2020-2021

Cyber-Espionage Report

verizon

Case file contents

01

Compass points and decoder keys

Welcome to the Cyber-Espionage Report (CER), our first-ever data-driven publication on advanced cyberattacks. The CER is one of the most comprehensive overviews of the Cyber-Espionage landscape, offering a deep dive into attackers, their motives, their methods and the victims who they target. The report serves as a tool for better understanding these threat actors and what organizations can do to hunt, detect and respond to Cyber-Espionage attacks.

This data-driven report draws from seven years of Data Breach Investigations Report (DBIR) content as well as more than 14 years of Verizon Threat Research Advisory Center (VTRAC) Cyber-Espionage data breach response expertise. The CER serves as a guide for cybersecurity professionals looking to bolster their organization's cyberdefense posture and incident response (IR) capabilities against Cyber-Espionage attacks.

More specifically, the CER is an elaboration of the "Cyber-Espionage" Incident Classification Pattern as reflected in the 2020 DBIR. And as with the DBIR, we use the same naming conventions, terms and definitions. Content in this section and in "Appendix A: Frameworks" will help serve as your compass points and decoder keys for the rest of the report. Download a copy of the CER at verizon.com/business/resources/reports/cyber-espionage-report/

Using this report

Throughout the CER, we present and compare findings from a seven-year perspective (content from the 2014 DBIR through the 2020 DBIR): Cyber-Espionage breaches vs. all breaches. At times, we also address findings from a one-year (2020 DBIR) perspective: Cyber-Espionage breaches vs. all breaches. All references to years in this report are in DBIR years. For example, "2020 DBIR timeframe" refers to DBIR year 2020, which in turn correlates with the DBIR dataset timeframe of October 2018 to October 2019.

Data Breach Investigations Report

The 2020 DBIR is our 13th edition, covering global cybercrime trends. The DBIR combines real data from scores of sources and provides actionable insight into tackling cybercrime. Download the 2020 DBIR here:

enterprise.verizon.com/resources/reports/dbir/

VERIS framework

The Vocabulary for Event Recording and Incident Sharing (VERIS) framework is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. See "Appendix A: Frameworks" for more information and read more about VERIS at the link below:

veriscommunity.net/

Incident Classification Patterns

Way back in 2014, to help us better understand and communicate the DBIR dataset, we grouped "like" incidents together and called them "Incident Classification Patterns." Nine patterns comprised the majority of data breaches back then and still do so today. These patterns are Crimeware, Cyber-Espionage, Denial of Service, Lost and Stolen Assets, Miscellaneous Errors, Payment Card Skimmers, Point of Sale, Privilege Misuse, Web Applications and the catchall Everything Else. For definitions and summaries, see pages 36 to 37 of the 2020 DBIR.

Cyber-Espionage pattern

The DBIR Cyber-Espionage pattern consists of espionage enabled via unauthorized network or system access. Nation-state or state-affiliated threat actors looking for those oh-so-juicy secrets primarily fall within this pattern.

Industry labels

We align the CER with the North American Industry Classification System (NAICS), a standard for categorizing victim organizations. NAICS uses two- to six-digit codes to classify organizations. For the CER, we use the two-digit classification level. We provide detailed analyses for seven NAICS-coded industries in "Appendix B: Industry dossiers." Detailed information on the codes is available here:

naics.com/search-naics-codes-by-industry/

NIST Cybersecurity Framework

We use the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) in this report. Specifically, we use the five functional areas of Identify, Protect, Detect, Respond and Recover. See "Appendix A: Frameworks" and here for more information:

nist.gov/cyberframework

CIS Critical Security Controls

We also use the 20 Center for Internet Security (CIS) Critical Security Controls (CSCs) in this report. See "Appendix A: Frameworks" and here for more information:

cisecurity.org/controls/cis-controls-list/

Contact us.

Questions? Comments? Feedback? Drop the VTRAC team a line at vtrac@verizon.com or find us on LinkedIn at #cyberespionagereport and #vtrac

02

State of Cyber-Espionage

Overview

We've conducted all sorts of investigations into cybersecurity incidents and data breaches over the years. None have been more challenging or perplexing than Cyber-Espionage attacks.

Indeed, Cyber-Espionage threat actors pose a unique challenge to cyberdefenders and incident responders. Through advanced techniques and a specific focus, these determined threat actors seek to swiftly and stealthily gain access to heavily defended environments. Depending on their goals, they move laterally through the network, obtain targeted access and data, and exit without being detected. Or, they stay back and maintain covert persistence.

Often, threat actors leave little to no indication of their actions, let alone objectives, to avoid detection and thwart response efforts. Many choose not to move immediately toward their objectives, opting to embed themselves in the environment where they persist quietly until their next move.

Threat actors conducting espionage can range from nation-states (or state-affiliated entities) to business competitors, and in some cases, organized criminal groups. Their targets are both the public sector (governments) and private sector (corporations). Their reasons? National security, political positioning and economic competitive advantage. They seek national secrets, intellectual property and sensitive information.

The Cyber-Espionage threat actor modus operandi includes gaining unauthorized access, maintaining a low (or no) profile and compromising sensitive assets and data. Technology makes espionage actors fast, efficient, evasive and difficult to attribute. In a nutshell, for the threat actor, Cyber-Espionage is an opportunity with relatively low risk (of being discovered), low cost (in terms of resources) and high potential (for payoff).

"The internet has made us richer, freer, connected and informed in ways its founders could not have dreamt of. It has also become a vector of attack, espionage, crime and harm."

George Osborne, British Politician and Newspaper Editor[1]

In seeking to accomplish their objectives, Cyber-Espionage threat actors leverage three primary actions:

- Social engineering by targeting employees through activities such as phishing
- Hacking systems and networks by using backdoors and command and control (C2) functions to establish and maintain access
- Deploying malicious software, such as Trojan downloaders, to extend their capabilities

Within the DBIR dataset, we identified the industries most impacted over the past seven years (2014-2020 DBIR timeframe) by Cyber-Espionage breaches: Education, Financial, Information, Manufacturing, Mining + Utilities, Professional and Public. We focused on these industries because they were the most often targeted by these threat actors.

Now, if your industry isn't featured within this report, you're not off the hook. Cyber-Espionage threat actors may still be targeting your assets and data—we may just not have visibility into those attacks. If you've got sensitive, classified, proprietary or internal secrets that you'd like to keep from getting into the wrong hands, turn the page and read on.

1 'Chancellor's speech to GCHQ on cybersecurity': public-sector.co.uk/article/ff8fa006cdcd35f4cf9ef4e030e08ff1

The ever-evolving threat landscape

To stay ahead of cyberdefenders and incident responders, Cyber-Espionage threat actors adjust their tactics, techniques, and procedures (TTPs) to embrace new technology, while keeping their tried-and-true TTPs operational. Here we map those TTPs to the VERIS Action varieties to give you an idea of what is in and what is out.

For example, Phishing (Social) and Backdoor (Malware) have served as go-to Action varieties. Downloader (Malware), Capture stored data (Malware) and Spyware/Keylogger (Malware) have all steadily declined from the 2014 DBIR to the 2020 DBIR, with Scan network (Malware) completely falling off the top 10 list by the time we get to the 2020 DBIR.

Password dumper (Malware), Trojan (Malware) and Remote Access Trojan (RAT) (Malware) are new to the 2020 DBIR top 10 list. And, while we see that since the 2014 DBIR, Backdoor (Malware), Use of backdoor or C2 (Malware) and C2 (Malware) have declined percentagewise over the years, these Action varieties consistently remain within the top five Action varieties for the entire timeframe.

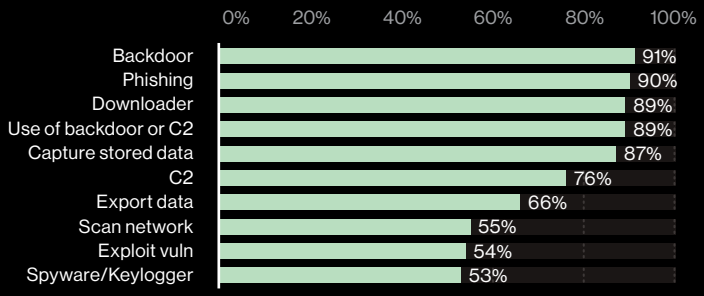


Figure #1: Top Action varieties within Cyber-Espionage breaches (2014 DBIR; n=282)

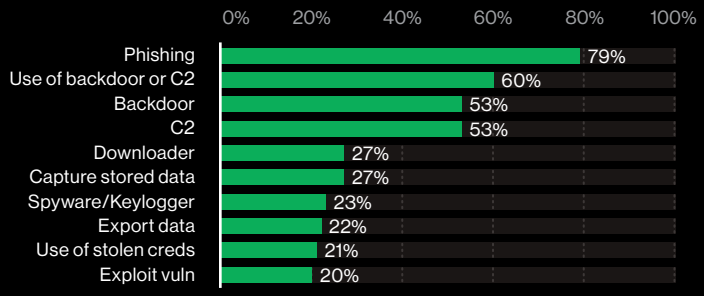


Figure #2: Top Action varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,465)

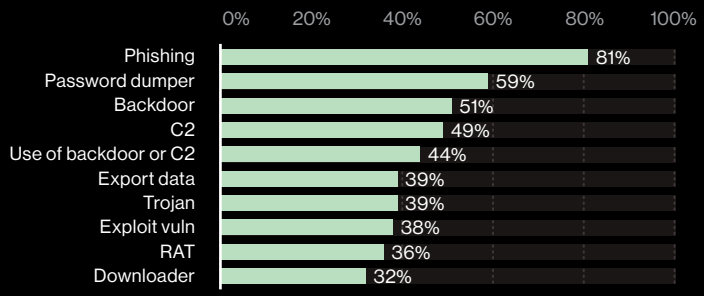


Figure #3: Top Action varieties within Cyber-Espionage breaches (2020 DBIR; n=114)

Patterns

Breach patterns

When it comes to overall breaches by Incident Classification Pattern for the 2014-2020 DBIR timeframe, we see that Cyber-Espionage ranks sixth (10%)—albeit within close striking distance of fourth: Privilege Misuse (ranked fourth at 11%) and the sagging Point of Sale intrusions (ranked fifth at 11%).

It is important to note that these Incident Classification Patterns are just those known, reported and collected. Because Cyber-Espionage attacks are difficult to detect, and the breaches within this pattern are under-reported, the number may be much higher. The kinds of data stolen in Cyber-Espionage breaches (e.g., Secrets, Internal or Classified) may not fall under the data types that trigger reporting requirements under many laws or regulations. Cyber-Espionage threat actors are not typically targeting customer data, or even employee data, but rather the intellectual property (or secret sauce if you will) that would give them a leg up in industrial espionage.

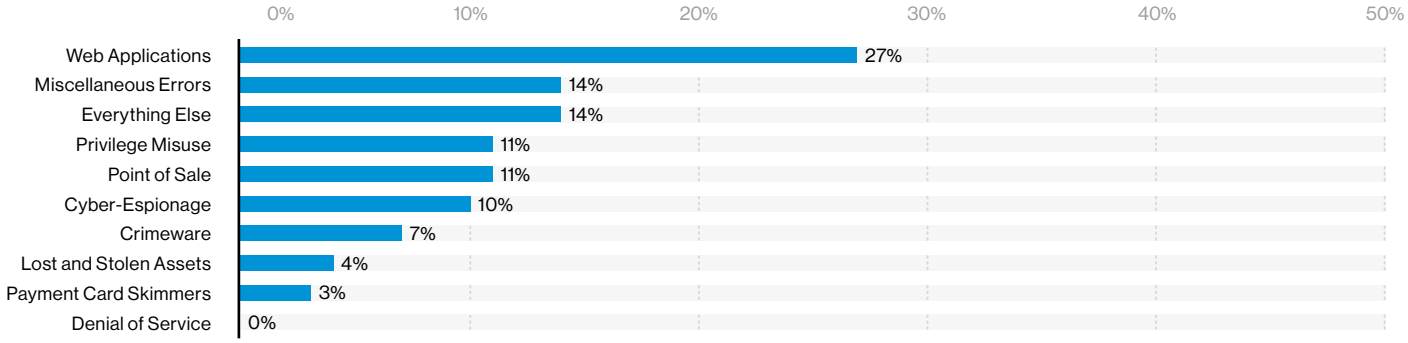


Figure #4: Breaches by pattern (2014-2020 DBIR; n=16,090)

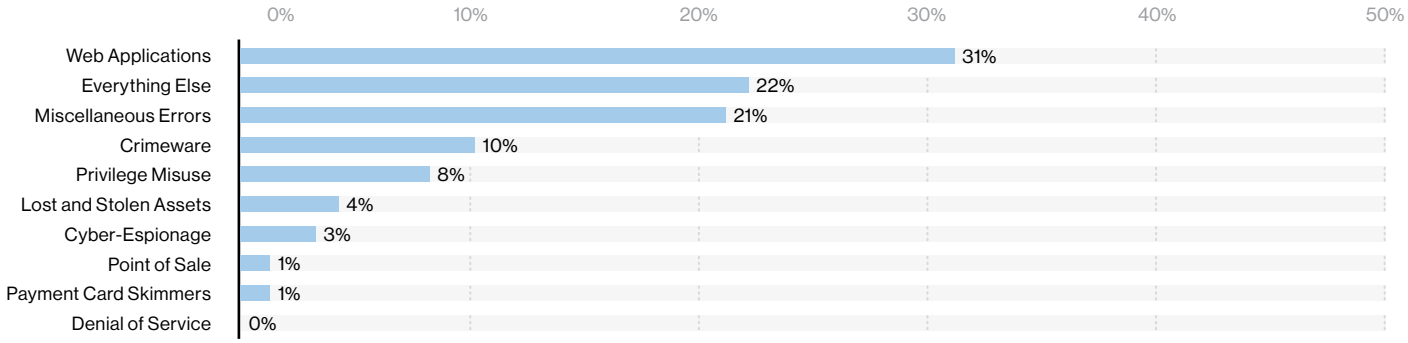


Figure #5: Breaches by pattern (2020 DBIR; n=3,950)

Timelines

Attacker timelines

One of the most effective ways to convey the current state of data breaches and their impact to victim organizations is through temporal analysis or timelining.

When we look at the DBIR dataset, four timelines manifest most clearly. Two are from the threat actor standpoint—Time to Compromise and Time to Exfiltration—and two are from the cyberdefender and incident responder standpoint—Time to Discovery and Time to Containment.

Traditionally, for all breaches, the DBIR has shown that successful threat actors have taken a short amount of time (seconds to minutes) to compromise, and a relatively short amount of time (minutes to days) to exfiltrate data.

Victim organizations have taken considerably longer (days to months) to discover breaches, and an uncomfortably long time (hours to weeks) to contain breaches.

While the timelines for all breaches may seem bleak, the same timelines for Cyber-Espionage breaches appear even more dire.

In the 2014-2020 DBIR timeframe, for Cyber-Espionage threat actors, the Time to Compromise ranges from mere seconds to days (91%, the sum of 23%, 19%, 23% and 26%), while the Time to Exfiltration ranges from minutes to weeks (88%).

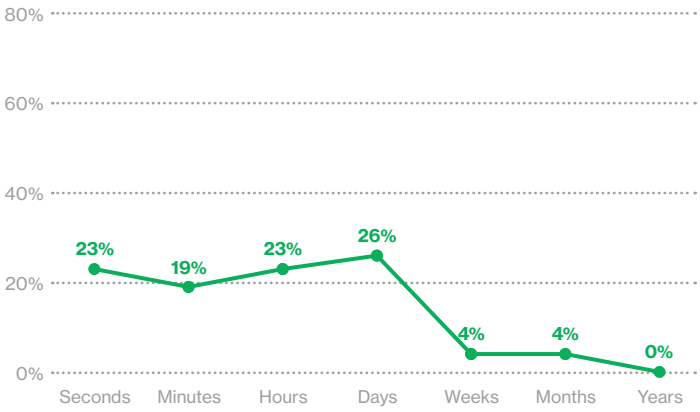


Figure #6: Time to Compromise within Cyber-Espionage breaches (2014-2020 DBIR; n=47)

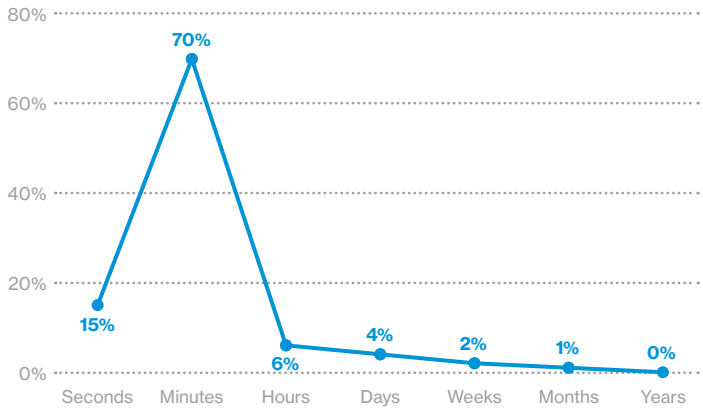


Figure #7: Time to Compromise within all breaches (2014-2020 DBIR; n=2,658)

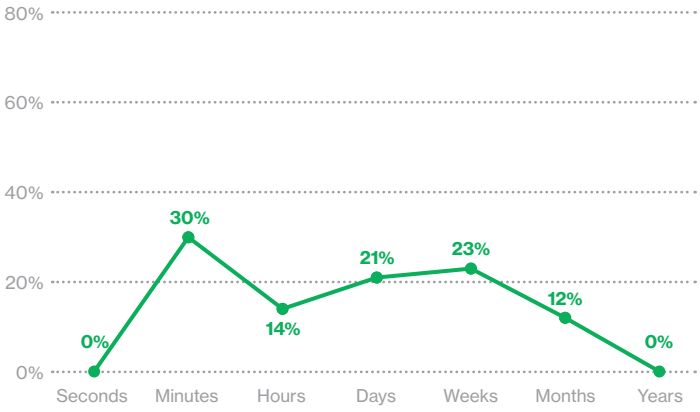


Figure #8: Time to Exfiltration within Cyber-Espionage breaches (2014-2020 DBIR; n=43)

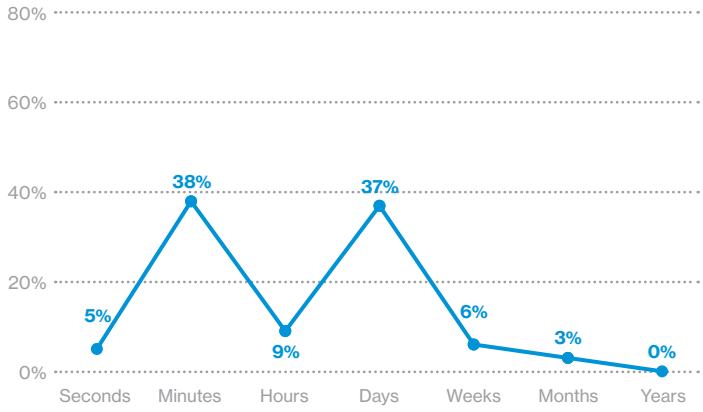


Figure #9: Time to Exfiltration within all breaches (2014-2020 DBIR; n=1,098)

Defender timelines

When we look closer, for cyberdefenders, we see the Time to Discovery within Cyber-Espionage breaches is months to years (69%, the sum of 30% and 39%) and the Time to Containment ranges from hours to weeks (64%, the sum of 10%, 25% and 29%).

The slow, methodical and lengthy process employed by threat actors versus the correspondingly plodding response from cyberdefenders speaks to the patience and complexity often accompanying Cyber-Espionage attacks.

Moreover, this is indicative of the threat actor's due diligence to not only understand their target's environment and cybersecurity posture, but also to leverage that knowledge to accomplish their objectives without detection.

Top controls

- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-12: Boundary Defense
- CSC-16: Account Monitoring and Control
- CSC-19: Incident Response and Management
- CSC-20: Penetration Tests and Red Team Exercises

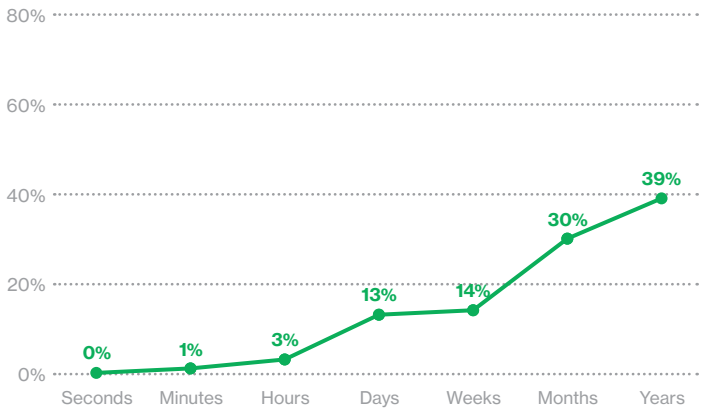


Figure #10: Time to Discovery within Cyber-Espionage breaches (2014-2020 DBIR; n=125)

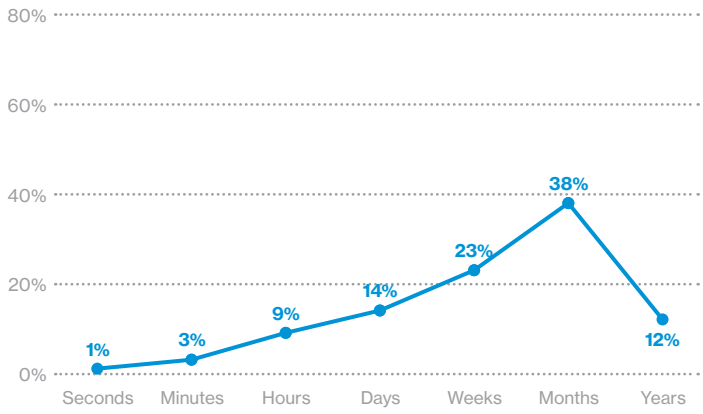


Figure #11: Time to Discovery within all breaches (2014-2020 DBIR; n=2,918)

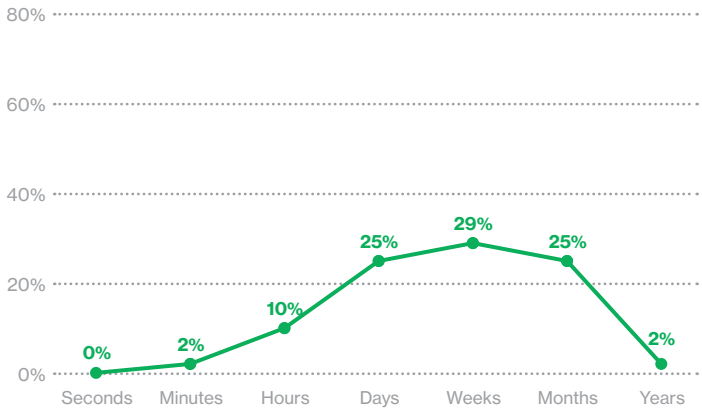


Figure #12: Time to Containment within Cyber-Espionage breaches (2014-2020 DBIR; n=51)

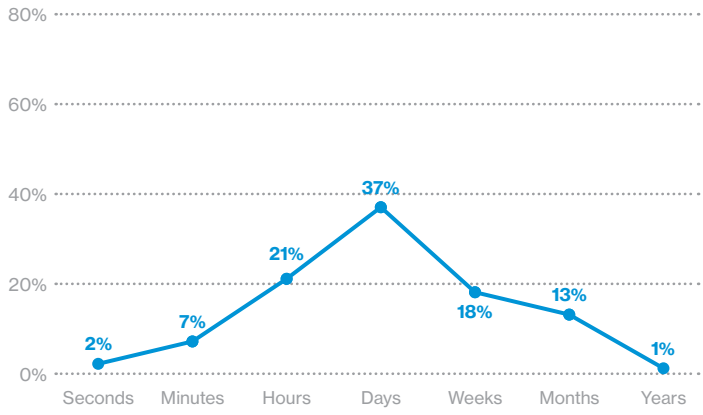


Figure #13: Time to Containment within all breaches (2014-2020 DBIR; n=789)

03

Targeted victims

NIST CSF Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.

A fundamental requirement for a solid information security posture is identifying assets before the adversary does. It's only when the unknowns become known that assets and data can be protected. After all, you don't know—and cannot protect—what you don't know.

Asset identification is a foundational part of the risk management process, which aims to define and prioritize risks for an organization. Risk managers often build matrices listing threats in order of severity. They also classify assets in terms of confidentiality, integrity and availability (referred to as the "CIA Triad"); consider the impact of security breaches on the organization; and estimate the likelihood of certain incidents.

Risk management also requires an organization to identify asset owners and asset access controls. Asset identification and risk management should align with the organization's business objectives to add value to the business and help gain buy-in from decision makers. For example, a business-driven risk management strategy could include:

- Defining objectives
- Identifying assets and threats
- Selecting and prioritizing targets
- Monitoring and detecting threats
- Responding and improving response capabilities

While it can be an overwhelming task to start from scratch, it's possible to develop a risk management process with smaller objectives by incorporating cyber threat intelligence and building and refining from there.

An organization that leverages cyber threat intelligence to prioritize Cyber-Espionage attacks as part of its risk management process can start by asking questions relevant to the organization, such as:

- How prevalent are Cyber-Espionage attacks compared to other cybersecurity attack patterns?
- Which Cyber-Espionage threat actors have been targeting other similar organizations? Based on this, how likely is the organization to be targeted?
- What assets and data are Cyber-Espionage threat actors targeting?
- What are the common TTPs of Cyber-Espionage threat actors?

If the answers to these questions point to lower risk, does it mean that in some industries, such as Healthcare or Accommodation, organizations should not be concerned with Cyber-Espionage? Not at all. This data shouldn't be analyzed without context. For example, while the number of Cyber-Espionage breaches may be lower in some industries, the impact of sensitive or proprietary data exposure on an organization in one of those lesser-targeted industries could be substantial.

Long story short: Just because your organization's industry has not been a typical target for Cyber-Espionage threat actors doesn't mean it won't be, can't be or hasn't been.

To contextualize information for an organization, it's not uncommon to deploy an internal cyber threat intelligence team or to wholly or partly outsource this capability.

Identification tips

- Identify assets, asset owners and asset access controls as part of an effective and comprehensive risk management strategy
- Align risk management with the organization's business objectives to add business value and gain buy-in from decision makers
- Leverage cyber threat intelligence to help prioritize Cyber-Espionage attacks as part of the risk management process
- Avoid complacency. Cyber-Espionage attacks can potentially impact all organizations—even those in lesser-targeted industries

VERIS and the Center for Internet Security (CIS) Critical Security Controls (CSCs), as well as the VERIS Common Attack Framework (VCAF)—a VERIS-to-MITRE ATT&CK® Framework introduced in the 2020 DBIR—are publicly available resources for formalizing incident and threat data. VERIS helps categorize security incidents, while CIS CSCs help focus on cybersecurity controls.

