the current security technologies do not provide ample protection against targeted attacks. This can be attributed to various limitations in these technologies such as their inability to detect sophisticated threats and zero-day attacks, high false alarm rates, usability issues, and dependability on human experts for management.

However, we want to emphasize that despite the limitations, these security technologies could still be useful for organizations in protecting against untargeted attacks caused by opportunists and cybercriminals that do not rely on sophisticated techniques. The organizations can use IDS, anti-malware systems, and vulnerability management systems to protect against known threats and vulnerabilities. DLP systems are more effective against inadvertent leakages caused by employees exporting data off-premises or uploading data on the internet. Multi-factor authentication systems can raise the bar for the attackers relying on stolen credentials. Moreover, organizations can use existing security technologies to partially implement the requirements highlighted in Table 3.

5.3 Future Research Directions

Based on the requirements we identified and our analysis of existing security technologies, we propose promising future research directions. Table 3 shows how the proposed research directions address various security requirements.

Robust Anti-Phishing. Phishing is the most common initial attack vector used in data breaches. A plethora of anti-phishing tools are available, but the attackers find ways to trick the users. Many organizations have thousands of employees and the attackers usually succeed in tricking some of them. There is a need to investigate why such solutions fail in practice, whether it is the problem with the anti-phishing tools or humans are careless and develop robust anti-phishing tools that do not depend upon human input.

Detecting Obfuscated Malware. Attackers employ a variety of methods to obfuscate the malware used to breach data, making it undetectable. Detecting obfuscated malware is crucial to prevent data breaches.

Secure Multiparty Computation. In almost all data breaches, once the attackers gain access to the servers storing data, they can easily exfiltrate all the data. Secure Multiparty Computation can address this issue by storing the data in multiple servers, such that the attacker would need to compromise all the servers, which makes the attacker job significantly harder. However, existing secure computation techniques are not efficient enough to support enterprise-scale computation. Therefore, there is a need to develop efficient secure computation techniques.

Trusted Hardware. We believe that using trusted hardware, such as Intel SGX, is a promising direction to protect data [121–125]. Using trusted hardware to hold the cryptographic keys for an encrypted database and limiting the number of records that can be retrieved with the SELECT query using trusted hardware could go a long way towards preventing data breaches.

Usability. In our breach analysis, we found that human error is one of the main reasons behind data breaches. Therefore, we believe that improving the usability of security tools and mechanisms is crucial. Most of the existing usability research is focused on authentication [104, 106, 116–118]. While there has been some work related to software usability in general [126], more research is needed to understand usability in the context of security tools and software to make them more usable, seamless, and non-disruptive.

Automatic Non-Disruptive Software Updates. Many breaches are caused by unpatched software. For most organizations, currently it is not possible to automatically update the software in a non-disruptive manner [127, 128]. We believe that more research is needed to understand the disruptive nature of software patching and how to automate the software updates in a non-disruptive fashion.

Detecting Malicious Insiders. For some organizations, a malicious insider could be a serious problem. Unfortunately, such attackers cannot be detected by most security tools as they are designed to protect the organization from the outside. Therefore, new methods are required to detect malicious insiders.

Non-technical Solutions. We believe that non-technical solutions can play a crucial role in preventing data breaches. Many breaches we studied were state-sponsored and diplomacy can help reduce such breaches. Policy, laws, and regulations could be used to either incentivize data protection, e.g., by giving tax breaks to organizations with no breaches, or disincentivizing data breaches, e.g., by penalizing breached organizations.

Towards Least Data Retention. We believe that it is crucial to understand how much data an organization needs to retain. Inspired by the principle of least privilege, we propose the principle of least data retention to retain the minimum amount of data needed. For example, the Ashley Madison breach that led to suicides and destroyed families [2, 129], could have been prevented if the company had decided not to retain the data revealing infidelity. We understand that many companies depend on the data to survive. However, if we want to protect our data, we need to find a reasonable trade-off.

