Cyberint
A Check Point Company

The Rise of Leaked Credentials

July 2025

Table of Contents

How to detect stolen credential attacks 3

The surge of leaked credentials 4

Stolen credential attack trends 5

How do hackers steal credentials? 8

How attackers use leaked credentials 9

How to protect against compromised credential attacks 10

Detecting leaked credentials before they're abused 12

Stopping credential leaks with Cyberint, now a Check Point Company 14

Reacting to leaked credentials: Two sample playbooks 15

Stopping leaked credential compromises, starting today 19

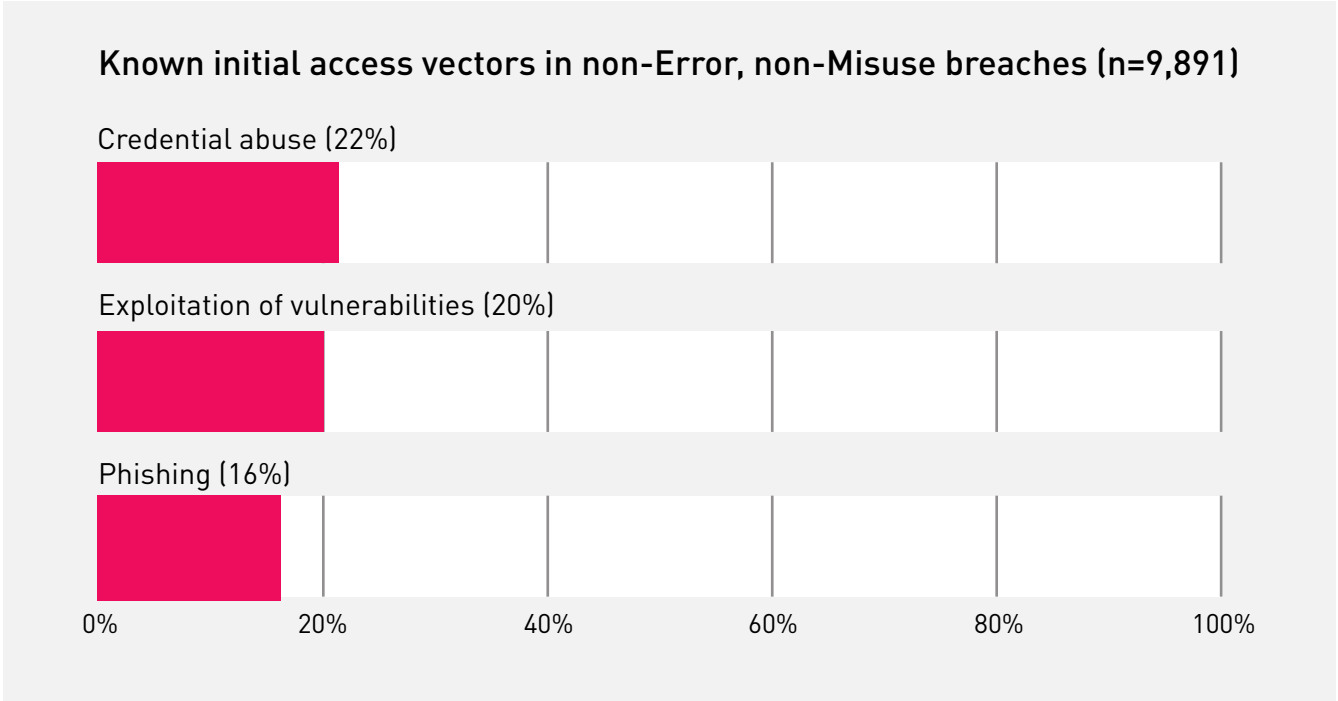
Contact Us 20

How to detect stolen credential attacks

When most people think of hacking attacks, they often think of attacks involving techniques like expertly exploiting obscure flaws in software applications or physically infiltrating data centers and plugging malware-laden USB sticks into servers.

In the real world, many cyber security breaches are less sophisticated – but equally harmful. They center on the use of stolen credentials, which hackers may purchase rather than pilfer themselves, to break into the accounts of a company's employees and customers.

