Dark Web Assessment Report
Galactic Bank
Apr 2026

Usage Guidance

- Treat as confidential
- Do not distribute, email, fax, or transfer against company policy
- Do not share
- Store in secure locations
- In many organizations, violating any of these instructions is grounds for termination

Executive Summary Section

Synapse Cyber has been tasked with determining which information is available to attackers publicly, including on the dark web. This includes credentials from the organization's domain. The information in this report has been compiled using various tools, data sources and collection techniques.

One (1) Domain was found with a total of **four (4)** SSL certificates, **zero (0)** of which have expired or are expiring in less than 60 days. **Sixteen (16)** compromised credentials were found, **fourteen (14)** of which are unique. Of the **sixteen (16)** credentials, **fourteen (14)** are plain text, **one (1)** is a cracked hash, and **one (1)** is a hash.

Domains Scanned

Domains	Subdomains Found	Certificates Found	Certificates Expiring in Less than 60 Day
galacticbank.com	4	4	0

Compromised Credentials

Total Compromised Credentials

16

Unique Compromised Emails

14

Plain Text	**14**
Suspected Hash	1
Cracked Hash	1

DNS Findings

Domain Summary - galacticbank.com

Fourteen (14) emails were found on the dark web accounting for **sixteen (16)** compromised credentials across **four (4)** different breaches. Most of the compromised credentials are of urgent severity and require immediate attention to ensure they are no longer in use.

Four (4) SSL certificates found. The closest expiration date is in **six hundred eighty-four (684)** days. See "SSL Certificate Information" for more details.

The domain registrar is **IONOS SE**.

DMARC is configured but will not help against email/domain spoofing until its enforcement settings are remedied. SPF is configured correctly which will help deter most email/domain spoofing. Anonymous Zone Transfers are allowed by the nameservers in use, which would give an attacker the ability to access every known IP and server hostname on the DNS server.

DNS Findings - galacticbank.com

Domain Creation Date: 24 February 2013

Domain Expiration Date: 24 February 2027

Anti Spoofing	✱ DMARC Enforcement ✓ SPF Configured	Attention
Domain Security	✓ Registrar Well Known ✓ Domain Locked ✓ Expiration > 6 months	Healthy
Zone Transfer	✕ Anonymous Disabled	Unsecure
Data Exposure	✓ Few Subdomains ✕ Masking Implemented	Attention

✓ Implemented and configured properly

✱ Implemented but **not enforced** (see DNS Findings Guidance)

✕ Not implemented

Compromised Credentials

Compromised Credentials- galacticbank.com

Email Alias	Source	Credential	Suspected Format
adavis	Antipublic	p@ssword	CRACKED
bbaney	Antipublic	malinios2	PT
bbaney	People Data Labs	brianbaney123	PT
dfoley	www.sandhuniforms.com (Cit0day)	sweet55	PT
dholland	Adobe	gRh7QtSsjJ86	PT
dholland	Adobe	superduper	PT
dstevenson	People Data Labs	chocolatebar	PT
horsey	People Data Labs	englishmuffin5	PT
kmuske	Antipublic	2gUrrI8HuC3k=	HASH
mfitzgerald	Antipublic	qwertyuiop123	PT
mmagano	Antipublic	86753091337	PT
nkeller	Adobe	@april142O25	PT

nwhitehead	Adobe	thisIsmyP@ssw0rd1	PT
pkapitan	People Data Labs	grizzlybear	PT
xrogers	Antipublic	notagoodpassword	PT
zandrews	People Data Labs	P@ssword1	PT

SSL Certificates

Domain	SSL Cert. Creation Date	SSL Cert. Expiration Date	Issuer	Expiration Less than 60 Days
connect.galacticbank.com	15 Feb 2018	15 Feb 2028	DigiCert Inc.	No
mail.galacticbank.com	15 Feb 2018	15 Feb 2028	DigiCert Inc.	No
portal.galacticbank.com	15 Feb 2018	15 Feb 2028	DigiCert Inc.	No
www.galacticbank.com	15 Feb 2018	15 Feb 2028	DigiCert Inc.	No

Domain Collision

Domain Collision List - @galacticbank.com **Creation Date - 24/02/2013**

Domain Name	Name Server	Email	Registrar Name	Registrant Name	Creation Date	Predates
galacticbanks.com	✔	✔	Dynadot Inc		04/10/2025	No
galacticrank.com	✔	✔	NameCheap, Inc.		04/04/2024	No
galaticbank.com	✔	✘	Network Solutions, LLC		30/04/2025	No
galac.ticbank.com	✔	✔	GoDaddy Online Services Cayman Islands Ltd.		28/05/2005	Yes
galacti.cbank.com	✘	✘	Network Solutions, LLC		30/07/1995	Yes
galact.icbank.com	✔	✘	Inames Co., Ltd.		20/03/2000	Yes
galacticbonk.com	✔	✔	GoDaddy.com, LLC		29/07/2025	No

Overview of Breaches

Below are brief explanations of the breaches included in this report. Also included are some helpful links for further information.