Risk analysis, asset identification and incident classification can inform the appropriate measures for preventing, mitigating, detecting and responding to threat actors while also maintaining the ability to meet organizational business objectives.

Regions

For the 2014-2020 DBIR timeframe, we see Cyber-Espionage breaches occurring most often in the Asia-Pacific (APAC) region (42%), followed by the Europe, Middle East and Africa (EMEA) region (34%), and North America (NA) (23%) region. This contrasts sharply with all breaches for this same timeframe, as NA (65%) dominates, followed by APAC (17%) and EMEA (16%).

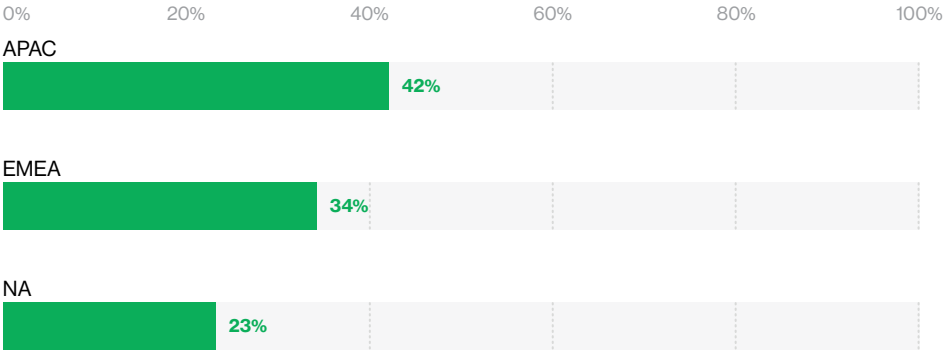


Figure #14: Cyber-Espionage breaches by region (2014-2020 DBIR; n=597)

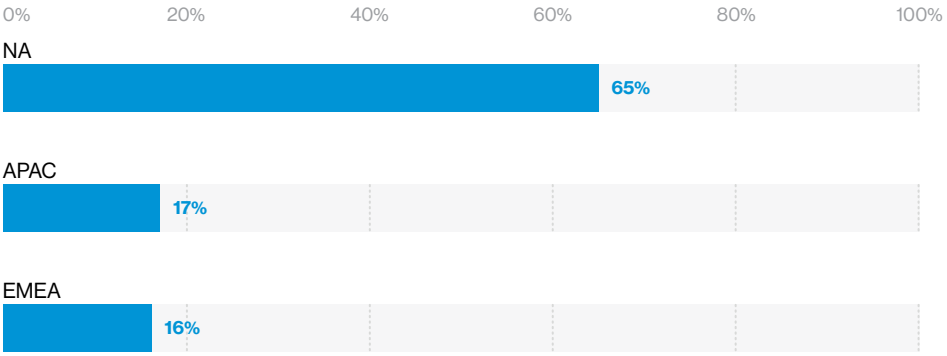


Figure #15: All breaches by region (2014-2020 DBIR; n=6,780)

Industries

Overall Cyber-Espionage breaches within select industries

One way to identify industries impacted by Cyber-Espionage attacks is by examining overall Cyber-Espionage breach numbers.

When we look at how the industries that were featured in the 2020 DBIR fared when it comes to Cyber-Espionage breaches, we can see that some were more strongly impacted than others. In particular, Public (31%), Manufacturing (22%) and Professional (11%) topped the list for Cyber-Espionage breaches.

This is a good time to point out that the DBIR dataset can only tell us what the DBIR dataset knows. The DBIR dataset consists of successful, reported and known data breaches (and cybersecurity incidents). It doesn't cover undiscovered, unreported or uncollected data (i.e., data originating outside of the 81 contributors to the 2020 DBIR).

While we have included more detailed, industry-specific Cyber-Espionage profiles in "Appendix B: Industry dossiers," here we provide insight into seven industries. These sectors are the most impacted by Cyber-Espionage breaches over the 2014-2020 DBIR timeframe and have sufficient content for analysis Industry (NAICS #): Education (61), Financial (52), Information (51), Manufacturing (31-33), Mining + Utilities (21+22), Professional (54) and Public (92).

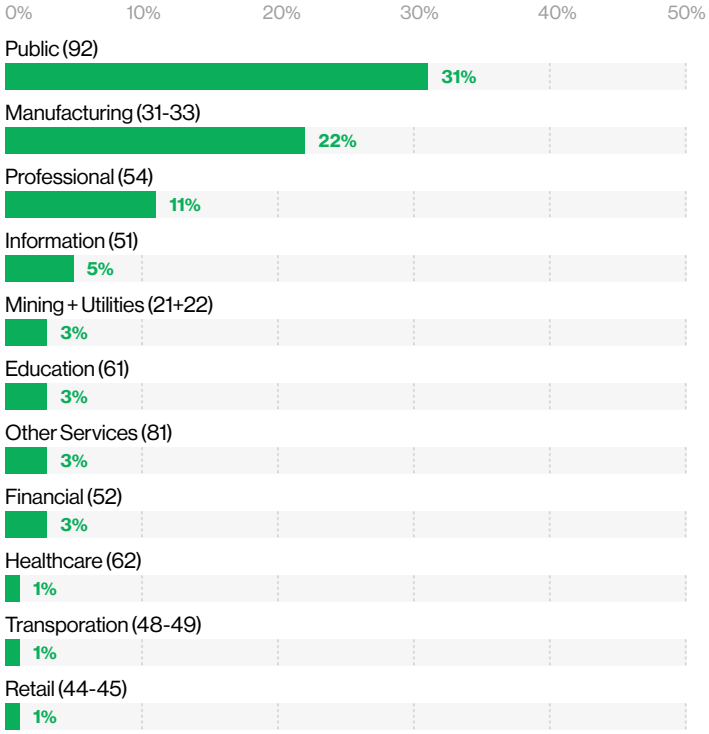


Figure #16: Cyber-Espionage breaches within select industries (2014-2020 DBIR; n=1,580)

Cyber-Espionage breaches within all breaches of select industries

Another way to look at industries impacted by Cyber-Espionage attacks is the number of Cyber-Espionage breaches within all breaches. For the 2014-2020 DBIR timeframe, we see Manufacturing (35%), Mining + Utilities (23%), Public (23%), Professional (17%), Education (8%), Information (7%) and Financial (2%) for percentage of Cyber-Espionage breaches within all breaches by industry.

We include more detailed, industry-specific Cyber-Espionage profiles in "Appendix B: Industry dossiers." Here we provide insight into Breaches by pattern, Cyber-Espionage within all breaches, Actors within Cyber-Espionage, Actions within Cyber-Espionage, Assets within Cyber-Espionage and compromised data within Cyber-Espionage for these seven industries.

Note: In Figure #16 and Figure #17, numbers in parentheses after each industry correspond to the 2-digit NAICS #.

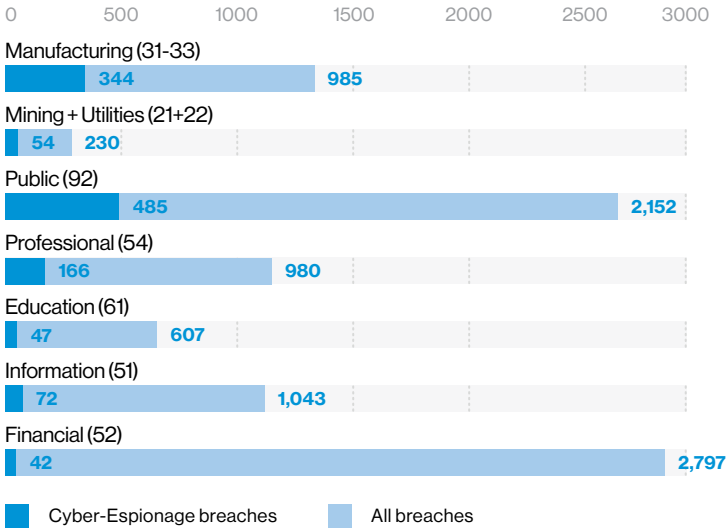


Figure #17: Cyber-Espionage breaches within all breaches of select industries (2014-2020 DBIR)

04

Essential Elements of Friendly Information

NIST CSF Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

Sophisticated threat actors often use stealthy methods to perpetrate Cyber-Espionage attacks. These methods can include utilizing compromised administrative credentials or leveraging dual-use tools that blend in with the environment.

These threat actors also deploy custom zero-day malware, which antivirus or other alerting software cannot detect. From our experience, Cyber-Espionage attacks—using sophisticated techniques; taking steps to avoid detection; and having specific, targeted objectives—tend to be considerably more difficult to detect and investigate than other breaches. Nevertheless, there are ways to protect against them even without specific knowledge of their custom/zero-day nature.

Access control

With administrative permissions and a flat (i.e., unsegmented) network, a threat actor has the freedom to roam. Even in segmented networks, a threat actor can find their way to the coveted data utilizing mapping and other dual-use tools. Network segmentation, strict access controls, layered security (the more access controls the better), a least-privilege practice and multifactor authentication for lateral movement into critical data areas can all help safeguard against Cyber-Espionage attacks.

Awareness and training

As seen in the 2020 DBIR, Cyber-Espionage attacks rely heavily on Social and Malware combined vectors, using Phishing in 81% of the incidents and some form of Malware in 92%. Training end users to recognize and report social attacks, such as phishing or pretexting, can help reduce poor outcomes related to Cyber-Espionage attacks.

Data security

Secure the data that is most valuable and sought after by cyber threat actors. Compile a critical data inventory and implement access controls and monitoring to ensure that data is safe.

Processes and procedures

Appropriately crafted corporate processes and procedures can help protect sensitive data. These should cover everything from ensuring that user devices are protected with encryption and strong passwords to restricting the use of public Wi-Fi and determining how sensitive data should be securely transmitted. Security practices should ensure safe and closely controlled access to potentially vulnerable data.

Maintenance

Cyber-Espionage risk mitigation is far from a set-it-and-forget-it strategy. Regular maintenance should be performed to ensure that employees follow proper cybersecurity measures and procedures so that data is protected.

Protective technology

Some Cyber-Espionage protective measures can be automated. Data Leakage Prevention (DLP) solutions send alerts when data leaves the network. These solutions also offer a large variety of features, such as detecting or blocking data copied to external locations, sent by email, or shared using file-sharing apps and sites; preventing protected data from being printed; and more. DLP solutions can even help identify unencrypted data destinations.

Protection tips

- Safeguard against Cyber-Espionage attacks with network segmentation, strict access controls, layered security, a least-privilege practice and multifactor authentication for lateral movement into critical data areas
- Train end users to recognize and report social attacks, such as phishing or pretexting
- Compile a critical data inventory and implement access controls and monitoring to ensure that data is safe
- Implement DLP solutions to detect and prevent sensitive data from being exported, shared or copied

Attributes

Compromised Attributes

In the 2014-2020 DBIR timeframe, for both Cyber-Espionage breaches and all breaches, the top compromised Attribute is Confidentiality (100%). This is by definition. For an incident to meet the VERIS requirement for breach classification, it has to exhibit a confirmed data compromise, which equates with Confidentiality. Thus, all Cyber-Espionage breaches impact the Confidentiality attribute.

Integrity (95%) and Availability (1%) follow Confidentiality for Cyber-Espionage breaches. Integrity, because Social actions impact the person targeted (Alter behavior), and Malware actions impact the asset where it was installed (Software installation). These two are among the favorite TTPs of the Cyber-Espionage threat actor. In contrast, most of these attacks do not affect the availability of the asset—as that would likely lead to faster discovery of the threat actor.

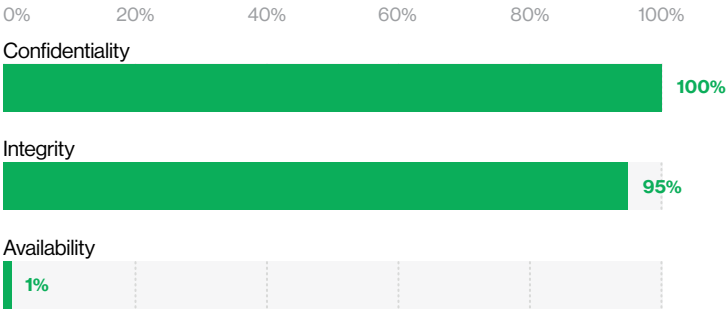


Figure #18: Compromised Attributes within Cyber-Espionage breaches (2014-2020 DBIR; n=1,580)

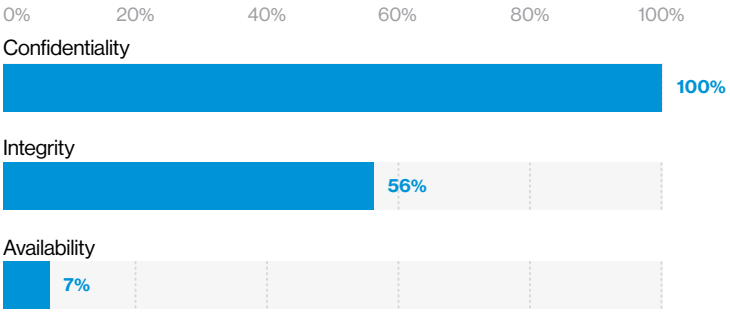


Figure #19: Compromised Attributes within all breaches (2014-2020 DBIR; 16,090)

CIA Triad

For VERIS, compromised asset security attributes are based on the expanded CIA Triad, which includes confidentiality/possession, integrity/authenticity and availability/utility. Multiple attributes can be affected for any one asset, and each attribute contains different metrics.

Compromised Attribute varieties

When we look at Cyber-Espionage breaches and the top compromised Attribute varieties for the 2014-2020 DBIR timeframe, we see Software installation (Integrity) (91%), Alter behavior (Integrity) (84%) and Secrets (Confidentiality) (73%) as top compromised Attribute varieties.

In comparing all breaches to Cyber-Espionage breaches during the 2014-2020 DBIR timeframe, we see Software installation (Integrity) (43%) and Alter behavior (Integrity) (32%) as first and second for all breaches, which parallels Cyber-Espionage breaches, albeit at a much lower percentage. For all breaches, the next two compromised Attribute varieties are Credentials (Confidentiality) (29%) and Personal (Confidentiality) (28%), whereas for Cyber-Espionage breaches, the third and fourth most compromised Attribute varieties are Secrets (Confidentiality) (73%) and Internal (Confidentiality) (29%).

Secrets and Internal compromised Attribute varieties ranking so high within Cyber-Espionage breaches comes as no surprise, as these are the top compromised Data varieties (see "Data" section of this report).

Top controls

- CSC-4: Controlled Use of Administrative Privileges
- CSC-5: Secure Configuration for Hardware and Software
- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-8: Malware Defenses
- CSC-13: Data Protection
- CSC-16: Account Monitoring and Control

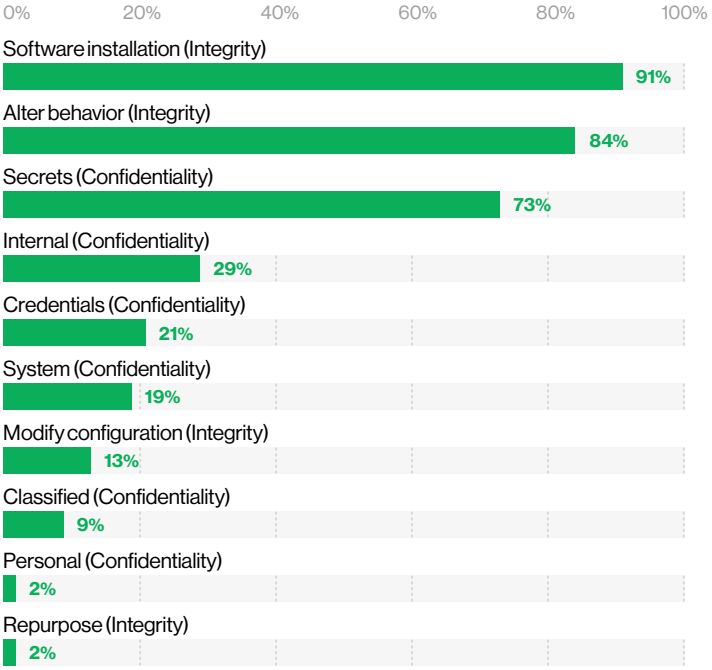


Figure #20: Top compromised Attribute varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,571)

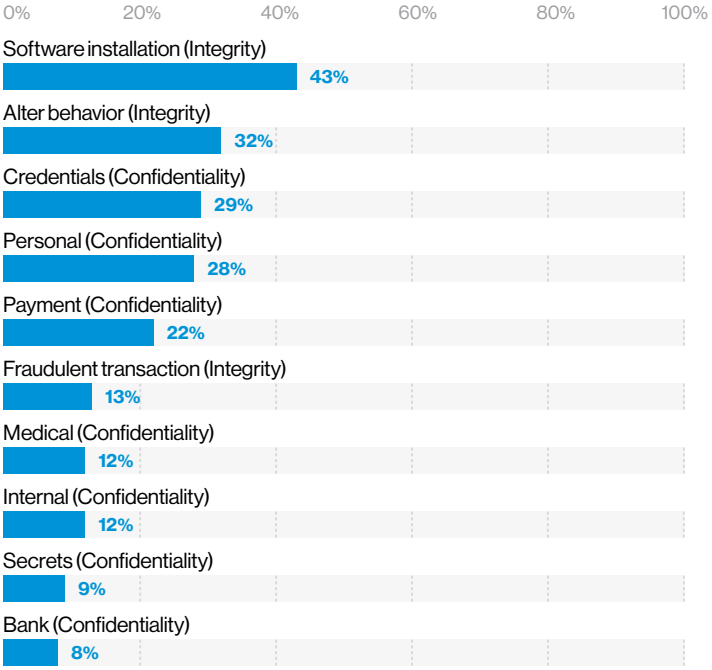


Figure #21: Top compromised Attribute varieties within all breaches (2014-2020 DBIR; n=14,736)

Assets

Compromised Asset varieties—Short term

At a high level, top compromised Assets (n=115) for the 2020 DBIR timeframe are User Device (87%), Person (82%) and Server (26%). Interestingly, if we look closer at compromised Asset varieties for this timeframe, we see contemporary assets being affected more so than over the 2014-2020 DBIR timeframe.

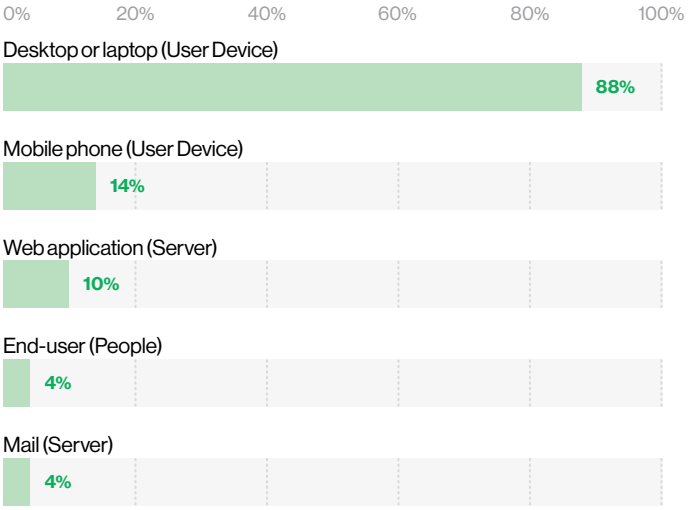


Figure #22: Top compromised Asset varieties within Cyber-Espionage breaches (2020 DBIR; n=113)

The top compromised asset varieties for the 2020 DBIR timeframe in Cyber-Espionage breaches were Desktop or laptop (88%), Mobile phone (14%) and Web application (10%). For all breaches, these are Web application (43%), Desktop or laptop (31%) and Mail (21%). The Desktop or laptop, Mobile phone and Mail compromised Assets are likely due to Cyber-Espionage attacks starting with Social action.

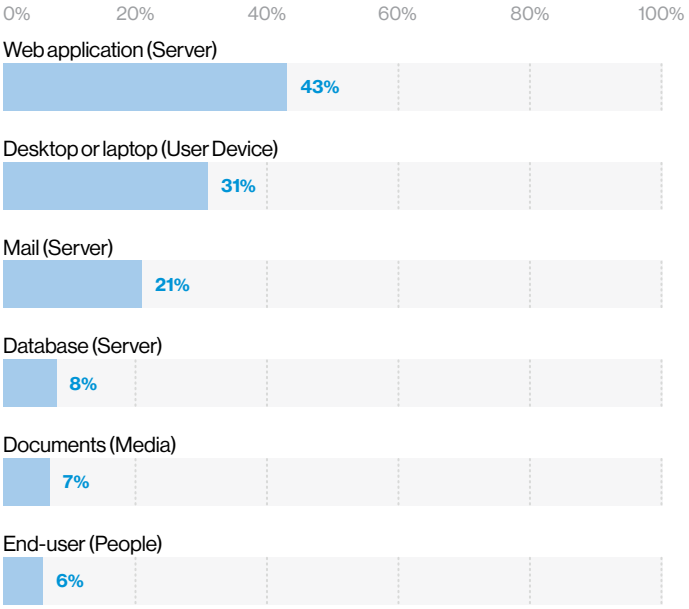


Figure #23: Top compromised Asset varieties within all breaches (2020 DBIR; n=2,667)

Compromised Asset varieties—long term

Also, at a high-level, for the 2014-2020 DBIR timeframe, top compromised Assets (n=1,492) are Person (88%), User Device (83%) and Server (34%). When we look at compromised Asset varieties impacted by Cyber-Espionage breaches for this timeframe, we see Desktop or laptop (89%) and Desktop (80%) leading the pack, with Mobile phones (9%) a very distant third followed by Router or switch (8%).

For top compromised Asset varieties within all breaches, Desktop or laptop (32%), Web application (30%) and Desktop (24%) are listed as the top three, with Point of Sale (POS) controller (13%), POS terminal (12%) and Database (12%) vying for fourth place.

Web application, POS controller and POS terminal speak to the wide variety of Assets that threat actors target in the all breaches category. The Desktop or laptop, Desktop and Mobile phone varieties speak to social engineering—a popular threat action for threat actors associated with Cyber-Espionage breaches as well as breaches in general.

Top controls

- CSC-5: Secure Configuration for Hardware and Software
- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-17: Implement a Security Awareness and Training Program
- CSC-18: Application Software Security
- CSC-20: Penetration Tests and Red Team Exercises

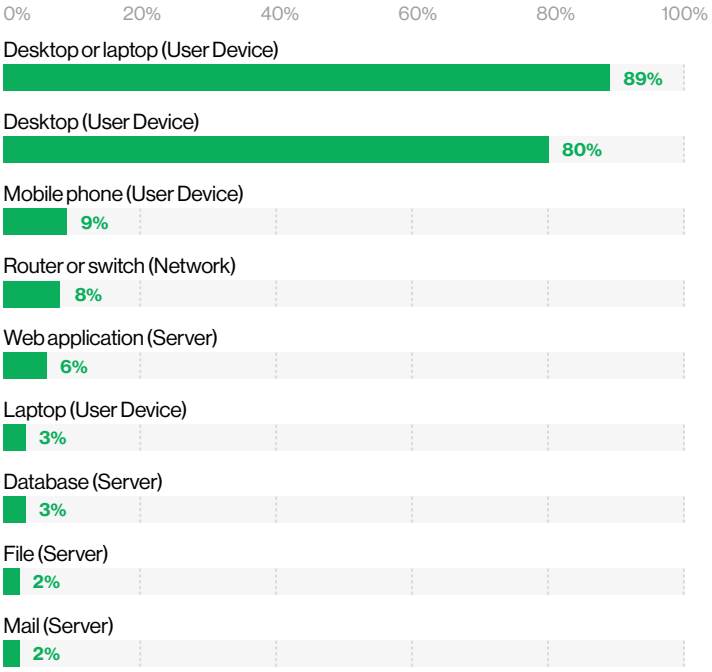


Figure #24: Top compromised Asset varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,297)

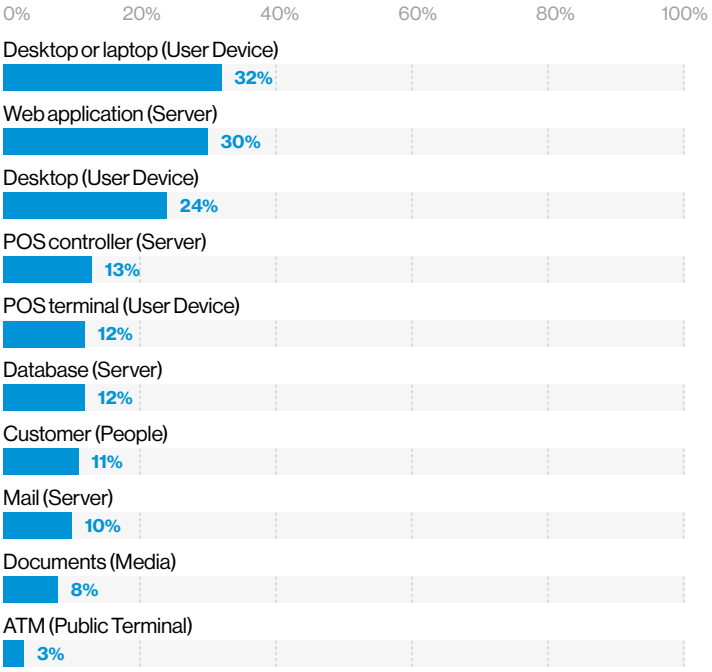


Figure #25: Top compromised Asset varieties within all breaches (2014-2020 DBIR; n=13,217)

Assets and vulnerabilities

Critical assets

Significant research and analysis have focused on developing models aimed at helping organizations identify, measure and monitor the criticality of their assets. These models, such as the NIST IR 8179 (Criticality Analysis Process Model), are aimed at helping organizations better identify, understand and protect their assets.

This approach focuses on not only the asset's criticality to business operations but also the potential damage/impact of the loss of the asset. However, many such analytical models tend to view assets through a single lens and don't necessarily assess them through the prism of Cyber-Espionage.

This nuance is particularly important when two factors are considered. First, while the overall significance of Cyber-Espionage as a whole is relatively low and appears to be decreasing (as indicated in the 2020 DBIR), a by-industry breakdown reveals a more nuanced picture.

Reported instances of Cyber-Espionage breaches have been concentrated in certain industries (such as Manufacturing, Mining + Utilities and Public), while other industries (Construction, Real Estate) reported none at all (note that this doesn't necessarily mean none occurred or that there is no risk for those particular industries, just that none were reported where we had visibility). This implies that any organization's critical asset/sensitive data management strategy may need to adjust to the Cyber-Espionage risk associated with their particular vertical.

