

# 2022 DBIR: Mining, Quarrying, and Oil & Gas Extraction + Utilities

(NAICS 21+22)

Snapshot

**Welcome to the Mining and Utilities snapshot from the 15th annual Verizon Data Breach Investigations Report (DBIR). It is truly hard to believe that it has been 15 years since our inaugural report.**

The DBIR examines common types of cybersecurity attacks and offers insights into how organizations can protect themselves. This year, we looked at 23,896 incidents. Mining and Utilities saw 403 of those incidents, 179 of which had confirmed data disclosure. This data represents real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors.

We hope that you can use this report and the information it contains to increase your awareness of the most common tactics used against Mining and Utilities and to help prepare your organization.

Read on for report highlights related to Mining and Utilities. Also, please pass this summary along to colleagues and download the full report at [verizon.com/dbir](https://verizon.com/dbir) for a more detailed view of the threat landscape in 2022.

**For all industry labels in the DBIR report, we align with the North American Industry Classification System (NAICS) standard to categorize the victim organization. The standard uses two- to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level, and we will specify NAICS codes along with an industry label. Detailed information on the codes and the classification system is available here: [census.gov/naics/?58967?yearbck=2012](https://census.gov/naics/?58967?yearbck=2012)**

## Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to the eight you see in this report.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

---

## Social Engineering

**Psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.**

The human element continues to be a key driver of 82% of breaches, and this pattern captures a large percentage of those breaches. Additionally, malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program.

- Fifty-nine percent of Social Engineering breaches compromised credentials, and 31% used stolen credentials. Credential compromise was three times more likely in Social Engineering breaches than in the rest of the patterns
- Phishing is more than twice as likely as Pretexting in the Social Engineering pattern
- A Financial motive is eight times more common than an Espionage motive in Social Engineering breaches

---

## Basic Web Application Attacks

**Simple web application attacks with a small number of steps or additional actions after the initial web application compromise.**

This pattern continues to largely be dominated by attackers using stolen credentials to access an organization's internet-facing infrastructure, like web servers and email servers.

- Four out of every five web app attacks involved stolen creds. This finding underlies the importance of password safeguards
- Espionage is four times more likely in Basic Web Application Attack (BWAA) breaches than in the rest of the patterns, indicating that Nation-states don't necessarily have to pursue complex attacks to leverage established and effective attacks to achieve their objectives
- Use of stolen credentials is six times more likely than Exploiting a vulnerability in BWAA breaches

---

## System Intrusion

**System Intrusion captures the complex attacks that leverage Malware and/or Hacking to achieve their objectives, including deploying ransomware.**

This pattern consists of more complex breaches and attacks that leverage a combination of several different actions, such as Social, Malware and Hacking, and is where we find Supply Chain breaches and Ransomware, both of which increased dramatically this year.

- Ninety-two percent of System Intrusion breaches are Financially motivated
- Use of stolen credentials is four times more likely than Exploiting vulnerabilities in System Intrusion breaches

---

## Miscellaneous Errors

**Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.**

This year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties. Misconfiguration is frequently paired with the discovery method of "Security researcher."

- Misconfigured servers accidentally exposed to the internet or Misdelivery actions in which users send emails to the wrong recipient represent 13% of total breaches
- External cloud assets have decreased 83% since last year in Miscellaneous Errors breaches, potentially indicating a shift in technologies leveraging a secure-by-default approach
- Eighty-five percent of Miscellaneous Error breaches involved servers

## Privilege Misuse

**Incidents predominantly driven by unapproved or malicious use of legitimate privileges.**

Most of these incidents result in successful data breaches. These actors are still motivated by greed (financial gain) and are stealing Personal data because it is easy to monetize.

- Documents are three times more likely in Privilege Misuse than in the rest of the patterns

---

## Lost and Stolen Assets

**Any incident where an information asset went missing, whether through misplacement or malice.**

The prevalence of theft is driven by the Financial motive—we believe many of the perpetrators of theft are committing the crime with the intention of an immediate payoff by selling the stolen asset.

- The type of data affected by these incidents is the same (almost exactly) as last year. External actors typically perpetrate the thefts, while employees are responsible for losing track of their assets
- Unaffiliated actors are 14 times more likely in Lost and Stolen Assets incidents than in the rest of the patterns

---

## Denial of Service

**Attacks intended to compromise the availability of networks and systems. Includes both network- and application-layer attacks.**

Large organizations are twice as common in Denial of Service (DoS) incidents than the rest of the patterns. While these attacks are a nuisance impacting a large range of organizations, some face these attacks on a regular basis, which may potentially affect their function.

---

## Everything Else

**Everything else isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns.**

## Mining and Utilities

Mining and Utilities face similar types of attacks as other industries, such as those targeting credentials and leveraging Ransomware, but in addition they have a high rate of Social Engineering attacks like Phishing.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	Less
Social Engineering	No change	No change	No change
System Intrusion	No change	No change	Less

Mining, Quarrying, and Oil & Gas Extraction + Utilities (or MQOGEU as we like to say) simply rolls off the tongue. It is an interesting “combined” industry that has had a higher number of engineers. This is perhaps fitting as it seems to be under barrage from the other form of “engineers”—the Social Engineers. This industry has had a higher rate of Social Engineering breaches than its peers.