6 Conclusion

We systematized information about how attackers breach data by developing the most plausible step-by-step data breach workflows for 10 famous data breaches followed by a study of 50 random data breaches. We believe that a promising way to protect our data is to understand how attackers breach data, tackle the data breaches as a holistic problem, develop threat models capturing real-world attacker behavior, building systems resilient to human error, develop approaches to minimize damage after a compromise, and retain the least amount of data necessary.

Acknowledgment

This work was partly supported by a Northrop Grumman Cybersecurity Research Consortium (NGCRC) grant.

References

[1] W. contributors, "Ashley madison data breach — Wikipedia, the free encyclopedia," Mar. 2020.

[2] C. Baraniuk, "Ashley madison: 'suicides' over website hack," Aug. 2015.

[3] T. Lamont, "Life after the ashley madison affair," Feb. 2016.

[4] J. Pagliery, "The ashley madison hack ruined my life," Aug. 2015.

[5] K. Zetter, "Hackers finally post stolen ashley madison data," 08 2015.

[6] C. at Microsoft, "Anatomy of a breach - how hackers break in and how you can fight back," tech. rep., Microsoft, Nov. 2017.

[7] C. at MWR InfoSecurity, "Detecting and deterring data exfiltration - guide for implementers," tech. rep., MWR InfoSecurity, Feb. 2014.

[8] C. at Symantec, "Anatomy of a data breach - why breaches happen and what to do about it," tech. rep., Symantec.

[9] A. Rashid, R. Ramdhany, M. Edwards, S. M. Kibirige, A. Babar, D. Hutchison, and R. Chitchyan, "Detecting and preventing data exfiltration," April 2014.

[10] C. Bielinski, "Trustwave global security report 2018," tech. rep., Trustwave, 2018.

[11] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, M. Bailey, and M. Liu, "Cloudy with a chance of breach: Forecasting cyber security incidents," in *USENIX Security 15*, 2015.

[12] L. Bilge, Y. Han, and M. Dell'Amico, "Riskteller: Predicting the risk of cyber incidents," 10 2017.

[13] K. M. Gatzlaff and K. A. McCullough, "The effect of data breaches on shareholder wealth," *RMIR*, pp. 61–83, 2010.

[14] P. Institute, "Cost of a data breach report 2019," tech. rep., Ponemon Institute, 2019.

[15] J. Winter, "Nsa played key role linking north korea to sony hack," Jan. 2015.

[16] G. Keizer, "Sony hackers targeted employees with fake apple id emails," April 2015.

[17] J. Cox, "Yahoo 'aware' hacker is advertising 200 million supposed accounts on dark web," Aug. 2016.

[18] B. Krebs, "Cards stolen in target breach flood underground markets," Dec. 2013.

[19] C. U. Libraries, "Evaluating online sources."

[20] M. Zimdars, "False, misleading, clickbait-y, and/or satirical "news" sources," 2016.

[21] U. Libraries, "Finding reliable sources: What is a reliable source?," Oct. 2019.

[22] U. Libraries, "Evaluating internet resources."

[23] O. Celestino, "Watering hole 101," Feb. 2013.

[24] Novetta, "Operation blockbuster. unraveling the long thread of the sony attack.," tech. rep., Novetta, 2016.

[25] RBA, "A breakdown and analysis of the december, 2014 sony hack," 2014.

[26] "Wikileaks sony breach archives," April 2015.

[27] A. DeSimone, "Sony's nightmare before christmas," tech. rep., The Johns Hopkins University Applied Physics Laboratory, April 2018.

[28] G. Sanchez, "Case study: Critical controls that sony should have implemented," tech. rep., SANS Intitute, June 2015.

[29] D. E. Sangar, "The world once laughed at north korean cyberpower. no more.," 2017.

[30] C. Osborne, "Sony hires fireeye's mandiant following internal security breach," Dec. 2014.

