Quarterly Business Report

Prepared for AGS IT-partner

04/01/2023 - 06/30/2023

Table of Contents

01. Summary

5 total compromises*

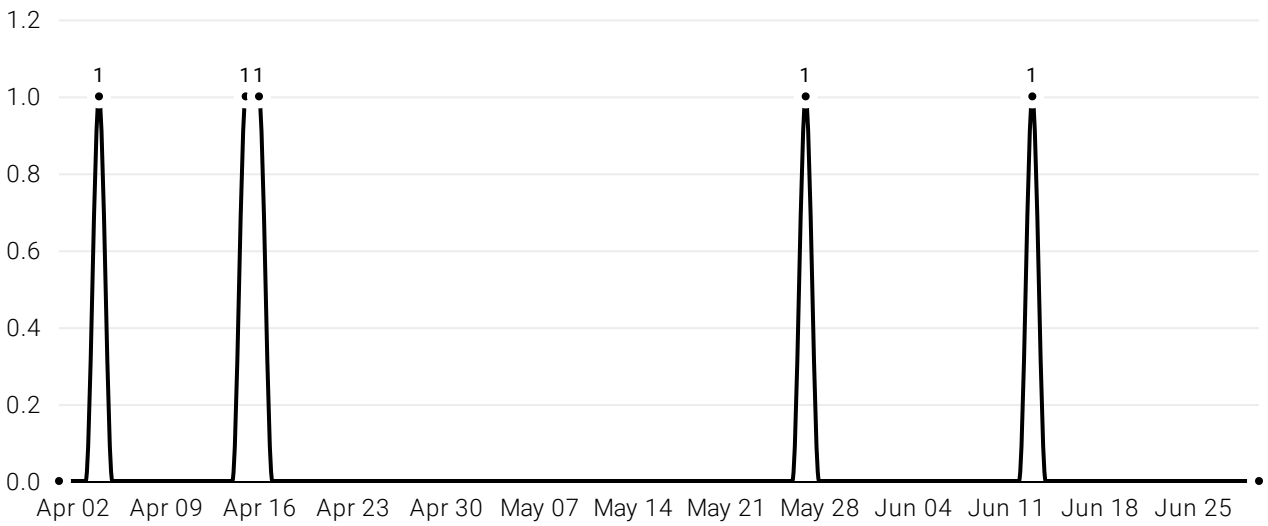
0
IPs* monitored

0
Personal Emails monitored

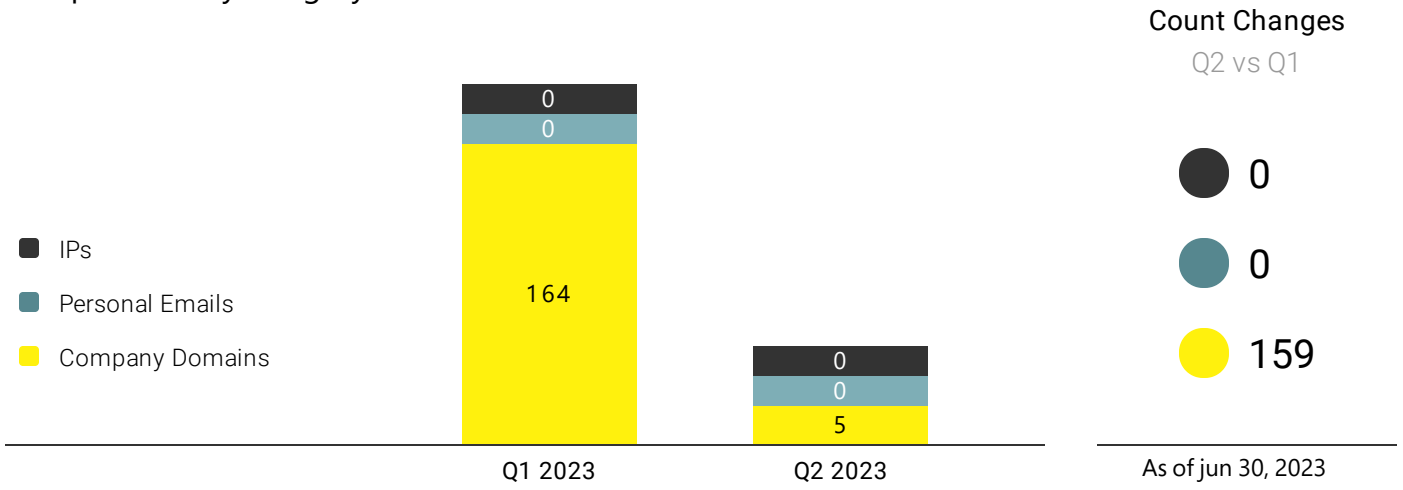
1
Company Domains* monitored

Monthly Compromises

01-04-2023 - 30-06-2023



Compromises by category



02. Benchmark Averages

Compromises

01-04-2023 - 30-06-2023

Your Organization

2983x

less than your industry size average

You are here

5 Compromises

LOW

HIGH

Customer Average

14.9K Compromises

03. Monitoring

01-04-2023 - 30-06-2023

0 IPs
0.0%

0 Personal Emails
0.0%

5 Domains
100.0%

0 IPs
0.0%

0 Personal Emails
0.0%

1 Domains
100.0%

Top 5 Compromised Values By Category

Domains	Compromise #
@ags.no	5

Personal Emails	Compromise #
No data	

IPs	Compromise #
No data	

04. Organizational Compromises

1 Brukerkonto

2 Hvor informasjonen er funnet

Added/Found	Monitored Value		Source	PII Value	Status
Added : 04-04-2023 Found : 27-02-2023	[redacted]@ags.no combolist Password hit: anne*****	Domain	id theft forum None		New Notes (0): No Notes
Added : 15-04-2023 Found : 27-02-2023	632abe5984185e23b5db0e3 s.no combolist Password hit: alex*****				New Notes (0): No N
Added : 16-04-2023 Found : 06-01-2023		Domain	id theft forum None	First Name Last Name User ID	New Notes (0): No Notes

3 Passordet til brukeren

Merk!
Selv om passordet ikke vises fullstendig på selve rapporten er det avedekket i sin helhet og lekket på Dark Web

Dette gjøres for å beskytte brukerens personopplysninger på rapporten

4 Status

Forteller om dette er en ny lekkasje eller en tidligere kjern lekkasje

5 Tidspunkt

Viser når informasjonen er funnet

Added/Found	Monitored Value		Source	PII Value	Status
Added : 27-05-2023 Found : 25-05-2023	[redacted]@ags.no combolist Password hit: B********	Domain	id theft forum None		New Notes (0): No Notes
Added : 13-06-2023 Found : 06-06-2023	[redacted]@ags.no [redacted] Password hit:	Domain	id theft forum None		Resolved Notes (2): Status changed to Resolved. Adresse finnes ikke. Får NDR

05. Breaches

Total of compromises: 5

Breaches	Description	Dates	About	Matching Compromises

No data

06. Glossary of Terms

Compromise Type

C2 SERVER

The IP address has been identified as being associated with a Command-and-control (C2) Server. Command-and-control servers are used by attackers to maintain communications with compromised endpoints within a targeted network. These compromised endpoints collectively are referred to as a botnet. This is achieved through infecting endpoints with malware. Botnets are leveraged by attackers to conduct malicious activity (send spam, distribute malware, etc) without the knowledge of the system owner.