It's reasonable to assume that the overall Cyber-Espionage rate suffers from chronic underreporting. Other motivations (i.e., Financial) lend themselves toward having a more clearly identifiable end state. Cyber-Espionage, on the other hand, can potentially be associated with longer attack timelines and potentially unending exploitation.

In self-assessing critical assets and sensitive data, organizations need to ensure that their assessment criteria account for the possibility of Cyber-Espionage. Specifically, their model should address:

1. Overall Cyber-Espionage risk
2. Assets/data susceptible to Cyber-Espionage
3. Safeguards and monitoring to alert on Cyber-Espionage attacks
4. Preventative measures for Cyber-Espionage, such as:
    a. Continuous critical asset/sensitive data identification, protection and monitoring
    b. Cyber threat intelligence/dark web research/ threat hunting
    c. Insider Threat Program
    d. Competitive landscape awareness (i.e., unexpected loss of competitive advantage)

Targeted vulnerabilities

Vulnerabilities occupy a huge amount of mindshare in information security. Security researchers, independent hackers, nation-state actors, organized criminal groups, customers and even employees discover thousands of vulnerabilities every year (https://www.cvedetails.com/browse-by-date.php).

Some discovered vulnerabilities are reported responsibly and some (including their exploit code) are stashed away for a multitude of reasons (most of which are nefarious in nature). Most application software and firmware vendors have established formal programs to release patches on a periodic basis, or on an emergency basis depending on the severity of the vulnerability.

Periodically, organizations discover scores of known vulnerabilities within their infrastructure using typical vulnerability scanning tools and patch them based on risk assessment. However, threat actors leverage a relatively small percentage of these vulnerabilities in breaches, as you can see in the diagram below from the 2020 DBIR.

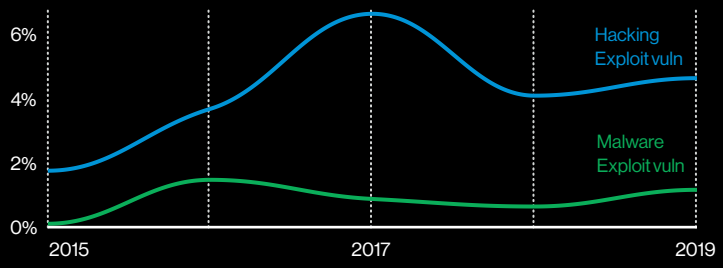


Figure #26: Vulnerability exploitation over time in breaches

Zero-day vulnerability exploits—those security weaknesses not disclosed to vendors or developers—make tackling vulnerabilities even harder for impacted organizations. More often than not, the exploitation of such vulnerabilities doesn't leave credible evidence on the system (although there may be some circumstantial evidence left somewhere else).

There were times when zero-day vulnerabilities were for sale on the dark web. Due to recent enforcement actions by some marketplace operators, the not-so-good researchers have become less active and have possibly moved to other avenues for financial gain and other motives. We've seen—and continue to see—organized crime syndicates or nation-state and state-affiliated actors use zero-day vulnerabilities to exploit systems for nefarious purposes.

It is important to realize that vulnerabilities are here to stay, and the typical patch-cycle mentality cannot solve this problem. A multilayered approach consisting of several controls, such as robust risk management, use of strict least-privilege principle, application whitelisting, threat hunting and deception-based detection techniques, can help protect against the invisible monster.

Data

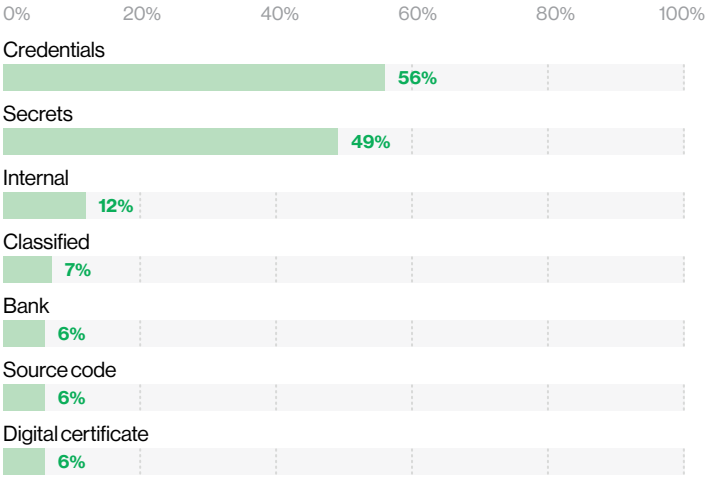


Figure #27: Top compromised Data varieties within Cyber-Espionage breaches (2020 DBIR; n=110)

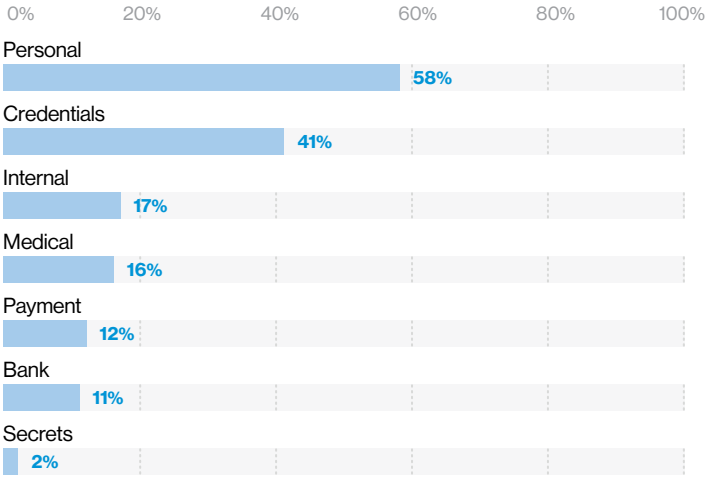


Figure #28: Top compromised Data varieties within all breaches (2020 DBIR; n=3,373)

Cyber-Espionage breaches—Short term

The top compromised Data varieties for Cyber-Espionage breaches for the 2020 DBIR timeframe are data types that fall outside regulatory reporting requirements: Credentials (56%), Secrets (49%), Internal (12%) and Classified (7%), with Bank (6%), Source code (6%) and Digital certificate (6%) all statistically tied for fifth. In addition, much like the 2014-2020 DBIR timeframe, this makes sense for Cyber-Espionage breaches, as threat actors would seek these Data varieties for competitive gain.

All breaches—Short term

When we look at compromised Data varieties for the 2020 DBIR timeframe, a different story emerges for all breaches. We find Personal (58%), Credentials (41%), Internal (17%) and Medical (16%) as the top compromised Data varieties for all breaches, with Payment (12%) and Bank (11%) bringing up the rear. With the exception of Credentials, these Data varieties align with regulatory reporting for data breaches in general.

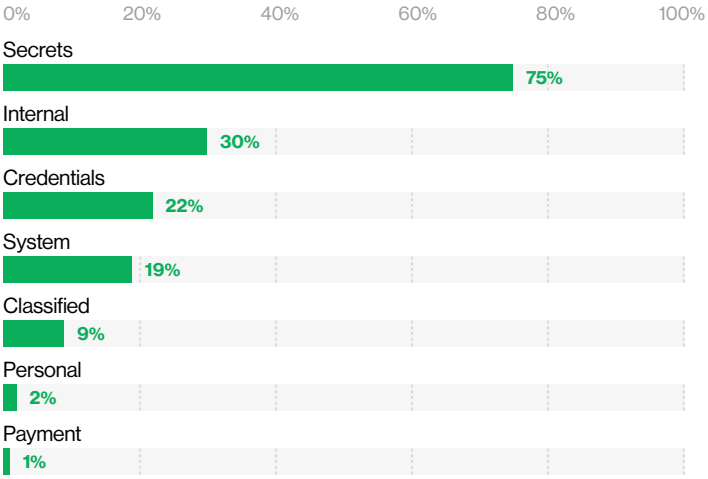


Figure #29: Top compromised Data varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,526)

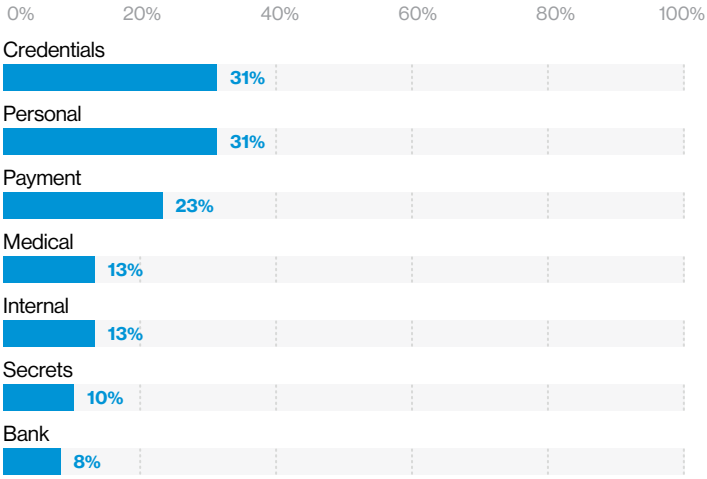


Figure #30: Top compromised Data varieties within all breaches (2014-2020 DBIR; n=13,657)

Cyber-Espionage breaches—Long term

For compromised Data varieties in the 2014-2020 DBIR timeframe, we find that Cyber-Espionage threat actors seek these data types most frequently: Secrets (75%), Internal (30%), Credentials (22%), System (19%) and Classified (9%). This makes sense for Cyber-Espionage breaches, as these data types are ostensibly sought after by threat actors targeting sensitive/propriety/classified information.

All breaches—Long term

For all breaches, we see Credentials (31%), Personal (31%), Payment (23%), Medical (13%) and Internal (13%) as more valuable targets for compromised Data varieties. Moreover, this is understandable because, with the exception of Credentials and Internal, these Data varieties fall within the realm of mandatory regulatory reporting requirements for breaches in general.

Top controls

- CSC-4: Controlled Use of Administrative Privileges
- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-13: Data Protection
- CSC-14: Controlled Access Based on the Need to Know
- CSC-16: Account Monitoring and Control
- CSC-17: Implement a Security Awareness and Training Program

05

Threat actors

NIST CSF Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

The 2016 DBIR reported that, in general, victim organizations seldom detect data breaches. Rather, external sources are more likely to make the discovery. This trend remains the same even years later in the 2020 DBIR and is especially true for Cyber-Espionage breaches in the 2014-2020 DBIR timeframe. These breaches tend to allow the adversary to siphon as much information as possible from their victim for as long as possible while remaining undetected.

The questions for organizations in 2016 were how could an organization improve its Time to Discovery trend? How can it avoid relying mostly on external sources that lie beyond its control? How can it detect intrusions as they occur if not before they occur? These questions led to innovation in the detection-technology space, which we cover later in the report.

However, despite some organizations adopting these new technologies, the problem remains. A possible explanation is that these new techniques often rely on the organization having first covered the basics, such as determining network activity baselines, defining cybersecurity incidents and specifying alert thresholds, which isn't always the case.

Before investing in new technology, an organization should verify that its cybersecurity foundations are solid. Security strategists can accomplish this by adopting the Capability Maturity Model (CMM) strategy, originally developed to improve software development processes. The CMM relies on measuring, controlling and regularly updating documentation and processes to limit the unknowns.

During VTRAC data breach investigations, crucial data is often unavailable. Gaps come in the form of missing log files, undocumented systems, poor data accessibility, network traffic flows, operational practices, and underestimated or under-documented data-sensitivity issues.

This lack of information not only hinders a data breach investigation and subsequent incident response efforts, but it also creates golden opportunities for the adversary to easily find and access potentially sensitive information.

One way to address the gap between compromise and detection speed in breaches involving adversaries using evasion tactics is to enhance detection capabilities while keeping up with new evasion techniques. Organizations should develop defensive capabilities, such as counterespionage deception techniques, specifically to reflect these emerging evasion TTPs.

The last few years have seen the development and enhancement of both network and host detection and prevention systems. These have been re-envisioned as Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) solutions. Event and telemetry data from these systems typically roll up into Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions to trigger response and containment, eradication, remediation and recovery actions.

These technologies have moved beyond outdated signature-based detection toward behavior-pattern detection enhanced with cyber threat intelligence, automation, and machine learning or artificial intelligence (i.e., statistical analysis and anomaly detection). Solutions also facilitate proactive analysis, often referred to as "security health checks."

It's also important to remember that having the best technology in your arsenal doesn't help unless you have equally mature processes as well as suitably skilled and trained personnel to manage it effectively.

Detection tips

- Verify that the organization's cybersecurity foundations are solid by adopting the CMM strategy
- Ensure the availability of crucial data by reducing the incidence of missing log files, undocumented systems, poor data accessibility, network traffic flows, operational practices, and underestimated or under-documented data-sensitivity issues
- Develop counterespionage detection techniques that evolve to reflect emerging evasion TTPs
- Move toward behavior-pattern detection enhanced with cyber threat intelligence, automation, and solutions based on machine learning or artificial intelligence
- Leverage experienced security professionals to manage advanced technology

Discovery methods

In terms of top Discovery methods for Cyber-Espionage breaches in the 2014-2020 DBIR timeframe, we see the top two methods as Suspicious traffic (48%) and Antivirus (23%), with Emergency response team a distant third (7%). This contrasts sharply with the top Discovery methods for all breaches for the same timeframe, in which we see Law enforcement (28%), Fraud detection (19%) and Customer (15%), respectively, at the top.

When we put on the threat actor "motive filter," this makes sense. Data breaches overall are dominated by the Financial motive, whereas Cyber-Espionage breaches align with the Espionage motive, which is much more targeted in its approach.

A factor at play here is that the Financial motive threat actor has to contend with the Payment Card Industry (PCI) Common Point of Purchase (CPP) fraud detection system. There is no corresponding detection service looking for theft of trade secrets, which contributes to longer discovery times.

Top controls

- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-8: Malware Defenses
- CSC-12: Boundary Defense
- CSC-19: Incident Response and Management

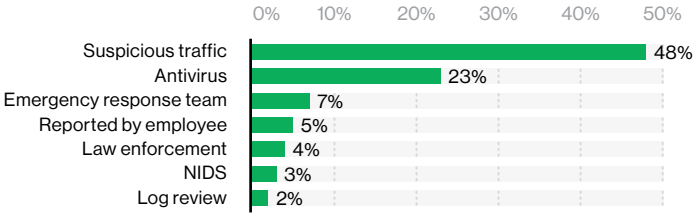


Figure #31: Top Discovery methods for Cyber-Espionage breaches (2014-2020 DBIR; n=408)

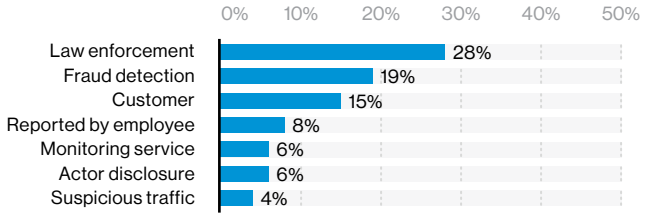


Figure #32: Top Discovery methods for all breaches (2014-2020 DBIR; n=7,025)

Actors

Actors over time

For the 2014-2020 DBIR timeframe, External actors have dominated Actor types, ranging from 69% to 88% over this timeframe, with Internal actors a distant second, ranging from 12% to 34% over the same timeframe.

When we look at Cyber-Espionage breaches for the 2014-2020 DBIR timeframe, External actors (State-affiliated, Nation-state, Organized crime, Former employee and Competitor combined) are at 100%. This makes sense, as within VERIS, Cyber-Espionage threat actors are coded as External actors in all breaches.

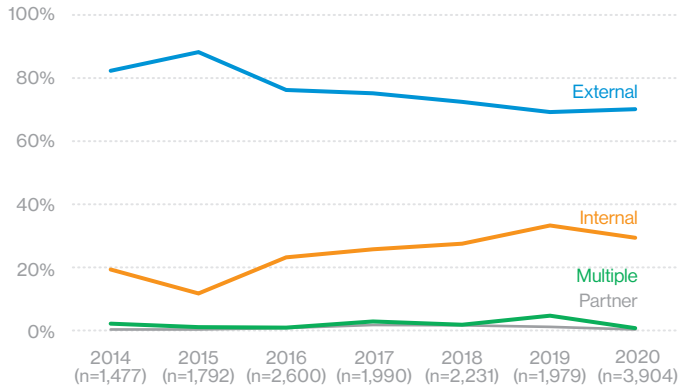


Figure #33: Actors over time for all breaches (2014-2020 DBIR)

Actor varieties

Attempting to identify Actor varieties is an immense challenge in cyberspace. Threat actors go to great lengths to maintain anonymity, obfuscate their activities and impede identification using bogus IP addresses (even MAC addresses can be spoofed), domain names, email addresses, file names and malware tools, among other indicators of compromise (IoCs).

The top Actor varieties in Cyber-Espionage breaches for the 2014-2020 DBIR timeframe are State-affiliated (85%), Nation-state (8%), Organized crime (4%) and Former employee (2%). This should be no surprise, as State-affiliated and Nation-state threat actors align more with the Espionage motive.

For all breaches during this same timeframe, we see a bit of a different picture, with Organized crime (59%) dominating the list of Actor varieties, followed by State-affiliated (13%), Unaffiliated (7%), and then End-user (6%) and System admin (4%). Organized crime has been identified mainly with the Financial motive, one that continues to dominate our DBIR dataset for all breaches over the years.

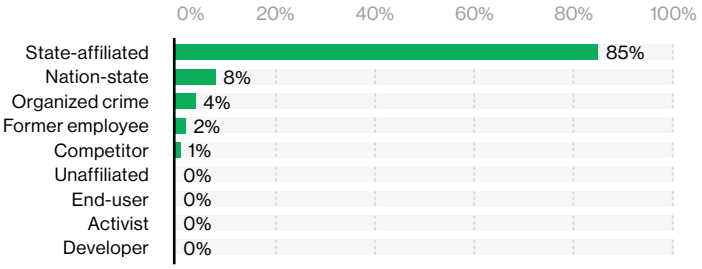


Figure #34: Actor varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,435)

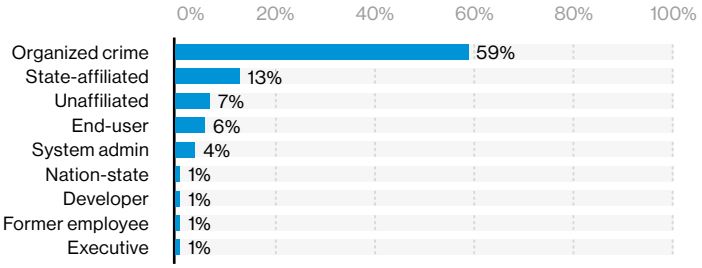


Figure #35: Actor varieties within all breaches (2014-2020 DBIR; n=9,077)

Threat actors defined

Threat actors are entities that cause or contribute to a data breach or cybersecurity incident. External actors originate from outside the organization and its network of partners and typically have no trust or privilege granted to them. Internal actors originate from within the organization and enjoy some level of trust and privilege. Partner actors include any third party that shares a business relationship with the organization and thus enjoys some level of trust and privilege.

The labyrinth: How attribution could be wrong

Digital forensic investigations should ideally answer the five Ws (who, what, where, when and why) and one H (How) questions. However, challenges related to the availability and granularity of detail in evidentiary data can leave many questions unanswered.

Cyberattack attribution in particular is meant to address the "Who" and "Why" questions. Investigators focus on threat actor TTPs, consult cyber threat intelligence reports and review IoCs to root out perpetrators and mount a defense.

However, IoCs such as IP addresses, domain names, file names, malware behavior and binary code sections can be misleading. Consequently, investigators shouldn't rely only on these to make a cyberattack attribution.

The current geopolitical climate, recent pandemic and heightened trade tensions provide a conducive environment for cyberattack misattribution. This is especially true for Cyber-Espionage attacks that typically involve tactics such as leveraging covert TTPs and "false flags." Threat actors associated with these attacks are attempting to thwart detection and response efforts, as well as conceal attack attribution for political and national security purposes.

On top of that, Tor (The Onion Router) networks, the dark web, business infrastructures that lack security, and privacy legislations in certain countries further complicate attribution. Using cryptocurrencies (especially altcoins, such as Monero, offering anonymity) or services, such as coin mixers, makes tracing the origin of attacks more difficult.

Another very important obstacle is the extreme difficulty of prosecuting cross-border cybercriminals, which nation-state actors inherently protect. The lack of local legal statutes, regulations or reliable evidence lessens deterrence and may even motivate threat actors.

Finally, it should be noted that attribution is a multidimensional challenge. Attribution—aside from forensic evidence—depends on various types of intelligence, including forensics evidence; Technical Intelligence (TECHINT); Human Intelligence (HUMINT); Signals Intelligence (SIGINT); Open Source Intelligence (OSINT); and adversarial tradecraft (i.e., TTPs), infrastructure and intent. All dimensions must align for sound and reliable attribution.

Motives

Motives over time

For the 2014-2020 DBIR timeframe, annually, we see Financial motive underlying breaches between 67% and 86% of the time and Espionage motive as the driver between 10% and 26% of the time.

Given their nature (e.g., stealthy tactics, specific targeting), Espionage attacks can be difficult to detect and identify as an actual Espionage-related attack (given scant IoCs and other details).

Whereas Financial attacks—if not detected while occurring or soon thereafter—eventually become apparent when money goes missing. At that point, the Financial motive, if not already ascertained, can be determined.

Motives

Within the dataset that shows all breaches, for both the 2020 DBIR and 2014-2020 DBIR timeframes, we see Financial motive as the overwhelming Actor motive (86% and 76%, respectively), with Espionage the second highest motive (10% and 18% respectively).

Actor motives consolidated in "The Rest" (6%) for the 2014-2020 DBIR timeframe include Fun (3%), Grudge (1%), Convenience (1%) and Ideology (1%).

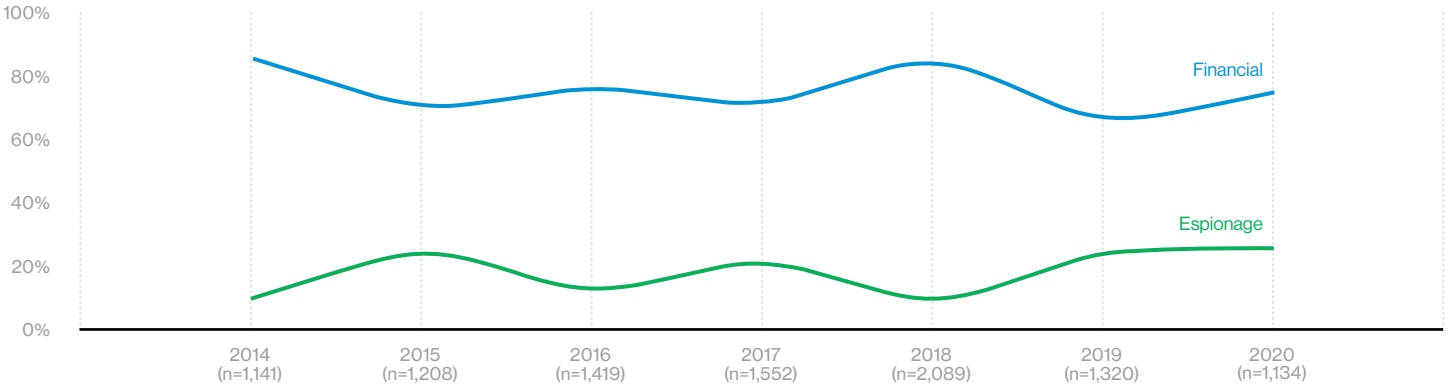


Figure #36: Actor motives over time within all breaches (2014-2020 DBIR)

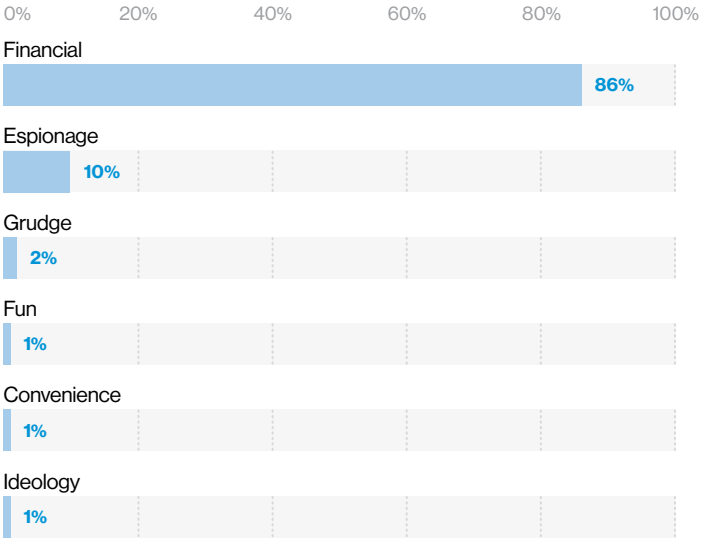


Figure #37: Actor motives within all breaches (2020 DBIR; n=1,141)

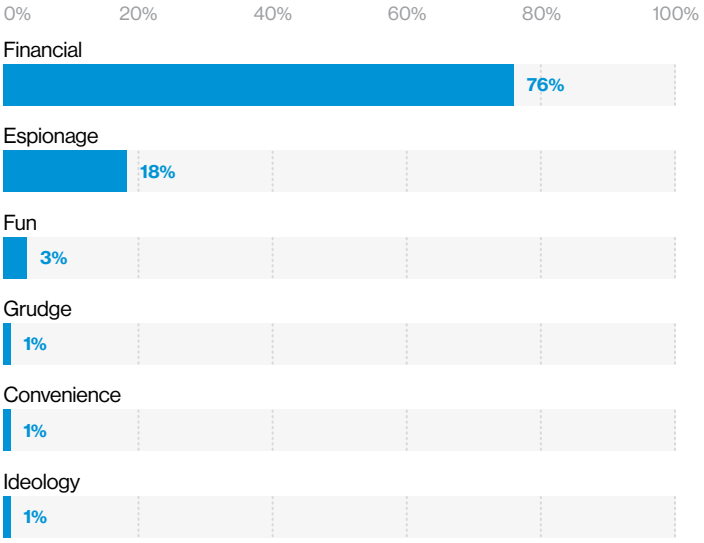


Figure #38: Actor motives within all breaches (2014-2020 DBIR; n=9,863)

Proactive defense: The best defense is a great offense.

Threat hunting | Behavioral analysis

Advanced threat actors attempt to blend in to evade automated cyberdefense measures. With the rise of zero-day and fileless attacks, it's harder than ever to protect endpoints with confidence. In addition, preventing and detecting these attacks can be a huge drain on organizational resources.

Compromise happens within minutes to hours, as we have seen consistently over the years in the DBIR. This is mainly attributable to the use of email and web-based threat vectors coupled with heavily automated attacks (nowadays also powered by machine learning).

