Cyberint

Preventing Account Takeovers and Detecting Leaked Credentials with Argos Edge™

FRESH CREDENTIALS ARE A HOT COMMODITY

Obtaining and using credentials are key in many attack vectors. Leaked credentials allow threat actors to enter an organization through the main door by taking over an employee account. Once a threat actor is within the organization's network, the ability to effectively detect them is exponentially more complex and equally urgent.

As such, threat actors are investing very big efforts to collect the freshest credentials, and extensive commerce in the deep and dark web is being conducted in specific markets, closed groups, and forums.

The fresher credentials are, the better chance a threat actor has carrying a successful account takeover - no stale passwords, obsolete users etc. Therefore, fresh credentials, as the title suggests, are a hot commodity.

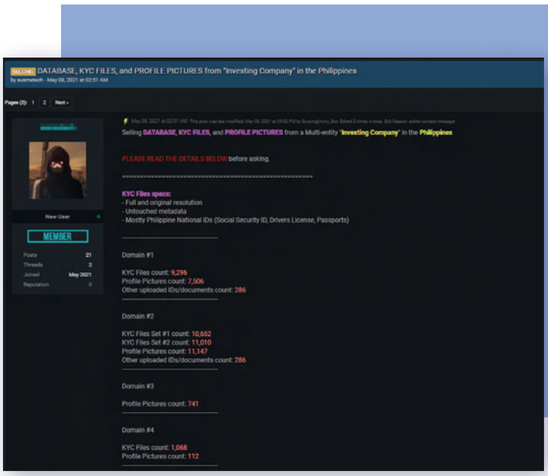
HOW FRESH CREDENTIALS ARE GATHERED

Leaked credentials are collected in several ways. The main three are hacked database leakage, successful phishing campaigns, and information stealers or “info stealers”:

1 HACKED DATABASE LEAKAGE

In most cases, threat actors are hacking into different applications and websites, and are extracting the data (which includes credentials), use it for the next step of an attack, or offer it for sale.

In other cases, the data is obtained as a result of a ransomware attack that includes internal data from an organization being collected by the attacker.
The credentials are usually shared or sold in different forums and Dark Web onions.



SELLING DATABASE, KYC FILES, and PROFILE PICTURES from "Investing Company" in the Philippines
by ausmetech - May 08, 2021 at 02:51 AM

May 08, 2021 at 02:51 AM This post was last modified: May 08, 2021 at 09:52 PM by [illegible] Edited 2 times in total. Edit Reason: added contact message

Selling DATABASE, KYC FILES, and PROFILE PICTURES from a Multi-entity "Investing Company" in the Philippines

PLEASE READ THE DETAILS BELOW before asking.

==

KYC Files specs:
- Full and original resolution
- Untouched metadata
- Mostly Philippine National IDs (Social Security ID, Drivers License, Passports)

Domain #1

KYC Files count: 9,296
Profile Pictures count: 7,506
Other uploaded IDs/documents count: 286

Domain #2

KYC Files Set #1 count: 10,652
KYC Files Set #2 count: 11,010
Profile Pictures count: 11,147
Other uploaded IDs/documents count: 286

