KOVRR
Cyber Decisions. Financially Quantified.

# *Investigating* the Risk of Compromised Credentials and *Internet-Exposed Assets*

GUY PROPPER | DATA TEAM LEAD

NOVEMBER 2023

www.kovrr.com

# Introduction

For this report, Kovrr collected and analyzed data to better understand one of the most common initial access vectors[1] - the use of compromised credentials (Valid Accounts - T1078)[2] to access internet-exposed assets (External Remote Services - T1133)[3]. The toxic combination of these two initial access vectors can allow malicious actors to gain a foothold in company networks before moving on to the next stage of their attack, which can be data theft, ransomware, denial of service, or any other action. There are numerous examples of breaches perpetrated by many attack groups that have occurred using this combination, for example, breaches by Lapsus[4] and APT39[5].

This report seeks to demonstrate which industries and company sizes have the highest percentage of compromised credentials and number of internet-exposed assets and face a higher risk of having their networks breached by the toxic combination of the initial access vectors mentioned above.

It should be noted that having an asset exposed to the internet does not inherently pose a risk or indicate that a company has poor security. In our highly digitized world, companies are required to expose services to the internet so these services can be accessed by customers, vendors, and remote employees. Such services include VPN servers, SaaS applications developed by the company, databases, and shared storage units. However, there are some common cases when having an asset exposed to the internet can be extremely risky, for example:

1. When a company unintentionally exposes an asset due to misconfiguration.
2. When a malicious third party obtains compromised credentials of a legitimate third party and accesses an exposed asset.

To limit unnecessary internet exposure, companies should employ the following possible mitigations:

1. Use Multi-Factor Authentication (MFA) for any services or assets that require a connection so that compromised credentials on their own will not be enough to breach an exposed asset.
2. Limit access to the asset to only specific accounts, domains, and/or IP ranges.
3. Segment the internal company network and isolate critical areas so that even if a network is breached through access to an external asset, attackers will not be able to use that access to reach wider or more sensitive areas of the company network.

[1] https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

[2] https://attack.mitre.org/techniques/T1078/

[3] https://attack.mitre.org/techniques/T1133/

[4] https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

[5] https://www.mandiant.com/resources/blog/apt39-iranian-cyber-espionage-group-focused-on-personal-information

# Summary

The following are the main findings from the collected data:

- The Services industry is by far the most exposed to attackers. Companies from this industry have the highest percentage of compromised credentials (74%). However, they have a relatively low amount of internet-exposed assets per company (34%). Still, given that an average cyber loss in this industry has been shown to be about $45M, this is highly concerning[6]. The Services industry (SIC Division I) is followed by Division E (Transportation, Communications, Electric, Gas, and Sanitary Services, with an average loss around $58M), which is followed by Division D (Manufacturing, with an average loss of around $25M).

- The revenue range for companies with the highest number of compromised credentials is $1M-$10M, followed by $10M-$50M.

  A similar trend is also observed when evaluating company size by the number of employees. Companies with fewer employees have a higher share of compromised credentials.

- On average, the larger the company (both in terms of revenue and number of employees), the greater the number of internet-exposed assets.

- There is a correlation between the industries and revenue ranges of companies targeted by ransomware and those with the highest share of compromised credentials.

# Methodology

The data for this research was collected as follows:

1. Data regarding compromised credentials was first collected from Hudson Rock, a provider of various cybercrime data. Data was collected for the previous six months, beginning March 2023.

2. This data was filtered to focus on compromised credentials employees use to access large cloud providers. The relevant credentials were then further filtered to focus only on credentials used for work-related access and not personal access.

3. The domains obtained from these credentials were then enriched with firmographic data such as industry, revenue, and number of employees.[7]

4. The domains that were successfully enriched (and thus deemed valid) were scanned in Shodan to uncover any internet-exposed assets.

[6] https://www.kovrr.com/reports/fortune-1000-cyber-risk-report

[7] Enrichment done through https://www.thecompaniesapi.com/api/

# Limitations

## It is important to note that the compromised credentials found are not necessarily credentials for the internet-exposed assets found on Shodan.

However, as password reuse is extremely common among users, with a recent survey showing 84% of users reuse passwords[8] and an older survey finding that 64% of Fortune 1000 employees reuse their passwords[9], it is likely that a compromised corporate identity will be reused for more than one corporate asset, and thus enable attackers to access exposed corporate assets.