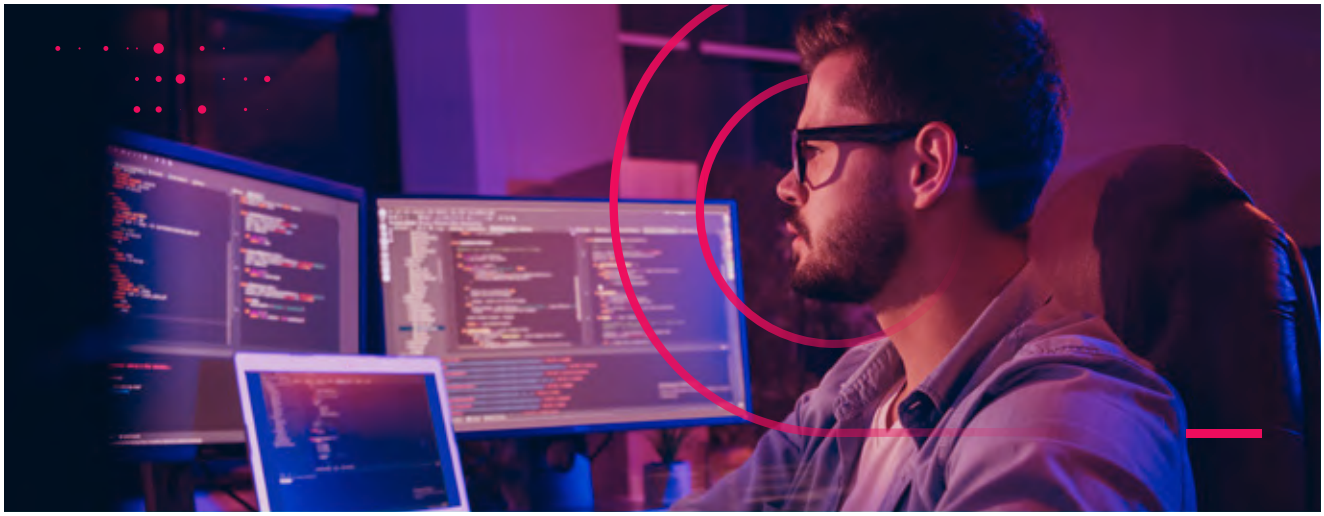
In fact, according to Verizon's 2025 Data Breach Investigation Report, stolen credentials were the root cause of 22 percent of data breaches in 2024 – an impressive figure that highlights just how widespread leaked credentials are as an attack technique.



It's easy enough to understand why: Unlike software vulnerability exploits or malware deployment, stolen credentials don't require especially sophisticated attack methods. Once threat actors obtain the credentials for a legitimate user – which they can do by breaking into databases or launching phishing attacks, among other methods – they can simply log in as if they were that user. In turn, they can access any resources available to that user. And they can typically do so without being easily detected, since they are not bypassing security controls or disabling systems.

Unfortunately, businesses have a limited ability to prevent the theft of login credentials. Protections like anti-phishing tools and email gateways can help, but they won't guarantee that credentials will never fall into threat actors' hands – as underscored by a June 2025 incident that exposed 16 billion credentials for companies including Facebook, Apple and Google, which has been called the "G.O.A.T. of all data breaches."

What organizations can do, however, is invest in measures that help them discover stolen credentials associated with their brand. Because threat actors rarely exploit stolen credentials right away, early detection of exposed login information allows businesses to change passwords or disable accounts before major damage occurs.



The surge of leaked credentials

Stolen credentials have long posed a cyber security risk. But evidence suggests that they're now a larger problem than ever.

Data from Cyberint, a Check Point company, shows that there has been an increase of more than 160 percent in leaked credentials to date in 2025 as compared to 2024. And in a single month late last year, we reported 14,000 cases in which employee credentials at our customers were exposed in data breaches (note these cases were flagged because they complied with company password policy, indicating a real risk).

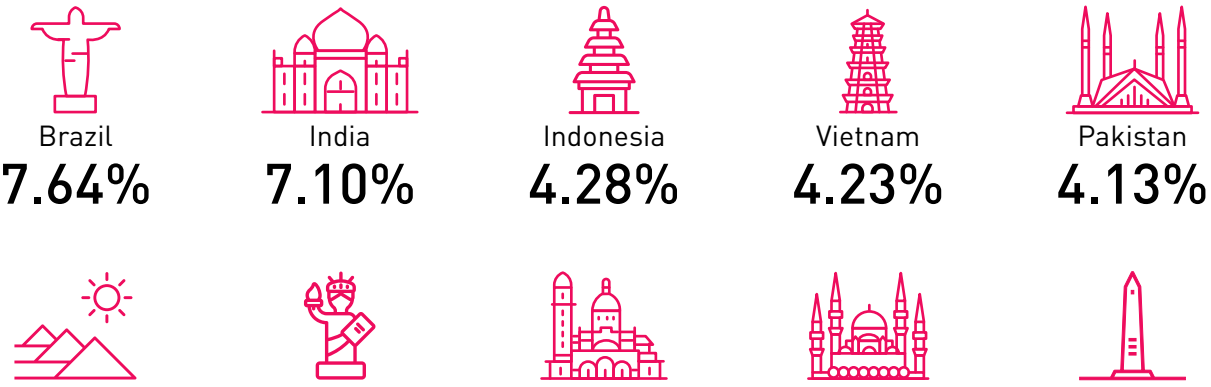
This significant increase could be due to several things, the rising use of AI increasing the sophistication of phishing attacks and an increasing number of stealer families, making it easier for less experienced threat actors to enter the playing field, using malware as a service.

Our research also shows that, in cases where stolen credentials originate from GitHub repositories, it takes 94 days on average for businesses to remediate the leaked secrets by revoking them or disabling affected accounts. This suggests that businesses struggle to identify leaked login information quickly, giving threat actors plenty of time to take advantage of it.

