



Executive Report



GreenAnimalsBank

Time Period: 2020/10/19 - 2021/10/19 | Report Date: 2021-10-19



4000 Legato Road, Suite 1100
Fairfax, VA 22033 USA

+1 (571) 249-4598

info@socradar.io

www.socradar.io

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence – all automated and supported by a global team of qualified intelligence analysts – provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.



4.9 OUT OF 5 STARS
IN 14 REVIEWS
★★★★★ AS OF 11/2020

Table Of Contents



Executive Summary

Actionable Alerts Overview

Key Findings

- > Deep & Dark Web
- > Critical Asset Exposure & Vulnerabilities
- > Malware-Bot Infected Users
- > Compromised Employee Credentials
- > Phishing Intelligence
- > Social Media & Brand Impersonation

The SOCRadar Advantage



The Executive Report has been prepared for GreenAnimalsBank by SOCRadar Digital Risk Protection and Cyber Threat Intelligence Platform. This report summarizes the blind spots of public-facing digital attack surface as well as sensitive data exposure of GreenAnimalsBank. The data used for this analysis has been collected by scanning a wide variety of sources across Surface, Deep and Dark Web using non-intrusive OSINT methodologies. Starting with company domain name, SOCRadar created a baseline of your organization's external attack surface in hours before initiating extensive monitoring. With this report, you can get executive insights and actionable intelligence into your organization's attack surface to better predict and defend cyber attacks.

Actionable Threat Intelligence

52

alerts have been generated

Industry: Banking

Country: United Kingdom

License: Enterprise | 651 assets subject to licensing

API Integration: Active

Modules: AttackMapper | RiskPrime | ThreatFusion

Deep & Dark Web Findings

72

Mentions in Threat Actor Communication Channels



Malware-Bot Infection Threats



4

Bot-infected Users Posing a High Data Breach Risk

Phishing Intelligence

34

Potential Phishing Domains



Social Media Brand Reputation Threats

11

Impersonating Social Media Profiles



Leaked Employee Login Credentials



46

Compromised Employee Login Credentials

Critical Asset Exposure & Vulnerabilities



1220

External-Facing Digital Assets



As an early warning system against external threats, the SOCRadar Platform generated 52 actionable threat intelligence alerts from a holistic perspective. To eliminate false positives, all alerts have been vetted by certified TIA team. For quick remediation, the platform also provides recommended mitigation actions.

Below you can see the significant alert types that were generated within the defined time period.

Compromised Employee Credentials **7**

By processing massive breach datasets and monitoring a broad variety of sources, SOCRadar has generated 7 account leak alerts.

Critical Asset Exposures And Vulnerabilities **10**

SOCRadar has continuously monitored your attack surface to identify hacker-facing vulnerabilities as well as critical ports and generated 10 alerts.

Stolen Credit Cards **3**

To improve your Anti-Fraud mechanisms, the platform generated 3 alerts including stolen credit card information and sources.

18

Deep & Dark Web Data Exposure

Through automated monitoring of thousands of deep and dark web (.onion) sources, SOCRadar has generated 18 alerts.

6

Phishing Domain Detection

To help you prevent phishing and BEC attacks against your customers and employees, SOCRadar has generated 6 alerts.

1

Customer Data Breach

SOCRadar has generated 1 alerts by detecting customer data and credentials which may result in regulatory fines or brand reputation loss.

7

Source Code Exposure

To prevent unknown sensitive data exposures on code repositories like GitHub, SOCRadar has generated 7 alerts.

SOCRadar uncovered where/how your organization has been exposed to deep and dark web threats. To find out the sensitive data exposures and threat actor activities targeting your industry, massive data collected from thousands of underground hacker forums, blackmarkets, onion sites, Telegram channels, Russian deep web marketplaces have been analyzed. Following table summarizes the findings.

Keywords: GreenAnimalsBank | greenanimalsbank.com

72
Mentions in threat actor communication channels

18
Stolen credit cards detected

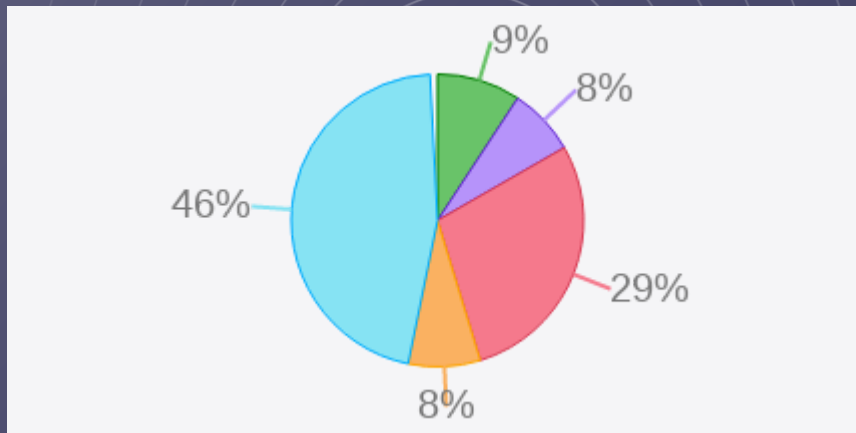
124
Threat actor posts related to your industry in the last 1 month

Latest Findings

Date	Source	Keyword
2021-06-04	Chatter Data	755849
2021-05-10	Hacker forum data	GreenAnimalsBank
2021-05-10	Hacker forum data	GreenAnimalsBank
2021-05-10	Hacker forum data	GreenAnimalsBank
2021-05-10	Hacker forum data	GreenAnimalsBank
2021-05-10	Telegram Hacker Channel Data	greenanimalsbank
2021-04-13	Hacker forum data	GreenAnimalsBank
2020-10-10	Paste Site Data	greenanimalsbank
2020-10-07	Discord Hacker Channel Data	greenanimalsbank

By using only your main domain as an input - SOCRadar has already uncovered your public-facing digital assets to enable your security team to take control of your digital footprint. Blind spots of your evolving attack surface are often targeted by threat actors.