Visibility and detection speed techniques play a very important role in this never-ending battle against cyberattacks. It is imperative that detection measures be a combination of signature- and behavior-based techniques. One cannot manage or defend against unknown threats using traditional means. Effective, efficient and multilayered threat hunting can help give you a significant advantage in detecting these unknowns.

Threat hunting consists of:

1. Making hypothesis-driven exercises
2. Proactively and reactively searching for threat actor activities
3. Effectively eliminating, or at least reducing, false negatives (indicators that signature-based detection approaches can overlook)
4. Assuming that threat actors are already present in the infrastructure
5. Placing a strong focus on indicators of attack (IoAs) combined with IoCs
6. Prioritizing overall threat types and looking for the most dangerous ones first

Additional actions

Consider taking these additional protective measures:

- Assign all users separate, unique accounts. Don't use generic or shared accounts or passwords
- Block outbound, unrestricted internet access from server infrastructure. This is intended to prevent adversaries from exfiltrating data to known or unknown IP addresses and using services, protocols or ports in an unauthorized manner
- Create adequate network segmentation to separate virtual local area networks (VLANs) from internet-facing infrastructure, server farms, internal networks and administrator networks. Appropriate segmentation makes it difficult for an adversary to move laterally within the network
- Restrict PowerShell and other native scripting to only individuals with an acknowledged legitimate use and track the assignment of such privileges
- Prohibit interactive log-ons using service accounts or "break-the-glass" accounts. Implement a rule in the SIEM to trigger an alert to the security operations team whenever an attempt is made to log on to any system interactively using service accounts
- Require two-factor authentication for all administrative access to infrastructure components. This implementation will mitigate the impersonation risk and prohibit access using unauthorized credentials

06

Tradecraft

NIST CSF Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Investigating Cyber-Espionage breaches differs from researching cybersecurity incidents. Thus, incident responders and forensic investigators may not initially realize that an attack is targeted and the motive is intellectual property theft. It's only as the investigation progresses and the complexity of the attack becomes apparent that investigators take a slightly different approach.

Before the investigation, investigators collect technical information such as network topology. Investigators also interview network and system administrators to scope out the incident and identify possible intrusion channels. In addition, investigators collect in-scope volatile data and system images plus all associated logs from various sources, such as system (including PowerShell or System Monitor), SIEM and proxy logs.

Understanding how the incident was detected helps an investigator triage and scope, as Cyber-Espionage attacks generally involve multiple systems and other infrastructure components. In-scope data sources require periodic review and re-scoping throughout the IR lifecycle.

One key objective for a Cyber-Espionage investigation is to identify "patient zero" and determine how the adversary gained access to the infrastructure. Common methods of entry include exploiting an internet-facing application, applying brute force to an account, using phishing email to gain an initial foothold or compromising the human factor—trust.

During Cyber-Espionage investigations, it is common to find phishing (or targeted phishing) emails as the initial vector. These emails usually are well crafted (industry specific) to lure the recipients either to click a URL hosting a malicious or lookalike website, or to open an attachment that executes malicious software. In some cases, obtaining user credentials is the goal for follow-on use in the initial penetration.

Based on the information received from the impacted organization and the results of the initial analysis, the threat-intelligence team endeavors to identify an associated threat actor. By identifying its goals, capabilities and methods, the team can develop attack models—based on the most common and most lethal cybersecurity incidents—to prepare for and better respond to cybersecurity attacks.

When combined with organization profiling, unique risk identification is possible and can provide valuable assistance to the investigation to find in-scope compromised or affected infrastructure components.

Sometimes, the cyber threat intelligence team encounters stolen data and credentials being traded by cybercriminals, and this data is all the adversary needs for further attacks on an organization.

One key challenge faced during Cyber-Espionage investigations is the identification of compromised systems. Many Cyber-Espionage attacks are associated with advanced persistent attacks—multistaged attacks that involve lateral movement.

Identifying compromised assets or assets posing as intermediaries can be a challenge. Cyber-Espionage attacks employ specifically created malware that causes multiple layers of obfuscation and malware variants, making IoC-based detection within the enterprise environment difficult.

A further challenge is that Cyber-Espionage attacks often leverage legitimate credentials and legitimate dual-use tools, such as network mapping or remote access software already being used in the environment. This makes it extremely difficult to differentiate between malicious actions and legitimate administrative tasks.

To circumvent challenges, EDR and NDR solutions help identify abnormalities and build the IoCs necessary to locate affected systems and infrastructure components.

Response tips

- Learn how the incident was detected to help investigators triage the incident and scope the response
- Identify "patient zero" and determine how the adversary gained access to the organization's network infrastructure
- Search for common vectors, such as phishing (or targeted phishing) emails that lure recipients to execute malicious software
- Deploy EDR and NDR solutions to aid incident response

The sweetener: Honeypots, honeytokens, honeynets

A honeypot is a system, or several networked systems, that waits for unsolicited requests. More specifically, honeypots observe unsolicited activity, attract possible threat actors and document their methods. Honeypots are effective for discovering opportunistic attacks, large-scale probes or computer worms, brute force authentication, misconfiguration, vulnerability exploits and web application attacks.

Information security researchers use honeypot technologies for counterespionage attacks because they can mimic the organization's production environment but with fake believable data as bait.

The purpose of honeypot technology isn't only to detect a threat actor, but to also:

- Slow down the threat actor
- Lure threat actors away from sensitive data
- Collect information on the threat actor
- Gain visibility into gaps in perimeter defenses

Honeypot technology requires the organization to have fundamental information security controls already in place. To reach this higher maturity level, organizations should:

- Identify crown jewels that the threat actor would potentially seek
- Enable monitoring, logging, alerting and response processes in associated infrastructure
- Integrate information security infrastructure components
- Train employees on incident response
- Segment the network and be able to redirect traffic easily, if needed

Once the maturity requirements are fulfilled, the next step is to start small and scale up gradually. Similar to building an SIEM infrastructure, it is best to deploy deception solutions based on use cases. Start with a high-risk scenario you want to address and build from there.

The scenario can be based on either risk analysis or real incidents. When using real incident scenarios, it is important to leverage cyber threat intelligence.

Start with your top identified Cyber-Espionage risk. Determine how the sensitive data is stored (digital documents, database), where it is stored (file server, database server, web application) and what the data looks like.

If sensitive data is stored in documents, for instance, create realistic documents with fake data. Then consider using a honeytoken with a canary value that, if used, will trigger a security alert.

A honeytoken can be as simple as an unused official email address, a link to an unused server, specific keywords or records. If a honeytoken is used, it should trigger an alert in the security-monitoring infrastructure. Honeytokens can also be extended to other components such as specific database records or invalid or unused user accounts.

Some organizations have gone further by intentionally using administrative account names such as "administrator" or "adm-yinzer" as honeytokens. These honeytokens can be made to appear even more enticing by associating them with critical servers such as domain controllers using "DC" in the system name.

You can extend the simple document and honeytoken approach to a system honeypot, such as a file server hosting the document. This allows security administrators to detect an intrusion before the adversary reaches the honeytoken document. Again, the system must pose as a standard file server to lure the adversary.

If we extend this concept, we reach the honeynet level, a network of honeypots.

Actions

Threat actions

Actions are measures that threat actors take to cause or contribute to an incident. They answer the question, "What tactics (actions) were used to affect an asset?"

For the 2014-2020 DBIR timeframe, the top three Actions align for Cyber-Espionage breaches and all breaches; however, the order in which they appear differs. For Cyber-Espionage breaches, the top Actions are Malware (90%), Social (83%) and Hacking (80%). For all breaches, the top Actions are Hacking (56%), Malware (39%) and Social (29%).

This implies more of a reliance on Malware and Social Actions for Cyber-Espionage threat actors than for all breach Actions.

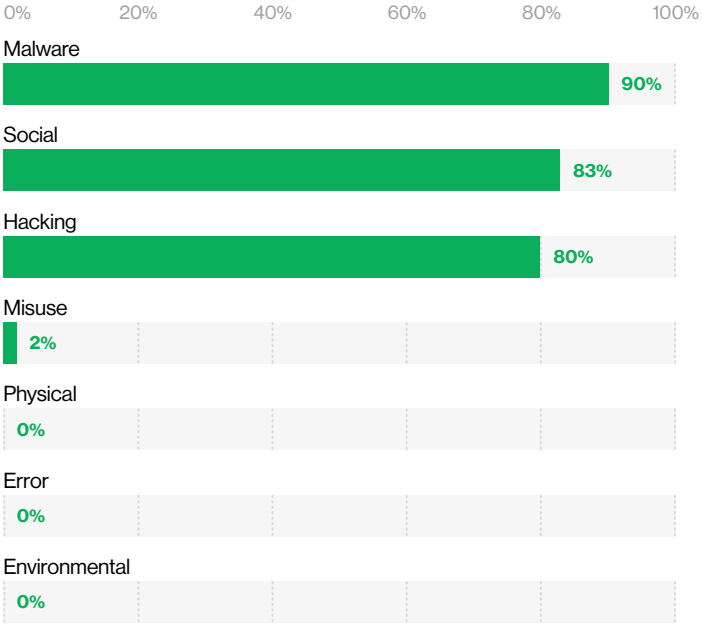


Figure #39: Actions within Cyber-Espionage breaches (2014-2020 DBIR; n=1,580)

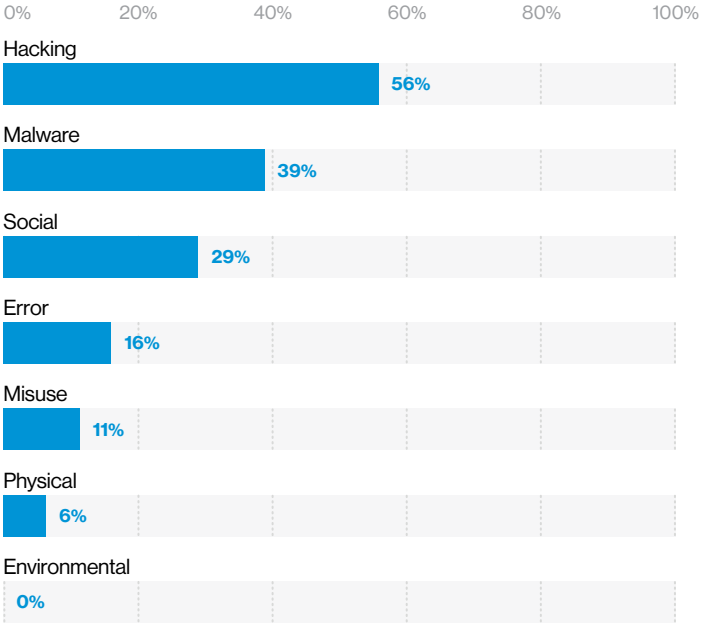


Figure #40: Actions within all breaches (2014-2020 DBIR; n=16,090)

Misuse

Misuse action varieties

Misuse action varieties use entrusted organizational resources or privileges granted for any purpose or in any manner—malicious or not—contrary to their original intentions.

Within the limited data for Cyber-Espionage breaches for the 2014-2020 DBIR timeframe, we find for Misuse action varieties that Privilege abuse (59%) and Data mishandling (32%) are far ahead of the three-way tie between Email misuse (14%), Unapproved hardware (14%) and Unapproved workaround (14%).

Top Misuse action varieties for all breaches during this same timeframe are somewhat similar to Cyber-Espionage breaches. Privilege abuse (74%) and Data mishandling (21%) also top this category; however, Possession abuse (11%), Unapproved hardware (7%) and Knowledge abuse (6%) occupy the next three positions for all breaches.

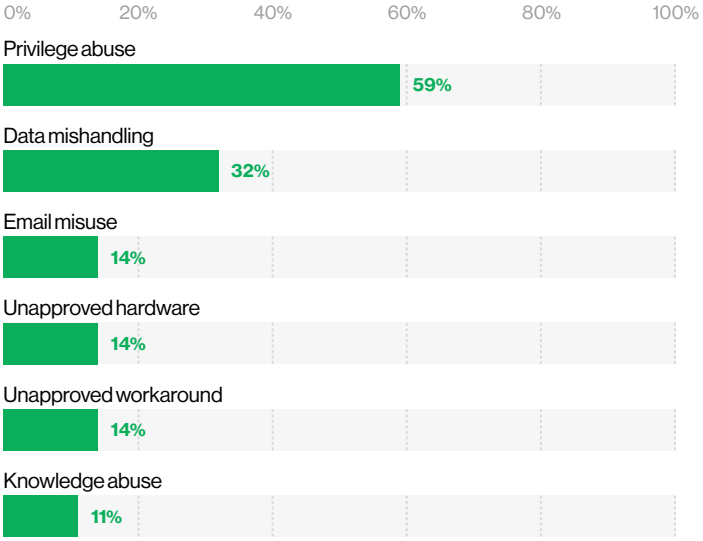


Figure #41: Top Misuse action varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=37)

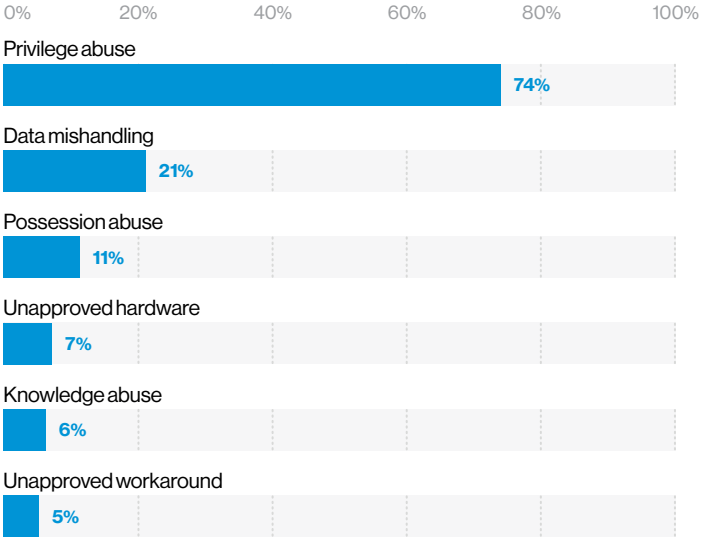


Figure #42: Top Misuse action varieties within all breaches (2014-2020 DBIR; n=1,769)

Social

Social action varieties

Social action varieties employ tactics, such as deception, manipulation and intimidation, to exploit the human users of information assets.

For Cyber-Espionage breaches during the 2014-2020 DBIR timeframe, the top Social action variety by far is Phishing (97%), with Pretexting (2%) and Bribery (1%) as a distant second and third, respectively.

For all breaches during this same timeframe, the top Social action varieties mirror Cyber-Espionage breaches, with a slightly lower percentage for Phishing (87%) and slightly higher percentages for Pretexting (9%) and Bribery (3%).

Top controls

- CSC-17: Implement a Security Awareness and Training Program
- CSC-19: Incident Response and Management
- CSC-20: Penetration Tests and Red Team Exercises

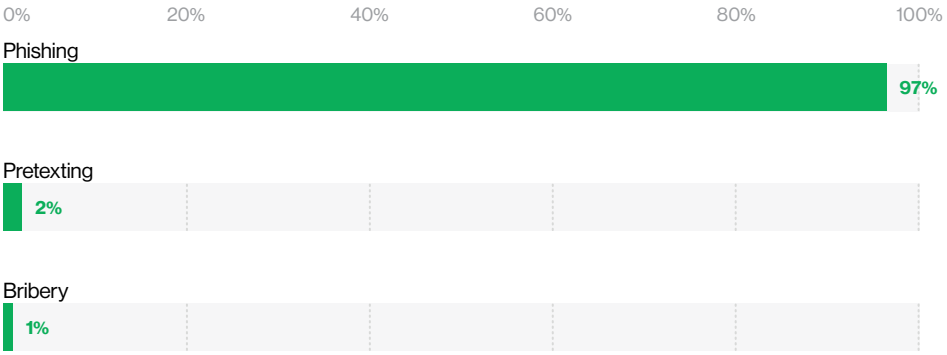


Figure #43: Top Social action varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,191)

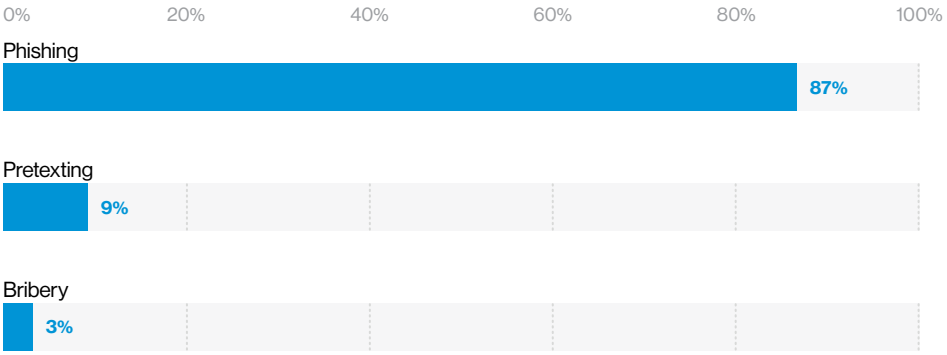


Figure #44: Top Social action varieties within all breaches (2014-2020 DBIR; n=4,529)

Hacking

Hacking action varieties

Hacking action varieties are all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

During the 2014-2020 DBIR timeframe, the top Hacking action varieties for Cyber-Espionage breaches are Use of backdoor or C2 (86%), Use of stolen creds (30%), Brute force (12%) and Exploit vuln (9%).

During this same timeframe, for all breaches, the top four Hacking action varieties align with the Cyber-Espionage breaches, albeit in a different order of primacy: Use of stolen creds (63%), Use of backdoor or C2 (39%), Brute force (18%) and Exploit vuln (9%).

Of the four top Hacking action varieties, Cyber-Espionage breaches rely more heavily on the sneakier Use of backdoor or C2, whereas all breaches rely extensively on the matter-of-fact Use of stolen creds.

Top controls

- CSC-4: Controlled Use of Administrative Privileges
- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-12: Boundary Defense
- CSC-16: Account Monitoring and Control
- CSC-19: Incident Response and Management
- CSC-20: Penetration Tests and Red Team Exercises

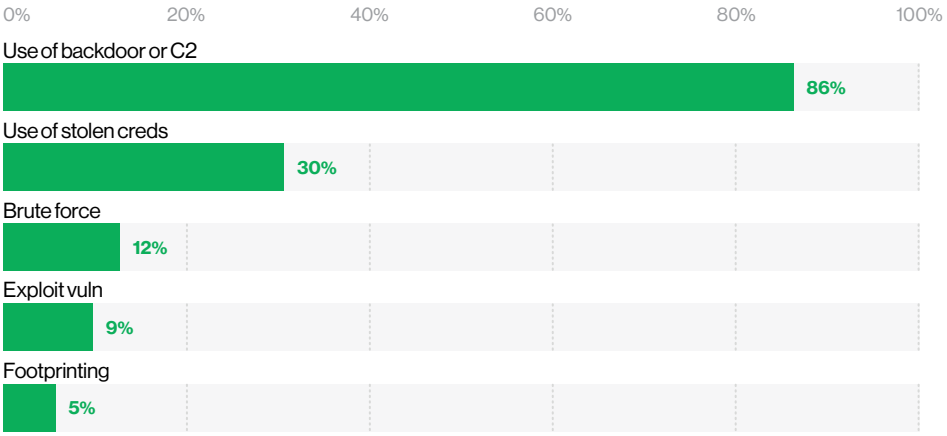


Figure #45: Top Hacking action varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,032)

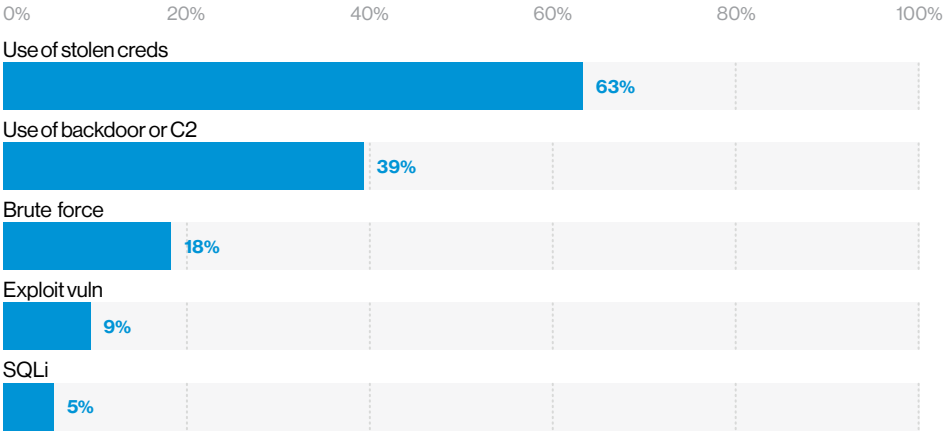


Figure #46: Top Hacking action varieties within all breaches (2014-2020 DBIR; n=6,581)

Malware

Malware action varieties

Malware actions are any malicious software, script or code that runs on a device to alter its state or function without the owner's informed consent.

For Cyber-Espionage breaches during the 2014-2020 DBIR timeframe, we see Cyber-Espionage threat actors place significantly more value on the top two Malware action varieties, Backdoor (78%) and C2 (77%), than the next four Malware action varieties: Downloader (40%), Capture stored data (40%), Spyware/Keylogger (33%) and Export data (32%).

During the same timeframe, the top Malware action varieties for all breaches group together more closely: C2 (48%), Export data (42%), Spyware/Keylogger (40%), RAM scraper (35%) and Backdoor (25%).

For top Malware action varieties, Cyber-Espionage threat actors place significant value in Backdoor and C2, while all breach threat actors similarly place value in C2, but tend to also favor Export data, Spyware/Keylogger and RAM scraper.

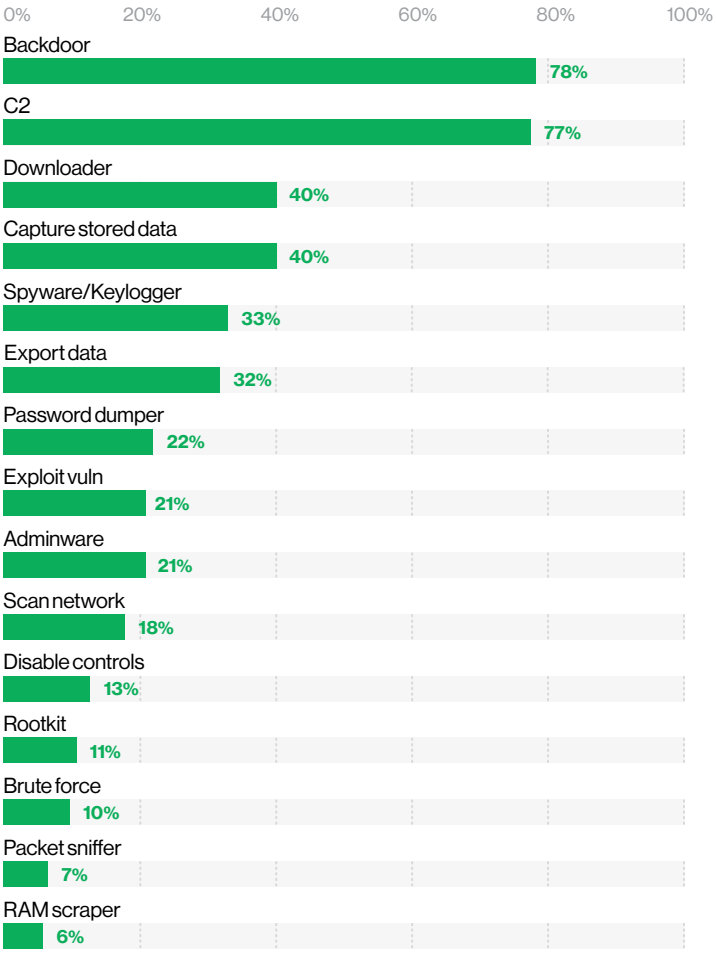


Figure #47: Top Malware action varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,005)

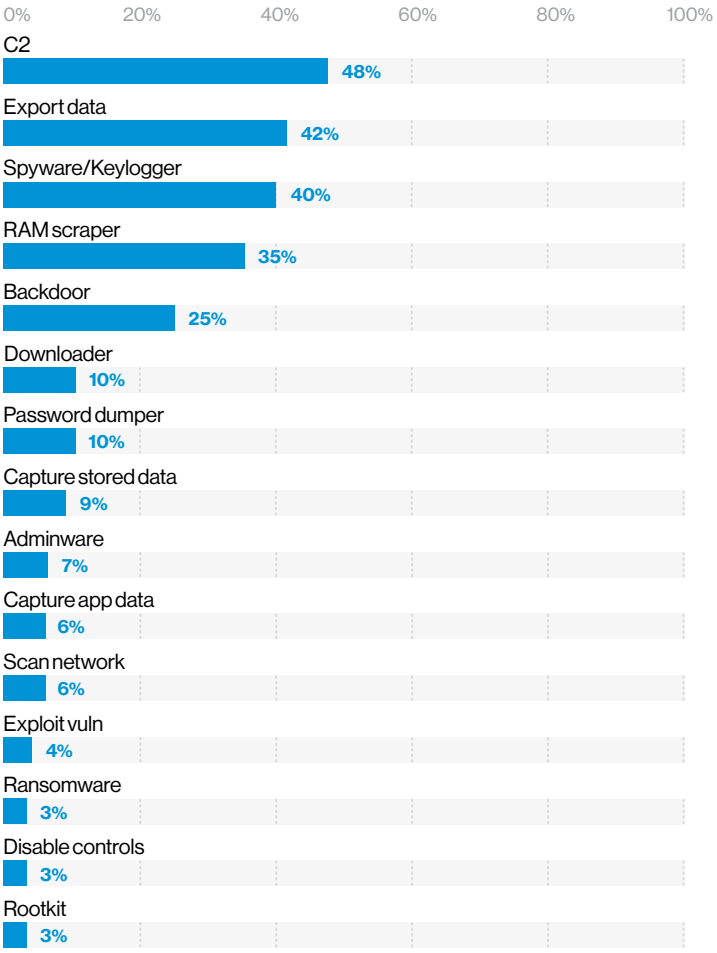


Figure #48: Top Malware action varieties within all breaches (2014-2020 DBIR; n=5,298)

Top controls

- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-8: Malware Defenses
- CSC-12: Boundary Defense
- CSC-13: Data Protection
- CSC-19: Incident Response and Management
- CSC-20: Penetration Tests and Red Team Exercises

Malware vector varieties

For Cyber-Espionage breaches during the 2014-2020 DBIR timeframe, the top Malware vector varieties are Email attachment (67%), Email link (17%), Web drive-by (11%) and Download by malware (11%).

For all breaches during the same timeframe, the top Malware vector varieties are Email attachment (43%), Direct install (39%) and Email link (9%).

In both Cyber-Espionage breaches and all breaches, threat actors rely on Email attachments and Email links for malware delivery. However, Web drive-by and Download by malware are next on the list for Cyber-Espionage breaches, while Direct install is next for all breaches. For Download by malware and Direct install, this implies that threat actors have already gained access to the asset or environment.

