CASE STUDY

Effectiveness of *AllCreds* in Combating Credential Stuffing Attacks: COMPANY M

An international, omni-channel retailer with significant global online sales could have slashed exploits of compromised customer login credentials from more than 532,000 to fewer than 49,000 by using AllCreds from myNetWatchman.

Credential stuffing is to ATO what card testing is to third party fraud.

INTRODUCTION

Consumers have the tendency to reuse passwords and credential pairs – the same username or email address and password used in tandem. This makes account takeover (ATO) all too easy for fraudsters who exploit this fact via credential stuffing attacks.

52%	CONSUMERS WHO REUSE AT LEAST ONE PASSWORD [1]
13%	CONSUMERS WHO USE THE SAME PASSWORD FOR ALL ACCOUNTS [1]
22.6%	SHARE OF LOGINS THAT ARE ATO ATTEMPTS [2]
$290	AVERAGE COST OF ATO PER ACCOUNT [3]

Credential stuffing attacks are a precursor to ATO similar to how card testing often precedes using compromised payment cards for larger fraudulent transaction attempts. Rather than test a list of compromised payment cards, credential stuffing attacks systematically test lists of compromised credentials pairs, which are plentiful as they are so frequently leaked in data breaches.

To better understand how myNetWatchman's *AllCreds* product reduces the number of successful accounts taken over from credential stuffing attacks and how organizations can detect and thwart them, myNetWatchman compiled this case study on an organization that we have anonymized and will be referred to as Company M, an international omni-channel retailer with a large, global online sales presence.

The case study analysis was performed in May 2024, examining credentials both attempted and successfully used against Company M between January and April.

91%

of the compromised credential attacks on Company M could have been thwarted

THE ATTACK

The scale of the credential stuffing attack against Company M that took place over the first four months of 2024 was massive, as is often the case with these systematically executed events. Over 54 million unauthorized log-in attempts occurred using 46.1 million unique usernames and 47.9 million credential pairs. The 1.8 million more credential pairs than usernames implies that many usernames had been externally compromised multiple times with two or more different passwords, and multiple combinations were tried over the course of the credential stuffing attack.

91%	CREDENTIALS TESTED ON OTHER SITES BEFORE USED AGAINST COMPANY M
10,000	NUMBER OF SITES CREDENTIALS TESTED IN PRIOR 12 MONTHS
10%	SHARE OF CREDENTIALS SUCCESSFUL AT BOTH PREVIOUS SITES AND COMPANY M

Of the 47.9 million unique credential pairs tested during the event, 533,000 were able to access the customer site, which was a 1.13% success rate. There were 54.2 million total events testing or using compromised credentials, and there was a higher success rate when looking at total attempts versus unique credential pairs, meaning credentials successfully tested were used multiple times. The success rate across all credential stuffing attack attempts was 1.7%, or 915,400 out of 54.2 million attempts.

As is the case in most credential stuffing attacks, Company M was just one of many targets. Analysis of the 533,000 credentials successfully used against Company M showed that they had been used or tested at nearly 10,000 other sites beforehand.

Ten percent of the credentials successfully used against Company M were valid elsewhere, meaning they had been successfully tested or used against other sites before they were attempted at Company M. This underscores the significant role of poor consumer password hygiene in enabling credential stuffing attacks.

Further, the credentials used in the attack were not newly compromised. Credentials being used against Company M were observed by myNetWatchman as being used in the 12 months before the attack, and 91% of the 533,000 successfully used credential pairs against Company M were tested at other sites first.

HOW myNETWATCHMAN ABATES ATTACKS

The case study analysis of the credential stuffing attack against Company M shows how myNetWatchman's proprietary data and insights could have greatly mitigated the credential stuffing attack as it unfolded. More than nine-tenths of the successful logins during this credential stuffing attack used credential pairs known to have been tested at other sites first, something that myNetWatchman's compromised credential screening service, *AllCreds*, notifies companies of before they allow account access.

Of the 533,000 compromised credentials used successfully against Company M, more than 485,000 would have been identified by myNetWatchman's *AllCreds* service before the unauthorized users gained access to customer accounts. This credential stuffing attack would have been less than one-tenth as successful or damaging.

AllCreds provides organizations with key insights that enable dynamic, risk-based decisions on a per-user basis. Understanding the level of risk each user or login event presents allows organizations to strategically, and sparingly, use forms of step-up authentication like two-factor (2FA) or multi-factor authentication (MFA). More than 90% of the successful credential stuffing attempts against Company M could have been thwarted by presenting step-up authentication where it was warranted, while the vast majority of users would have continued enjoying a low-friction, seamless login experience.