Adobe - 153 million Adobe accounts were compromised in 2013, disclosing account ID's, usernames, emails, poorly encrypted passwords, and the associated password hints in plain text.

AntiPublic - A "combo list" named AntiPublic disclosed 458 million unique emails, many with multiple passwords from various services. This was largely used for attempting to discover reused passwords across services.

Data Leak - The exposure of sensitive data to an unauthorized party. This can be proprietary information, personal information, credentials, documents etc and can occur intentionally through a breach or unintentionally through misconfigurations.

People Data Labs - In 2019, an unsecured elasticsearch server disclosed 1.2 Billion records of data, including 622 Million unique email addresses. Information exposed included emails, phone numbers, social media profiles and employment history.

www.sandhuniforms.com (Cit0day) - 226 Million unique email addresses spanning over 23,000+ websites were disclosed in November 2020. Emails were paired with passwords, often represented as hashes as well as their cracked, plaintext versions.

DNS Findings Guidance

Having DMARC and SPF configured correctly is the best way to prevent email/domain spoofing, but only if configured and enforced correctly.

DMARC, or Domain-based Message Authentication Reporting and Conformance, is a way for ensuring an email sender is legitimately who they say they are, and what actions to take if they are found not to be. DMARC is a proposed standard which validates sender/receiver information so email exchange can be more trustworthy.
For simple instructions regarding creation of a DMARC record, visit:
https://mxtoolbox.com/DMARCRecordGenerator.aspx

Enforcement of DMARC is just as important as implementation because only when you reject or quarantine unauthorized sent mail do you benefit from DMARC's email/domain spoofing functionality. The default setting for how a mail server treats mail which fails DMARC is monitoring mode (option: "p=none") which allows the mail to be sent, but forwards information to the mail server's administrator, or another specified email. In this situation DMARC is implemented but is not enforced since the potentially malicious emails will be delivered. More secure options would be to either reject the sent mail entirely or quarantine the sent mail by delivering it to a spam folder instead.

SPF, or Sender Policy Framework, is a way for an email recipient to validate the alleged identity of the email sender. A recipient mail server can verify the email originated from the domain it claims by ensuring the mail came from an authorized IP address.
For simple instructions regarding the configuration of SPF, visit:
https://mxtoolbox.com/spf.aspx

Zone transfers are common ways for a DNS server to replicate zone information to a secondary DNS server. This allows for DNS redundancy and the use of multiple DNS servers for load balancing. A zone transfer is a way for the primary DNS server to give the secondary DNS server all its stored information such as IP addresses and server hostnames, which is a gold mine of information to a bad actor. The significance of this information is why zone transfers must only be accessible by authorized servers. Unsecured/Anonymous zone transfers must be prohibited in the DNS server configuration.
SANS Zone Transfer whitepaper:

https://www.sans.org/white-papers/868/

Appendix

Suspected Format Explanations

Breached Credential Format is determined by various criteria including credential format, existence in password dictionaries, attribution to explicit content (Ashley Madison, markets, etc.) and current state exploitability.

(PT) Plaintext

The red font indicates high severity and requires urgent attention because PT stands for Plaintext. This means the credential is not obfuscated or encrypted at all and can be exploited as is. Breaches listing accounts with plaintext passwords are highly sought after and are commonly the most valuable for a bad actor since there is no additional processing/mangling necessary to exploit these accounts.

(CR) Cracked Hash

The red font indicates high severity and requires urgent attention because Cracked represents any hash that has been or is very easily cracked. This means the credential is no longer obfuscated and can be exploited. Breaches listing accounts with easily cracked hashes are highly sought after since they function as plaintext passwords.

(HASH) Suspected Hash

Hash is a broad term and may refer to any hashing algorithm. Hashes are one-way functions which means there is no way to dehash a password once it has been obfuscated. Hashes are generally a fixed length of characters representing the original input string. Hashes are used across the landscape of the internet for storing passwords in databases, ensuring validity of data etc.