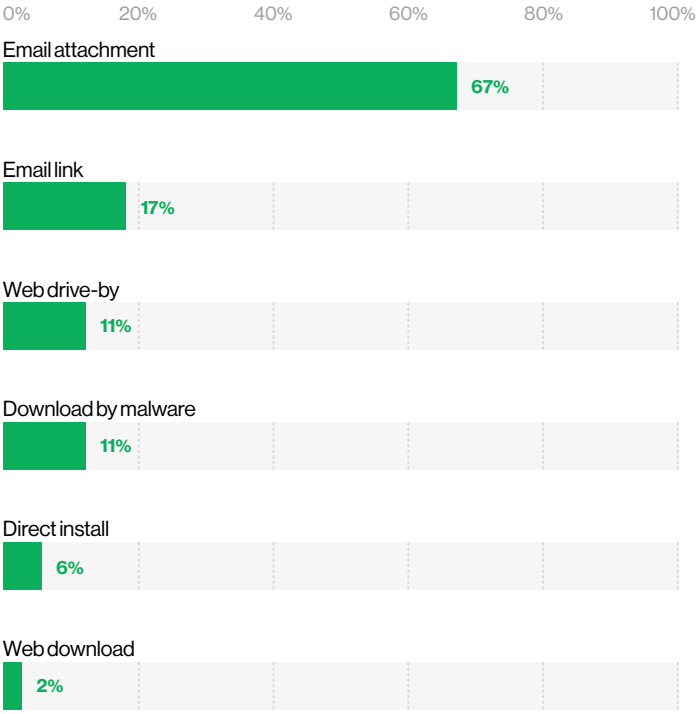


Figure #49: Top Malware vector varieties within Cyber-Espionage breaches (2014-2020 DBIR; n=1,212)

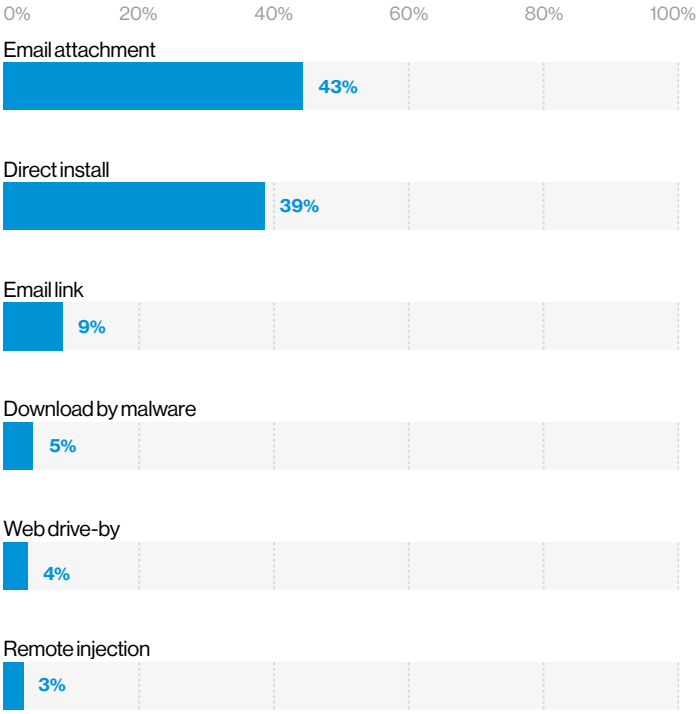


Figure #50: Top Malware vector varieties within all breaches (2014-2020 DBIR; n=5,252)

Top controls

- CSC-4: Controlled Use of Administrative Privileges
- CSC-6: Maintenance, Monitoring and Analysis of Audit Logs
- CSC-8: Malware Defenses
- CSC-12: Boundary Defense
- CSC-17: Implement a Security Awareness and Training Program
- CSC-19: Incident Response and Management
- CSC-20: Penetration Tests and Red Team Exercises

Deeper dive—Action varieties

For this deeper dive into Action varieties, we filtered the DBIR dataset for External actors and for Espionage and Financial motives within breaches.

During the 2014-2020 DBIR timeframe, the top four Action varieties by External actor with Espionage motive within breaches are Phishing (81%), Use of backdoor or C2 (60%), Backdoor (54%) and C2 (53%). Capture stored data (27%) and Downloader (27%) are tied for a distant fifth.

This high percentage across four Action varieties (which can be simplified further into Phishing, Backdoor and C2) implies that these are the primary go-to choices for threat actors with Espionage motive.

For this same timeframe, the Use of stolen creds (47%) topped the list of Action varieties by External actor with Financial motive. The next six Action varieties are closely grouped: Phishing (33%), Export data (30%), C2 (28%), RAM scraper (28%), Spyware/Keylogger (27%) and Use of backdoor or C2 (26%).

This close grouping of Action varieties implies that threat actors with Financial motive use a greater variety of options than those with Espionage motive to attain their objectives.

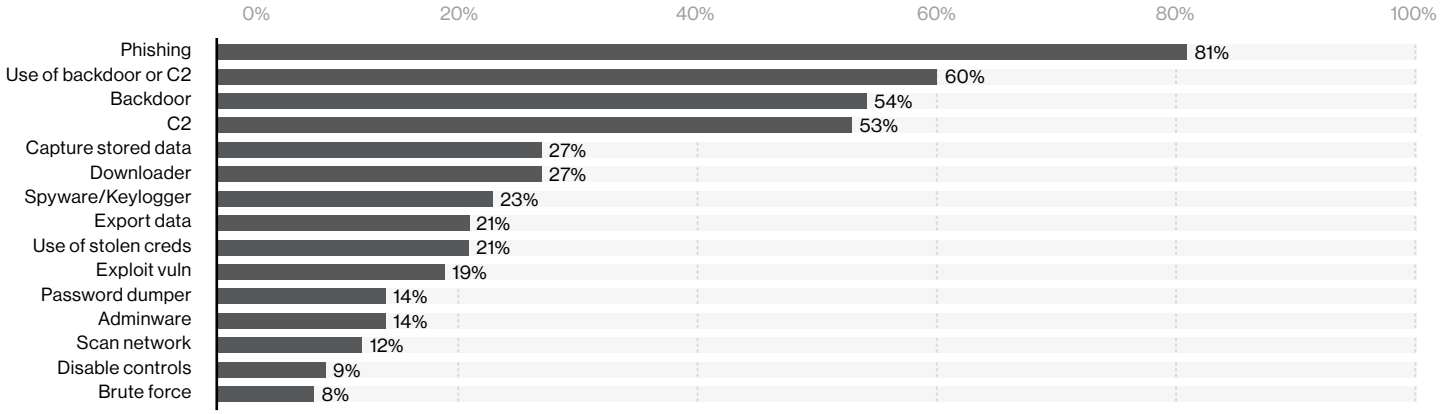


Figure #51: Top Action varieties by External actor and Espionage motive within breaches (2014-2020 DBIR; n=1,422)

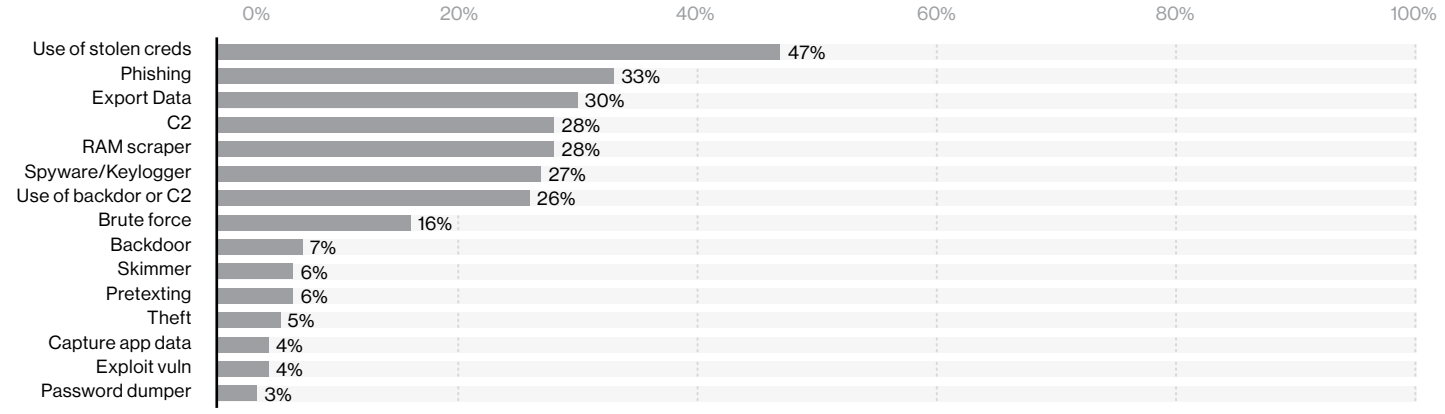


Figure #52: Top Action varieties by External actor and Financial motive within breaches (2014-2020 DBIR; n=6,436)

Deeper dive—Action vectors

For a look into Action vectors, we filtered the dataset for External actors and for Espionage and Financial motives within breaches.

The top three Action vectors by External actor and Espionage motive during the 2014-2020 DBIR timeframe are Email (84%), Email attachment (60%) and Backdoor or C2 (60%).

Much like the Action varieties above, this high percentage over three Action vectors implies that they are the primary go-to choices for threat actors with Espionage motive.

For threat actors with Financial motive during this same timeframe, the top Action vectors are Web application (44%), Email (41%), Direct install (31%), Backdoor or C2 (28%) and Email attachment (24%).

Compared to threat actors with Espionage motive, these Action vectors are much more varied, implying that threat actors with Financial motive prefer to use a larger selection of Action vectors to accomplish their objectives.

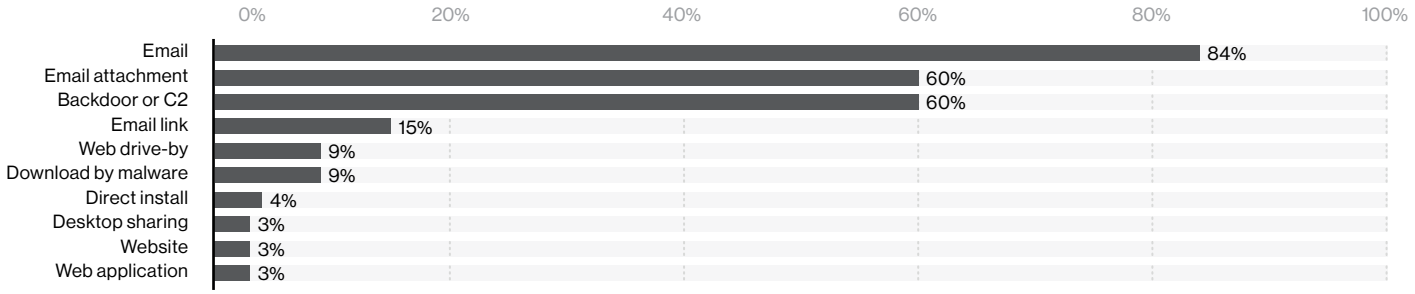


Figure #53: Top Action vectors by External actor and Espionage motive within breaches (2014-2020 DBIR; n=1,348)

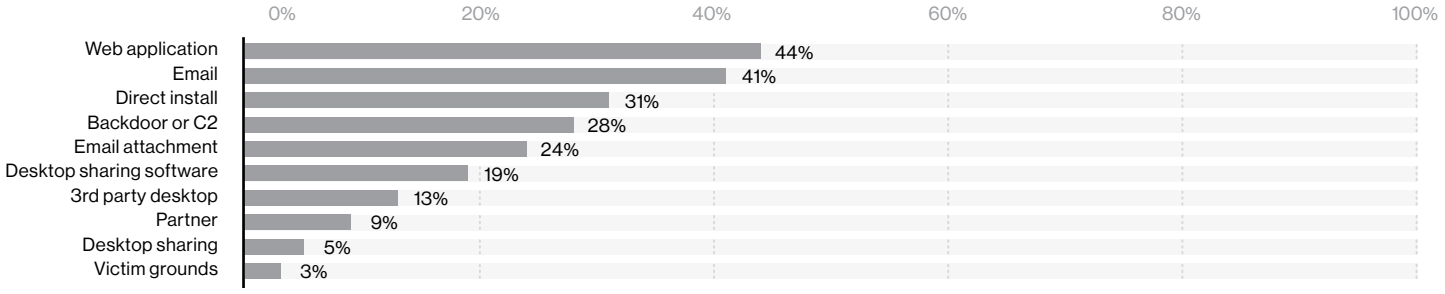


Figure #54: Top Action vectors by External actor and Financial motive within breaches (2014-2020 DBIR; n=5,969)

MITRE ATT&CK® framework aspects

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. In the 2020 DBIR, we mapped VERIS (threat actions) to MITRE ATT&CK.® If your organization uses MITRE ATT&CK,® here are some questions to ask:

- How was "initial access" gained? (e.g., known vulnerability exploitation, drive-by download, phishing attack vector, compromised credential access)
- How was "persistence" achieved? (e.g., new accounts, hooking, startup item, registry run keys, batch jobs, scheduled tasks)
- How did the adversary escalate privileges? (e.g., account bypass, Dynamic Link Library hijacking, vulnerability exploitation, process injection)
- Were there any indications of lateral movement? (e.g., remote service exploitation, local admin account log-ons, pass the hash vs. pass the ticket, network sniffing)
- How did C2 servers access the environment? (e.g., unknown or unexpected traffic or http, https, ftp, etc.; data encoding or obfuscation; domain fronting; uncommon ports)

EDR and NDR technologies

Using an EDR solution during a Cyber-Espionage investigation can significantly increase the effectiveness of the investigation. This technology can provide much needed visibility into understanding adversary TTPs, monitoring lateral movement, identifying persistence mechanisms and expediting the return to normal business operations.

EDR technology can accelerate the speed of the investigation by utilizing behavioral detection tactics combined with IoC-based searches (in near real time) within the infrastructure, leading to further identification of compromised or affected system components.

Network traffic can provide keen insight into threat actors' breach defenses and impact assets and data. Utilizing NDR solutions gives organizations in-depth visibility into the network, which helps network forensics investigators gain insights into packet-level activities. Such insight helps investigators identify new IoCs using behavioral analysis and heuristics techniques.

NDR deployments give investigators access to large amounts of data, which they can index for rapid searches to identify anomalies. This can lead to the discovery of other unidentified, infected infrastructure components and help build up the IoCs needed to find more impacted and compromised systems.

EDR and NDR solutions can be efficient toolsets for organizations to leverage during an incident and hasten the return to normal business operation.

07

The way forward

NIST CSF Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

After-action reviews (a.k.a. postmortem sessions) should be completed as part of any IR effort. This is particularly important for the closeout of more advanced IR efforts, such as those focused on Cyber-Espionage attacks.

Complete the review by conducting a lessons-learned discussion, noting participant feedback (e.g., what went well, what went not so well and what can be improved upon in the next session).

Assemble feedback and countermeasure solutions in an action plan to update the IR Plan, determine additional IR resource requirements and identify internal IR stakeholder and tactical responder training needs. Ensure that an organization's IR lifecycle includes an explicit provision directing continual maturation via the after action-review process.

Recovery tips

- Complete a postmortem review of any IR actions
- Develop a post-incident action plan to incorporate lessons learned
- Ensure that the after action-review process becomes part of the organization's maturation process

Takeaways

Victim impact

Timelines. For Cyber-Espionage breaches, Time to Compromise was seconds to days (91%), Time to Exfiltration was minutes to weeks (88%), Time to Discovery was months to years (69%) and Time to Containment was days to months (79%).

For all breaches, Time to Compromise was seconds to minutes (85%), Time to Exfiltration was seconds to days (89%), Time to Discovery was days to months (75%) and Time to Containment was hours to weeks (76%).

Patterns. Among the nine DBIR Incident Classification Patterns, Cyber-Espionage ranked sixth (10%).

Industries. For Cyber-Espionage breaches, Public (31%), Manufacturing (22%) and Professional (11%) were most common. Manufacturing (35%), Mining + Utilities (23%) and Public (23%) were most common by percent within breaches.

Attribute varieties. For Cyber-Espionage breaches, top Attribute varieties, Software installation (Integrity) (91%), Alter behavior (Integrity) (84%), Secrets (Confidentiality) (73%), Internal (Confidentiality) (29%), Credentials (Confidentiality) (21%) and System (Confidentiality) (19%) were most impacted.

For all breaches, top Attribute varieties were Software installation (Integrity) (43%), Alter behavior (Integrity) (32%), Credentials (Confidentiality) (29%), Personal (Confidentiality) (28%) and Payment (Confidentiality) (22%).

Asset varieties. For Cyber-Espionage breaches, top compromised Asset varieties (2020 DBIR) were Desktop or laptop (88%), Mobile phone (14%) and Web application (10%).

For all breaches (2020 DBIR), top compromised Asset varieties were Web application (43%), Desktop or laptop (31%) and Mail (21%).

Data varieties. Top compromised Data varieties for Cyber-Espionage breaches (2020 DBIR) were Credentials (56%), Secrets (49%), Internal (12%) and Classified (7%).

Personal (58%), Credentials (41%), Internal (17%) and Medical (16%) topped compromised Data varieties for all breaches.

Actor activities

Discovery. Top Discovery methods for Cyber-Espionage breaches were Suspicious traffic (48%), Antivirus (23%) and Emergency response team (7%).

For all breaches, top Discovery methods were Law enforcement (28%), Fraud detection (19%) and Customer (15%).

Actors. For Cyber-Espionage breaches, top Actor varieties were State-affiliated (85%), Nation-state (8%) and Organized crime (4%).

For all breaches, top Actor varieties were Organized crime (59%), State-affiliated (13%) and Unaffiliated (7%).

Motives. Within all breaches, Actor motives were Financial (76%), Espionage (18%) and "The Rest" (6%).

Actions. Top Actions for Cyber-Espionage breaches were Malware (90%), Social (83%) and Hacking (80%).

For all breaches, top Actions were Hacking (56%), Malware (39%) and Social (29%).

Action varieties. Phishing (81%), Use of Backdoor | C2 (53% | 60%), Capture stored data (27%) and Downloader (27%) were top Action varieties for External actors with Espionage motive within breaches.

For External actors with Financial motive, Use of stolen creds (47%), Phishing (33%) and Export data (30%) were top Action varieties.

Action vectors. Email (84%), Email attachment (60%) and Backdoor or C2 (60%) were top Action vector varieties for External actors with Espionage motive within all breaches.

For External actors with Financial motive within all breaches, Use of stolen creds (47%), Phishing (33%) and Export data (30%) were top Action vector varieties.

Key Cyber-Espionage CIS Critical Security Controls

CSC-4: Controlled Use of Administrative Privileges

CSC-5: Secure Configuration for Hardware and Software

CSC-6: Maintenance, Monitoring and Analysis of Audit Logs

CSC-8: Malware Defenses

CSC-12: Boundary Defense

CSC-13: Data Protection

CSC-14: Controlled Access Based on the Need to Know

CSC-16: Account Monitoring and Control

CSC-17: Implement a Security Awareness and Training Program

CSC-18: Application Software Security

CSC-19: Incident Response and Management

CSC-20: Penetration Tests and Red Team Exercises

Mappings

VERIS category	CER key takeaways	Top CIS Critical Security Controls
Timelines	Time to Compromise was seconds to days (91%), Time to Exfiltration was minutes to weeks (88%), Time to Discovery was months to years (69%), Time to Containment was days to months (79%)	CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-12: Boundary Defense CSC-16: Account Monitoring and Control CSC-19: Incident Response and Management CSC-20: Penetration Tests and Red Team Exercises
Discovery	Suspicious traffic (48%), Antivirus (23%), Emergency response team (7%)	CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-8: Malware Defenses CSC-12: Boundary Defense CSC-19: Incident Response and Management
Attribute varieties	Software installation (Integrity) (91%), Alter behavior (Integrity) (84%), Secrets (Confidentiality) (73%), Internal (Confidentiality) (29%), Credentials (Confidentiality) (21%), System (Confidentiality) (19%)	CSC-4: Controlled Use of Administrative Privileges CSC-5: Secure Configuration for Hardware and Software CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-8: Malware Defenses CSC-13: Data Protection CSC-16: Account Monitoring and Control
Asset varieties (2020 DBIR)	Desktop or laptop (User Device) (88%), Mobile phone (User Device) (14%), Web application (Server) (10%)	CSC-5: Secure Configuration for Hardware and Software CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-17: Implement a Security Awareness and Training Program CSC-18: Application Software Security CSC-20: Penetration Tests and Red Team Exercises
Data varieties (2020 DBIR	Credentials (56%), Secrets (49%), Internal (12%)	CSC-4: Controlled Use of Administrative Privileges CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-13: Data Protection CSC-14: Controlled Access Based on the Need to Know CSC-16: Account Monitoring and Control CSC-17: Implement a Security Awareness and Training Program
Social varieties	Phishing (97%), Pretexting (2%), Bribery (1%)	CSC-17: Implement a Security Awareness and Training Program CSC-19: Incident Response and Management CSC-20: Penetration Tests and Red Team Exercises
Hacking varieties	Use of backdoor or C2 (86%), Use of stolen creds (30%), Brute force (12%)	CSC-4: Controlled Use of Administrative Privileges CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-12: Boundary Defense CSC-16: Account Monitoring and Control CSC-19: Incident Response and Management CSC-20: Penetration Tests and Red Team Exercises
Malware varieties	Backdoor (78%), C2 (77%), Downloader (40%), Capture stored data (40%)	CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-8: Malware Defenses CSC-12: Boundary Defense CSC-13: Data Protection CSC-19: Incident Response and Management CSC-20: Penetration Tests and Red Team Exercises
Malware vectors	Email attachment (67%), Email link (17%), Web drive-by (11%), Download by malware (11%)	CSC-4: Controlled Use of Administrative Privileges CSC-6: Maintenance, Monitoring and Analysis of Audit Logs CSC-8: Malware Defenses CSC-17: Implement a Security Awareness and Training Program CSC-19: Incident Response and Management CSC-20: Penetration Tests and Red Team Exercises

Figure #55: Mapping VERIS categories to CER key takeaways to CIS top Critical Security Controls

Appendix A: Guides

VERIS framework

Overview

Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.

VERIS was crafted as a response to one of the most critical and persistent challenges in the security industry—a lack of quality information.

VERIS targets this problem by helping organizations to collect useful incident-related information and to share it—anonymously and responsibly—with others. The overall goal is to lay a foundation from which we can constructively and cooperatively learn from our experiences to better measure and manage risk.

A4 threat model

VERIS employs the A4 threat model, which was developed originally by the Verizon RISK Team (now known as VTRAC). In the A4 threat model, an incident is viewed as a series of events that adversely affect the information assets of an organization. The A4 threat model elements are:

- Actors: Whose actions affected the asset?
- Actions: What actions affected the asset?
- Assets: Which assets were affected?
- Attributes: How were assets affected?

Threat actors

Entities causing or contributing to an incident are referred to as threat actors.

External actors: External threats originate from sources outside of the organization and its network of partners. Typically, no trust or privilege is implied for external entities.

Internal actors: Internal threats originate from within the organization. Insiders are trusted and privileged (some more than others).

Partner actors: Partners include any third party that shares a business relationship with the organization. Some level of trust and privilege is usually implied between business partners and the organizations.

Threat actions

Threat actors conduct threat actions to cause or contribute to an incident. VERIS uses seven primary categories for threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. For this report, we focus on four: Misuse, Social, Hacking and Malware.

Misuse: Using entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended

Social: Employing tactics such as deception, manipulation and intimidation to exploit the human element, or users, of information assets

Hacking: Attempting to intentionally access or harm information assets, without (or exceeding) authorization, by circumventing or thwarting logical security mechanisms

Malware: Any malicious software, script or code that runs on a device to alter its state or function without the owner's informed consent

Assets and attributes

A compromised asset is one that suffers from any loss of confidentiality/possession, integrity/authenticity or availability/utility (primary security attributes of the expanded CIA Triad). An incident can involve multiple assets and affect multiple attributes (each of which contains different metrics) of those assets.

Additional resources

Further information on VERIS can be obtained from these resources:

- DBIR facts, figures and data: github.com/vz-risk/dbir/tree/gh-pages/2020
- VERIS framework: veriscommunity.net
- VERIS schema: github.com/vz-risk/veris
- VERIS Community Database (VCDB): github.com/vz-risk/vcdb

VIPR process

Overview

Based in our previous proactive IR engagements, we've formulated a six-phase approach to investigative response and IR readiness: the Verizon Incident Preparedness and Response (VIPR) process. VIPR consists of six phases: (1) Planning and Preparation, (2) Detection and Validation, (3) Containment and Eradication, (4) Collection and Analysis, (5) Remediation and Recovery, and (6) Assessment and Adjustment.

Further insight into these IR phases and their corresponding sub-components can be found in the VIPR report:

enterprise.verizon.com/resources/reports/vipr/

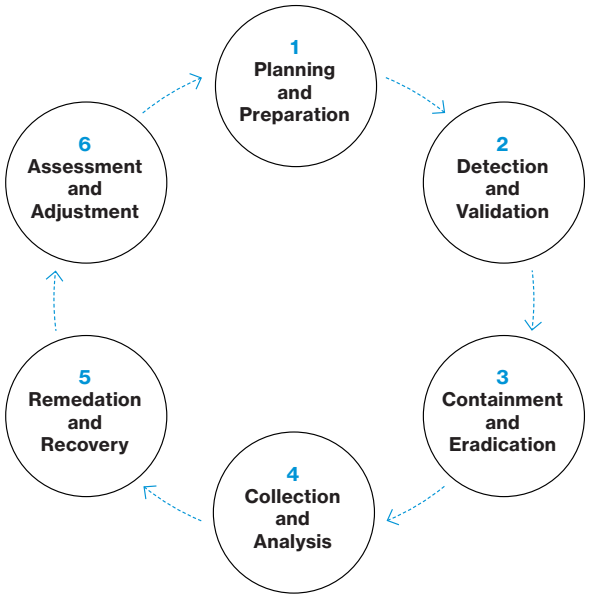


Figure #56: VIPR phases

VIPR report key takeaways

Having an efficient and effective IR Plan is the key to successful incident response. Capturing this efficiency and effectiveness is the ultimate purpose of our VIPR report.

The VIPR report is a data- and scenario-driven approach to incident preparedness and response. It's based on three years (2016-2018) of our IR Plan assessment engagement observations and recommendations, as well as our data breach simulation recommendations. Findings presented in the VIPR report culminated in 20 key takeaways.

