BLOG

“Keys to the Kingdom” at Risk: Analyzing Exposed SSO Credentials of Public Companies

Written by Noah Stone

Research by Matan Tamir, Dana Gindes, Nuno Cardoso

BITSIGHT®
The Standard in SECURITY RATINGS

BLOG

"Keys to the Kingdom" at Risk: Analyzing Exposed SSO Credentials of Public Companies

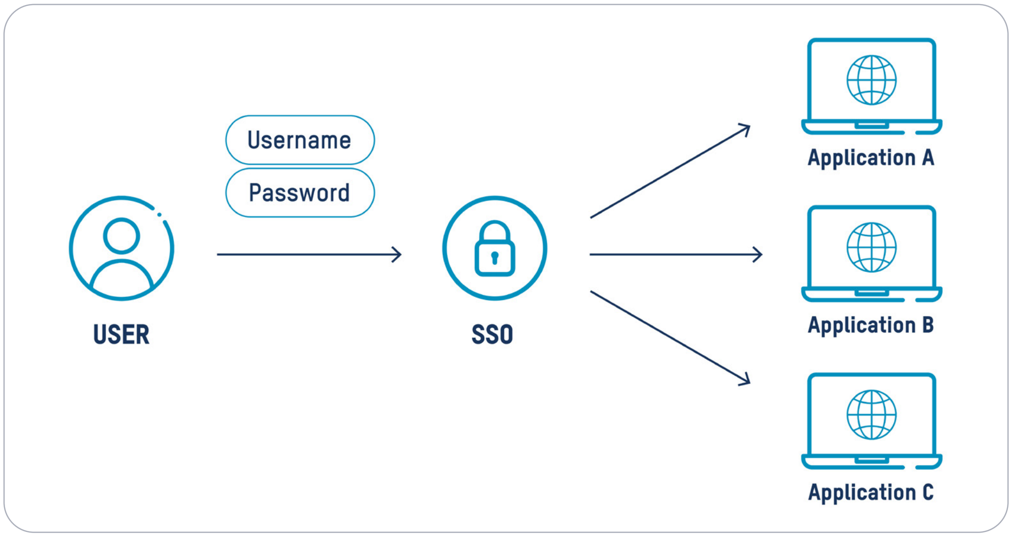
Single sign-on (SSO) credentials are considered "the keys to the kingdom" by cybersecurity professionals. Employees access many applications by logging in once with these credentials, and they're the last thing an organization wants stolen or for sale on the dark web. If malicious actors obtain your organization's SSO credentials, they could access your systems and data like a trusted insider, including payroll, contracts, intellectual property, and more. In short, a malicious actor can inflict significant damage upon an organization by obtaining its SSO credentials.

Unfortunately, even the world's largest and most important companies are struggling to secure these critical assets. Scouring the dark web for critical SSO credentials associated with publicly traded companies, BitSight found that **25% of the S&P 500** and **half of the top 20 most valuable public U.S companies have had at least one SSO credential for sale on the dark web in 2022**. These affected companies may be at risk, along with their global customer bases.

This analysis will review our findings and explain how your organization can protect itself.

WHAT IS SSO, AND WHY IS IT POPULAR?

With SSO, a user accesses many applications with one login. If signed into the SSO, an access token is sent to the application thereby granting the user access. Otherwise, the user is prompted to sign into the SSO to gain access. Ultimately, the user signs in once and freely navigates to applications without entering additional credentials.



Connected applications could include Gmail, Google Drive, Zoom, Slack, Salesforce, Microsoft 365, and others.

Many organizations use SSO. Here's why it's so popular:

- Fewer credentials mean less phishing targets.
- Less login time means employees spend more time working on business-critical tasks.
- Fewer credentials mean fewer password reset requests, thereby lowering IT costs.

Although SSO is strongly recommended by cybersecurity professionals, improper implementation, misuse, or SSO credential theft can present critical security threats.

STOLEN CREDENTIALS CAN LEAD TO SERIOUS DATA BREACHES

Cyber attackers can cause harm to an organization by stealing either **the organization's credentials or their third-party suppliers' credentials.**

Malicious actors leverage the dark web to buy and sell these stolen credentials. The dark web is an intentionally-hidden area of the Internet used for illegal activity. Users must use a specific browser and may need special authorization to access these dark sites.

