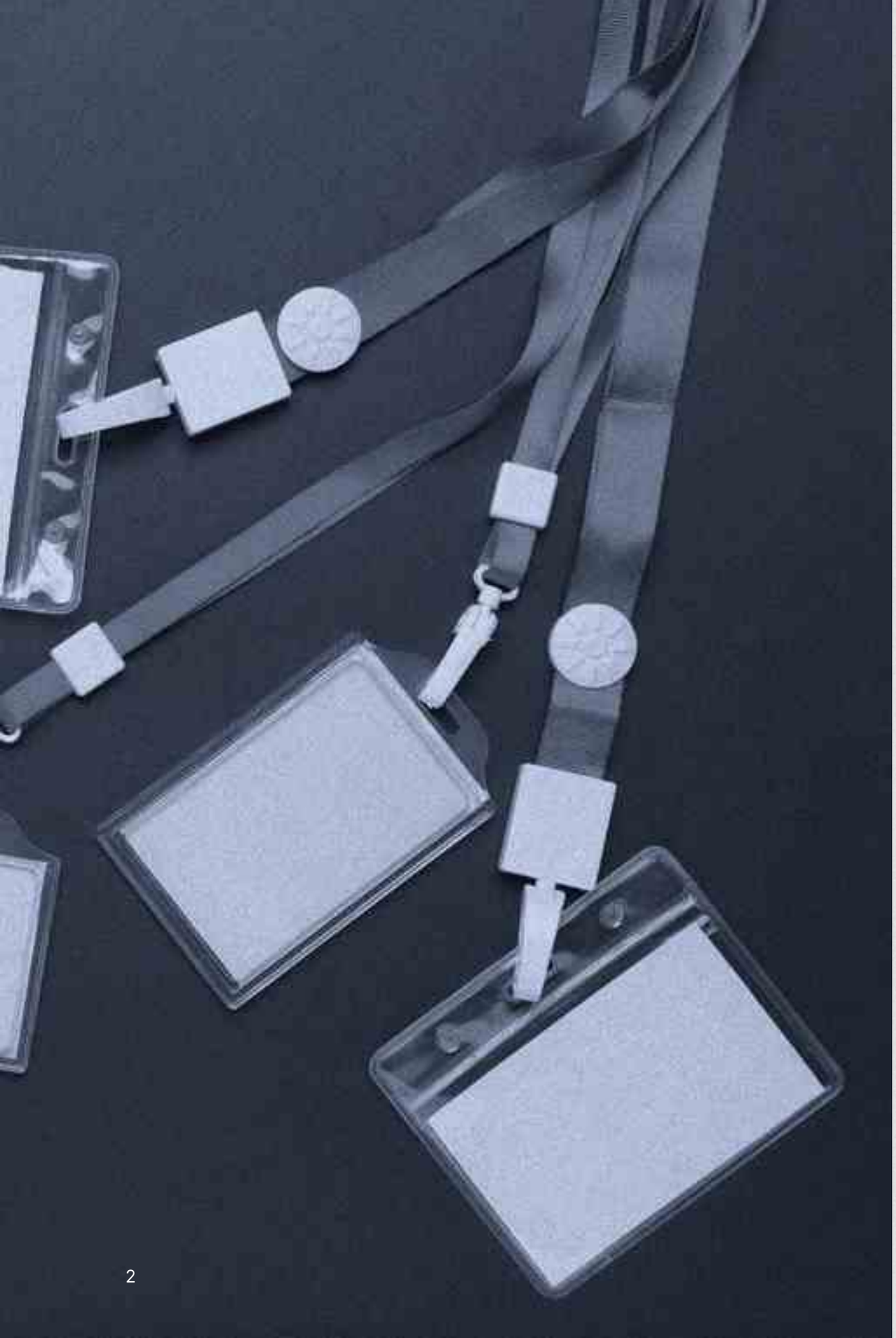
Recorded Future®

EXECUTIVE BRIEF

Leaked Credentials: The Threat They Pose and How to Reduce Your Risk



Credentials—especially those with privileges—open doors to the network, sensitive information, and intellectual property. Used properly, they connect employees and users to critical applications and services. Unfortunately, many organizations and users fail to adequately protect credentials; criminals understand this is an easy path to gain access and wreak havoc. A deeper understanding of the problem, and a proven triage process can help keep valued credentials out of the hands of the criminal underworld.