Domain #3

Profile Pictures count: 741

Domain #4

KYC Files count: 1,068
Profile Pictures count: 112

Figure 1 - Example of a threat actor offering for sale 2 hacked databases

2 SUCCESSFUL PHISHING CAMPAIGNS

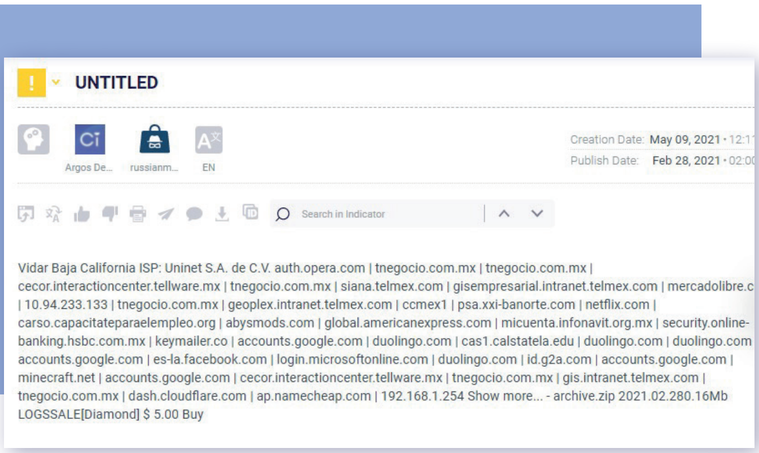
Threat actors collect credentials using sophisticated phishing campaigns which trick users into surrendering their most up to date credentials. There are great efforts to create effective and up-to-date phishing sites as well as phishing kits (Cyberint detects hundreds of new phishing sites daily) - and there is vast trade in phishing related tools, products, and services in the deep and dark web.

3 INFORMATION STEALERS

An info stealer is a type of malware that is focused on gathering sensitive and confidential information from the compromised system. While this information is often related to the user’s credentials, they have also been known to seek financial and personal information.

Oftentimes, threat actors offer for sale fresh and updated credentials in marketplaces in the darknet, as they know the value it could bring to other threat actors who are executing a malicious campaign.

Stealers, on many occasions, are operated as a “malware-as-a-service” model in which the credentials are offered for sale. Elaborated description about Information Stealers, how they are being used and distributed as well as the risk they pose could be found in Cyberint report - Info Stealers Ecosystem Introduction.



Creation Date: May 09, 2021 • 12:1
Publish Date: Feb 28, 2021 • 02:0

Vidar Baja California ISP: Uninet S.A. de C.V. auth.opera.com | tnegocio.com.mx | tnegocio.com.mx | cecor.interactioncenter.tellware.mx | tnegocio.com.mx | siana.telmex.com | gisempresarial.intranet.telmex.com | mercadolibre.c | 10.94.233.133 | tnegocio.com.mx | geoplex.intranet.telmex.com | ccmex1 | psa.xxi-banorte.com | netflix.com | carso.capacitateparaelempleo.org | abysmods.com | global.americanexpress.com | micuenta.infonavit.org.mx | security.online-banking.hsbc.com.mx | keymailer.co | accounts.google.com | duolingo.com | cas1.calstatela.edu | duolingo.com | duolingo.com accounts.google.com | es-la.facebook.com | login.microsoftonline.com | duolingo.com | id.g2a.com | accounts.google.com | minecraft.net | accounts.google.com | cecor.interactioncenter.tellware.mx | tnegocio.com.mx | gis.intranet.telmex.com | tnegocio.com.mx | dash.cloudflare.com | ap.namecheap.com | 192.168.1.254 Show more... - archive.zip 2021.02.280.16Mb LOGSSALE[Diamond] $ 5.00 Buy

Figure 2 - Russian market offers fresh harvested credentials for sale, obtained via stealers

THE FRESH CREDENTIAL OBTAINED IN THE METHODS ABOVE WOULD RELATE TO TWO MAIN TYPE OF USERS:

- Internal employee – obtaining access to the enterprise internal systems
- Customer – obtaining access to customer accounts (example customer bank account)

Both cases are valuable to the threat actors, each in a different way as detailed below.

