INTERNETEK

Monthly Business Report

Prepared for [redacted]

05/01/2024 - 05/31/2024

Table of Contents

INTERNETEK

Prepared for [redacted]

01. Summary

9 total compromises*

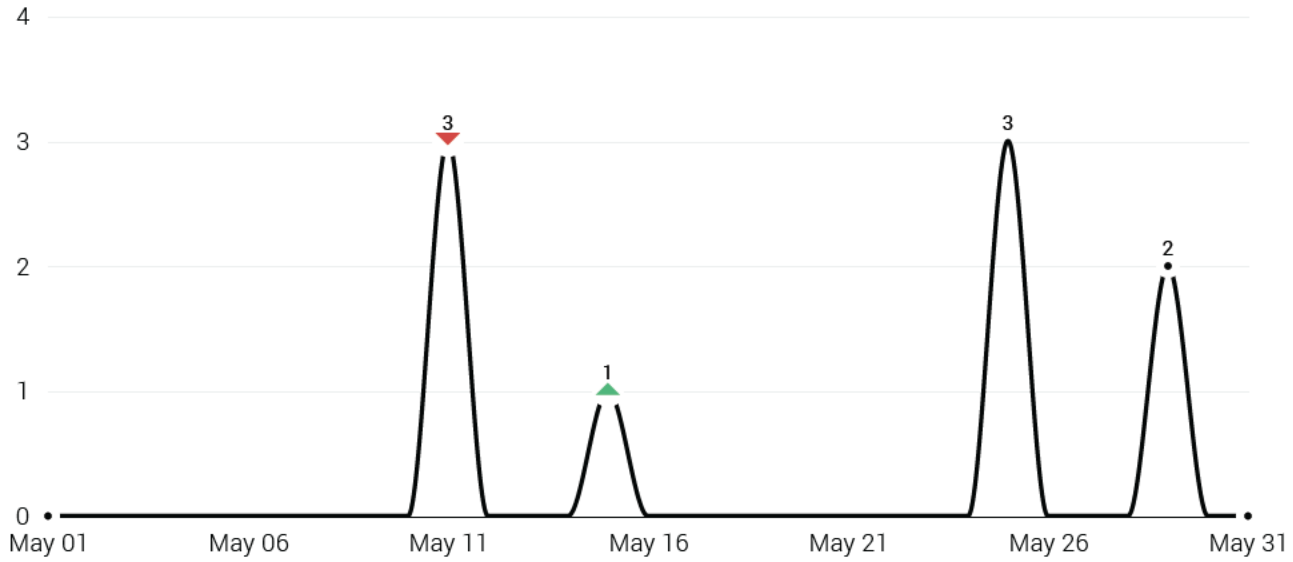
0
IPs* monitored

7
Personal Emails monitored

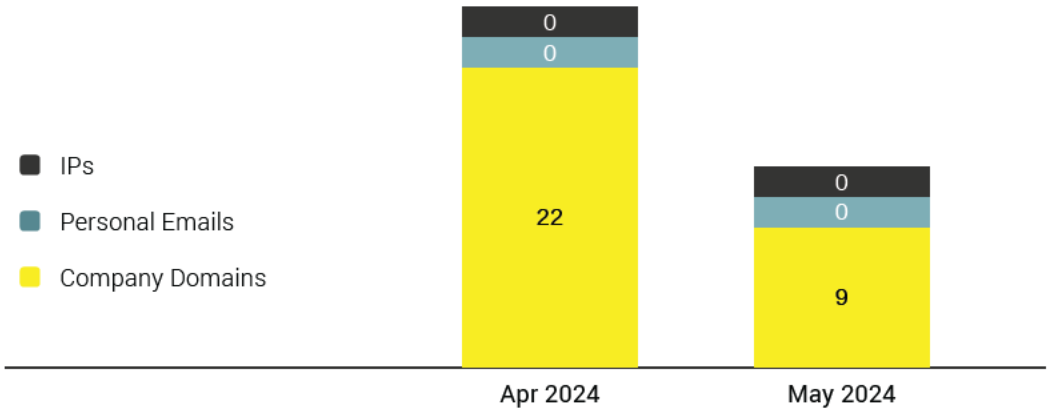
1
Company Domains* monitored

Monthly Compromises

05/01/2024 - 05/31/2024



Compromises by category



Count Changes

May vs Apr

0

0

13

As of May 31, 2024

02. Benchmark Averages

Compromises

05/01/2024 - 05/31/2024

Your Organization

841x

less than your industry size average

You are here

9 Compromises

Customer Average

7.6K Compromises

03. Monitoring

05/01/2024 - 05/31/2024

9

Compromises*

0 IPs

0.0%

0 Personal Emails

0.0%

9 Domains

100.0%

3

Associated Breaches*

0 IPs

0.0%

0 Personal Emails

0.0%

3 Domains

100.0%

Top 5 Compromised Values By Category

Domains	Compromise #
@[redacted]	9

Personal Emails	Compromise #
No data	

IPs	Compromise #
No data	

04. Organizational Compromises

Added/Found	Monitored Value	Source	PII Value	Status
Added : 05/11/2024 Found : 04/29/2024	m[redacted].com breach Domain Password hit:	id theft forum bloomstoday.com	First Name Last Name Address 1 City 2 More...	Resolved Notes (1) Status changed to Resolved
Added : 05/11/2024 Found : 04/29/2024	s[redacted].com breach Domain Password hit	id theft forum bloomstoday.com	First Name Last Name Address 1 City 2 More...	Resolved Notes (1): Status changed to Resolved.
Added 05/11/2024 Found 04/29/2024	a[redacted].com breach Domain Password hit	id theft forum bloomstoday.com	First Name Last Name Phone	Resolved Notes (1): Status changed to Resolved.

Added/Found	Monitored Value	Source	PII Value	Status
Added 05/15/2024 Found 05/02/2024	[redacted]com [redacted] Domain Password hit	id theft forum dataasfoundonofficialusa.com(apeoplefindersite)	First Name Last Name Address 1 City 2 More...	New Notes (0): No Notes
Added 05/25/2024 Found 05/22/2024	[redacted].com [redacted] Domain Password hit:	id theft forum None	First Name Last Name Zip Phone	New Notes (0) No Notes
Added : 05/25/2024 Found : 05/22/2024	[redacted]com [redacted] Domain Password hit:	id theft forum None	First Name Last Name	New Notes (0) No Notes

Added/Found	Monitored Value		Source	PII Value	Status
Added 05/25/2024 Found 05/22/2024	k[redacted].com [redacted] Password hit	Domain	id theft forum None	First Name	New Notes (0): No Notes
Added 05/29/2024 Found : 05/27/2024	c[redacted].com [redacted] combolist Password hit Gree*****	Domain	id theft forum None		New Notes (0): No Notes
Added : 05/29/2024 Found : 05/27/2024	c[redacted].com [redacted] combolist Password hit: Icke*****	Domain	id theft forum None		New Notes (0) No Notes

05. Breaches

Total of compromises: 9

	Breaches	Description	Dates	About	Matching Compromises
new	**bloomstoday.com**	Unavailable	Found Breach April 2024 Added to DWID May 4, 2024	Number: Unknown Types Unknown	**3** Domains
new	**dataasfoundonofficialusa.com (apeoplefindersite)**	Unavailable	Found Breach May 2024 Added to DWID May 11, 2024	Number: Unknown Types Unknown	**1** Domains

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.