2020-2021

Cyber-Espionage Report

Executive insights

verizon

The Cyber-Espionage Report (CER) is our first-ever data-driven publication on advanced cyberattacks. This report draws from seven years of Verizon Data Breach Investigations Report (DBIR) content, as well as from 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.

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.

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

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).

Within the CER, not only do we identify the aspects surrounding the Cyber-Espionage threat actors and their targeted victims, but we also identify the frameworks and tools needed to help you improve your ability to better prevent, mitigate, detect and respond to these cyberattacks. These frameworks and tools include the Vocabulary for Event Recording and Incident Sharing (VERIS) framework, Verizon Incident Preparedness and Response (VIPR) report phases, National Institute of Standards and Technology (NIST) Cybersecurity Framework, Center for Internet Security (CIS) Critical Security Controls (CSCs), and the North American Industry Classification System (NAICS).

veriscommunity.net/

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

www.nist.gov/cyberframework

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

www.naics.com/

Breach patterns

When it comes to the overall most prevalent types of breaches for the 2014–2020 DBIR time frame, we see that Cyber-Espionage ranks sixth (10%), albeit within close striking distance of Privilege Misuse (ranked fourth at 11%) and the sagging Point of Sale intrusions (ranked fifth at 11%).

Because Cyber-Espionage is a difficult incident pattern to detect, the numbers 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 regulatory requirements.

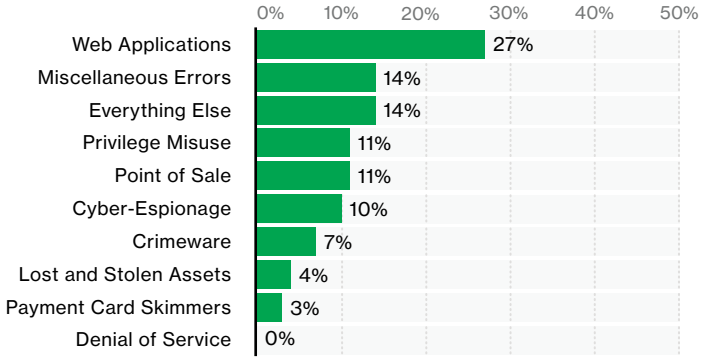

Figure #1: Breaches by pattern (2014–2020 DBIR; n=16,090)

Time to Discovery

In the 2014–2020 DBIR time frame, for Cyber-Espionage threat actors, the Time to Compromise ranges from mere seconds to days, while the Time to Exfiltration ranges from minutes to weeks. For cyberdefenders, the Time to Discovery for Cyber-Espionage breaches is months to years and the Time to Containment ranges from hours to weeks.

The slow, methodical and lengthy process that threat actors employ speaks to the patience and complexity often accompanying Cyber-Espionage attacks. It is indicative of the threat actor's due diligence in understanding the target's environment and cybersecurity posture, and in leveraging that knowledge to accomplish their objectives without detection.

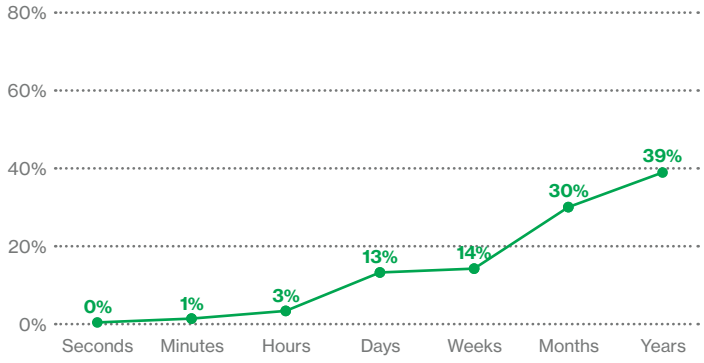

Figure #2: Time to Discovery within Cyber-Espionage breaches (2014–2020 DBIR; n=125)

Targeted victims

Breached industries

Within the DBIR dataset, we identified the industries impacted the most by Cyber-Espionage breaches in the previous seven years (the 2014–2020 DBIR time frame). These industries were (Industry [NAICS #]): Education (61), Financial (52), Information (51), Manufacturing (31–33), Mining + Utilities (21+22), Professional (54) and Public (92).