The purpose of this report is not to uncover specific internet-exposed assets which are easy to exploit but rather to understand which types of companies face a higher risk from having both compromised credentials and internet-exposed assets. An opportunistic attacker might exploit some of the compromised credentials, which could be used for an internal company service, to gain access to external company services.

[8] https://bitwarden.com/blog/a-closer-look-at-password-statistics/

[9] https://spycloud.com/blog/password-reuse/

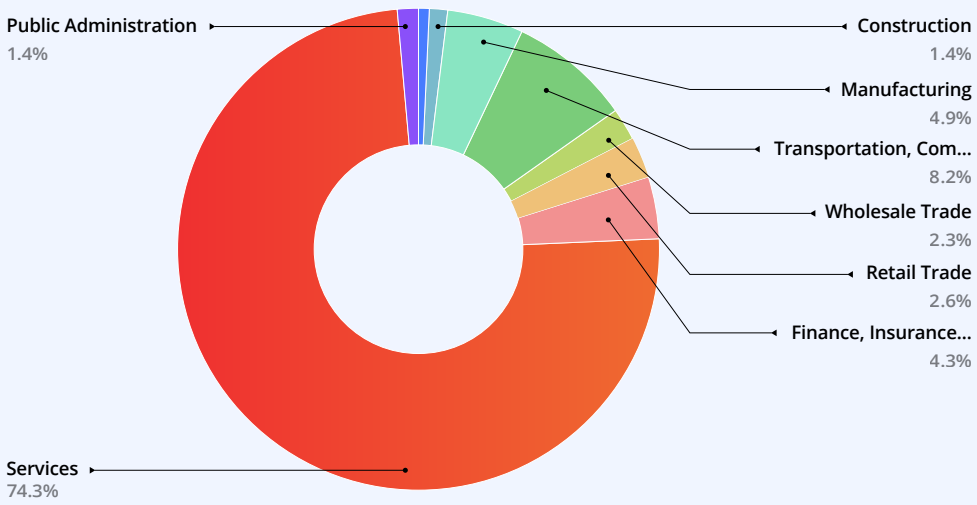
# Findings

The findings from the collected data are presented in the following section. We first analyzed the results based on industry, followed by company size. In each analysis, we show relative risk broken down by several firmographic elements to reveal which company profiles have the highest relative risk of loss triggered by the toxic combination of compromised credentials and internet-exposed assets.

# Exposure by Industry

The first finding presented in the report is the percentage of compromised credentials per industry. Industries were classified according to SIC divisions. Figure 1 shows the distribution of compromised credentials by the SIC division.

Figure 1: Compromised Credentials by SIC Division




The Services industry (Division I) is by far the most exposed industry, with included companies having the highest percentage of compromised credentials. The second riskiest industry by a wide margin is Division E (Transportation, Communications, Electric, Gas, and Sanitary Services), followed by Division D (Manufacturing). The prominence of compromised credentials within the Services industry could be explained by a high reliance on providing services to third parties and being a heavy user of cloud infrastructure and other online services.

Within these industries, we also collected data on the SIC Major Groups with the highest share of compromised credentials. Major Groups offer a more granular overview of the riskiest industries, as each SIC Division[10] contains several SIC Major Groups.

The top two groups by a large margin are Business Services (Major Group 73) and Educational Services (Major Group 82). Both of these industries have a

[10] https://www.osha.gov/data/sic-manual

high number of external third-party clients, especially in the Education industry, where each company provides services to many students. Therefore, it is much more challenging to monitor the security and exposure of these clients due to their larger attack surface. The Education industry also has a greater amount of decentralized administration, especially in Higher-Ed institutions, where research programs often go unmonitored by central IT and security teams.

In addition to the data above, the average number of internet-exposed devices per SIC division was also examined. It can be seen in Figure 2 that the industry with the most devices exposed on average per company is Public Administration, with 61.55 devices, while the second most exposed industry is Wholesale Trade, with 55 devices per company.

Figure 2: Internet-Exposed Assets by SIC Division, Average per Company


By combining the two sources of data, we gain a more concrete understanding of the riskiest industries, which are those that have both a high share in the ratio of compromised credentials and a relatively high number of internet-exposed assets per company.