Stolen credential attack trends

Interestingly, there is significant variation between countries when it comes to stolen credential theft:

2025 Top 10 Countries



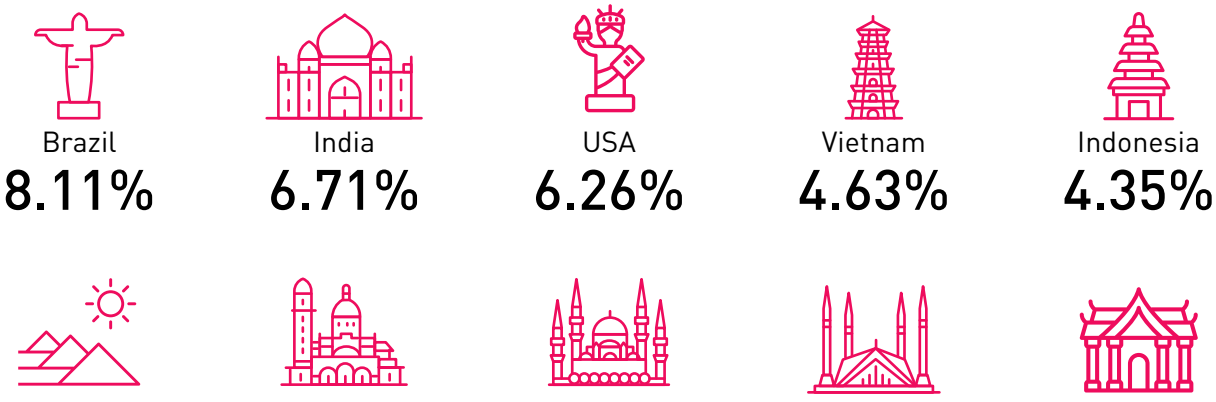
Brazil	India	Indonesia	Vietnam	Pakistan
7.64%	7.10%	4.28%	4.23%	4.13%

Egypt	USA	Philippines	Turkey	Argentina
3.89%	3.59%	3.55%	3.08%	3.04%

As indicated above, Brazil and India are outliers, with users based in those countries facing especially high rates of credential theft. It's worth noting however that they are 2 of the most populated countries in the world. Reasons for them topping the charts could also be to do with a lower cyber security awareness in their population.

These trends generally carried over from the previous year – with the exception that credential leakage for U.S.-based users has declined significantly since 2024, as the following figures indicate:

2024 Top 10 Countries



Brazil	India	USA	Vietnam	Indonesia
8.11%	6.71%	6.26%	4.63%	4.35%

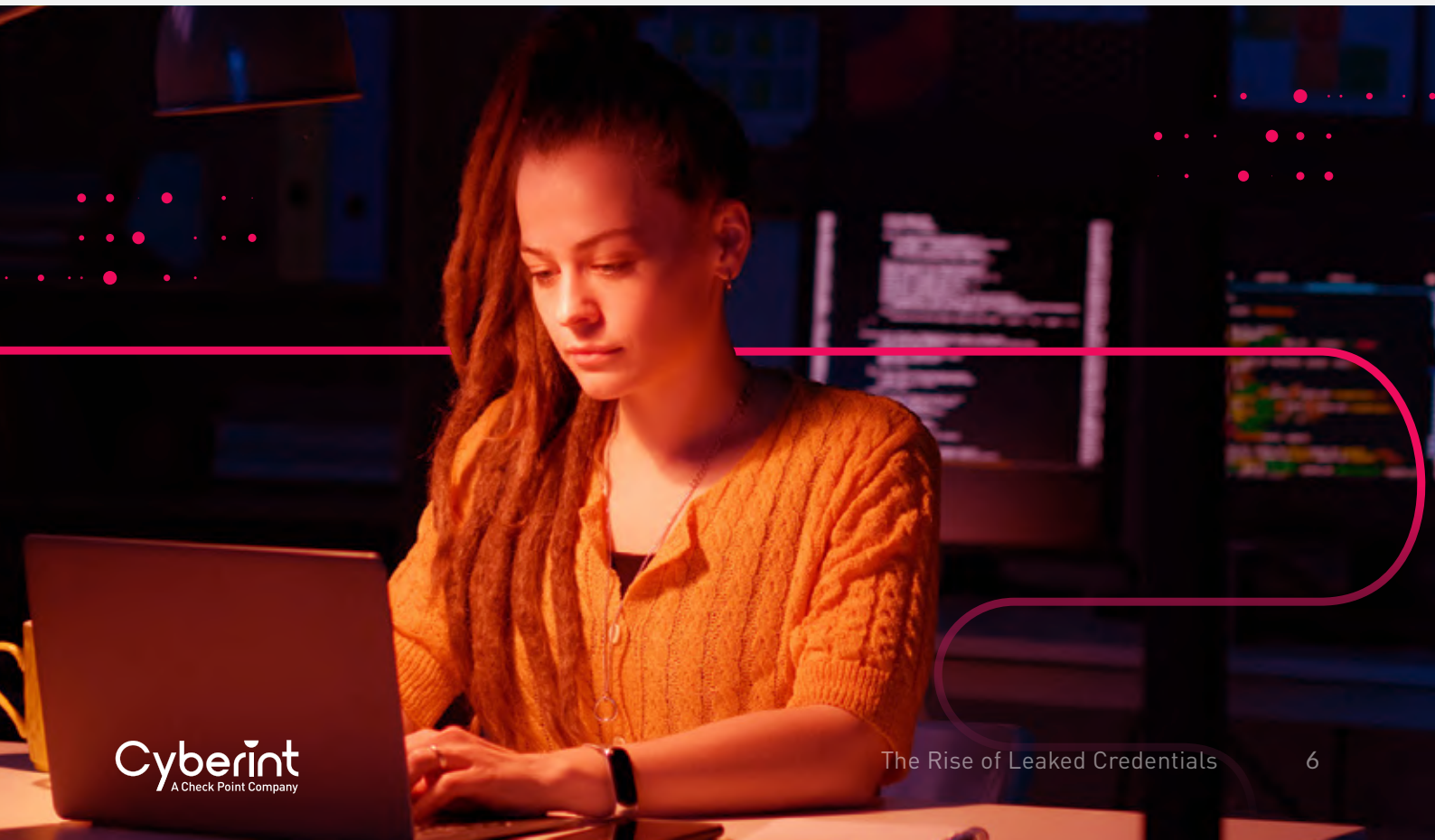
Egypt	Philippines	Turkey	Pakistan	Thailand
3.64%	3.62%	3.38%	3.29%	3.13%