HOW CYBERINT DETECTS LEAKED EMPLOYEE CREDENTIALS

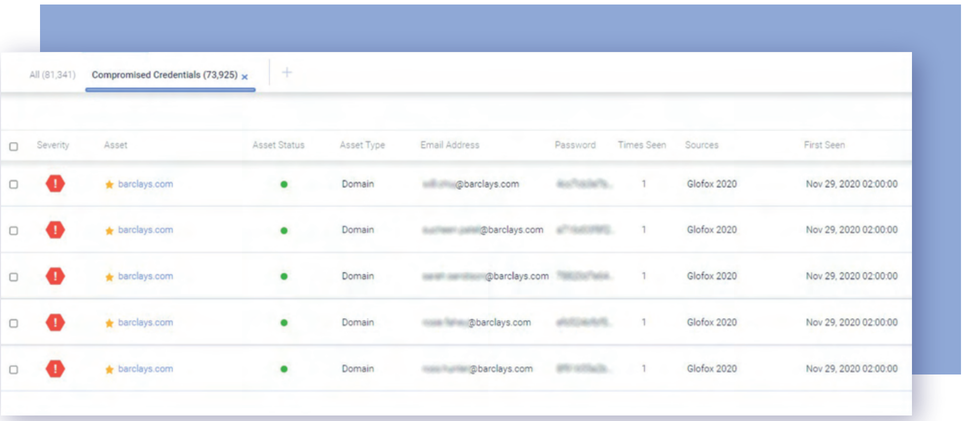
Argos Edge™ contains a database of compromised credentials of over 9 billion lines that is continuously updated. Dumps are proactively added and released periodically. In many cases these sources are identified before other platforms. approximately 1000 databases are added every year, each including hundreds to millions of records.

In addition, Argos Edge™ is automatically tracking paste sites and other forums in which credentials are being published. Username and password combinations (known as “combos”) are recognized, parsed out and automatically pushed to the Argos Edge database.

The solution also intercepts malware logs from stealers, which contain stolen credentials. This enables visibility into the credentials that were stolen in the exfiltration phase, which means they were newly stolen and most likely are up to date i.e. fresh credentials. This provides users with a big advantage compared to users of most traditional Threat Intelligence providers as the latter rely on dumps **after** they are published.

Argos Edge™ detects leaked credentials **before they are even being sold on the dark markets** so Cybersecurity teams can prevent the next ATO attack, investigate, and further harden security so another leak is less likely to happen.

The solution offers deep visibility and aids in understanding exactly what was leaked: You can drill into the details of the leaked credentials the passwords detected for each email, the number of times that each combination of email and password was seen, the sources of credentials, the first time they were published, and the last time they were published.



□	Severity	Asset	Asset Status	Asset Type	Email Address	Password	Times Seen	Sources	First Seen
□	!	★ barclays.com	●	Domain	[redacted]@barclays.com	[redacted]	1	Glofox 2020	Nov 29, 2020 02:00:00
□	!	★ barclays.com	●	Domain	[redacted]@barclays.com	[redacted]	1	Glofox 2020	Nov 29, 2020 02:00:00
□	!	★ barclays.com	●	Domain	[redacted]@barclays.com	[redacted]	1	Glofox 2020	Nov 29, 2020 02:00:00
□	!	★ barclays.com	●	Domain	[redacted]@barclays.com	[redacted]	1	Glofox 2020	Nov 29, 2020 02:00:00
□	!	★ barclays.com	●	Domain	[redacted]@barclays.com	[redacted]	1	Glofox 2020	Nov 29, 2020 02:00:00

Figure 3 - Argos Edge Employee leaked credentials module

As described, employee credentials can potentially be used to infiltrate the organization’s systems and therefore pose a critical risk. There is a common misconception that leaked credentials generated from 3rd party data breaches, are only meaningful if they can be used to access internal network and company assets.

LEAKED CREDENTIALS POSE A RISK FOR THREE REASONS:

1

They allow an inroad if they are the same as the domain password in the organization’s internal network. Password reuse is a common situation, so the password to a 3rd party site could be the same password as the organization login.

2

They can support social engineering attempts: Takeover of social media accounts or other online accounts of an employee, being collected of a 3rd party breach, can be used to launch spear phishing attacks against other employees or managers in the company.

3

They allow for better Dictionary/brute force attacks: As over 70% of people reuse their password or similar passwords in one way or another, using employee credentials as a base for a dictionary attack can help an attacker to recover the user’s actual network password by applying simple modification algorithms to leaked passwords.