While the Services industry has an extremely high share of compromised credentials, the average number of exposed assets per company is relatively low, signifying that attackers have less exposed assets to target with these credentials, potentially decreasing the chances of a successful attack. On the other hand, while the Public Administration industry has a very low share of compromised credentials, an average company in the industry has a relatively high number of exposed assets, increasing its attack surface.

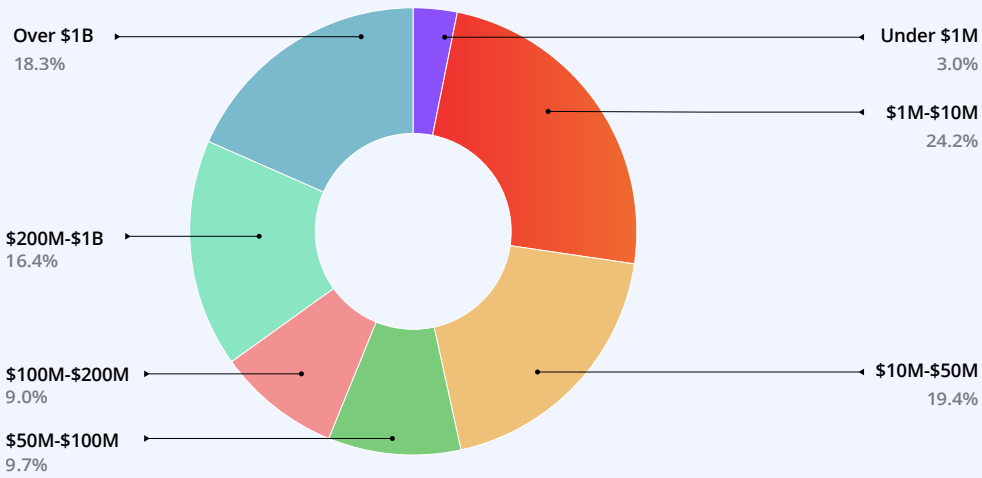
## Exposure by Company Size

Another factor that determines the risk of a company is its size. Company size is often determined by its revenue, number of employees, or both. The next section will give an overview of company exposure byz company size, presenting data for both company revenue and employee range.

## By Company Revenue

Figure 3 shows the percentage of compromised credentials by company revenue.

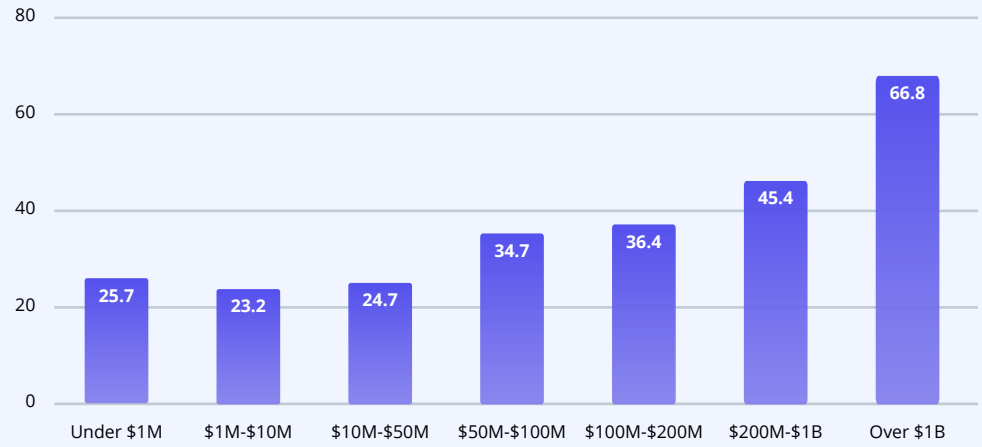
Figure 3: Compromised Credentials by Revenue




The revenue range with the highest percentage of compromised credentials is $1M-$10M, followed by $10M-$50M, then >$1B. This trend could be because companies with a lower revenue range, while in general having fewer assets and employees than companies with a higher revenue range, have a lower level of security expertise and security investment compared to large enterprises. Thus, they are ill-equipped to prevent or monitor their exposure as efficiently as larger companies.

We also collected data on the number of internet-exposed devices per revenue range, which can be seen in Figure 4.