Leaked Credentials: Why Do They Matter?

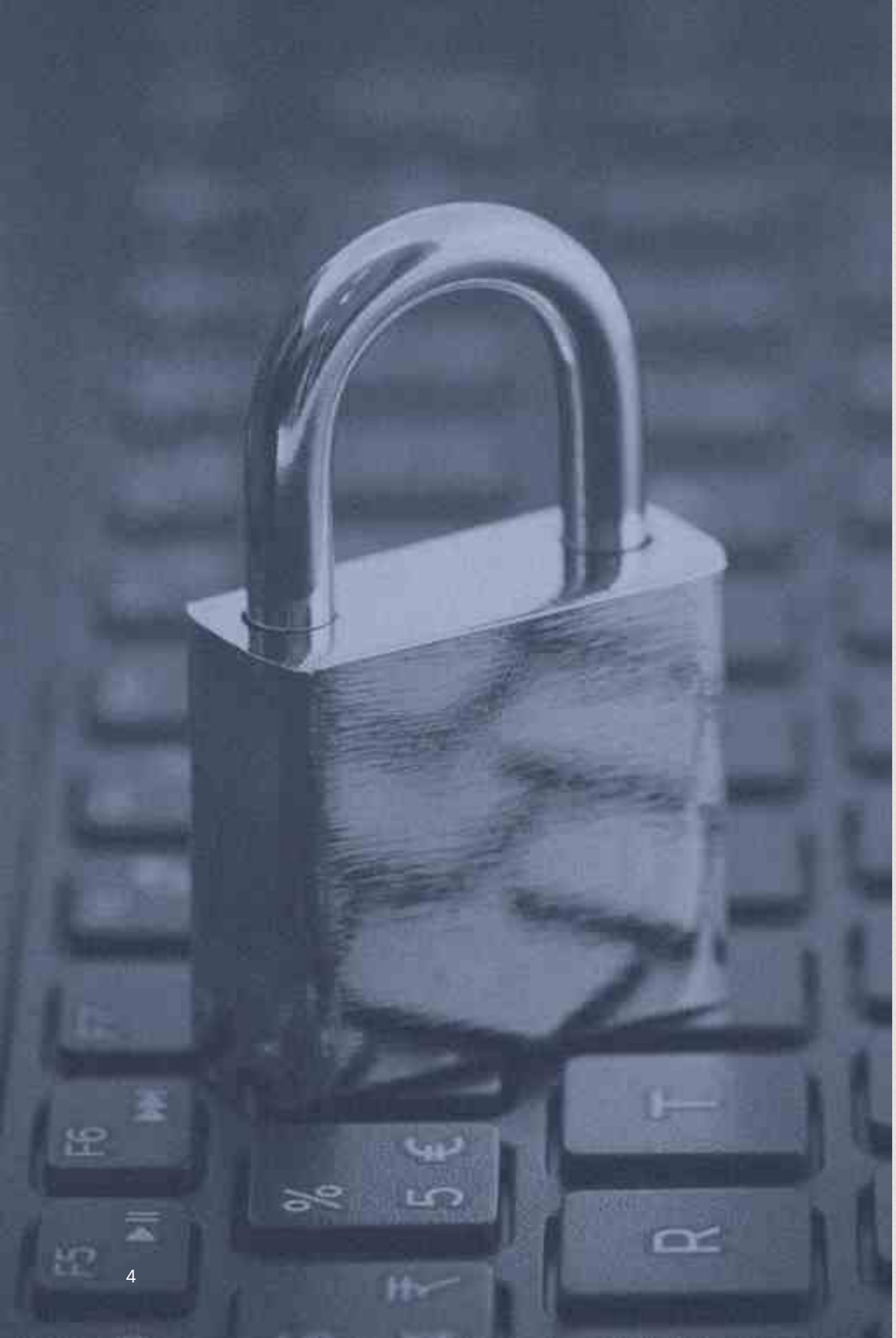
Leaked credentials are an open invitation for criminals to invade the corporate network. Credentials don't even have to be stolen outright: many users give them up voluntarily. When users fall for spam, or a phishing or spear phishing attack, they often assume that a link in the email will take them to a legitimate site and enter their username and password. Criminals immediately harvest the credential and can add it to a database of leaked credentials that can be used in credential stuffing attacks.