It's too early to say whether this is a longstanding trend that reflects better credential protections by U.S. based companies, or simply a statistical anomaly.

A notable trend shows the gap narrowing among top countries. While a few countries once held significantly higher percentages, more nations now have similar volumes, spreading the activity more evenly worldwide.

As for the websites and domains most frequently impacted by leaked credential attacks, those owned by Discord, Microsoft (which owns live.com) and Facebook top the list:

	2024 Top URLs	2025 Top URLs
discord.com	1.29%	1.01%
login.live.com	1.63%	1.55%
www.facebook.com	1.74%	1.76%
www.roblox.com	2.29%	2.02%
accounts.google.com	3.70%	3.72%



Gmail accounts are also frequently implicated in stolen credential attacks, accounting for the vast majority of exposures that involve email hostnames:

2024 Top 5 Exposed Email Hostnames

gmail.com	Other	hotmail.com	yahoo.com	outlook.com
68%	15%	9%	3%	2%

Notably, personal email accounts are far more likely to be impacted by stolen credential attacks than work emails. While this suggests that the majority of breaches focus on individual consumers rather than employees of a company, it still poses a risk to businesses because threat actors could use stolen personal email logins to breach customer accounts.

Plus, there is a risk that employees may use the same passwords for their work emails as they use for personal accounts, allowing threat actors targeting a particular company to break into work accounts using passwords that they steal from consumers. Not, only that but there is a risk of company information being shared via personal emails, that could lead to data leakage.

How do hackers steal credentials?

Part of the challenge posed by stolen credentials is that there are many potential paths threat actors can follow for stealing this data:

- **Hacked databases:** Cyber criminals can obtain login credentials by breaching an organization's systems and gaining access to databases that house usernames and passwords. The specific methods they may use to do this vary. For example, attackers may exploit unpatched database software vulnerabilities, compromise admin accounts that use default, publicly known passwords or carry out injection attacks to "trick" applications into exporting login information from databases. Once stolen, credentials from hacked databases are typically compiled into "combo-lists," which consolidate data from multiple breaches, and sold on the Dark Web.

- **Phishing:** By sending deceptive phishing emails – or using more sophisticated phishing methods, like vishing and smishing – threat actors may succeed in obtaining sensitive login data directly from employees. While some phishing attacks result in the theft of credentials for just one user at a time, it's also possible to use phishing to gain access to large credential databases by, for example, tricking an IT employee into handing over the database login details.

- **Malware:** Threat actors can plant certain types of malware on a business's computers or servers to steal login information. For example, keyloggers can record usernames and passwords as employees enter them. More advanced spyware tools can take screenshots or steal sensitive data as it moves over the network as a means of obtaining credentials.

    - **Infostealers:** Infostealers are a particular type of malicious software designed to extract sensitive data from infected devices. They frequently target browser credentials, saved passwords, cookies and financial information. They often compile the data into logs, which threat actors can then sell on the Dark Web.

If there were just one common method for stealing credentials, blocking the attacks would be easy. Unfortunately, that's not the case.

How attackers use leaked credentials

There are also multiple ways in which hackers can abuse stolen credentials, making it challenging to predict exactly what they will do or take steps to block exploitation of the data.

One common action is account takeover. An account takeover is an identity attack in which threat actors gain unauthorized access to legitimate attacks, which they use to carry out phishing, financial scams and so on. This practice can be especially threatening to a company's brand, and particularly harmful to targets, because it's much easier for threat actors to impersonate a legitimate business or employee when they can send messages from an employee's actual account.