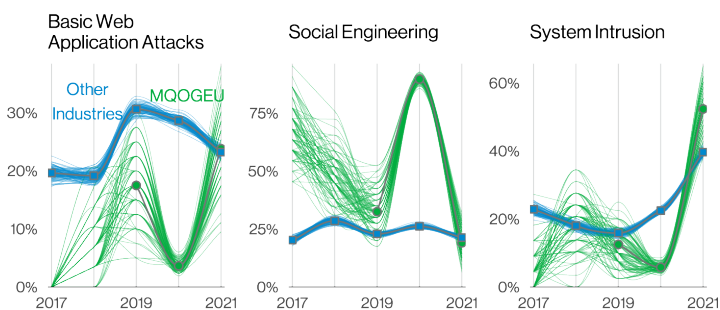
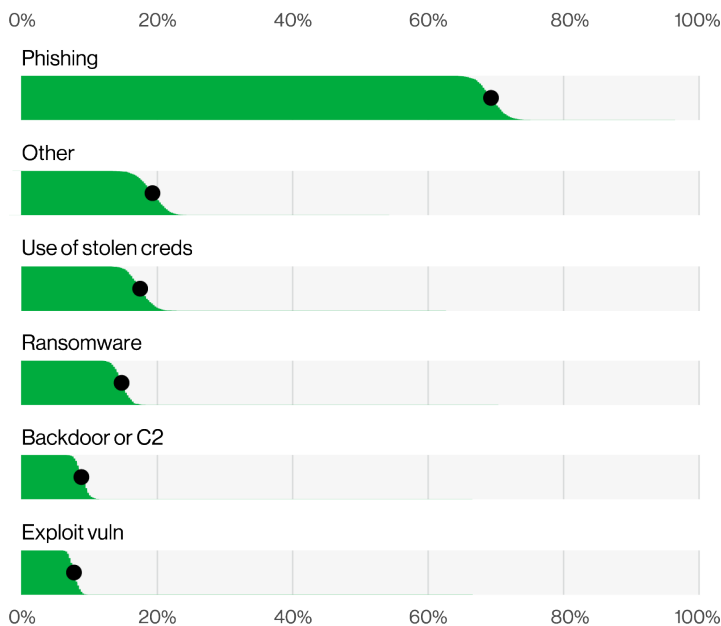


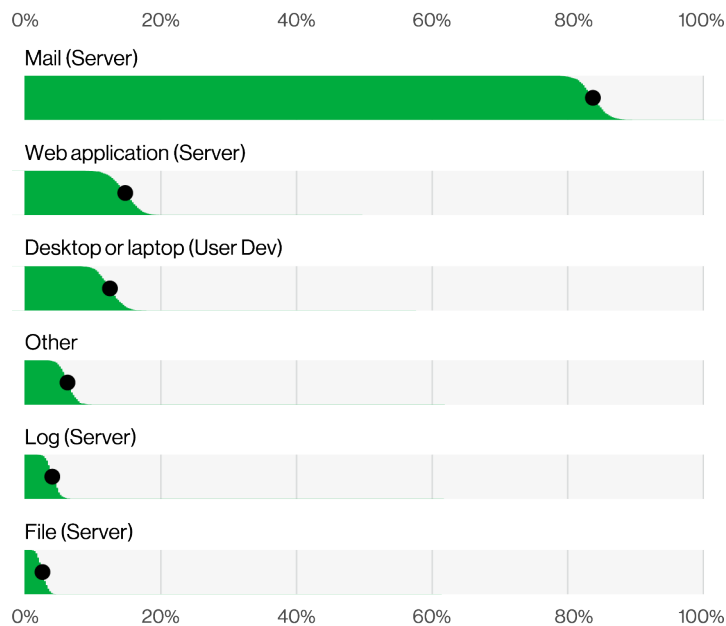
Figure 1. Top patterns over time in MQOGEU breaches

<b>Frequency</b>	403 incidents, 179 with confirmed data disclosure
<b>Top patterns</b>	Social Engineering, System Intrusion and Basic Web Application Attacks represent 95% of breaches
<b>Threat actors</b>	External (96%), Internal (4%) (breaches)
<b>Actor motives</b>	Financial (78%), Espionage (22%) (breaches)
<b>Data compromised</b>	Credentials (73%), Personal (22%), Internal (9%) (breaches)
<b>Top IG1 protective Controls</b>	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
<b>What is the same?</b>	This industry continues to be targeted by financially motivated actors as well as actors committing espionage.





**Figure 2.** Top Action varieties in MQOGEU breaches (n=153)



**Figure 3.** Top Asset varieties in MQOGEU breaches (n=130)

**Being confident in our data**

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain.

The slant on the slanted bar chart represents the uncertainty of that data point to a 95% confidence level (which is standard for statistical testing).

Spaghetti charts, and our relative newcomer, pictogram plots, attempt to capture uncertainty in a similar way to slanted bar charts but are more suited for a single proportion.

And it shows, as more than 60% of all breaches are Phishing (Figure 2), followed by stolen credentials (potentially gathered by Phishing) and Ransomware (potentially tangential to Phishing). Given the key importance of this industry to our everyday well-being, we certainly hope that those credentials aren't the only thing keeping our utilities and mining operations safe, especially since that's one of the most commonly breached data types.

Considering the high prevalence of Phishing and credential attacks, it's not too surprising to have Email servers as this industry's most commonly breached asset, followed by Web application and Desktop. Even though the infrastructure that runs these complex systems isn't traditional IT infrastructure, the company can still be exposed to the very same threats as any other organization.

**Stay informed and threat ready.**

Successfully navigating through the cyberthreats facing Mining and Utilities today requires intelligence from a source you can trust. The full DBIR contains real-world details on the actors, actions and patterns that can help you to prepare your defenses and educate employees.

**Read the full 2022 DBIR at [verizon.com/dbir](https://www.verizon.com/dbir)**