Phase	Key takeaway
1 – Planning and Preparation	1. Construct a logical, efficient IR Plan
	2. Create IR playbooks for specific incidents
	3. Periodically review, test and update the IR Plan
	4. Cite external and internal cybersecurity and incident response governance and standards
	5. Define internal IR stakeholder roles and responsibilities
	6. Require internal IR stakeholders to periodically discuss the cybersecurity threat landscape
	7. Train and maintain skilled tactical responders
	8. Periodically review third-party cybersecurity services and contact procedures
2 – Detection and Validation	9. Define cybersecurity events (along with incidents)
	10. Classify incidents by type and severity level
	11. Describe technical and non-technical incident detection sources
	12. Specify incident and event-tracking mechanisms
	13. Specify escalation and notification procedures
3 – Containment and Eradication	14. Provide containment and eradication measures
4 – Collection and Analysis	15. Specify evidence collection and data analysis tools and procedures
	16. Specify evidence handling and submission procedures
5 – Remediation and Recovery	17. Provide remediation and recovery measures
6 – Assessment and Adjustment	18. Feed lessons-learned results back into the IR Plan
	19. Establish a data and document retention policy
	20. Track incident and incident response metrics

Figure #57: VIPR report key takeaways

NIST Cybersecurity Framework

Overview

The NIST Cybersecurity Framework (CSF) is voluntary guidance based on existing standards, guidelines and practices to help organizations better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders.

nist.gov/cyberframework

Figure #58: NIST Cybersecurity Framework

The NIST CSF provides a common language for understanding, managing and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization:

nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Five functions

The five functions of the NIST CSF are as follows:

Identify. Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.

Examples of outcome categories include Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.

Protect. Develop and implement appropriate safeguards to ensure delivery of critical services.

Examples of outcome categories include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect. Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Examples of outcome categories include Anomalies and Events, Security, Continuous Monitoring, and Detection Processes.

Respond. Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Examples of outcome categories include Response Planning, Communications, Analysis, Mitigation and Improvements.

Recover. Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Examples of outcome categories include Recovery Planning, Improvements and Communications.

CIS Critical Security Controls

Overview

The Center for Internet Security (CIS) Critical Security Controls (CSCs) are internationally recognized cybersecurity best practices for defense against common threats. They are a consensus-developed resource that brings together expert insight on cyber threats, business technology and security.

Organizations with varying resources and risk exposure use the CIS CSCs to build an effective cyber-defense program:

cisecurity.org/controls/cis-controls-list/

DBIR Implementation

The 2020 DBIR best describes the implementation of CIS CSCs:

For those who are unacquainted with the CIS CSCs, they are a community-built, attacker-informed prioritized set of cybersecurity guidelines that consist of 171 safeguards organized into 20 higher-level controls.

One of the unique elements of the CIS CSCs is their focus on helping organizations understand where to start their security program. This prioritization is represented in two ways:

- *Through the ordering of the CSCs so that they allow a loose prioritization (CSC-1: Inventory of Hardware is probably a better place to start than CSC-20: Penetration Testing)*
- *Introduced in version 7.150 is the concept of Implementation Groups, in which the 171 safeguards are grouped, based on the resources and risks the organizations are facing. This means that a smaller organization with fewer resources (Implementation Group 1) shouldn't be expected to implement resource and process-intensive controls such as Passive Asset Discovery even if it's within CSC-1, while an organization with more resources and/or a higher risk level may want to consider that control*

Critical Security Controls

Type	#	Description
Basic	CSC-1	Inventory and Control of Hardware Assets
	CSC-2	Inventory and Control of Software Assets
	CSC-3	Continuous Vulnerability Management
	CSC-4	Controlled Use of Administrative Privileges
	CSC-5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
	CSC-6	Maintenance, Monitoring and Analysis of Audit Logs
Foundational	CSC-7	Email and Web Browser Protections
	CSC-8	Malware Defenses
	CSC-9	Limitation and Control of Network Ports, Protocols and Services
	CSC-10	Data Recovery Capabilities
	CSC-11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
	CSC-12	Boundary Defense
	CSC-13	Data Protection
	CSC-14	Controlled Access Based on the Need to Know
	CSC-15	Wireless Access Control
	CSC-16	Account Monitoring and Control
Organizational	CSC-17	Implement a Security Awareness and Training Program
	CSC-18	Application Software Security
	CSC-19	Incident Response and Management
	CSC-20	Penetration Tests and Red Team Exercises

Figure #59: CIS Critical Security Controls

09

Appendix B: Industry dossiers

Educational Services

NAICS	61 – Educational Services
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	607 (2014-2020) | 228 (2020)
Actors	External (69%), Internal (32%), Partner (2%), Multiple (2%)
Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%)
Cyber-Espionage breaches	
Frequency	47 (8%) (2014-2020)
Actors	External (100%)
Actions	Social (91%), Hacking (91%), Malware (94%)
Assets	Person (96%), User Dev (73%), Server (7%)
Data	Secrets (94%), Credentials (9%)

Cyber-Espionage breach dossier	
NAICS	All industries
All breaches (2014-2020)	
Frequency	16,090 (2014-2020) | 3,950 (2020)
Actors	External (75%), Internal (26%), Multiple (2%), Partner (1%)
Motives	Financial (76%), Espionage (18%), Fun (3%)
Cyber-Espionage breaches (2014-2020)	
Frequency	1,580 (2014-2020)
Actions	Malware (90%), Social (83%), Hacking (80%)
Assets	Person (88%), User Dev (83%), Server (34%)
Data	Secrets (75%), Internal (20%), Credentials (22%), System (19%)

Summary

Since 2014, confirmed data breaches with Espionage motive made up about 8% of the breaches reported in the Educational Services industry. In 2019, the percentage was only 1%. While the percentage is low, this percentage is somewhat driven down due to the very high rate of Ransomware (80%) financially motivated breaches that target this industry.

Another consideration when looking at the numbers for the Educational Industry is that Cyber-Espionage threat actors are known to use ransomware to cover up data theft, and in many cases the threat actor succeeds in preventing analysts from determining what if any data was exfiltrated from the network. This is particularly true when the organization doesn't have sufficient logging in place to properly investigate.

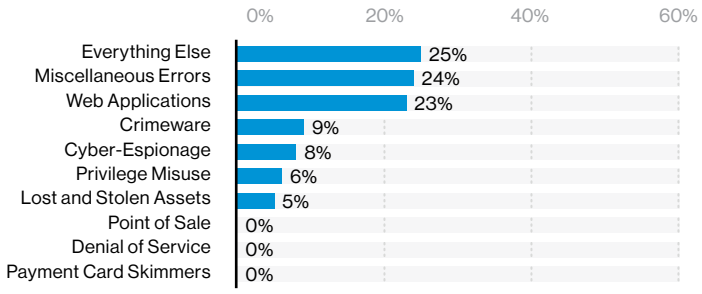


Figure #60: Breaches by pattern for Education (2014-2020 DBIR; n=607)

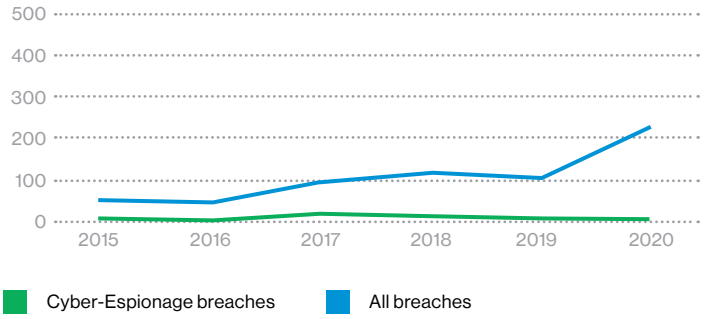


Figure #61: Cyber-Espionage breaches within all breaches annually for Education (2015-2020 DBIR)

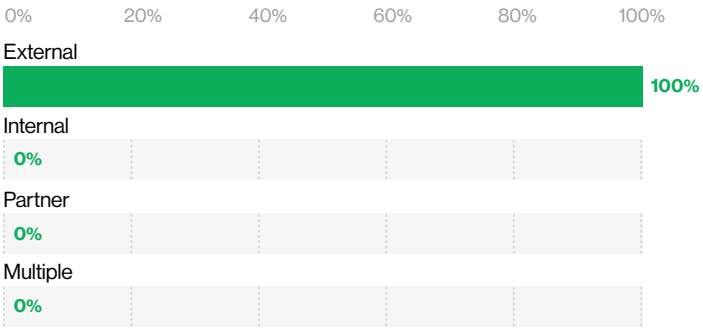


Figure #62: Actors within Cyber-Espionage breaches for Education (2014-2020 DBIR; n=47)

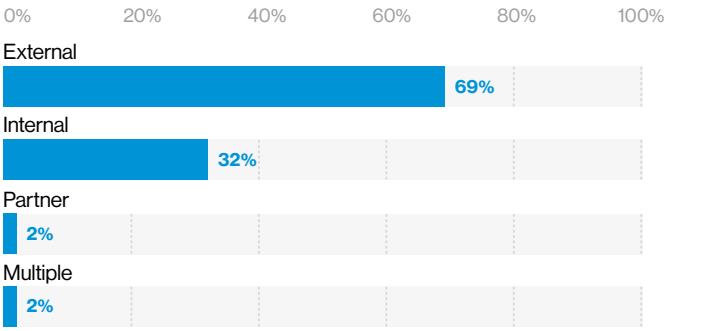


Figure #63: Actors within all breaches for Education (2014-2020 DBIR; n=598)

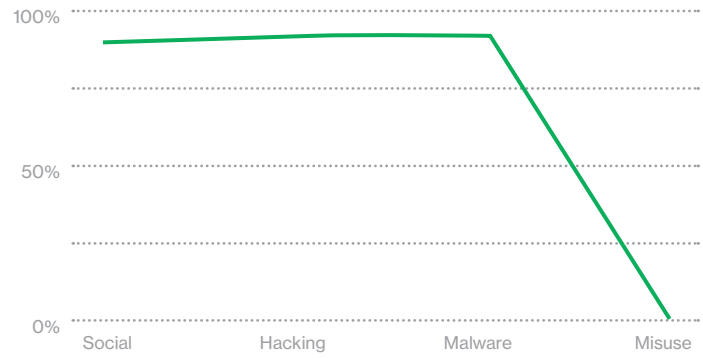


Figure #64: Actions within Cyber-Espionage breaches for Education (2014-2020 DBIR; n=47)

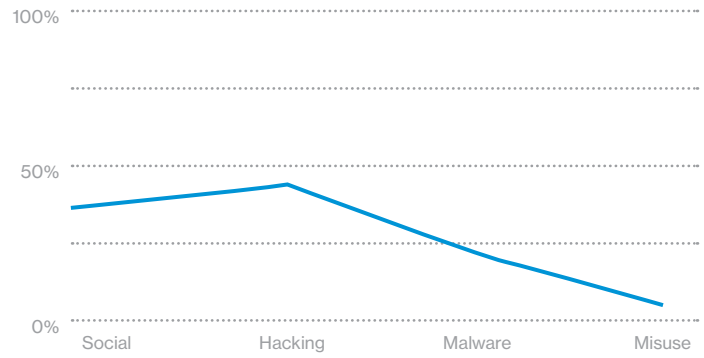


Figure #65: Actions within all breaches for Education (2014-2020 DBIR; n=592)

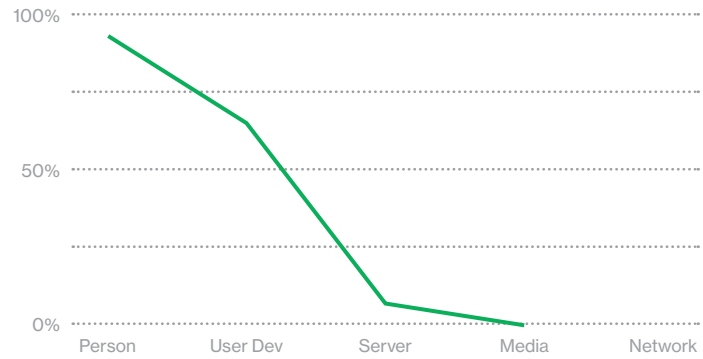


Figure #66: Assets within Cyber-Espionage breaches for Education (2014-2020 DBIR; n=45)

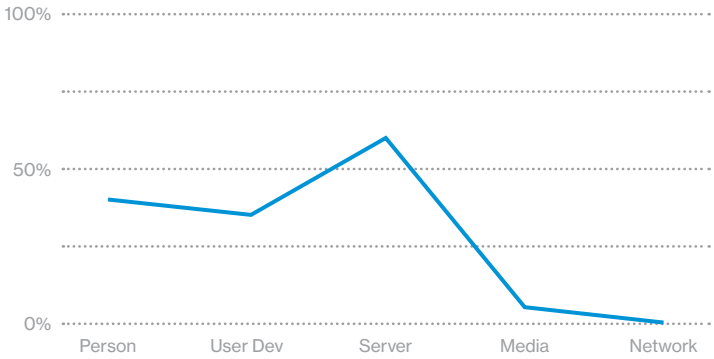


Figure #67: Assets within all breaches for Education (2014-2020 DBIR; n=552)

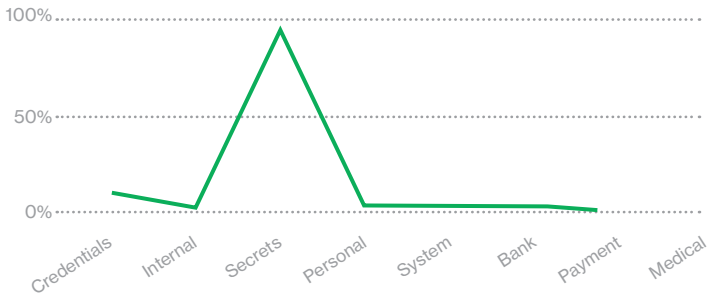


Figure #68: Compromised Data varieties within Cyber-Espionage breaches for Education (2014-2020 DBIR; n=47)

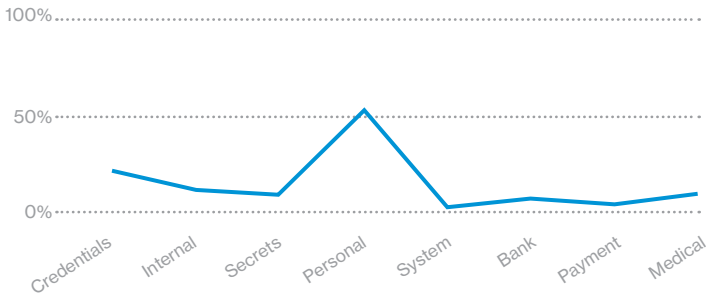


Figure #69: Compromised Data varieties within all breaches for Education (2014-2020 DBIR; n=507)

Financial and Insurance

NAICS	52 – Financial and Insurance
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	2,797 (2014-2020) | 448 (2020)
Actors	External (87%), Internal (14%), Partner (1%), Multiple (2%)
Motives	Financial (91%), Espionage (3%), Grudge (3%)
Cyber-Espionage breaches	
Frequency	42 (2%) (2014-2020)
Actors	External (100%), Internal (2%), Partner (2%), Multiple (5%)
Actions	Social (56%), Hacking (90%), Malware (85%)
Assets	Person (58%), User Dev (70%), Server (58%)
Data	Secrets (38%), Payment (31%), Internal (15%), Credentials (15%)

Summary

The DBIR dataset pertaining to Cyber-Espionage in the Financial and Insurance industry has seen some significant changes in percentages. For the past seven years (2014-2020 DBIR timeframe), Financial on average was approximately 3%; however in the last three years, it made up 6.3% of Cyber-Espionage breaches. In 2018, there was a significant increase where it reached 10.3%.

Remember, these numbers represent only reported breaches. When the compromised data doesn't fall within reporting criteria, a private organization may choose not to disclose a breach. This makes Cyber-Espionage breaches, which are already challenging to detect, even less likely to be discovered and by extension, reported. There is no way to truly gauge the magnitude of Cyber-Espionage attacks, especially in any of the private industries.

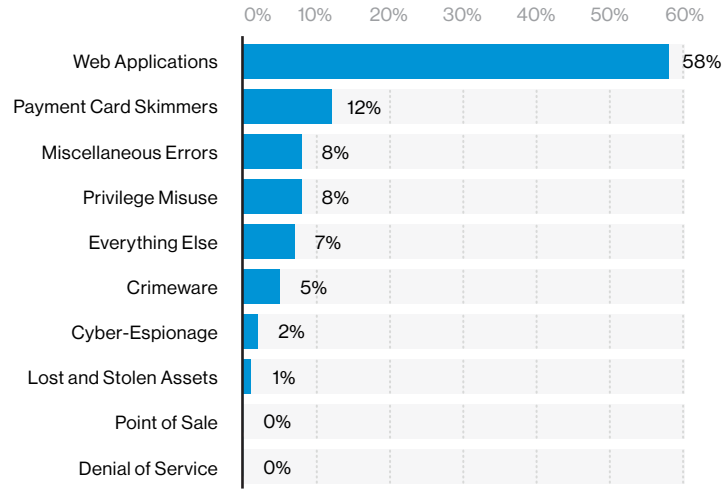


Figure #70: Breaches by pattern for Financial (2014-2020 DBIR; n=2,797)

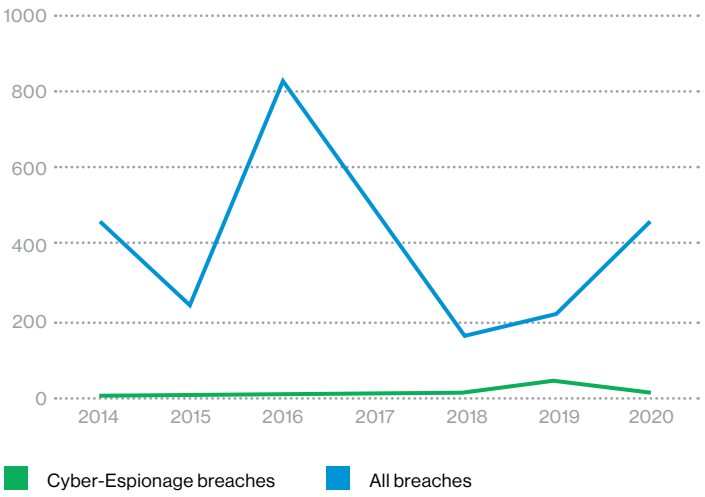


Figure #71: Cyber-Espionage breaches within all breaches annually for Financial (2014-2020 DBIR)

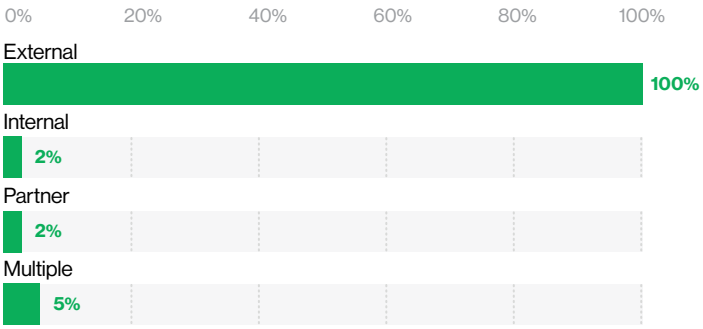


Figure #72: Actors within Cyber-Espionage breaches for Financial (2014-2020 DBIR; n=42)

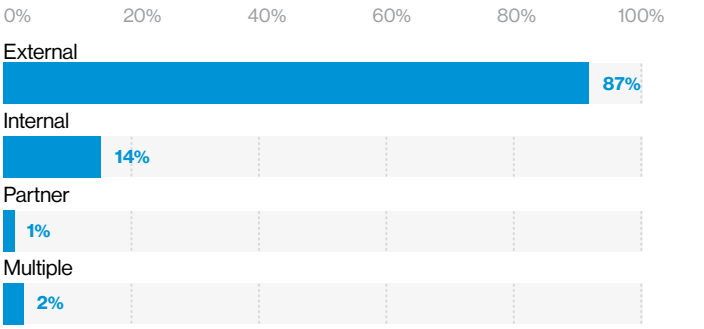


Figure #73: Actors within all breaches for Financial (2014-2020 DBIR; n=2,787)

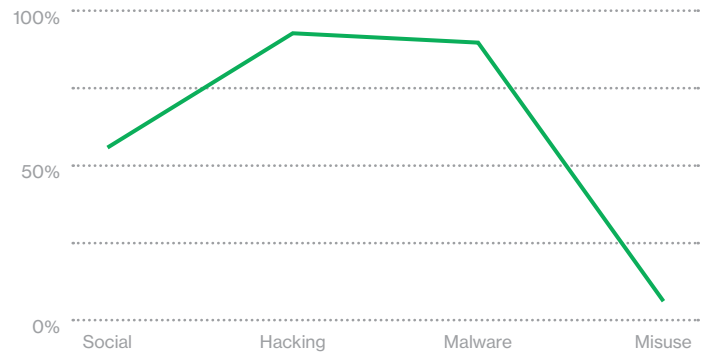


Figure #74: Actions within Cyber-Espionage breaches for Financial (2014-2020 DBIR; n=41)

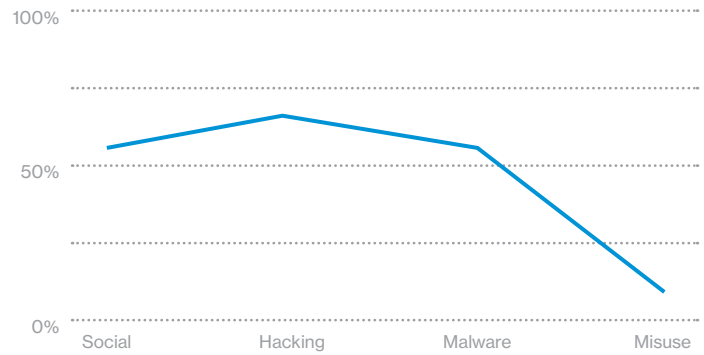


Figure #75: Actions within all breaches for Financial (2014-2020 DBIR; n=2,331)

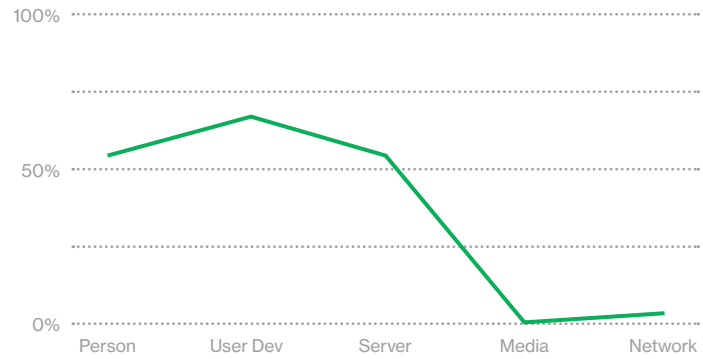


Figure #76: Assets within Cyber-Espionage breaches for Financial (2014-2020 DBIR; n=40)

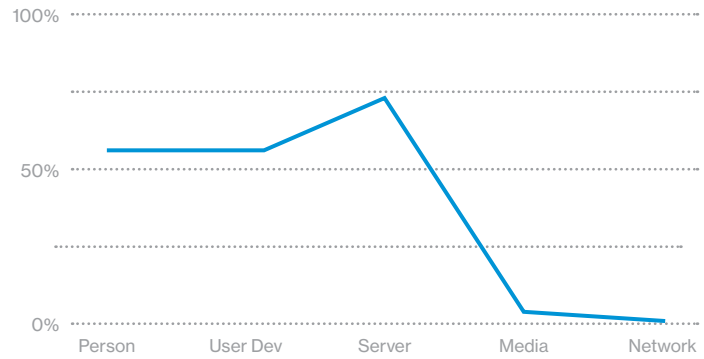


Figure #77: Assets within all breaches for Financial (2014-2020 DBIR; n=2,238)

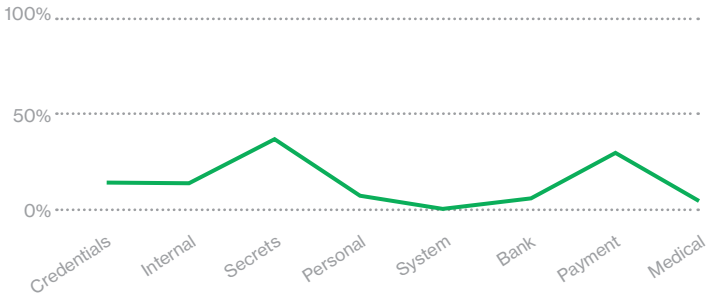


Figure #78: Compromised Data varieties within Cyber-Espionage breaches for Financial (2014-2020 DBIR; n=39)

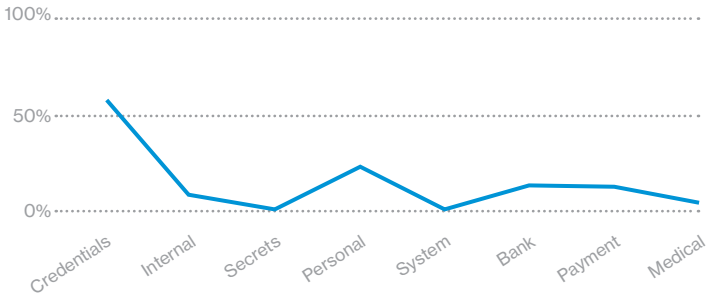


Figure #79: Compromised Data varieties within all breaches for Financial (2014-2020 DBIR; n=2,205)

Information

NAICS	51 – Information
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	1,043 (2014-2020) | 360 (2020)
Actors	External (70%), Internal (30%), Partner (2%), Multiple (2%)
Motives	Financial (88%), Espionage (7%), Fun (2%), Grudge (2%)
Cyber-Espionage breaches	
Frequency	72 (7%) (2014-2020)
Actors	External (100%), Internal (4%), Multiple (4%)
Actions	Social (59%), Hacking (78%), Malware (67%)
Assets	Person (61%), User Dev (61%), Server (48%)
Data	Secrets (70%), Credentials (30%), Internal (13%)

Summary

The Information industry reported the fourth-highest amount of Cyber-Espionage-motivated data breaches during the 2014-2020 DBIR timeframe. Information is a vast industry, which encompasses all organizations involved in the creation, storage or transmission of information.

The bread-and-butter motivation for Information industry data breaches is Financial; however, we have still seen 7% of breaches with a Cyber-Espionage motive.

An important factor for breaches in the Information industry is that since 2019, there has been a significant increase in web applications attacks, which are leveraging both stolen credentials and vulnerability exploitation. Misconfiguration errors were a main contributing factor to breaches in the Information industry.