Another frequent use case for leaked credentials is for attackers to attempt to break into other accounts using the information from a compromised account. For example, if an employee uses the same password for both a personal email account and work email, attackers who have stolen the personal email login may try to break into the work email account as well. (Even if they only know the work account's password and not the username, the latter is typically easy to look up in publicly available directories or to guess by, since usernames commonly follow predictable patterns, such as a first initial followed by a last name.)

Using compromised accounts to distribute spam is another common practice. The ability to send messages from legitimate email accounts can make it easier for threat actors to evade filters that would otherwise block their messages.

In a similar vein, compromised accounts can be used to carry out attacks on social media wherein threat actors run "bot farms" to manipulate social media engagement by, for example, using hacked accounts to generate followers and likes.

Likewise, threat actors could use stolen accounts to gain sign up or referral bonuses from vendors, effectively abusing legitimate promotion channels.

In cases that are rarer, but that can be particularly damaging for victims, attackers may use stolen credentials as a specialized form of ransomware attack. They'll contact an affected individual or company, then demand a ransom payment in exchange for not abusing the credentials. Although victims could simply change their passwords instead of paying the ransom, users who are not technically savvy may not realize this. In addition, businesses that are unaware of the scope of a credential breach, or how much damage threat actors are prepared to cause, may decide that it's safer to pay the ransom than to try to remediate leaked credentials on their own.

How to protect against compromised credential attacks

A first step in defending against risks linked to stolen credentials is to invest in measures that make it more challenging for threat actors to obtain and exploit login data. Effective protections include:

- **Password management policies:** Businesses should establish policies that require employees to update passwords regularly. This helps ensure that if attackers manage to steal a password, they have a limited window of time for exploiting it before the user updates to a new password. In addition, password policies should prohibit employees from using the same password across accounts.

- **MFA:** Multi-factor authentication (MFA) can help to mitigate stolen credential abuse by preventing attackers from logging in if they know only a username and password, but not additional access credentials. However, it's important to note that MFA can be circumvented and is far from a silver bullet against the threat of leaked credentials.

- **SSO:** Where single sign on can be used as opposed to credential login it is preferred as then the threat of compromised credentials is reduced.

- **Limited login attempts:** Placing limits on how many times a user can attempt to log in can help to prevent cross-account attacks in which attackers attempt to use passwords for one account to break into other accounts owned by the same user.

- **PoLP:** Adhering to the Principle of Least Privilege (PoLP) by restricting access rights for users to the bare minimum necessary to perform their work reduces the scope of resources that threat actors can compromise if they manage to break into an account.

- **Phishing education:** Educating employees in resisting phishing attacks helps to make them less susceptible to phishing as a vector for stealing credentials.
- **Network defenses:** Network-level protections, such as intrusion detection systems and firewalls, can detect and block connections from untrusted endpoints, restricting attackers' ability to reach databases that store credentials.
- **Encryption:** Encryption – both of data in motion as it moves over the network, and of data at rest, including credentials stored in databases – makes it more challenging for threat actors to exploit stolen credentials, since they won't be able to decrypt them unless they also steal the encryption key. Note, however, that if attackers manage to gain access to an entire database of credentials, it's likely that they'll find a way to obtain decryption keys, too, such as by phishing them out of an IT employee.
- **Blocking third-party sites:** Blocking access to third-party websites can help to reduce the risk that these sites – which often employ weaker security protections than a company uses internally – will become vectors for planting malware on employees' devices.

The threats of third-party sites:

Weaker Encryption:

Many third-party sites do not use robust encryption methods, making it easier for threat actors to intercept communications and access sensitive information.

Inadequate Security Audits:

Many third-party sites do not use robust encryption methods, making it easier for threat actors to intercept communications and access sensitive information.

Lower Awareness of Cyber Threats:

Third-party sites may not be as vigilant about emerging cyber threats. They may lack the resources or expertise to implement the latest security protocols, making them more susceptible to attacks.

Detecting leaked credentials before they're abused

The measures above help to reduce the risk that threat actors will steal and abuse credentials. But again, it's impossible to guarantee that usernames and passwords will never leak. Despite extensive cybersecurity protections and training, attackers still may manage to break into databases or use phishing to trick even the most savvy employees into revealing login information (a risk made all the worse by AI, which helps attackers execute sophisticated phishing breaches at scale).

So, rather than investing in prevention alone, businesses must also ensure that when passwords associated with their employees, customers or brand are leaked, they know right away.

This is particularly important because threat actors don't usually exploit stolen logins immediately. When they breach a database, it takes them time to analyze the data and determine what to do with it.