When we look at how these seven industries fared for Cyber-Espionage breaches, some were more strongly impacted than others: Public (31%), Manufacturing (22%) and Professional (11%) topped the list for Cyber-Espionage breaches.

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—you may just not have visibility into those attacks.

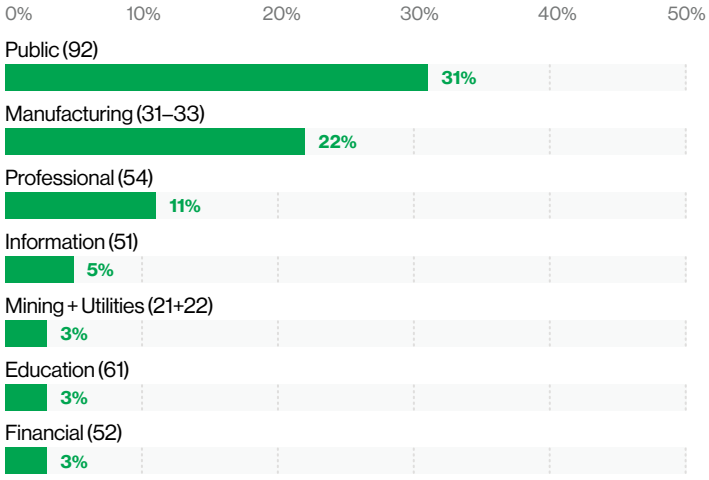

Figure #3: Cyber-Espionage breaches within select industries (2014–2020 DBIR; n=1,580)

Attribute varieties

The top compromised Attribute varieties in Cyber-Espionage breaches include Software installation (Integrity) (91%), Alter behavior (Integrity) (84%), Secrets (Confidentiality) (73%), Internal (Confidentiality) (29%), Credentials (Confidentiality) (21%) and System (Confidentiality) (19%).

In contrast, 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%).

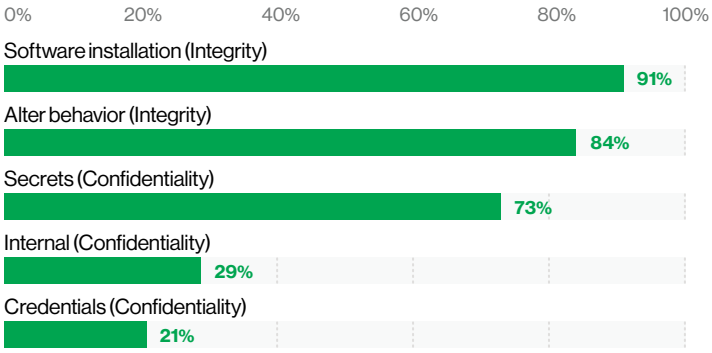

Figure #4: Top compromised Attribute varieties within Cyber-Espionage breaches (2014–2020 DBIR; n=1,571)

Asset varieties

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

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

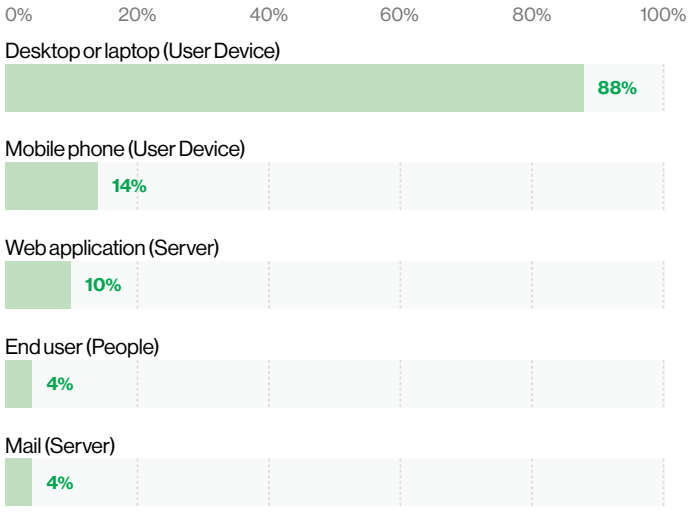

Figure #5: Top compromised Asset varieties within Cyber-Espionage breaches (2020 DBIR; n=113)

Data varieties

The 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%) were the top compromised Data varieties for all breaches.