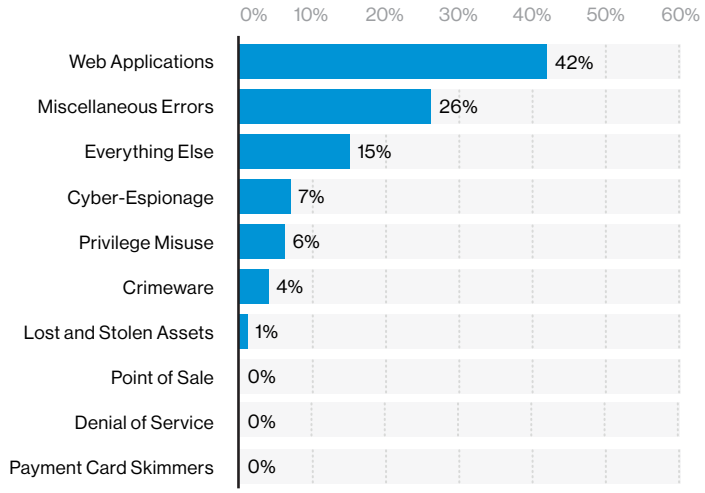


Figure #80: Breaches by pattern for Information (2014-2020 DBIR; n=1,043)

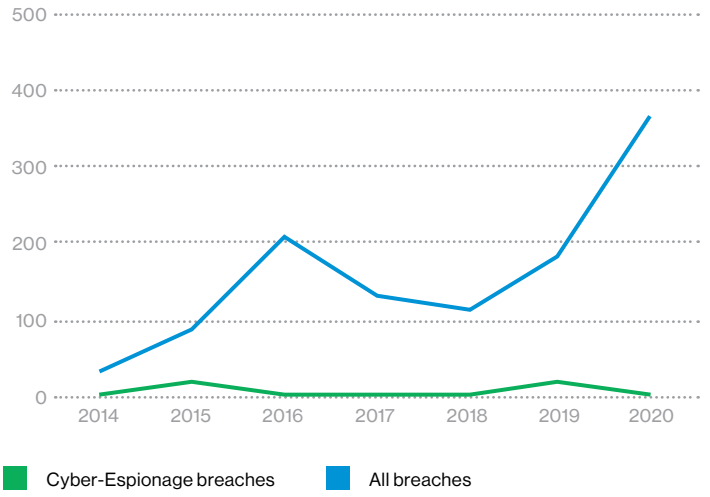


Figure #81: Cyber-Espionage breaches within all breaches annually for Information (2014-2020 DBIR)

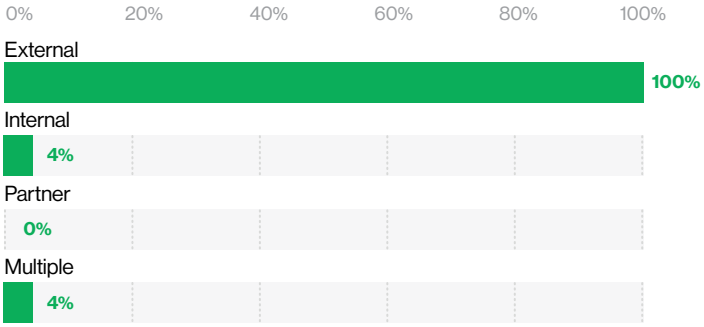


Figure #82: Actors within Cyber-Espionage breaches for Information (2014-2020 DBIR; n=72)

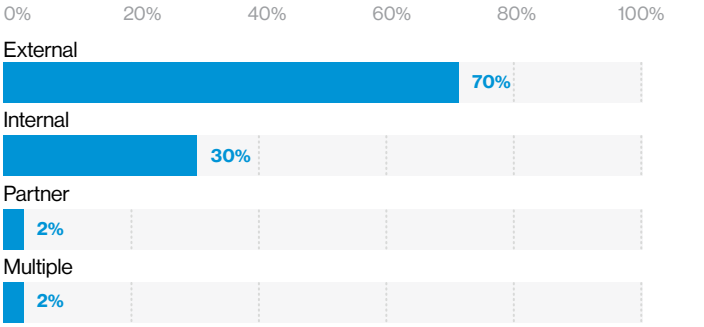


Figure #83: Actors within all breaches for Information (2014-2020 DBIR; n=1,036)

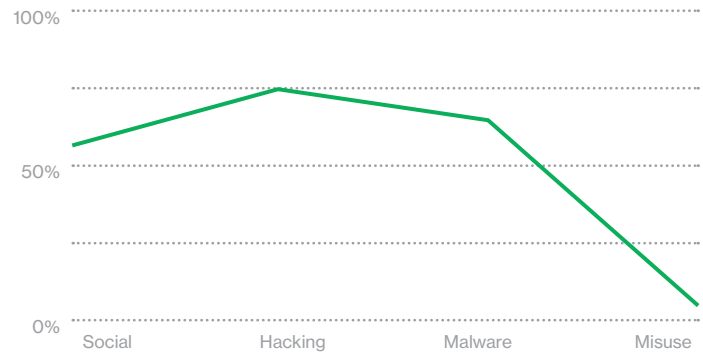


Figure #84: Actions within Cyber-Espionage breaches for Information (2014-2020 DBIR; n=63)

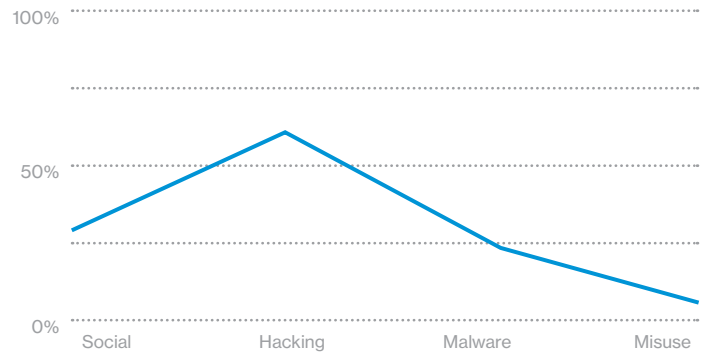


Figure #85: Actions within all breaches for Information (2014-2020 DBIR; n=1,013)

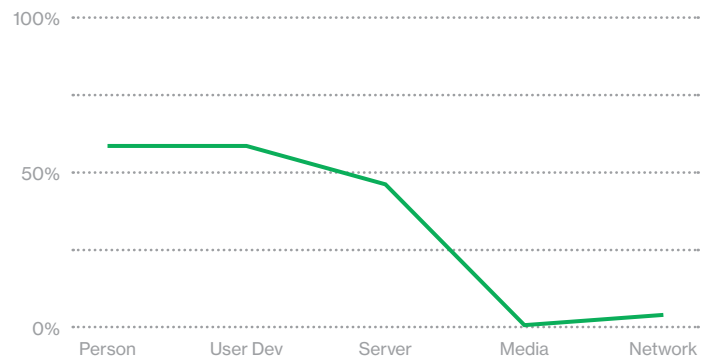


Figure #86: Assets within Cyber-Espionage breaches for Information (2014-2020 DBIR; n=61)

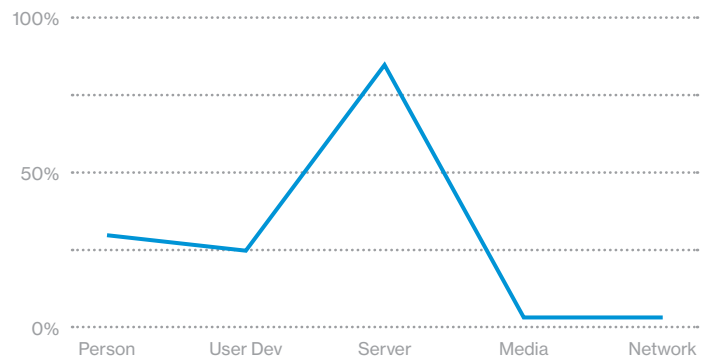


Figure #87: Assets within all breaches for Information (2014-2020 DBIR; n=937)

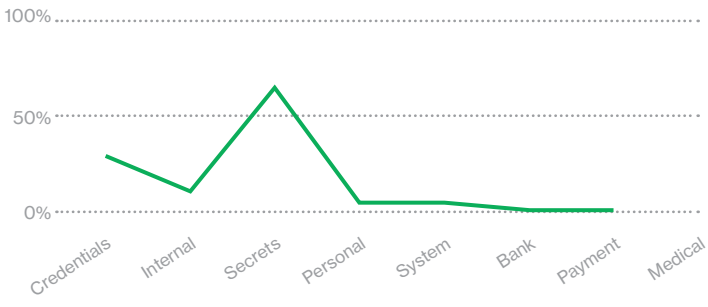


Figure #88: Compromised Data varieties within Cyber-Espionage breaches for Information (2014-2020 DBIR; n=61)

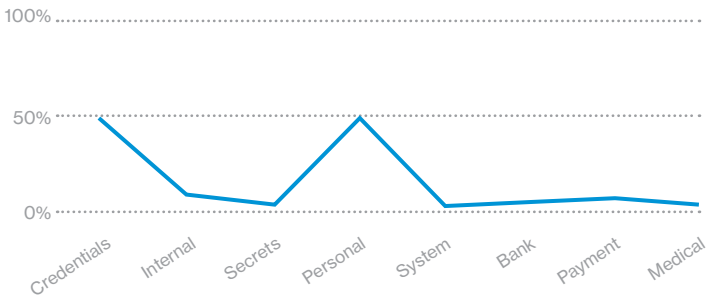


Figure #89: Compromised Data varieties within all breaches for Information (2014-2020 DBIR; n=806)

Manufacturing

NAICS	31-33 – Manufacturing
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	985 (2014-2020) | 381 (2020)
Actors	External (84%), Internal (17%), Partner (1%), Multiple (1%)
Motives	Financial (73%), Espionage (27%)
Cyber-Espionage breaches	
Frequency	344 (35%) (2014-2020)
Actors	External (100%), Internal (1%), Multiple (1%)
Actions	Social (85%), Hacking (58%), Malware (84%)
Assets	Person (86%), User Dev (73%), Server (13%)
Data	Secrets (85%), Credentials (21%), Internal (2%)

Summary

In 2019, the Manufacturing industry had the largest number of Cyber-Espionage-motivated breaches compared to other industries. Overall between 2014 and 2020, it's ranked as the second-highest-hit industry at nearly 22% of all reported Cyber-Espionage breaches.

In 2018, we noted a significant drop in reported Cyber-Espionage breaches in the Manufacturing industry. However, we believe this was due in part to a change that year in DBIR contributors who typically provide specific metrics around Cyber-Espionage breaches in Manufacturing.

Cyber-Espionage threat actors primarily target Secrets and – like all other industries – Credentials as a means to acquire these Secrets.

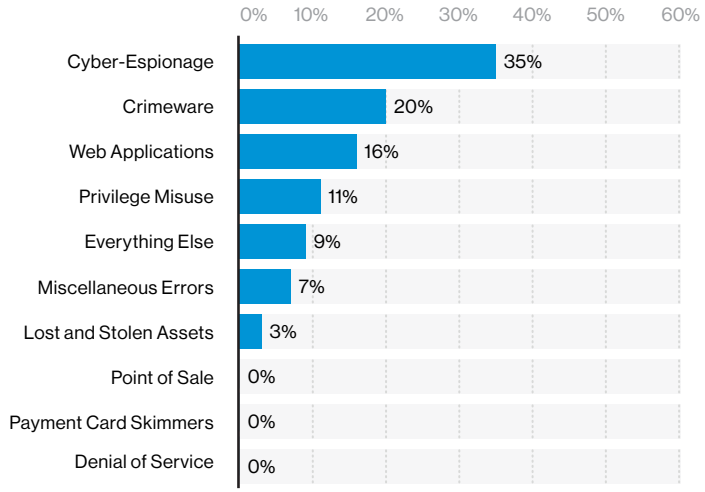


Figure #90: Breaches by pattern for Manufacturing (2014-2020 DBIR; n=985)

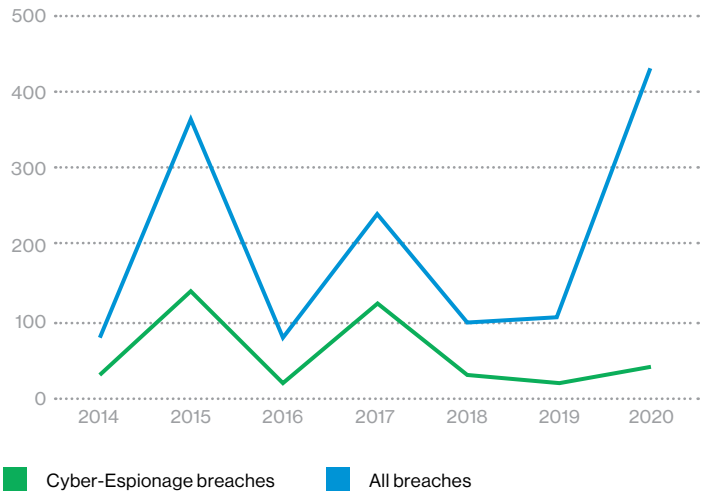


Figure #91: Cyber-Espionage breaches within all breaches annually for Manufacturing (2014-2020 DBIR)

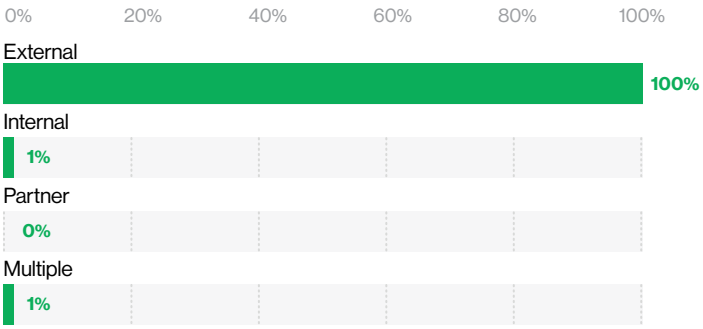


Figure #92: Actors within Cyber-Espionage breaches for Manufacturing (2014-2020 DBIR; n=344)

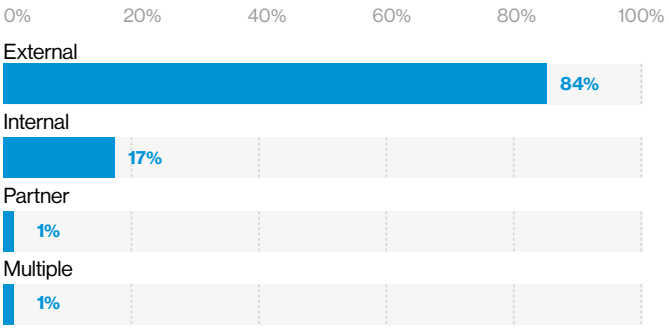


Figure #93: Actors within all breaches for Manufacturing (2014-2020 DBIR; n=977)

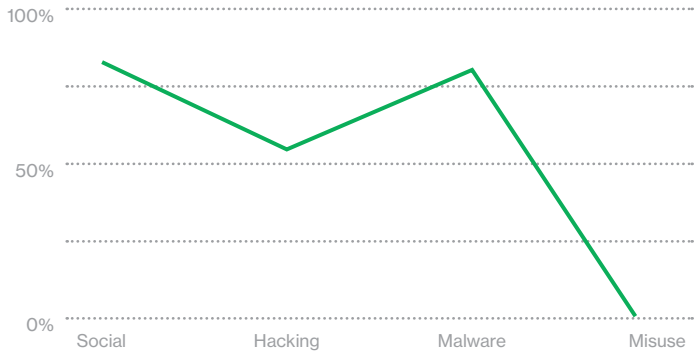


Figure #94: Actions within Cyber-Espionage breaches for Manufacturing (2014-2020 DBIR; n=320)

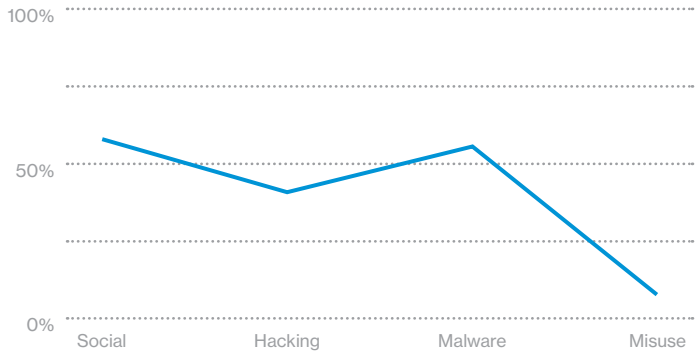


Figure #95: Actions within all breaches for Manufacturing (2014-2020 DBIR; n=937)

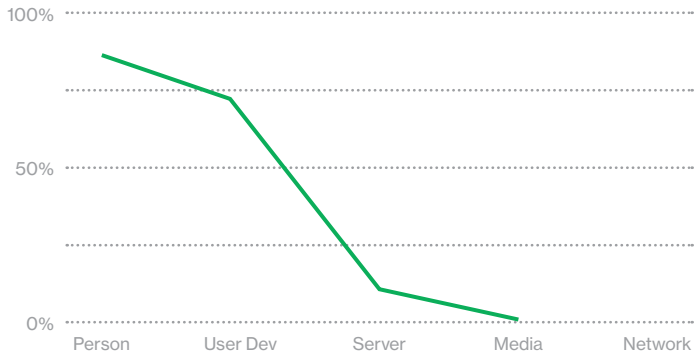


Figure #96: Assets within Cyber-Espionage breaches for Manufacturing (2014-2020 DBIR; n=316)

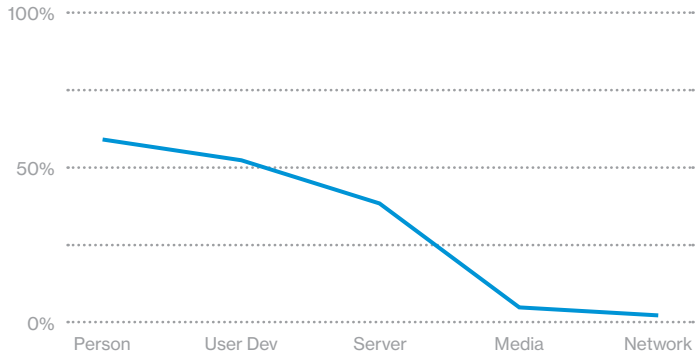


Figure #97: Assets within all breaches for Manufacturing (2014-2020 DBIR; n=874)

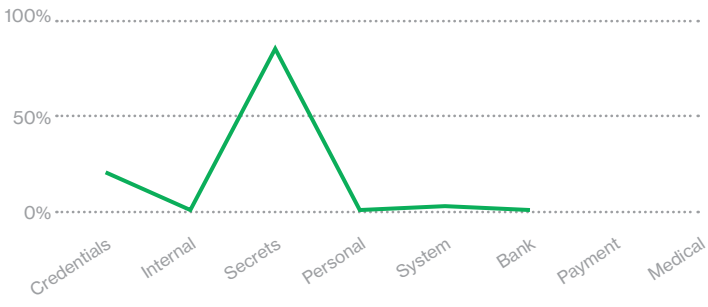


Figure #98: Compromised Data varieties within Cyber-Espionage breaches for Manufacturing (2014-2020 DBIR; n=312)

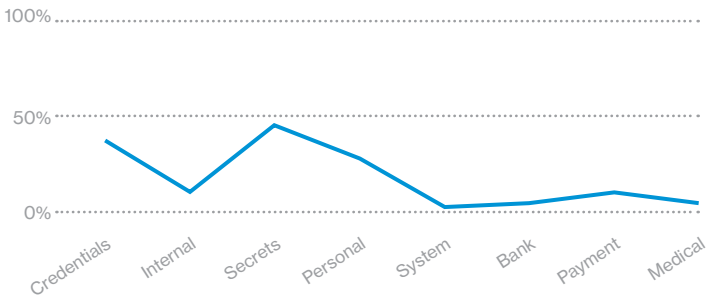


Figure #99: Compromised Data varieties within all breaches for Manufacturing (2014-2020 DBIR; n=767)

Mining, Quarrying, Oil & Gas Extraction + Utilities

NAICS	21+22 – Mining, Quarrying, Oil & Gas Extraction + Utilities
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	230 (2014-2020) | 43 (2020)
Actors	External (80%), Internal (24%), Multiple (4%)
Motives	Financial (63%-95%), Espionage (8%-43%)
Cyber-Espionage breaches	
Frequency	54 (23%) (2014-2020)
Actors	External (100%), Internal (13%), Multiple (13%)
Actions	Social (88%), Hacking (79%), Malware (79%)
Assets	Person (90%), User Dev (80%), Server (27%)
Data	Secrets (62%), Internal (27%), Credentials (14%)

Summary

In 2019, less than half of breaches in the Mining, Quarrying, Oil & Gas Extraction + Utilities industries had confirmed motives, resulting in significant ranges for Financial and Espionage motive percentages.

For this industry combination, we observed a range of 8%-43% in Espionage motives, making the degree of this threat uncertain. The range also highlights the challenges in identifying Espionage-motivated attacks and determining just how prevalent the threat is in this industry.

We see the dominant action for Cyber-Espionage breaches in this industry as Social followed closely by Malware and Hacking.

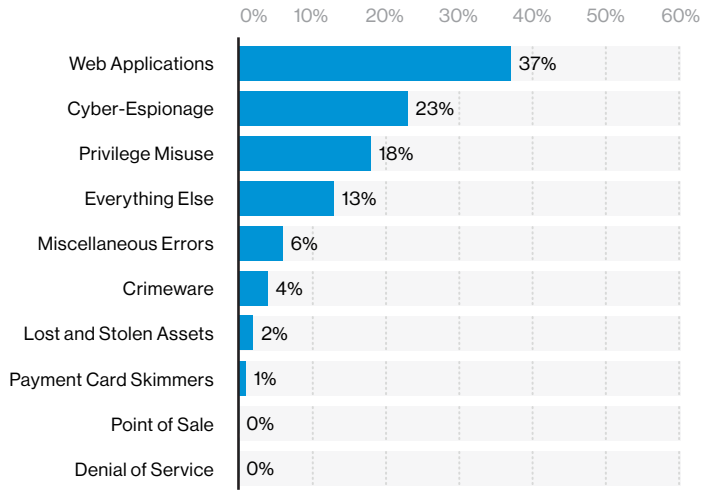


Figure #100: Breaches by pattern for Mining + Utilities (2014-2020 DBIR; n=230)

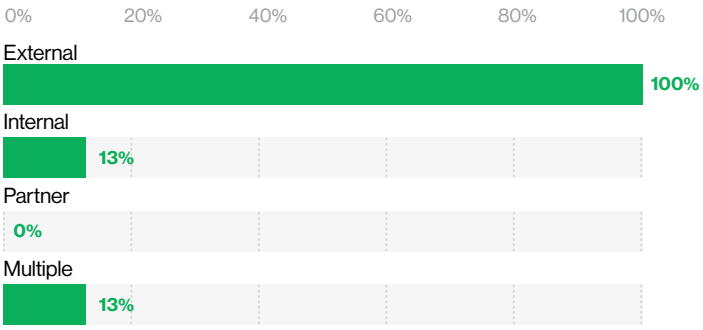


Figure #101: Actors within Cyber-Espionage breaches for Mining + Utilities (2014-2020 DBIR; n=54)

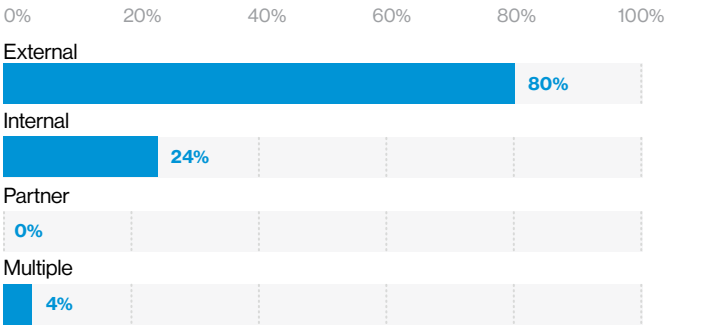


Figure #102: Actors within all breaches for Mining + Utilities (2014-2020 DBIR; n=227)

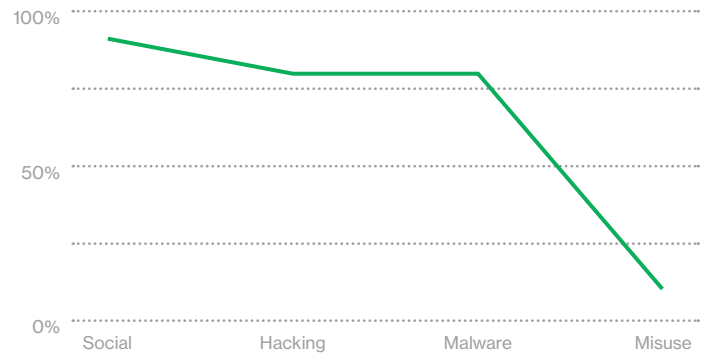


Figure #103: Actions within Cyber-Espionage breaches for Mining + Utilities (2014-2020 DBIR; n=42)

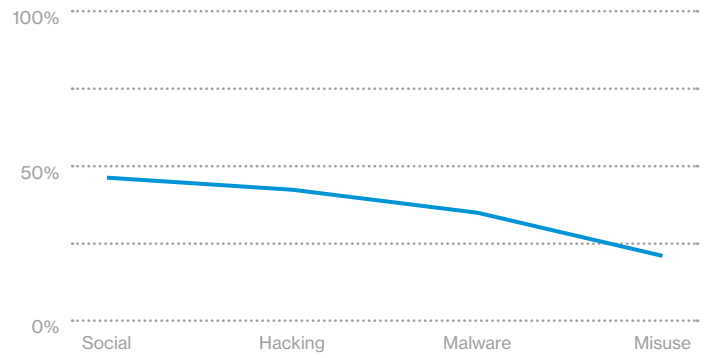


Figure #104: Actions within all breaches for Mining + Utilities (2014-2020 DBIR; n=140)

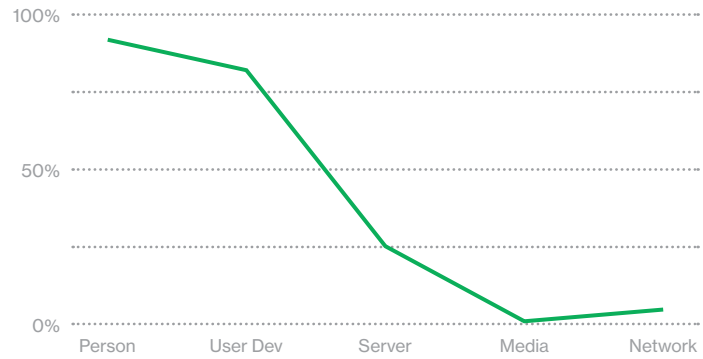


Figure #105: Assets within Cyber-Espionage breaches for Mining + Utilities (2014-2020 DBIR; n=41)

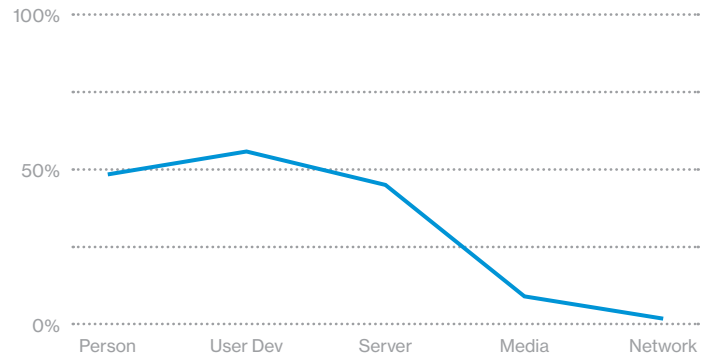


Figure #106: Assets within all breaches for Mining + Utilities (2014-2020 DBIR; n=131)

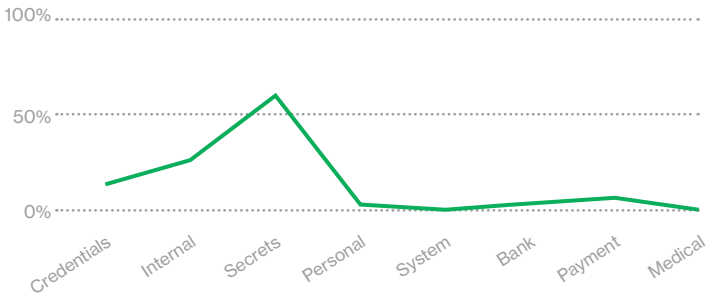


Figure #107: Compromised Data varieties within Cyber-Espionage breaches for Mining + Utilities (2014-2020 DBIR; n=37)

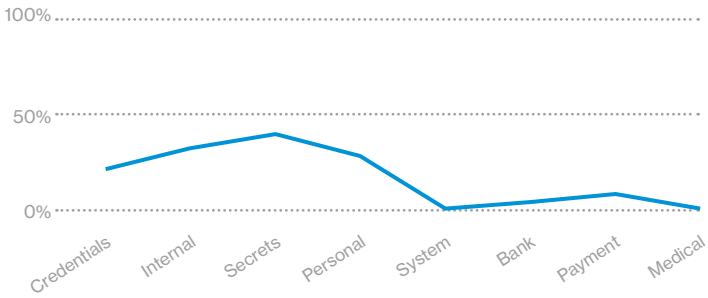


Figure #108: Compromised Data varieties within all breaches for Mining + Utilities (2014-2020 DBIR; n=113)

Professional, Scientific, and Technical Services

NAICS	54 – Professional, Scientific, and Technical Services
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	980 (2014-2020) | 326 (2020)
Actors	External (77%), Internal (23%), Partner (3%), Multiple (2%)
Motives	Financial (93%), Espionage (8%), Ideology (1%)
Cyber-Espionage breaches	
Frequency	166 (17%) (2014-2020)
Actors	External (100%), Internal (2%), Multiple (2%)
Actions	Social (74%), Hacking (58%), Malware (84%)
Assets	Person (79%), User Dev (77%), Server (20%)
Data	Secrets (80%), Credentials (14%), Internal (8%)

Summary

The Professional, Scientific, and Technical Services industry has seen approximately 11% of the Cyber-Espionage breaches between 2014 and 2019. Like other private industries, not all Cyber-Espionage breaches are reported.