[31] "Targeted destructive malware," Dec. 2014.

[32] C. at Microsoft, "Ms-smb: Server message block (smb) protocol," tech. rep., Microsoft, July 2013.

[33] W. contributors, "Server message block — wikipedia - the free encyclopedia," 2019.

[34] W. contributors, "Lan manager — wikipedia - the free encyclopedia," 2018.

[35] W. contributors, "Nt lan manager — Wikipedia, the free encyclopedia," 2019.

[36] C. at Microsoft, "Microsoft kerberos," tech. rep., Microsoft, May 2018.

[37] C. Sanders, "How i cracked your windows password (part 1)," Jan. 2010.

[38] Spiceworks, "The future of network and endpoint security," tech. rep., June 2019.

[39] J. MULLIGAN, "Protecting personal consumer information from cyber attacks and data breaches," March 2014.

[40] E. A. Haris, "For target, the breach numbers grow," Jan. 2014.

[41] "Cyxtera - easy solutions."

[42] J. Finkle, "Target cyber breach hits 40 million payment cards at holiday peak," Dec. 2013.

[43] A. Labs, "The untold story of the target attack step by step," tech. rep., Aorato Labs, August 2014.

[44] K. Jarvis, "Inside a targeted point-of-sale data breach," tech. rep., Dell, Jan. 2014.

[45] ThreatScape, "Kaptoxa point-of-sale compromise," tech. rep., ThreatScape, Jan. 2014.

[46] B. Krebs, "Inside target corp., days after 2013 breach," Sep. 2015.

[47] B. Krebs, "New clues in the target breach," Jan. 2014.

[48] B. Krebs, "A first look at the target intrusion, malware," Jan. 2014.

[49] Semantic, "Trojan.zbot," Jan. 2010.

[50] J. Segura, "Citadel: a cyber-criminal's ultimate weapon?," Nov. 2012.

[51] P. Trivedi, "File inclusion attacks," Dec. 2014.

[52] M. Kumar, "23-year-old russian hacker confessed to be original author of blackpos malware," Jan. 2014.

[53] C. Poulin, "What retailers need to learn from the target breach to protect against similar attacks," Jan. 2014.

[54] C. at Microsoft, "Active directory domain services overview," May 2017.

[55] B. Ewaida, "Pass-the-hash attacks: Tools and mitigation," tech. rep., SANS Institute, 2010.

[56] "Microsoft ntlm," 2018.

[57] "mimikatz."

[58] M. Russinovich, "Psexec v2.2," June 2016.

[59] N. Perlroth, "Yahoo says hackers stole data on 500 million users in 2014," Sept. 2016.

[60] U. S. D. C. N. D. O. California, "Indictment," Feb. 2017.

[61] V. Goel, "Russian agents were behind yahoo hack, u.s. says," March 2017.

[62] M. Williams, "Inside the russian hack of yahoo: How they did it," Oct. 2017.

[63] S. GALLAGHER and D. KRAVETS, "How did yahoo get breached? employee got spear phished, fbi suggests," Mar. 2017.

[64] J. Goldman, "Russian fsb officers charged with involvement in yahoo breach," March 2017.

[65] A. Mitre, "Privilege escalation."

[66] B. Oliveira, "My 5 top ways to escalate privileges," Dec. 2012.

[67] N. Provos and D. Mazières, "A future-adaptive password scheme," in *Proceedings of the Annual Conference on USENIX Annual Technical Conference*, ATEC '99, pp. 32–32, USENIX Association, 1999.

[68] A. Mitre, "Deep panda."

[69] "Multistate targeted market conduct and financial examination," tech. rep., Dec. 2016.

[70] J. DiMaggio, "The black vine cyberespionage group," tech. rep., Symantec, Aug. 2015.

[71] "Sakula."

[72] "Sakula," 2017.