Recent reports have revealed a close relationship between stolen credentials and successful cyber attacks. According to the 2022 Verizon Data Breach Investigations Report, stolen credentials are:

- Responsible for nearly 50% of all cyber attacks.
- The most common attack vector.
- Up nearly 30% from 2017.

These trends continue in 2022:

- In an attack targeting major SSO vendor Okta, attackers used **compromised credentials from one of Okta's vendors to breach Okta**. Okta promptly terminated their relationship with the vendor.
- A massive phishing attack **compromised nearly 10,000 login credentials and over 5,000 multi-factor authentication (MFA) codes from 136 companies.** Twilio's internal systems were breached, compromising 163 customers' data, including Okta.

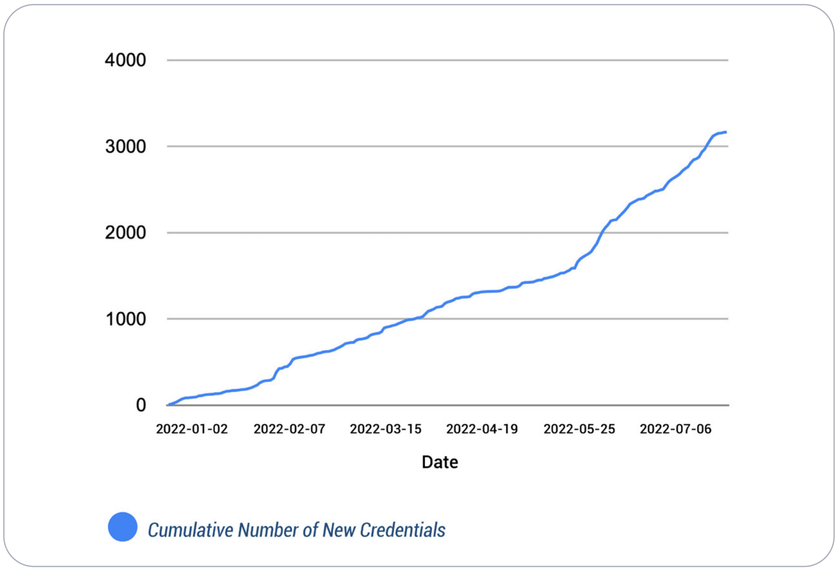
It's clear – attackers are ruthlessly leveraging stolen credentials to breach organizations. And there's arguably no more important credential than the SSO credential because of the unique, broad access it provides the user.

BITSIGHT'S ANALYSIS OF EXPOSED PUBLIC COMPANY SSO CREDENTIALS

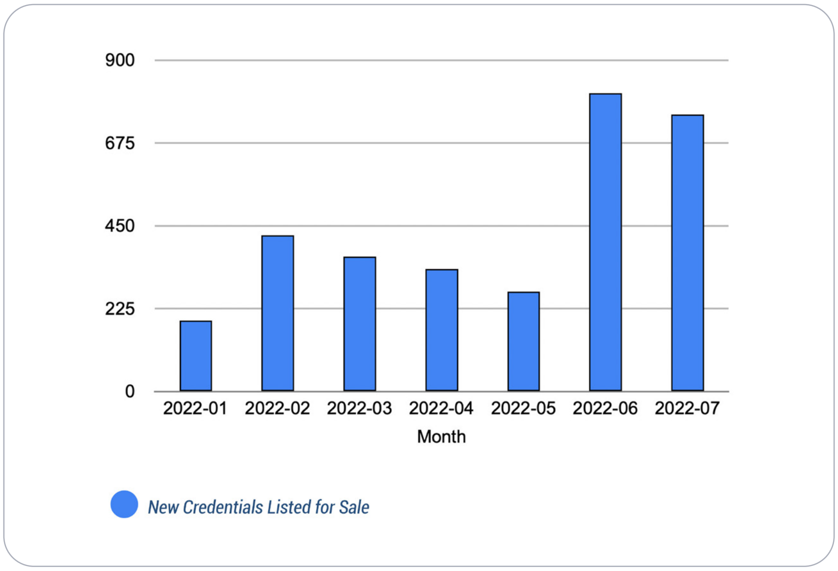
Given the criticality of the SSO credential, are organizations effectively protecting these assets? BitSight analyzed the security posture of three thousand publicly traded companies to understand how the world's most valuable and best-resourced companies are protecting their critical SSO credentials. We found that **over 25% of the S&P 500, and half of the top 20 most valuable public U.S. companies had SSO credentials for sale on the dark web in 2022. The affected companies represent $11 trillion in value**, roughly equivalent to the combined economies of Germany, India, the U.K., and France.