Threat actors

Actor varieties

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

Actor motives

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

Threat actions

For the 2014–2020 DBIR time frame, 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 threat actors.

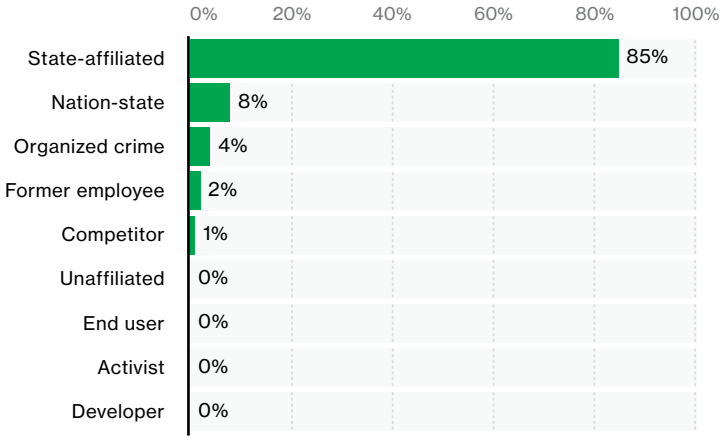

Figure #6: Actor varieties within Cyber-Espionage breaches (2014–2020 DBIR; n=1,435)

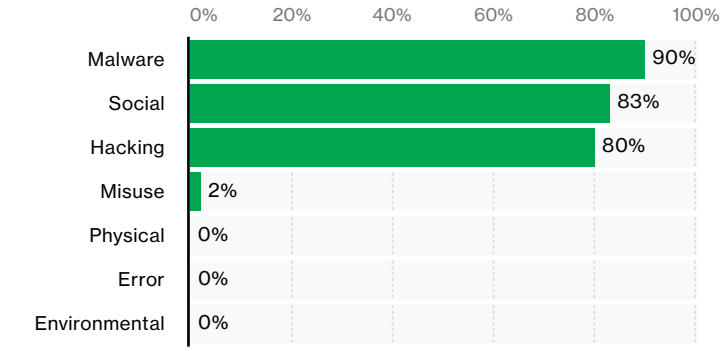

Figure #7: Actions within Cyber-Espionage breaches (2014–2020 DBIR; n=1,580)

Cyber-Espionage vs all breach Action varieties and vectors (2014–2020 DBIR time frame)

VERIS category	Cyber-Espionage breaches	All breaches
Social varieties	Phishing (97%), Pretexting (2%), Bribery (1%)	Phishing (87%), Pretexting (9%), Bribery (3%)
Hacking varieties	Use of backdoor or C2 (86%), Use of stolen creds (30%), Brute force (12%)	Use of stolen creds (63%), Use of backdoor or C2 (39%), Brute force (18%)
Malware varieties	Backdoor (78%), C2 (77%), Downloader (40%), Capture stored data (40%), Spyware/Keylogger (33%), Export data (32%)	C2 (48%), Export data (42%), Spyware/Keylogger (40%), RAM scraper (35%), Backdoor (25%)
Malware vectors	Backdoor (78%), C2 (77%), Downloader (40%), Capture stored data (40%), Spyware/Keylogger (33%), Export data (32%)	Email attachment (43%), Direct install (39%), Email link (9%)

Overall takeaways

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 breach 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.

Asset varieties

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

Data varieties

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

Time lines

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%).

Discovery

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

Actors

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

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.

Action vectors

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

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%)

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

About VTRAC

The Verizon Threat Research Advisory Center has been assisting customers globally with maturing and improving their IR readiness for more than 14 years. We use 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.

If you have any questions or feedback for the VTRAC, send us a note at vtrac@verizon.com or find us on LinkedIn at #cyberespionagereport and #vtrac. To read the full CER, visit enterprise.verizon.com/resources/reports/cyber-espionagereport/