[73] D. Stama, "Backdoor.mivast," Feb. 2015.

[74] A. Mitre, "Credential dumping."

[75] A. Mitre, "Bypass user account control."

[76] "The opm data breach: How the government jeopardized our national security for more than a generation," tech. rep., Oversight and Government Reform, Sep. 2016.

[77] B. Koerner, "Inside the cyberattack that shocked the us government," 2016.

[78] "Plugx," 2017.

[79] A. Sternstein and J. Moore, "Timeline: What we know about the opm breach (updated)," June 2015.

[80] Symantec, "The waterbug attack group," Jan. 2016.

[81] GovCERT.ch, "Technical report about the espionage case at ruag," tech. rep., GovCERT, May 2016.

[82] "Process injection."

[83] E. Snowden, *Permanent Record*. Metropolitan Books, 09 2019.

[84] "Review of the unauthorized disclosures of former national security agency contractor edward snowden," tech. rep., House Permanent Select Committee on Intelligence, 9 2016.

[85] ICO, "Carphone warehouse monetary penalty notice," Jan. 2018.

[86] J. Leyden, "Hackers hid carphone warehouse breach with ddos smokescreen – report," Aug. 2015.

[87] M. J. Schwartz, "Carphone warehouse breach: 'striking' failures trigger fine," Jan. 2018.

[88] "Nikto web scanner."

[89] "Meet wordpress."

[90] GAO, "Actions taken by equifax and federal agencies in response to the 2017 breach," tech. rep., United States Government Accountability Office, Aug. 2018.

[91] "CVE-2017-5638." National Vulnerability Database, Mar. 2017.

[92] S. Sahu, "Cve-2017-5638: Apache struts 2 vulnerability leads to remote code execution."

[93] G. Patidar, "Security notice," May 2017.

[94] G. Patidar, "Security notice update," May 2017.

[95] D. Goyal, "Security update – what really happened? and what next?," May 2017.

[96] L. Franceschi-Bicchierai, "Crowdfunding site patreon gets hacked," Oct. 2015.

[97] M. McGee, "Fraud case centers on alleged stolen pediatric clinic data," Sep. 2016.

[98] ICO, "Talktalk cyber attack – how the ico's investigation unfolded," Oct. 2015.

[99] C. at DataBreaches.net, "Mx: Vivanuncios user data stolen by hacker (nah – scraped by competitor)," Mar. 2015.

[100] H. Journal, "North east medical services hipaa breach reported: 69,246 affected," Aug 2015.

[101] A. Greenberg, "Oakland family services notifies 16k clients of information breach," Sep. 2015.

[102] BreachLevelIndex, "Data breach database."

[103] E. Bursztein, B. Benko, D. Margolis, and T. Pietraszek, "Handcrafted fraud and extortion: Manual account hijacking in the wild," in *IMC '14*, 2014.

[104] M. Golla, M. Wei, J. Hainline, L. Filipe, M. Dürmuth, E. Redmiles, and B. Ur, ""what was that site doing with my facebook password?": Designing password-reuse notifications," CCS '18, 2018.

[105] S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection," Aug. 2000.

[106] K. Krol, M. Moroz, and M. A. Sasse, "Don't work. can't work? why it's time to rethink security warnings," in *2012 CRiSIS*, pp. 1–8, Oct 2012.

[107] H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security patch management: Share the burden or share the damage?," 2008.

[108] Microsoft, "Microsoft security intelligence report," tech. rep., Dec. 2013.

[109] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, ""my religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking," in *SIGCHI CHI '14*, 2014.

[110] Dissent, "Update: Sterlingbackcheck breach impacted 100,000," Aug. 2015.

[111] P. Institute, "Measuring and managing the cyber risks to business operations," tech. rep., Ponemon Institute, 2019.

[112] P. Institute, "Data risk in the third-party ecosystem," tech. rep., Ponemon Institute LLC, November 2018.