CHAT ROOM

This data was discovered in a hidden Dark Web internet relay chatroom (IRC).

CUTWAIL

The IP address has been identified as associated with the Cutwail botnet and is mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called Pushdo. It affects computers running Microsoft Windows.

FILE SHARING

The IP address has been identified as associated with malicious file sharing activities.

ID THEFT FORUM

This data was discovered being exchanged on a dark web forum or community associated with ID theft activities.

P2P FILE

This data was discovered as part of a file being exchanged through a peer-to-peer file sharing service or network.

PUBLIC WEB SITE

This data was discovered on a publicly-accessible web forum or data dump site.

SOCIAL MEDIA

This data was discovered being shared as a post on a social media platform.

WEBPAGE

This data was discovered on a hacker website or data dump site.

ZERO ACCESS

The IP address has been identified as associated with the Zero Access botnet. At the time of discovery, the ZeroAccess rootkit responsible for the botnet's spread is estimated to have been present on at least 9 million systems (2012).

Terms to Know

ADDED DATES

The date the compromise was added to Dark Web ID.

BREACHES

The name of the associated breach - See list of breaches for more details regarding a specific breach.

COMPROMISE

An instance of that individual's information appearing on the Dark Web.

FOUND DATES

The date we found the compromise on the Dark Web.

Website

NOT DISCLOSED

The origin of the breach has not been disclosed for one of two reasons: The name of the site has not yet been determined or the breached organization has not yet publicly acknowledged a cyber incident.

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

HOW ARE CREDENTIALS COMPROMISED?

PHISHING

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLES

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACKS

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Passwords are twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto servers including corporate networks, social media sites, e-commerce sites and others.

39%

Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500

Average number of breached data records, including credentials, per U.S. based company

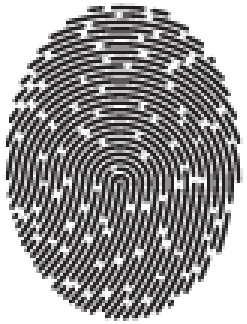
User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

$1 - $8

Typical price range for individual compromised credentials

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?



- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others can organizations protect their business from the perils of the dark web.