Since 2015, we have seen a definite decline in reported Espionage-motivated attacks in the Professional industry. We cannot account for the number of unreported breaches.

From the reported breaches, however, we can see that assets Person and User Dev were the top compromised assets and that 80% of compromised data was classified as Secrets.

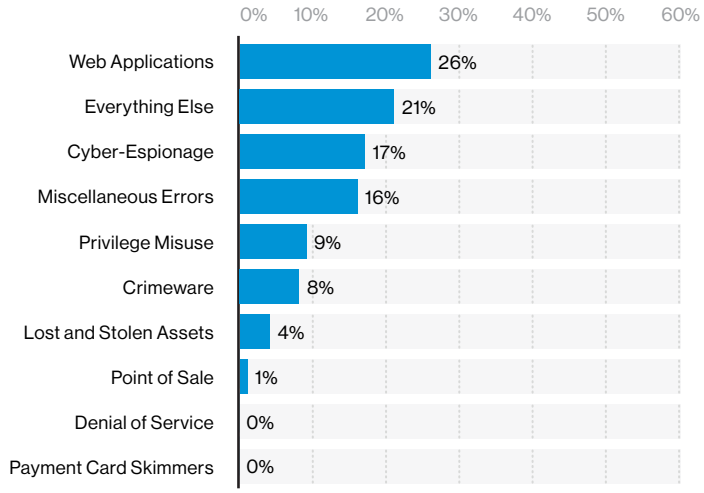


Figure #109: Breaches by pattern for Professional (2014-2020 DBIR; n=980)

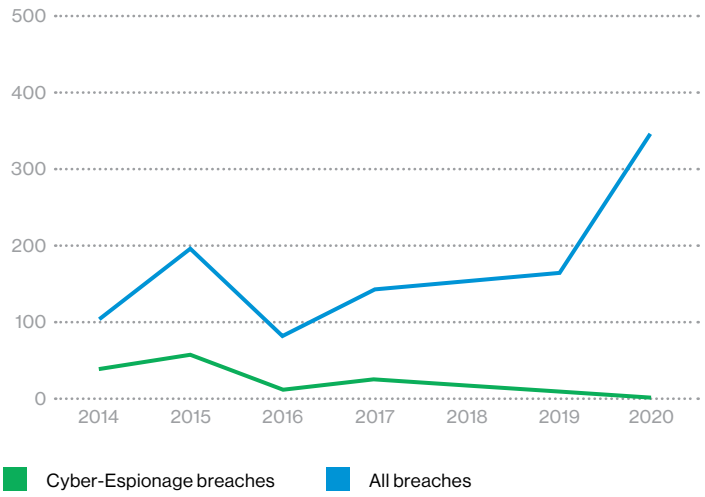


Figure #110: Cyber-Espionage breaches within all breaches annually for Professional (2014-2020 DBIR)

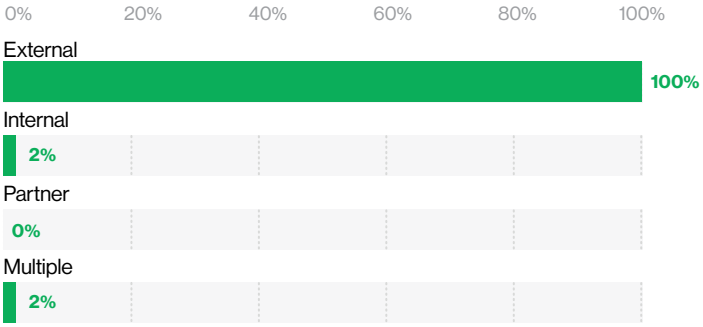


Figure #111: Actors within Cyber-Espionage breaches for Professional (2014-2020 DBIR; n=166)

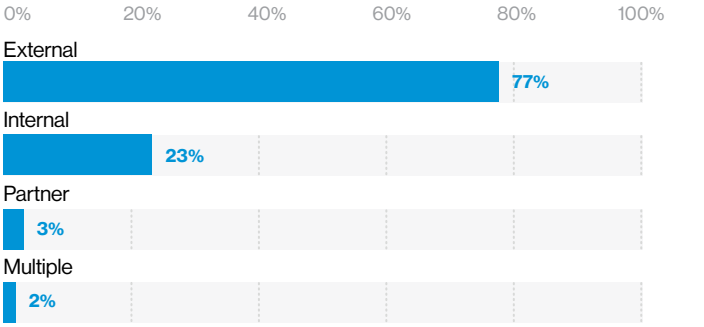


Figure #112: Actors within all breaches for Professional (2014-2020 DBIR; n=976)

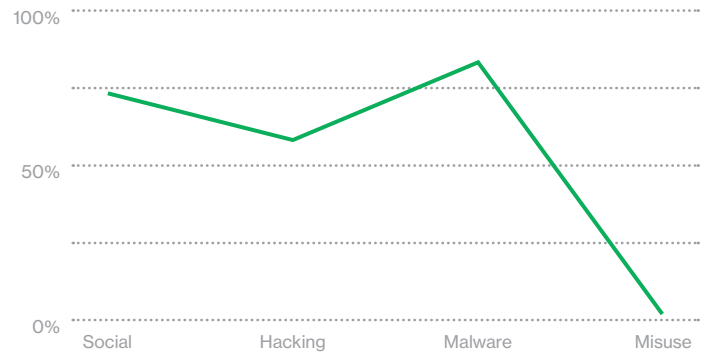


Figure #113: Actions within Cyber-Espionage breaches for Professional (2014-2020 DBIR; n=125)

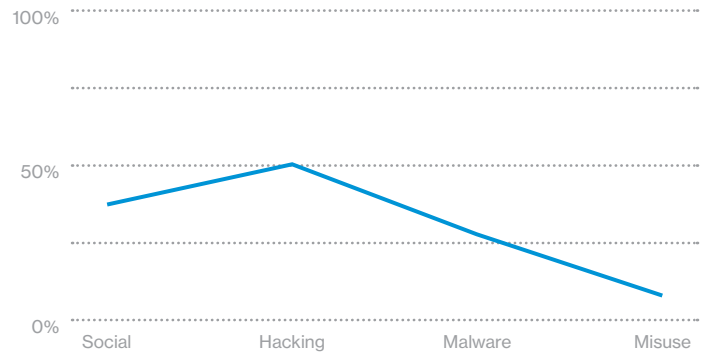


Figure #114: Actions within all breaches for Professional (2014-2020 DBIR; n=923)

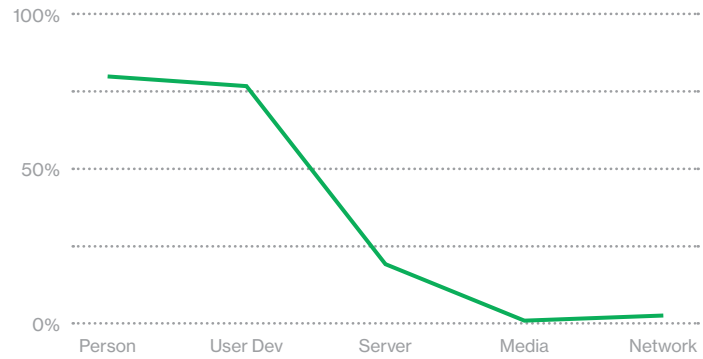


Figure #115: Assets within Cyber-Espionage breaches for Professional (2014-2020 DBIR; n=117)

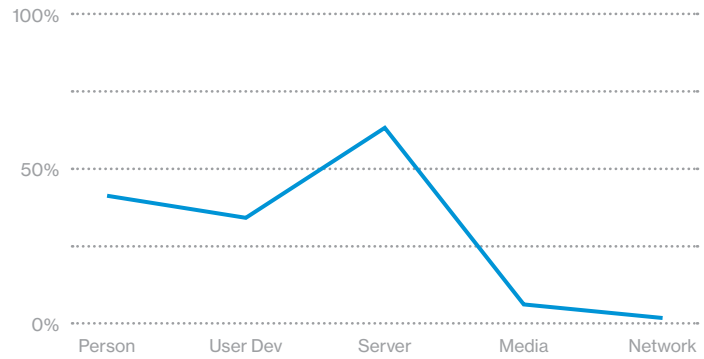


Figure #116: Assets within all breaches for Professional (2014-2020 DBIR; n=859)

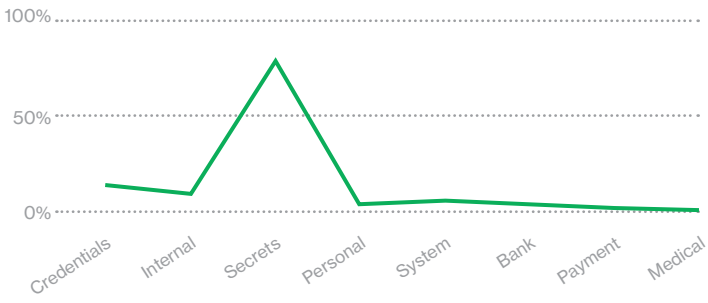


Figure #117: Compromised Data varieties within Cyber-Espionage breaches for Professional (2014-2020 DBIR; n=124)

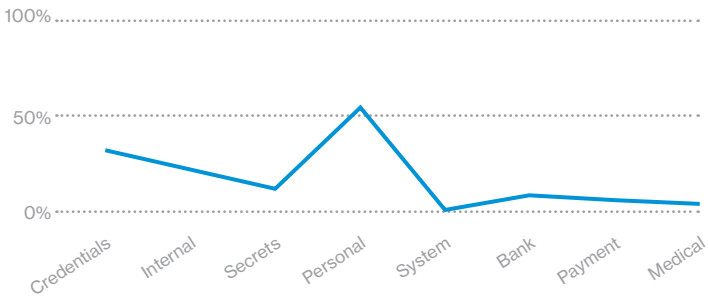


Figure #118: Compromised Data varieties within all breaches for Professional (2014-2020 DBIR; n=816)

Public Administration

NAICS	92 – Public Administration
Remarks	*Unless otherwise stated, information covers the 2014-2020 DBIR timeframe. Also, note the change in scale among figures.*
All breaches	
Frequency	2,152 (2014-2020) | 338 (2020)
Actors	External (61%), Internal (40%), Multiple (3%), Partner (1%)
Motives	Financial (75%), Espionage (19%), Fun (3%)
Cyber-Espionage breaches	
Frequency	485 (23%) (2014-2020)
Actors	External (100%)
Actions	Social (94%), Hacking (93%), Malware (97%)
Assets	Person (96%), User Dev (95%), Server (25%)
Data	Secrets (55%), Internal (42%), Credentials (12%)

Summary

The Public Administration industry has ranked in the past several years as one of the top industries reporting confirmed data breaches with a Cyber-Espionage motive. In fact, in the past three years, nearly half of Cyber-Espionage breaches were reported in the public sector. And, since 2014, nearly a quarter of the Cyber-Espionage breaches were reported in this industry.

There are a few factors to consider when looking at these numbers. We know that government data is one of the top data types of interest to Nation-state and State-affiliated actors, so these numbers don't surprise us. However, it is important to point out that the public industry has more stringent reporting requirements than the private sector, which will inevitably result in more breaches being reported.

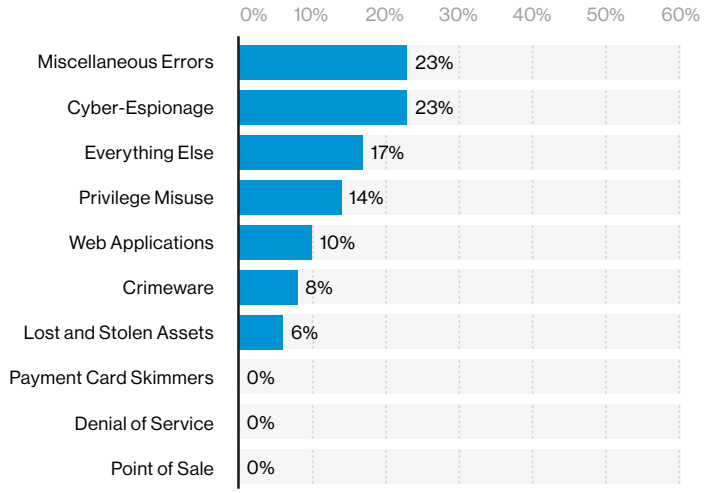


Figure #119: Breaches by pattern for Public (2014-2020 DBIR; n=2,152)

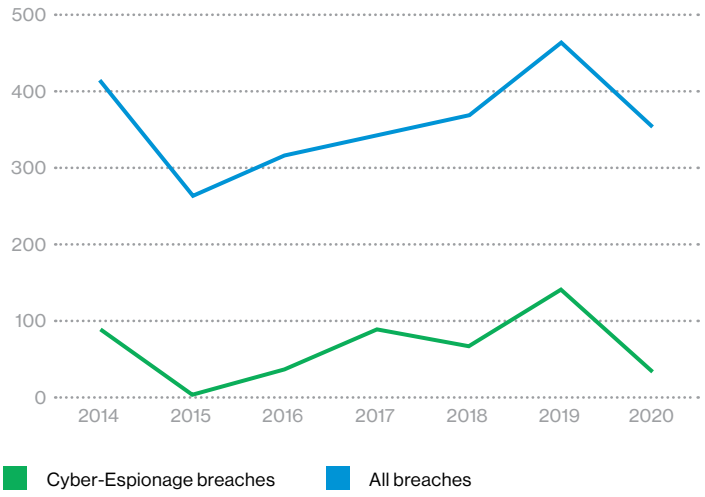


Figure #120: Cyber-Espionage breaches within all breaches annually for Public (2014-2020 DBIR)

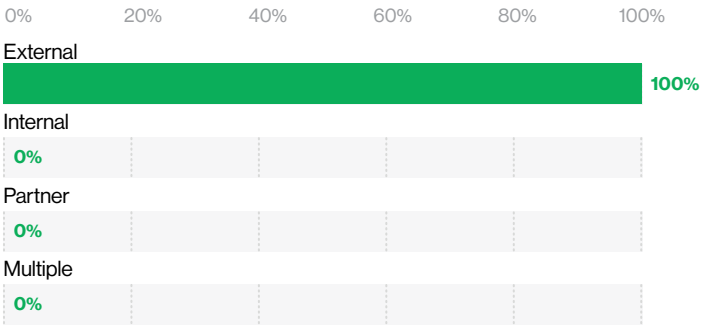


Figure #121: Actors within Cyber-Espionage breaches for Public (2014-2020 DBIR; n=485)

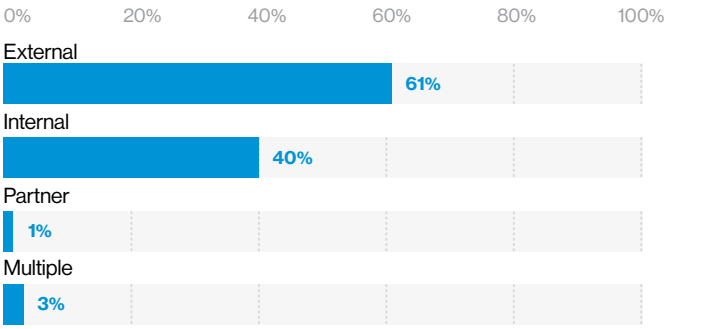


Figure #122: Actors within all breaches for Public (2014-2020 DBIR; n=2,138)

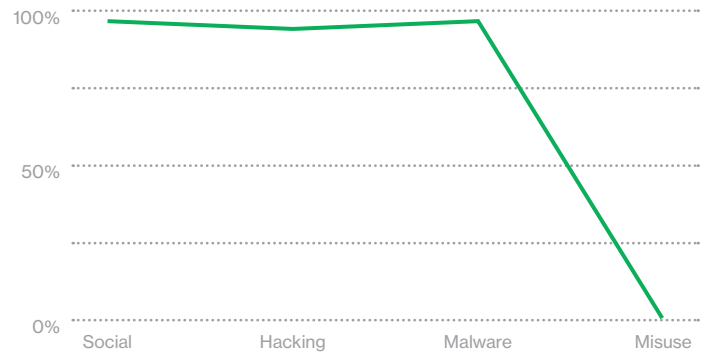


Figure #123: Actions within Cyber-Espionage breaches for Public (2014-2020 DBIR; n=380)

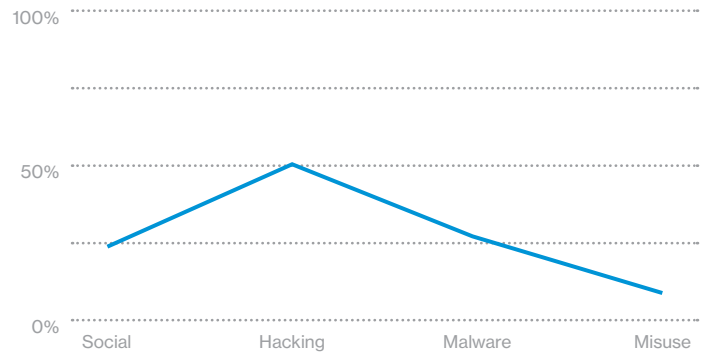


Figure #124: Actions within all breaches for Public (2014-2020 DBIR; n=1,826)

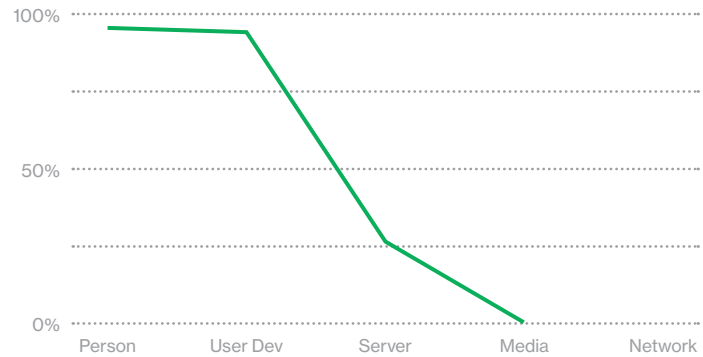


Figure #125: Assets within Cyber-Espionage breaches for Public (2014-2020 DBIR; n=374)

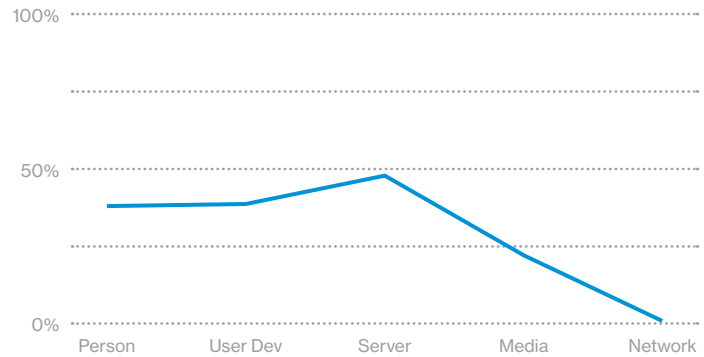


Figure #126: Assets within all breaches for Public (2014-2020 DBIR; n=1,367)

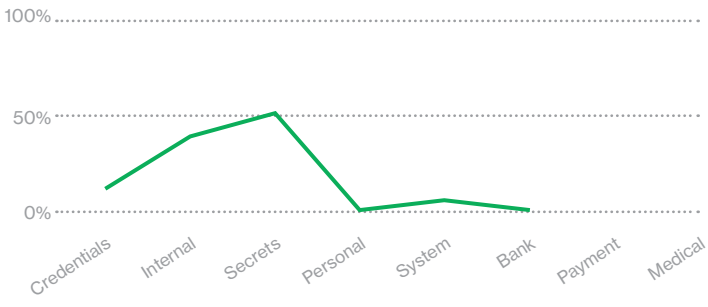


Figure #127: Compromised Data varieties within Cyber-Espionage breaches for Public (2014-2020 DBIR; n=370)

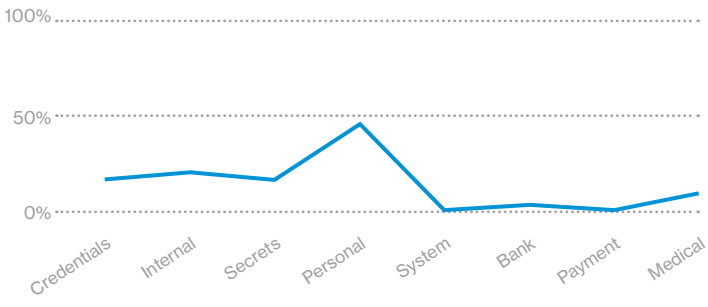


Figure #128: Compromised Data varieties within all breaches for Public (2014-2020 DBIR; n=1,268)

Final notes

Cyber-Espionage Report Team

The Cyber-Espionage Report (CER) Team is a subset of VTRAC combined with elements of the DBIR Team. We've spent years investigating advanced threat actor data breaches, assessing cybersecurity postures and advising on IR measures in our current roles and previous lives.

Managing Director

Chris Novak

Authors

John Grim, Ashish Thapar, Amy Ayers, Anshuman Sharma, Nicolas Villatte, Damian John Werts, Domingo Jesus Alvarez-Fernandez

Contributors

David Kennedy, Alex Pinto, Phillipe Langlois, Suzanne Widup

About VTRAC

The Verizon Threat Research Advisory Center (VTRAC) has been assisting customers globally with maturing and improving their IR readiness for more than 14 years. In conducting its engagements, VTRAC uses industry best practices—such as the NIST Cybersecurity Framework—and our VIPR phases, as well as our expertise from the more than 500 incidents we investigate globally each year. We cover all five functional areas of the NIST Cybersecurity Framework.

Our capabilities include endpoint forensics, network forensics, malware reverse engineering, threat intelligence, threat hunting, dark web research, mobile device forensics and complex data recovery, as well as breach simulations, cyber threat landscape briefings, IR capability assessments, first responder training, and IR Plan and playbook development.

VTRAC has written the book—literally—on data breaches, from starting the DBIR phenomenon and contributing annually to the Payment Security Report to creating the Data Breach Digests, Insider Threat Report, Incident Preparedness and Response Report and now the CER.

With the CER now under our proverbial belts, the only question left unanswered is:

What will VTRAC set its sights on next? *Stay tuned to find out...*

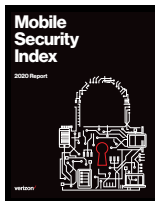
About the cover

Cyber-Espionage breaches occur when external attackers, such as State-affiliated or Nation-state threat actors, penetrate victim organization cyberdefenses to steal sensitive data or proprietary information. The cover image for our first-ever Cyber-Espionage Report depicts a Cyber-Espionage breach at the moment the attacker pierces the veil of security en route to plundering their targeted victim's critical assets and most sensitive information.

Verizon thought leadership

Data Breach Investigations Report (DBIR)

- Data Breaches/Cybersecurity Incidents
- 9 x Incident Classification Patterns | 9 x CIS CSCs
- enterprise.verizon.com/resources/reports/dbir/

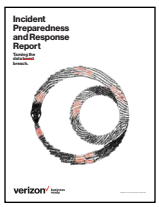


Mobile Security Index (MSI)

- Mobile Devices/IoT/Wi-Fi Security Insight
- 5 x Fortify Levels
- enterprise.verizon.com/resources/reports/mobile-security-index/

Insider Threat Report (ITR)

- Insider Threat Breaches/Cybersecurity Incidents
- 5 x Breach Scenarios | 11 x Countermeasures
- enterprise.verizon.com/resources/reports/insider-threat-report/



Verizon Insider Preparedness and Response (VIPR) Report

- IR Plan review and breach simulation exercise insight
- 5 x Breach Scenarios | 6 x VIPR Phases | 20 x Key Takeaways
- enterprise.verizon.com/resources/reports/vipr/

Payment Security Report (PSR)

- PCI Assessment/PFI Investigation Insight
- 12 x PCI DSS Requirements
- verizon.com/business/resources/reports/payment-security-report/

verizon

verizon.com/business/resources/reports/cyber-espionage-report/
REP11431120