[113] J. Finkle, "Millions of t-mobile customers exposed in experian breach," Oct. 2015.

[114] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *NCA*, 2016.

[115] M. Alvarez, "Are you digging deep? when antivirus is not enough," Oct. 2014.

[116] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," 05 2018.

[117] K. Krol, E. Philippou, E. D. Cristofaro, and M. A. Sasse, ""they brought in the horrible key ring thing!" analysing the usability of two-factor authentication in uk online banking," *ArXiv*, 2015.

[118] D. D. Strouble, M. Alan, and S. Alsop, "Productivity and usability effects of using a two-factor security system," 01 2009.

[119] K. Zetter, "How ram scrapers work: The sneaky tools behind the latest credit card hacks," Sep. 2014.
[120] G. Bruneau, "Scanning for apache struts vulnerability cve-2017-5638," Mar. 2018.
[121] J. Beekman, J. Manferdelli, and D. Wagner, "Attestation transparency: Building secure internet services for legacy clients," 05 2016.
[122] B. Fisch, D. Vinayagamurthy, D. Boneh, and S. Gorbunov, "Iron: Functional encryption using intel sgx," in *2017 ACM SIGSAC*, 2017.
[123] A. Gribov, D. Vinayagamurthy, and S. Gorbunov, "Stealthdb: a scalable encrypted database with full sql query support," *PoPETs*, 11 2017.
[124] C. che Tsai, D. E. Porter, and M. Vij, "Graphene-sgx: A practical library OS for unmodified applications on SGX," in *(USENIX ATC 17)*, July 2017.
[125] S. Eskandarian, J. Cogan, S. Birnbaum, and Brandon, "Fidelius: Protecting user secrets from compromised browsers," 09 2018.
[126] J. C. Lee and D. S. McCrickard, "Towards extreme(ly) usable software: Exploring tensions between usability and agile software development," in *AGILE 2007*, 2007.
[127] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *SOUPS 2014)*, July 2014.
[128] K. Vaniea and Y. Rashidi, "Tales of software updates: The process of updating software," 05 2016.
[129] M. MAILONLINE, "'i was sent a video of my wife having sex'," Aug. 2016.
[130] "Pass the ticket."
[131] "Snopes is the internet's definitive fact-checking resource."
[132] "Latest email and social media hoaxes - current internet scams - hoax-slayer."
[133] "Politi fact, the poynter institute."
[134] "Factcheck.org a project of the annenberg public policy center."
[135] "Media bias/fact check the most comprehensive media bias resource."
[136] "Muck rack for journalists."
[137] H. Williams, "Ex-talk talk ceo shares lessons from massive 2015 data breach," June 2018.
[138] S. Khandelwal, "Two talktalk hackers jailed for 2015 data breach that cost it £77 million," Nov. 2018.
[139] M. J. Schwartz, "Talktalk slammed with record fine over breach," Oct. 2016.
[140] Z. Rodionova, "Talktalk given record fine over data breach that led to data theft of nearly 157,000 customers," Oct. 2016.

Appendices

A Malware

A.1 SMB Worm Used in Sony Pictures Breach

The SMB worm spreads across Windows hosts by brute-forcing SMB authentication password. The malware has a listening implant to receive commands from the command and control server via TCP port 195 and 444. The malware has a lightweight backdoor and a proxy tool to transfer files, perform reconnaissance, execute arbitrary code, open ports in victim machine's firewall etc. The malware has a destructive hard drive tool, and a target cleaning tool to wipe machine hard drives and over-write Master Boot Record making the machine unbootable. It employs secure file deletion where the content of the files are first replaced with random data, the file is renamed with random characters and then finally deleted making the data recovery impossible.