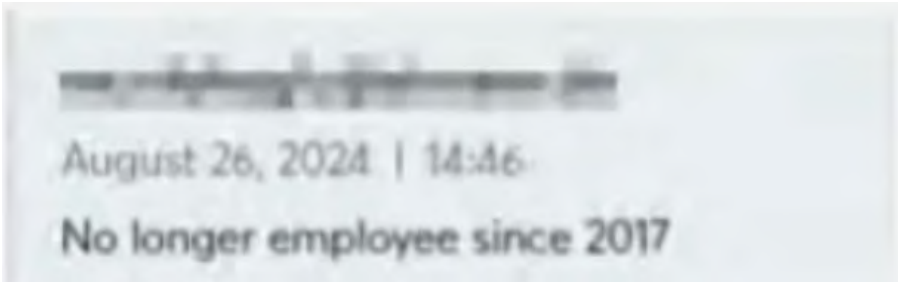
As a result, companies that are able to detect leaked credentials quickly – when they're still "fresh" in the eyes of attackers – have an opportunity to block attacks. They can simply disable breached accounts or update passwords.

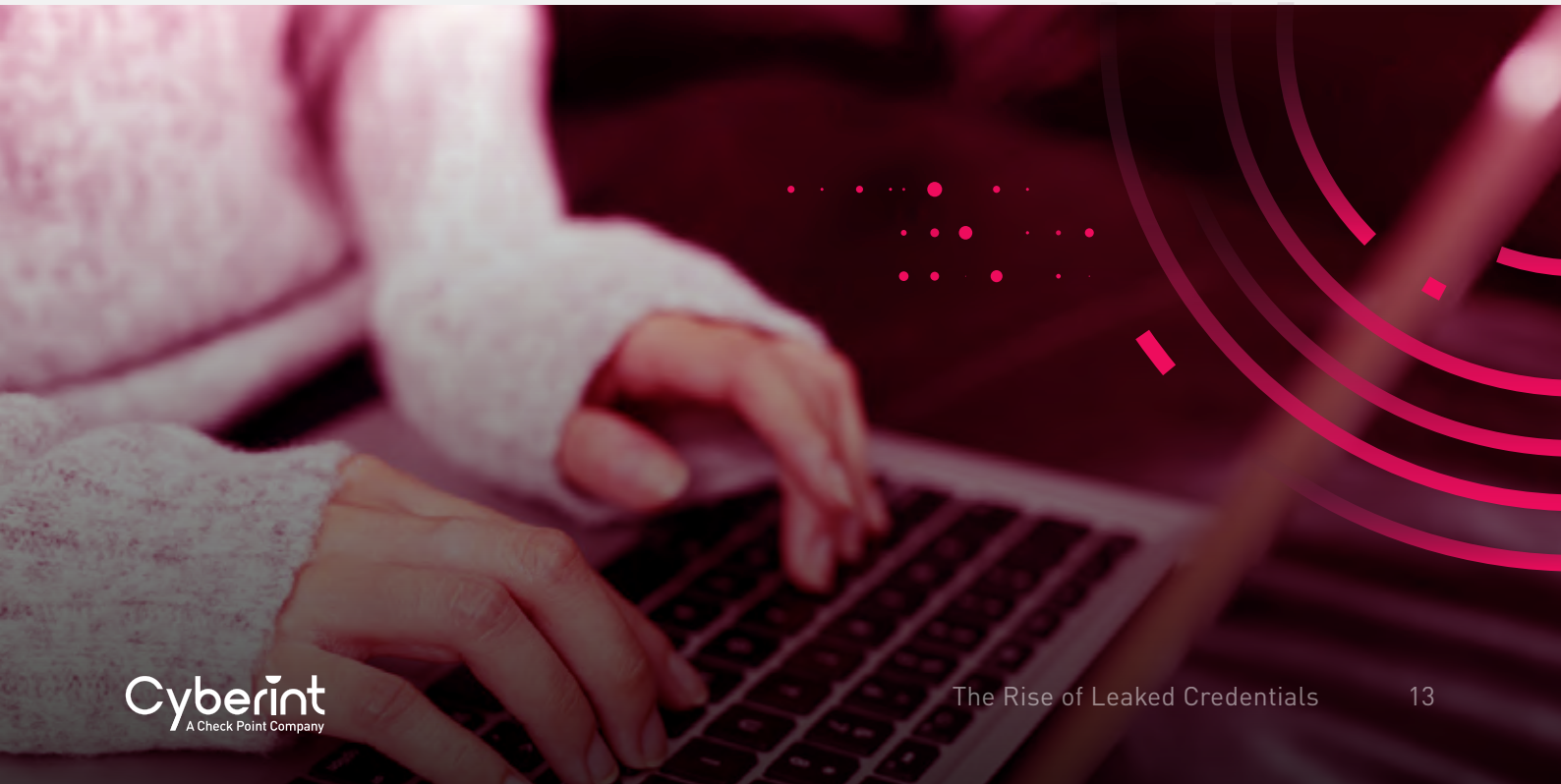
Effective methods for detecting leaked credentials include:

- **Forum scanning:** Deep and Dark Web forums can be scanned to identify username/password combinations associated with a particular company. This isn't always easy because threat actor communities may restrict who can view their forum discussions, but if you're adept at navigating these worlds – as we are at Cyberint – it's possible to gain access to the information necessary to reveal leaked credentials through these forums.