SSO Credentials For Sale on the Dark Web are Skyrocketing

BitSight began our study in January 2022. Since then, we have observed steady growth in the number of public company SSO credentials available for sale on the dark web. (Note: these credentials have not been tested by BitSight.)



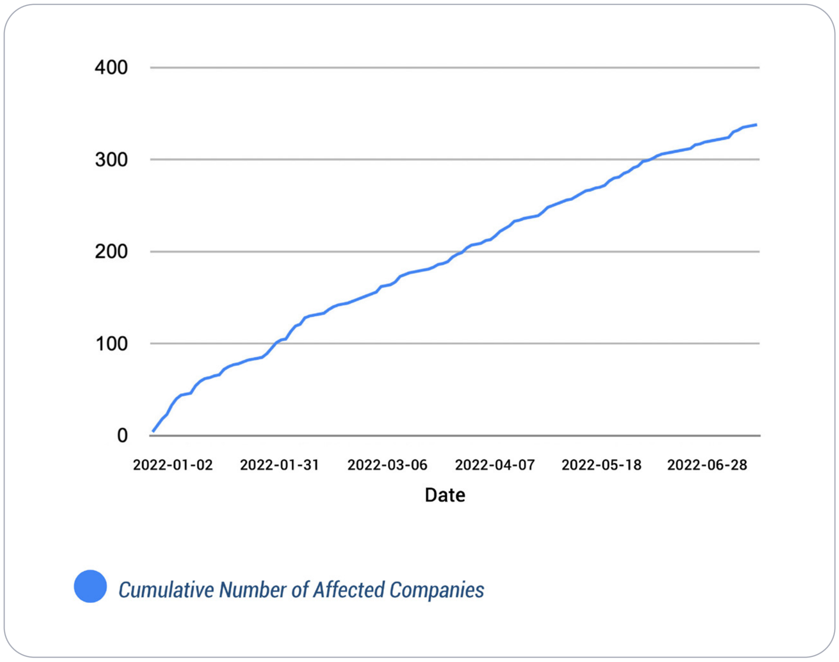
Over 1,500 new SSO credentials became available for sale in June and July alone.



How can so many credentials be impacted? SSO credentials can be easily stolen and challenging to protect, making subsequent threats very real. "Credentials can be relatively trivial to steal from organizations, and many organizations are unaware of the critical threats that can arise specifically from stolen SSO credentials. These findings should raise awareness and motivate prompt action to become better acquainted with these threats," says BitSight Co-Founder and CTO Stephen Boyer.

Growing Number of Impacted Companies

In addition to the sheer number of credentials being stolen and sold on the dark web, BitSight also observed a steady increase in the number of public companies that have SSO credentials for sale on the dark web.

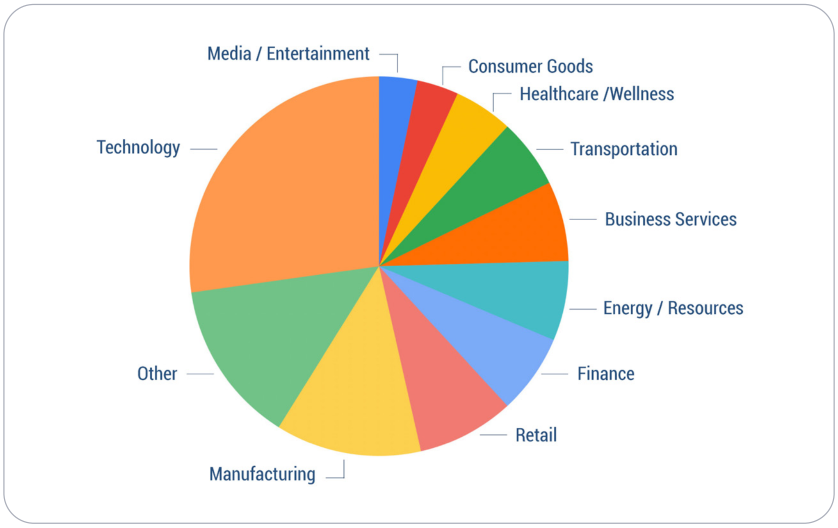


These credentials can be used to gain access to an organization's sensitive information and operations, potentially impacting the organization as well as its customer base.