The malware uses various obfuscation techniques to avoid detection. To prevent detection while calling Windows API functions, the malware uses dynamic API loading to load desired functions at runtime. The malware obfuscates the API function names using techniques, such as XOR encryption, adding unnecessary characters in function names, such as dots, spaces, greater than, less than, and underscore characters e.g. using Cha<ngeSe<rviceC<onfig<2A instead of ChangeServiceConfig2A, and Caracachs encryption. Similarly to obfuscate communication with the command and control server, the malware uses Caracachs encryption, RSA, and XOR encryption [24].

A.2 Customized BlackPOS Malware Used in Target Breach

BlackPOS is a RAM-scraping malware installed on POS terminals to scrape Track 1 and Track 2 data stored on the magnetic stripe of payment cards, from the memory of the process interacting with the card reader. BlackPOS, written by a young Russian hacker [52], first surfaced in the early 2013 and was originally sold on Black Market [48]. The malware source code was later leaked. The attackers customized the source code of BlackPOS to meet their needs. None of the commercial antivirus tools at that time detected the malware [45, 48]. The malware installs itself as a system service to achieve persistence. The malware looks for the process named 'pos.exe' and reads its memory in

10Mb chunks to recover the payment card data which it stores incrementally in a local Base64 encoded DLL file.

A.3 Sakula Trojan used in Anthem Breach

Sakula is a remote access trojan that maintains persistence by installing itself as a system service or by setting the Windows Registry Run key. Adding an entry to the registry run keys causes the program to be executed automatically whenever the user logs in. Sakula can be used to bypass Windows User Account Control to gain elevated privileges, execute arbitrary OS commands, upload files, download and execute the payload, communicate with the command and control server over HTTP, uninstall itself and removing run key entries, etc. The malware uses single-byte XOR obfuscation to hide the malicious payload and communication with command and control server [70].

A.4 PlugX Malware used in OPM Breach

PlugX [78] is a modular RAT used to run arbitrary OS commands, log keystrokes, capture screenshots and video of user activity, modify files, etc. The malware achieves persistence by setting the Windows Registry Run key or by registering itself as a service to be automatically invoked on startup. The malware can be configured to use various network protocols such as HTTP, DNS, raw TCP, and UDP, etc. and the traffic is XOR encrypted while communicating with the command and control server to avoid detection. The attacker used different variants of PlugX malware which shows he was continuously modifying the malware. The malware masqueraded as McAfee antivirus software using filenames, such as 'mcsync.exe', 'mcUtill.dll', and 'mcsync.eal' which also led to its detection later since OPM didn't use any of the McAfee's products.

B Attacks

B.1 Pass-the-ticket and Golden Ticket Attack in RUAG Breach

Pass-the-ticket [130] is used to authenticate with other machines on the network by passing Kerberos tickets obtained through the victim machine memory. Kerberos is a network authentication protocol used to authenticate a client to a server and provides better security than the previous NTLM authentication protocol. Nodes using Kerberos protocol communicate using Kerberos *tickets* to prove their identity instead of the plaintext password. The attacker can access this ticket stored in the memory to authenticate with other machines on the network. The attacker can also use Mimikatz to perform a Golden Ticket attack that allows them to generate arbitrary Kerberos tickets for any account in the domain. The attack works by the attacker first gaining privileged access to Active Directory in order to access the NTLM hash of Key Distribution Service account (KRBTGT). KRBTGT is a special account used to encrypt and sign all Kerberos tickets in the domain. Access to KRBTGT NTLM hash allows the attacker to generate Kerberos tickets for all domain accounts using Mimikatz and spread across the network easily.