Even a single username/password combination can make a significant difference: if the user accesses their corporate systems using the same credentials as they do for Facebook, a breach of the latter can give criminals easy access to corporate assets. It is a known fact that users reuse passwords. At least 65% of users admit to reusing passwords across sites[1] and the number is probably a lot higher

But we're not talking about a credential or two being leaked. Over the last five years, 11.7 billion credentials have been leaked[2]. Given this volume, every organization should assume that some of its users' credentials are available to attackers and can provide a potential open door to their network, valuable databases, and intellectual property.

[1] Google / Harris Poll Online Security Survey, Feb 2019 – retrieved from https://services.google.com/fh/files/blogs/google_security_infographic.pdf

[2] F5 Labs 2021 Credential Stuffing Report – Feb 09, 2021 – retrieved from https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report



Increased Risk and Cost to the Organization

The assumption that an organization's credentials have been leaked leads naturally to the corollary that the organization is at risk of a breach. That's because some 61% of breaches are due to leaked credentials[3]. They are cheap to purchase (often for just pennies each), and easily accessible by criminals. In addition, although many of the passwords are encrypted, it is relatively easy for criminals to decipher and extract them in plaintext thanks to tools such as rainbow tables. From that point on, it's a simple matter of playing the odds: even though only 1-2% of leaked credentials will result in a successful breach, with millions available there is a high probability of success. Once a network is breached, criminals can implant malware such as ransomware. Simply because one user reused a password that was later leaked.

The damage can be significant. The number of ransomware attacks rose 435% from 2019 to 2020, and the cost of such attacks is expected to increase by 60% in 2021[4]. Leaked credentials are also used frequently by advanced persistent threats (APTs) in which threat actors conduct prolonged attacks with the purpose of infiltrating and/or exfiltrating valuable data without being discovered.

[3] 2021 Verizon Data Breach Investigations Report – retrieved from https://www.verizon.com/business/resources/reports/dbir/

[4] Cybersecurity Ventures 2019 Cybersecurity Market Report – retrieved from Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021 (cybersecurityventures.com)

The reality is that most organizations, lacking the ability to monitor, only find out that their credentials have been leaked when they are notified of a breach.

A Difficult Problem to Solve

The first step to solving any problem is realizing you have one. In this case, even that first step is difficult. Leaked credentials appear in a variety of locations across the Internet including paste sites, private communication channels, and the dark web. Cybercriminals often use the dark web to trade information and sell/buy leaked credentials.

Accessing these sources is neither easy nor cheap, requiring huge investments in monitoring tools and human expertise. Simply finding them on the dark web, which is only accessible via special browsers or software, is a big challenge. Even harder is finding leaked credentials in the closed criminal underground, a private part of the dark web that requires special authorization and vetting to access at all. In fact, only 42% of companies gather intelligence from closed or dark web sources[5]. Because the data is being updated constantly, their monitoring efforts must be constant. The reality is that most organizations, lacking the ability to monitor, only find out that their credentials have been leaked when they are notified of a breach.

Steps to Triage the Threat From Leaked Credentials

Beyond finding and accessing sources of potential leaked credentials, the organization needs a solid process to unpack and validate the data, determine its relevance, and triage the threats. The first step is to deduplicate the data because such datasets can be quite large (more than a billion credentials[6]) consisting of data that has been patched together over the years. Next, those that apply to the organization or domain must be separated out. From that smaller (but likely still quite large) set of data, email addresses must be extracted, and mapped to usernames.

[5] 2020 SANS Cyber Threat Intelligence (CTI) Survey – https://www.sans.org/white-papers/39395/

[6] Hackers are Passing Around a Megaleak of 2.2 Billion Records – Wired Magazine – retrieved from https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Only now can the organization dig in to determine if the credentials constitute a problem. Is the email account still active? If so, hashed passwords in the datasets need to be converted to plaintext to determine if the password conforms to the organization's password policy. If true, has the organization already detected this particular leaked credential and dealt with it? (That in itself requires a data base of such information, which may present legal challenges). If not, the password must be reset and the IT team engaged to check for recent suspicious activity, in which case normal threat response activities must be conducted.

All of this is difficult, time-consuming, and costly for a single leaked credential: studies show that the cost to reset just one compromised password is $70[7], and nearly half of businesses spend 1-5 hours remediating a single incident of a compromised user account[8]. Imagine how intractable the problem can be, at scale. Don't forget that in the process of searching for leaked credentials related to the organization, it is possible to encounter leaked credentials that belong to a third-party supplier. While the urgency relates to solving the organization's credential issues, a later crucial step is to engage the relationship owner to notify partners so they can take action on their own.