- **Logs:** To advertise stolen credentials that they want to sell, attackers may post logs as evidence of their attacks on the Deep or Dark Web. Looking for these assets can reveal signs of a breach that impacts a particular company. When posting these logs they often don't name the particular company, but rather share details such as company size, industry and geography. Cyberint, now a Check Point Company, excels at putting the pieces together to isolate the victim and notify them.

When searching for signs of credential breaches on the Deep and Dark Webs, it's particularly important to assess how fresh the credentials are. Often, a breach includes not just up-to-date login information, but also outdated passwords or credentials for expired accounts. Thus, just because a company's credentials have been exposed doesn't always mean there's an acute risk. It's critical to determine whether, and to what extent, active accounts are at risk – as opposed to those for employees that have long since left the company, for example.





Stopping credential leaks with Cyberint, now a Check Point Company

When it comes to detecting credential leaks that affect your company or customers, Cyberint, now a Check Point company, has you covered.

In addition to scanning the Deep and Dark Webs for credential leaks, Cyberint performs undercover investigations to verify threats and assess their scope.

Cyberint also integrates with SIEM and SOAR tools to enable fast, automated notification when leaked credentials appear. In addition, businesses can configure automated remediations to mitigate attacks by, for example, immediately requiring employees to update passwords when credential theft is detected.

These protections extend not just to accounts that employees access through corporate devices, but also personal computers. We can detect instances where workers use company accounts on personal devices, even in cases where endpoint monitoring and security tools are not present on those devices – which is the case for 46 percent of devices associated with leaked corporate credentials, according to Cyberint data.

Reacting to leaked credentials: Two sample playbooks

To illustrate how businesses can deploy credential theft protections as part of real-world security operations, here's a look at two example playbooks for managing compromised credentials.

Compromised employee credentials playbook

This playbook provides a guide for security teams to respond to incidents involving employee compromised credentials. The goal is to mitigate risks and secure the organization's systems when such credentials are exposed.

☑ Monitoring and detection:

- ✓ Leverage threat intelligence services to monitor Leaked credentials and logs.
- ✓ Automatically review logs and lists released on the open, deep and dark web and correlate to your brand.
- ✓ Initial Assessment:
- ✓ Upon receiving an alert about a potential credential compromise, verify the source's credibility and if the password matches the employee corporate password.

☑ Containment and mitigation:

- ✓ Credential Revocation: Immediately and automatically disable or revoke access for the compromised credentials within the systems.
- ✓ Automatically reset password.
- ✓ Enhanced Authentication:
- ✓ Implementing MFA or SSO for all accounts in your organization to greatly enhance security.
- ✓ Enforce strict password policies, requiring immediate password changes for any accounts linked to the compromised credentials.

☑ Access review:

- ✓ If the exposed credentials match the employee's corporate credentials, review recent access logs and activities associated with the affected credentials to identify any suspicious actions.
- ✓ If unauthorized access is detected, escalate the response by following the incident response plan (such as isolating systems or engaging in forensic analysis).

☑ Communication and coordination:

- ✓ Notify relevant internal stakeholders (e.g., IT, legal, compliance) about the incident and actions taken.

☑ Post-incident review:

- ✓ Incident Analysis.
- ✓ Conduct a post-incident review to analyze the root cause of the credential compromise and evaluate the effectiveness of the response.
- ✓ Document lessons learned and update the playbook or other security protocols as needed.
- ✓ Strengthen Defenses.
- ✓ Based on the review, implement additional security measures to prevent similar incidents in the future, such as enhanced monitoring and stricter access controls.

Third-party credentials playbook

This playbook will provide a guide for security teams to respond to incidents involving compromised credentials belonging to vendors. The goal is to mitigate risks and secure the organization's systems when such credentials are exposed.

☑ Monitoring and detection:

- ✓ Leverage threat intelligence services to monitor Leaked credentials and logs of vendors.
- ✓ Regularly review vendor security bulletins and breach notifications.
- ✓ Initial Assessment:
- ✓ Upon receiving an alert about a potential credential compromise, verify the source's credibility and if the password matches the employee corporate password.
- ✓ Identify the affected third-party vendor and the extent of the exposure.

☑ Containment and mitigation:

- ✓ Credential Revocation:Immediately and automatically disable or revoke access for the compromised credentials within the systems.
- ✓ Notify the third-party vendor of the potential compromise and request they revoke or reset the affected credentials.
- ✓ Enhanced Authentication:
- ✓ Implementing MFA or SSO for all accounts in your organization to greatly enhance security.
- ✓ Enforce strict password policies, requiring immediate password changes for any accounts linked to the compromised credentials.

☑ Access review:

- ✓ If the vendor has access to company systems, review recent access logs and activities associated with the affected credentials to identify any suspicious actions.
- ✓ If unauthorized access is detected, escalate the response by following the incident response plan (such as isolating systems or engaging in forensic analysis).