C Tables

Accuracy		
Article clearly states information sources?		95.2%
Sources support the article claims?		97.6%
Article/website is not reported as hoax		100%
Factual reporting rating of website is high?		100%
Reliability		
Global Alexa percentile rank of website > 99.5%		100%
Total website backlinks (02/23/20 – 02/29/20)	100-1000	15.3%
	1000-50000	53.8%
	>50000	30.7%
Age of organization (years)	5-10	7.6%
	10-20	30.7%
	>20	61.5%
Author's credentials can be verified?		100%
Author has a background in technology reporting?		95.2%
Author has a verified Muck Rack account?		100%
Author's experience as a reporter (years)	1-5	5.8%
	5-20	58.8%
	>20	32.2%
Number of articles published by the author	100-1000	42.1%
	1000-5000	52.6%
	>5000	5.2%
Timeliness		
Article last updated after 2013?		100%

Table 4. Metrics for gauging accuracy, reliability, and timeliness of the information sources we used. To check if a website/article has been previously reported as hoax we use 4 different fact-checking websites [131–134]. We obtain the Factual Reporting rating of the news organization from Media Bias [135]. The website backlinks provide the number of websites that referenced this website in a week. Muck Rack is a popular Media Contact Database used by journalists [136].

Article Ref	Organization	Authors
[29]	NY Times	David E. Sanger, David D. Kirkpatrick and Nicole Perlroth
[59]	NY Times	Nicole Perlroth
[61]	NY Times	Vindu Goel and Eric Lichtblau
[15]	The Intercept	Jana Winter
[16]	Computer World	Gregg Keizer
[137]	Computer World	Hannah Williams
[30]	ZDNET	Charlie Osborne
[46]	Krebs on Security	Brian Krebs
[47]	Krebs on Security	Brian Krebs
[48]	Krebs on Security	Brian Krebs
[52]	The Hacker News	Mohit Kumar
[138]	The Hacker News	Swati Khandelwal
[62]	CSO Online	Martyn Williams
[17]	Motherboard Vice	Joseph Cox
[63]	Ars technica	Sean Gallagher and David Kravets
[77]	Wired	Brendan I. Koerner
[86]	The Register	John Leyden
[87]	Bank info Security	Mathew J. Schwartz
[139]	Bank info Security	Mathew J. Schwartz
[140]	The Independent	Zlata Rodionova

Table 5. Online Resources (news & blog posts) used during data breach analysis of 10 case studies

Organization	Industry
Metropolitan State University, UC Berkeley Financial System , UC Berkeley Financial System	Education
UC Berkeley Financial System	Education
University of Hawaii, Cornell University	Education
University of Oregon	Education
North Shore-Long Island Jewish Health System	Financial
Tokyo Chamber of Commerce	Financial
UniCredit.au/RBC.au/RosBusinessConsulting	Financial
World Trade Organization (WTO)	Financial
IRS	Government
Japan's pension system	Government
Oakland Family Services	Government
Principal Controller of Defence Accounts	Government
RUAG	Government
Sacred Heart Health Systems	Government
U.S Department of the Interior, U.S. Office of Personnel Management	Government
Hepatology & Nutrition of Florida	Healthcare
Illinois Valley Podiatry Group	Healthcare
Indiana State Medical Association	Healthcare
LSU Health New Orleans School of Medicine	Healthcare
McLean Hospital	Healthcare
Medical Informatics	Healthcare
New West Health	Healthcare
North East Medical Services	Healthcare
Saint Agnes Healthcare	Healthcare
Seim Johnson	Healthcare
St. Luke's Cornwall Hospital	Healthcare
St. Vincent Hospital	Healthcare
University of Pittsburgh Medical Center	Healthcare
Valley Hope Association	Healthcare
Hemmakv_ll	Retail
MAPP.NL	Retail
VTech Holdings	Retail
Walmart Canada /PNI Digital Media	Retail
Wetherspoon	Retail
Interxion	Technology
Nexus Mods	Technology
Steam/Valve	Technology
vBulletin	Technology
Vivanuncios (Vivastreet)	Technology
AshleyMadison.com	Other
Patreon	Other
PaymyPCN.net	Other
PHP Freaks Forum	Other
SterlingBackcheck	Other
T-Mobile/Experian	Other
TalkTalk	Other
The Archdiocese of Denver	Other
TV Channel MyTF1	Other
Utah Food Bank	Other
Wounds International	Other