OPPORTUNITY TO BUILD BRAND TRUST

Although users leave their accounts vulnerable to credential stuffing and ATO when they reuse credential pairs, consumers typically view the organization holding their account that was compromised as the party responsible for the ATO, even when the data breach that compromised their shared credentials occurred elsewhere. This puts the onus of ATO and credential stuffing attack protection on all organizations that offer user accounts, even when their users re-used shared credentials that were compromised in breaches against other companies. In this regard, credential stuffing attacks and the ATO that often results afterwards present significant brand risks, on top of the $13 billion in direct ATO losses that occurred in the US in 2023, according to Javelin.[4]

> Consumers tend to blame the site where they suffered ATO, despite user reuse of compromised credentials

myNetWatchman's *AllCreds* service can help organizations turn events that represent brand risk into an opportunity to build brand trust. Even when the correct credential pair is provided, knowing that these credentials are not only compromised but actively being used or tested elsewhere provides the impetus for users to update their credentials. The organization can encourage users to secure impacted accounts with proactive communications. For example:

> "There was an attempt to login using your correct password, but we don't think it was you."
>
> "This password is known to be compromised in an external data breach, and bad actors have been seen trying to use this password at many sites."
>
> "Please update your password so we can continue to protect your account, as your business and security are important to us."

With this proactive approach, credential stuffing is detected, ATO is thwarted, and brand trust is strengthened with myNetWatchman. Otherwise, credential stuffing attacks continue unabated and undetected to the detriment of users or customers.

ATO COSTS GREATER WITH WORKPLACE ACCOUNTS

Users are not just guilty of reusing passwords for personal accounts, they also have a tendency to reuse them for accessing business and workplace accounts, whether they are direct employees or contractors. Bad actors frequently target employee and contractor accounts because of the high-value information protected behind these logins.

Often, credential stuffing attacks against business user accounts target hosted cloud services or access to internal data and systems. This may be customer data, resulting in a significant data breach if personally identifiable information (PII) is accessed. According to IBM, the average cost of a data breach in 2023 was $4.45 million.[5]

Screening credentials with *AllCreds* when employees or contractors choose or reset their passwords prevents them from using known compromised credentials from the start

$5 MILLION	MINIMUM COST OF NEARLY 1 IN 3 RANSOM PAYMENTS (2023)
$2 MILLION	AVERAGE DATA RANSOM PAYMENT (2023)
30%	RANSOM PAYMENTS EXCEEDED $1 MILLION (2023)

Depending on the workplace account that is targeted, the threat actor may be attempting compromised credentials to access proprietary or confidential information. Whether it's trade secrets or PII, rather than use or sell this data to a third party, the cyber attacker may hold it ransom. According to Sophos, the average data ransom payment was $2 million in 2023, while 63% of ransom demands were at least $1 million and 30% were at least $5 million.[6]

The victim organization is often locked out of the system and not able to access their own data, or has the threat of the data being sold or leaked if the ransom is not paid by the attacker's deadline.

Just as myNetWatchman's *AllCreds* service protects consumer accounts against credential stuffing attacks and the reuse of compromised credentials, the same protection can be applied to employee and contractor accounts. This can be applied not only at login events, but also account creation and password change events, as well as to existing active directories, eliminating the opportunity for a known-compromised password to be used by an employee, contractor, or threat actor.

myNetWatchman is continuously updated, capturing live fraudster use of over 15 million newly-exploited credentials each and every day

ABOUT *AllCreds*

AllCreds is myNetWatchman's compromised credential screening service. Risk and reputation scoring is provided on specific users based on whether we see their credential pairs implicated in data breaches or successfully used by bad actors on other sites. These insights enable organizations to make dynamic, risk-based decisions on each user or login attempt, to strategically present forms of step-up authentication, or to require password resets. Many compromised credential pairs are used or tested elsewhere before they are attempted against your users or site. myNetWatchman lets you proactively protect your organization.

AllCreds is built on myNetWatchman's live data surveillance and proprietary data repository of over 35 billion exposed credential pairs and over 600 million protected user accounts. Not just compromised passwords, but credentials pairs. Not just credentials that have been breached, but ones that are actively being used.

ABOUT myNETWATCHMAN

myNetWatchman has been providing cyber fraud intelligence data for more than 20 years to retailers, financial services, insurance, and other industries. With over 10 years of live data surveillance, the company has protected over 600 million users and has in our data repository over 35 billion exposed credential pairs—with 15+ million newly-exploited logins added each and every day.

> *AllCreds* leverages myNetWatchman's data repository of 35+ billion exposed credential pairs and 600+ million protected user accounts, providing actionable insights that enable organizations to make dynamic, risk-based decisions on each user or login attempt

myNetWatchman

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech

[1] - https://services.google.com/fh/files/blogs/google_security_infographic.pdf
[2] - https://internetretailing.net/40-of-traffic-to-ecommerce-sites-comes-from-bots-raising-cyber-security-threat-level/
[3] - https://miracl.com/blog/account-takeover-fraud-to-exceed-25-billion-in-2020/
[4] - https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html
[5] - https://www.ibm.com/reports/data-breach
[6] - https://www.infosecurity-magazine.com/news/ransom-payments-surge-500/