Figure 4: Internet-Exposed Assets by Revenue, Average per Company

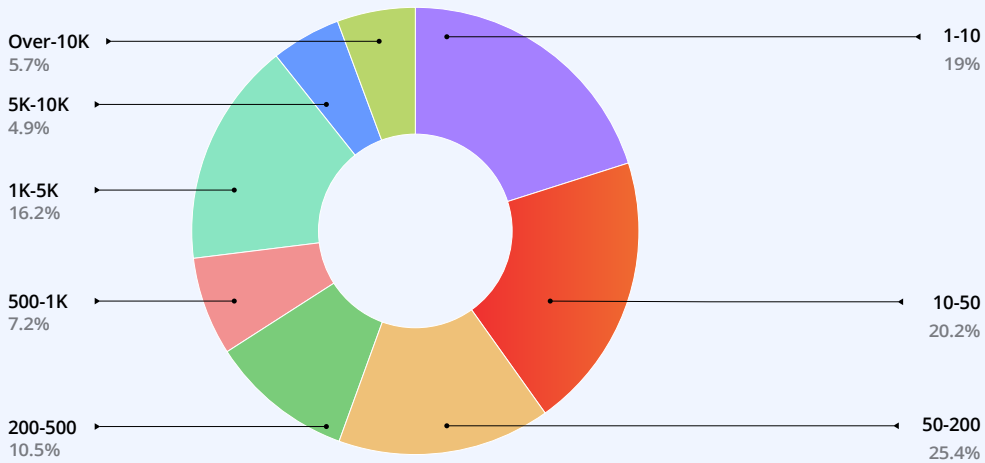


In general, the larger the company's revenue range, the higher the number of exposed assets. This finding is expected, given that a company's revenue range highly correlates with its size.

## Exposure by Number of Employees

Data on the percentage of compromised credentials by the number of employees was also evaluated. As the revenue data reveals, companies with fewer employees also have a higher share of compromised credentials.

Figure 5: Compromised Credentials by Number of Employees




Additionally, the average number of internet-exposed assets also increases along with the number of employees in a company.

Figure 6: Internet-Exposed Assets by Number of Employees, Average per Company

# Ransomware Risk

In July 2023, Kovrr released the Ransomware Threat Landscape Report for H1-2023[11]. In the report, we analyzed the exposure of various industries and company sizes to ransomware attacks.

The report identified Services (42% of attacks), Manufacturing (18%), and Wholesale Trade (8.5%) as the industries most targeted by ransomware in the first half of 2023. Though the exact numbers differ, the trend seen in the current report is very similar. The industry with the most compromised credentials is the Services industry, followed by Transportation, Communications, Electric, Gas, and Sanitary Services (the 4th most ransomware-targeted industry), and Manufacturing. Although outside the scope of the current report, it can be assumed that the higher amount of compromised credentials is one of the reasons why ransomware actors target these industries.

The Ransomware report also identified small companies with a revenue range of $1M-$50M as the most common ransomware targets (targeted in 59% of all attacks during this period). The ratio of compromised credentials for this revenue range within the current report is also very similar, with around 43% of companies with compromised credentials having a revenue range of $1M-$50M.

One key difference between the two reports is that companies with the largest revenue range (>$1B) are not common ransomware targets (8% of attacks) but nevertheless have a large share of compromised credentials, just over 18%. This could be due to a simple reason: Companies with a larger revenue are generally bigger companies with more employees. Therefore, they are more likely to have at least one of their credentials compromised than smaller companies.

[11] https://www.kovrr.com/reports/the-ransomware-threat-landscape-h123

**GUY PROPPER** is the Head of Data at Kovrr and has extensive expertise in reverse engineering, malware research, and threat actor analysis. Prior to that, Guy was the head of the Threat Intelligence and Deep Learning Group at Deep Instinct, and participated as a speaker in Defcon 26. Guy has over ten years of cyber security experience, and holds a B.Sc. in Biology and Cognitive Science from the Hebrew University in Jerusalem.

KOVRR's cyber risk quantification platform empowers enterprise decision-makers to manage cyber exposure more effectively by providing an in-depth risk analysis that drives actionable, financially justified decisions.

Regardless of an organization's current framework, model, or risk register, Kovrr leverages the data and elevates the relative level of insight. Our enterprise-ready solution offers security teams a sharper, more granular risk assessment that's scalable on demand.

Learn more about how Kovrr can help your enterprise revamp its cyber risk management program today with CRQ by reaching out to contact@kovrr.com.