Table 6. 50 Organizations Breached in 2015

Category	Examples
Management Tools	RSA NetWitness Orchestrator, McAfee Cloud Workload Security, McAfee DLP Discover, McAfee Enterprise Security Manager, McAfee ePolicy Orchestrator, Symantec Control Compliance Suite
Firewall	McAfee Network Security Platform, Symantec Web Application Firewall(WAF) and Reverse Proxy
Anti-malware Software	McAfee Advanced Threat Defense, McAfee Application Control, McAfee MOVE AntiVirus, Symantec Content & Malware Analysis, Symantec Malware Analysis Service
Intrusion Detection and Prevention	RSA NetWitness UEBA, McAfee Advanced Correlation Engine, McAfee Event Receiver **End-Point:** RSA NetWitness Endpoint, RSA NetWitness Logs, McAfee Active Response, McAfee Change Control, McAfee Endpoint Security, McAfee Host Intrusion Prevention for Desktop/ Server, ATP Endpoint, Symantec Endpoint Detection and Response, Symantec Endpoint Protection, Symantec Endpoint Protection Cloud, Symantec Endpoint Protection for VDI, Symantec Endpoint Protection Mobile, Symantec Trusted Mobile Device Security Service, Symantec Endpoint Protection Small Business Edition, Symantec Endpoint Threat Defense for Active Directory, McAfee Endpoint Protection for SMB (small and medium businesses) **Network:** RSA NetWitness Network, McAfee Application Data Monitor, McAfee Host Intrusion Prevention for Desktop/Server, McAfee Network Security Platform, ATP Network, Symantec Network Forensics: Security Analytics **Web:** McAfee Web Gateway, McAfee Web Gateway Cloud Service, ATP Roaming, Symantec Virtual Secure Web Gateway, Symantec Web Isolation **Email:** McAfee Security for Email Servers, Symantec Messaging Gateway, ATP Email, Symantec Email Threat Detection and Response **Cloud Security:** McAfee MVISION Cloud **Data Center:** Symantec Data Center Security
Data Leakage/Loss Prevention System	**End-Point:** RSA DLP Endpoint, McAfee Complete Data Protection, McAfee Complete Data Protection Advanced, McAfee Device Control, McAfee DLP Endpoint, Symantec Endpoint Encryption, Symantec File Share Encryption, Symantec Data Loss Prevention **Network:** Network, McAfee DLP Monitor, McAfee DLP Prevent **Web:** McAfee Web Gateway, McAfee Web Gateway Cloud Service **Email:** McAfee Security for Email Servers, Symantec Messaging Gateway, Symantec Data Loss Prevention Cloud Service for Email **Cloud:** McAfee MVISION Cloud, Symantec Data Loss Prevention Cloud and Symantec CloudSOC **Data Center:** RSA DLP Datacenter
Vulnerability Scanning and Patch Management	McAfee Data Center Security Suite for Databases, Symantec Endpoint Threat Defense for Active Directory, Nexpose, Nikto, sqlmap, Burp
Security Testing Tools	Metasploit, Wireshark, Cain and Abel, Scapy, Aircrack, Netcat, John the Ripper, THC Hydra
Multi-factor Authenticators	RSA SecurID Access, Symantec VIP, Symantec VIP Access Manager
Threat Intelligence Systems	McAfee Global Threat Intelligence, McAfee Threat Intelligence Exchange, DeepSight Adversary, Intelligence, Symantec WebFilter/Intelligence Services
Security Incident Investigation and Forensics	McAfee Enterprise Log Manager, McAfee Enterprise Log Search, McAfee Investigator
Staff Training and Education	Symantec Phishing Readiness, Security Awareness Service, McAfee Investigator
Data Breach Alert Services	CybelAngel Data Leak Detection Service

Table 7. Categorization of 84 Security Defence Tools Studied.