☑ Communication and coordination:

- ✓ Notify relevant internal stakeholders (e.g., IT, legal, compliance) about the incident and actions taken.

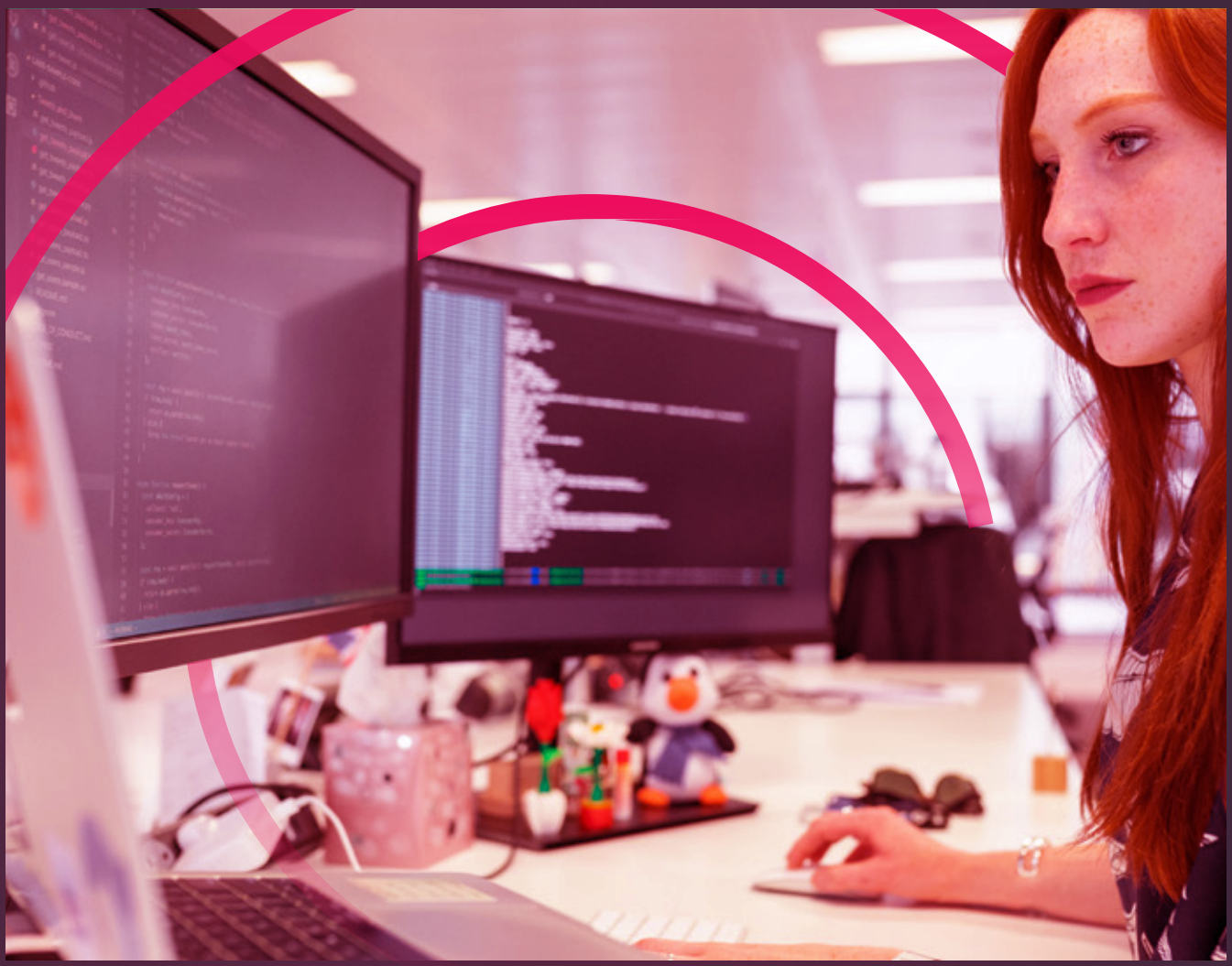
☑ Post-incident review:

- ✓ Incident Analysis.
- ✓ Conduct a post-incident review to analyze the root cause of the credential compromise and evaluate the effectiveness of the response.
- ✓ Document lessons learned and update the playbook or other security protocols as needed.
- ✓ Strengthen Defenses.
- ✓ Based on the review, implement additional security measures to prevent similar incidents in the future, such as enhanced monitoring, stricter access controls, or updated vendor contracts.

Stopping leaked credential compromises, starting today

Stolen credentials are a cyber security threat that – if trending data is any indication – will only get worse from here.

Taking measures to prevent credential theft is a first step in mitigating this growing risk. But it's equally critical to ensure that you can detect leaked credentials – especially those that are "fresh" and ripe for compromise – as quickly as possible when they impact your company, employees or customers.



Schedule a demo

To learn more about how the threat intelligence capabilities offered by Cyberint, now a Check Point company, can help protect your brand against the scourge of stolen credential attacks.

Contact Us

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm

© Cyberint, 2025. All Rights Reserved.