Interestingly, **organizations that demonstrate stronger cybersecurity performance as measured by BitSight are less likely to have exposed SSO credentials**. Of the three thousand public companies we analyzed, BitSight found that organizations with their SSO credentials for sale on the dark web had a mean BitSight rating of 672; organizations that did not have SSO credentials exposed have a mean BitSight rating of 711.

Sector impact

While BitSight observes that public companies from all sectors and industries have compromised SSO credentials for sale, we find that companies in Technology, Manufacturing, Retail, Finance, Energy, and Business Services are most affected.



The fact that so many public Technology companies have SSO credentials for sale is highly concerning. “Businesses need to be aware of the risks posed by their major IT vendors. As we’ve seen repeatedly, insecure vendor credentials can provide malicious actors with the access they need to target large customer bases at scale. The impact of a single exposed SSO credential could be far reaching,” adds Boyer.

THREE THINGS ORGANIZATIONS SHOULD DO

How should organizations protect themselves from threats to their most sensitive credentials? In addition to those presented in a previous BitSight blog, security professionals should keep a few key recommendations in mind.

Go Beyond Traditional MFA

Phishing is a popular way to steal SSO credentials, even if MFA is enabled. A bad actor might impersonate an organization’s SSO provider by sending a fake login page to an employee. Once the employee enters their credentials and provides their MFA code, the bad actor can log into the account and access data and applications like a trusted insider. MFA is rendered useless if your employees hand them over to bad actors. More secure options include:

Adaptive MFA

- Requires MFA based on geolocation, day and time, and suspicious activity.

Universal two-factor (U2F) authentication

- Uses an origin-bound physical key, **causing authentication to fail on fake sites**. A recent attack on Cloudflare was thwarted because of Cloudflare’s use of U2F keys.

Implement Least Privilege

Limit who can access critical systems so an attacker using a compromised account can do less damage. This means reducing the number of applications the average employee can access to only those that are necessary for the job.

Manage Risk from Third-Party Vendors

Attackers could breach your organization by breaching a third-party vendor. It is important to understand the security posture of vendors to ensure they are adequately protecting their organization and yours.

- Analyze your third-party suppliers’ cybersecurity prior to entering into a business relationship. Leverage continuous monitoring to baseline what’s normal and to detect suspicious activity on your third parties’ networks.
- Examine your Technology relationships closely. Know what you share with your SaaS providers. How sensitive is the data? Who has access to it?

In addition to understanding your own organization’s exposure, it’s critical to manage risk arising from your third-party ecosystem. Stolen credentials from a single vendor could lead to the breach of your organization, threatening your business relationships and the confidentiality of your data. Contact BitSight to learn how we can help.

ABOUT BITSIGHT

BitSight transforms how organizations manage cyber risk. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third-party risk; underwrite cyber insurance policies; conduct financial diligence; and assess aggregate risk. With the largest ecosystem of users and information, BitSight is the Standard in Security Ratings. For more information, please visit **www.bitsight.com**

OUR OFFICE LOCATIONS

BOSTON (HEADQUARTERS)
111 HUNTINGTON AVE
SUITE 2010
BOSTON, MA 02199, USA
PHONE: +1-617-245-0469

RALEIGH
510 GLENWOOD AVE, SUITE 301
RALEIGH, NC 27603, USA

LISBON (EMEA HEADQUARTERS)
CENTRO EMPRESARIAL ESPAÇO 7 RIOS
ESCRITÓRIO 50 (0.04), PISO -1
RUA DE CAMPOLIDE, Nº 351
1070-034 LISBON, PORTUGAL
PHONE: +351 217252110

ISRAEL
TOTZERET HAARETZ ST. 7
4TH FLOOR
TEL AVIV-YAFO, ISRAEL

SINGAPORE
7 TEMASEK BOULEVARD
LEVEL 32 SUNTEC TOWER 1
SINGAPORE 038987

FOLLOW US ON:

BITSIGHT®
The Standard in SECURITY RATINGS