[7] Best Practices: Selecting, Deploying and Managing Enterprise Password Managers. Forrester Research. Retrieved from Forrester

[8] State of Fraud Report 2021 – (https://www.arkoselabs.com/wp-content/uploads/2021-State-of-Fraud-Report.pdf)

“MFA is a Panacea,” and Other Leaked Credential Myths

There are several misconceptions about how an organization can deal with leaked credentials, based on the underlying belief that there may be some quick fixes. In reality, this difficult and complex problem has tentacles that reach into obscure places.

First, many people believe that a single leaked username/password doesn’t really matter. However, all it takes is one credential for a criminal to break into the network. And because there is a high probability of passwords being reused across multiple sites, a single leaked credential can unleash a cascade of unwanted access.

Second, it’s commonly believed that a multi-factor authentication (MFA) system will eliminate the problem. The reality is that if there is even one legacy system that doesn’t support MFA, that could be the weak link—and most organizations do not have full MFA coverage. That is what happened with the Colonial Pipeline attack: hackers broke in through an inactive account that did not use MFA, and used a compromised password[9]. It doesn’t help matters that many MFA implementations are not hyper-secure. MFA systems that send an authentication code can fall victim to Man-in-the-Middle (MitM) phishing toolkits where all traffic goes through a reverse proxy system, so criminals have access to authentication codes and related cookies.

[9] https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa

The Difficult Problem of Leaked Credentials

1. All it takes is a single leaked password to breach a network.

2. MFA implementations often have loopholes that criminals can exploit.

3. Hashed passwords are not a major obstacle to attackers.

4. Purchasing leaked credentials doesn’t remove them from the market – it only increases their perceived value.

Third, some feel that if passwords are hashed or even salted, they can't be deciphered by attackers. The truth is that criminals have figured out how to decode the actual password, using a wide variety of tools. While the task might take some time, that is not a problem for someone determined to break into corporate networks. On the other hand, the beleaguered IT team has little time to deal with the complex issue of leaked credentials.

Fourth, some organizations that discover their credentials are for sale think the answer is to purchase them and take them off the market. Unfortunately, it's not that simple. While the organization might be able to buy the credentials, there is no guarantee they haven't already been sold countless times, nor that they won't be sold again. Furthermore, purchasing them just validates the value of the credentials. All of a sudden, the organization has a big target on its back.

Intelligence Is Essential for Effectively Reducing Leaked Credential Risk

Fortunately, there are three things an organization can do to reduce the threat and mitigate the effects of leaked credentials.

AUTOMATE THE COLLECTION

Don't try to do this alone. While it might be technically possible to identify all leaked credentials from all possible sources, it's extremely labor-intensive, error-prone, and expensive – and the probability of success is low. Instead, rely on platforms with the resources to provide widespread visibility to discover when leaked credentials appear. They perform constant monitoring of multiple sources, including obscure dark web and criminal underground forums, providing you with intelligence virtually impossible to obtain otherwise. Stand on the shoulders of those who have the expertise to continuously monitor and alert you to issues.

AUTOMATE THE TRIAGE

Automation is absolutely necessary to use this real-time intelligence. Rather than sifting through billions of records to try to find those related to your organization, rely on solutions that can automate the bulk triage of credential leaks, presenting only the data relevant to your organization that can be integrated into existing identity workflows and systems. Advanced automated solutions include added context (such as processes that include password property filters, identify novel exposures, and retrieve details).

Three Ways to Reduce the Threat and Mitigate the Impact of Leaked Credentials

1. Automate the collection.
2. Automate the triage.
3. Automate the mitigation.

AUTOMATE THE MITIGATION

Automate mitigation as well. Automated processes can check internal resources to make sure the email is still active, and even issue password resets at scale, or inform users and ask them to take remedial action.

Automated leaked credential solutions (which can be complementary to MFA and existing perimeter security solutions) can provide increased visibility into dark web credential leaks. They can address this complex and time-consuming problem, helping the organization proactively detect threats and block unauthorized access in real time. When it comes to leaked credentials, the only response is automation.

To learn how you can use intelligence to reduce leaked credential risk, **request a demo from Recorded Future**.

About Recorded Future

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets.

By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.