HOW CYBERINT DETECTS LEAKED CUSTOMER CREDENTIALS

As mentioned above, Cyberint collects live streams of freshly harvested credentials by information stealers. This information includes the URL which was used during the login. Based on this information Argos Edge can automatically find potentially breached credentials of customers of the organization in focus.

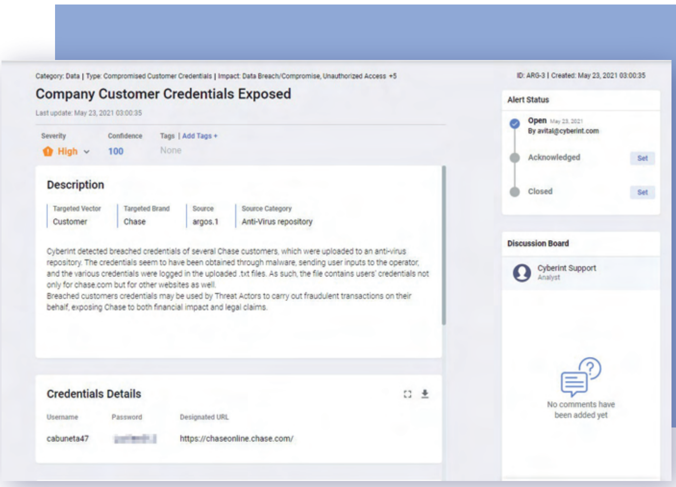
Breached customer credentials may be used by threat actors to carry out fraudulent transactions, exposing the company to monetary loss, legal claims, and brand damage.

MITIGATION BEST PRACTICES:

1. **Enforce password reset on the compromised accounts.**

2. **Investigate internally whether any of the accounts have been involved in fraudulent transactions, at least up to the time of detection. In case the accounts were involved in any fraudulent activity, it is recommended to identify and extract relevant action taken by the threat actor (for example trying to obtain a loan in a banking site), and monitor them within the organization.**

3. **Implement MFA (multi-factor authentication) and CAPTCHA mechanisms. The former will create another obstacle for threat actors trying to abuse the account, and help block credentials-stuffing tools. This will reduce the chance of a customer ATO.**



Category: Data | Type: Compromised Customer Credentials | Impact: Data Breach/Compromise, Unauthorized Access +5

ID: ARG-3 | Created: May 23, 2021 03:00:35

Company Customer Credentials Exposed

Last update: May 23, 2021 03:00:35

Severity	Confidence	Tags | Add Tags +
High	100	None

Description

Targeted Vector	Targeted Brand	Source	Source Category
Customer	Chase	argos.1	Anti-Virus repository

Cyberint detected breached credentials of several Chase customers, which were uploaded to an anti-virus repository. The credentials seem to have been obtained through malware, sending user inputs to the operator, and the various credentials were logged in the uploaded .txt files. As such, the file contains users' credentials not only for chase.com but for other websites as well.
Breached customers credentials may be used by Threat Actors to carry out fraudulent transactions on their behalf, exposing Chase to both financial impact and legal claims.

Credentials Details

Username	Password	Designated URL
cabuneta47	[redacted]	https://chaseonline.chase.com/

Alert Status

- Open May 23, 2021 By avital@cyberint.com
- Acknowledged Set
- Closed Set

Discussion Board

Cyberint Support
Analyst

No comments have been added yet

Figure 4 - Customer Credentials leakage alerts in Argos Edge

SUMMARY

Leaked credentials have become a serious risk to most organizations. Visibility into the leaked data allows organizations to mitigate and remediate account take over and breaches in earlier stages, avoiding fraud and other malicious attacks. Cyberint leverages autonomous discovery of leaked credentials from an unparalleled array of sources to allow cybersecurity teams to effectively detect both employees' and customers' leaked credentials, prevent account takeovers, and protect their brand.

About Cyberint

Cyberint fuses threat intelligence with attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.
Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities and more, ensuring continuous external protection from cyber threats.

Contact us: www.cyberint.com | sales@cyberint.com | blog.cyberint.com

Cyberint