External-facing Digital Asset Distribution



997
Assets

- Domain Infrastructure
- Websites & SSL
- IPs & DNS Records
- Employees & Social Accounts/Apps
- Services & Cloud Techs

Possible blind spots / Shadow IT assets

257 Open critical ports
MySQL, PostgreSQL,
Microsoft SQL Server, RDP

0 Expired SSL
certificates

17 Technologies at risk

Ms14-066:
Vulnerability In
Schannel Could
Allow Remote
Code Execution
(2992611)
(Unauthenticated
Check)

| CVE-2014-6321

| CVSS: 10.0

Nginx 1.9.5 <
1.16.1 / 1.17.X <
1.17.3 Multiple
Vulnerabilities

| CVE-2019-9516

| CVSS: 6.8

Nginx 0.6.X <
1.20.1 1-Byte

As one of the emerging underground market, threat actors are selling stolen identities from malware bot-infected devices frequently advertised as stealer logs. These bots-for-sale marketplaces affect not just users whose credentials and digital identities are stolen, but also the organizations that users are working for. SOCRadar provides you the continuous visibility to detect this evolving threat.

Related malware families

AZORult Trojan

The AZORult malware was first discovered in 2016 to be an information stealer that steals browsing history, cookies, ID/passwords, cryptocurrency information and more. It can also act as a downloader of other malware. It was sold on Russian underground forums to collect various types of sensitive information from an infected computer.

Raccoon Infostealer

Raccoon emerged as Malware as a Service (MaaS) in April 2019. The malware is capable of stealing login credentials, credit card information, cryptocurrency wallets, and browser information. Raccoon has basic infostealer functions but an aggressive marketing campaign and overall good user experience proved enough to make up for its lack of additional features.

4 Bot-infected Users Posing a High Data Breach Risk

Latest Findings

Date	Source	Url
2020-10-12	Cybercriminal Marketplace	greenanimalsbank
2020-10-11	Cybercriminal Marketplace	greenanimalsbank
2020-10-10	Cybercriminal Marketplace	greenanimalsbank
2020-10-10	Cybercriminal Marketplace	greenanimalsbank

Having credentials exposed can have far reaching effects, such as data breaches, loss of brand reputation, as well as financial losses. By processing unknown and well known breach datasets leaked on Darknet marketplaces, the platform has identified the credentials of your employees including your C-level executives. To mitigate possible threats, we recommend you to reset/disable these accounts and apply 2FA mechanisms.

46

Employee Credentials Detected

11

VIP Credentials Detected

Recently detected credentials

Date	Email Address	Source	Category
2021-08-03	john.doe@example.com	Combolist	VIP
2021-06-18	c.thomas@gmail.com	Combolist	VIP
2021-05-03	lacygorman21@gmail.com	Combolist	VIP
2021-05-03	lacy.gorman@greenanimals.com	Combolist	VIP
2021-05-03	raineeyy@gmail.com	Combolist	VIP
2021-05-03	raine.bradley@greenanimals.com	Combolist	VIP
2021-05-03	cory.thomas@greenanimals.com	Combolist	VIP

- Same as industry average

- No increase on attacks targeting your industry for last 30 days

A phishing domain is easy to create, and can act as the catalyst for malicious email campaigns and phishing sites. To prevent cyber criminals from leveraging your brand credibility through lookalike domains, SOCRadar continuously performs monitoring at scale across a variety of data sources including Newly Registered Domains and SSL certificates.

Detection methods: homoglyph | punycode | missing dot | repetition | transposition | replacement | omission | insertion

34

Potential Phishing Domains Detected

2

 Initiated Domain Takedown

- Same as industry average
- No increase on attacks targeting your industry for last 30 days

Recently detected potential phishing domains

Domain	Active	MX Record
www.greenanimals.de	<input type="checkbox"/>	<input type="checkbox"/>
greenanimalsbbank.42web.io	<input checked="" type="checkbox"/>	<input type="checkbox"/>
greenanimalsbank.xyz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
greenanimalsbank.ml	<input checked="" type="checkbox"/>	<input type="checkbox"/>
greenanimals.de	<input type="checkbox"/>	<input type="checkbox"/>
greenanimals.org	<input checked="" type="checkbox"/>	<input type="checkbox"/>
greenanimalsbank.xyz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
greenanimalsbank.online	<input checked="" type="checkbox"/>	<input type="checkbox"/>





Brand impersonation or Brandjacking takes place when a threat actor creates a social account pretending to be your brand. SOCRadar can spot fraudulent and fake social accounts by monitoring well known social media platforms like Facebook, Instagram, Twitter and YouTube so that you can quickly take action to stop possible phishing scams.

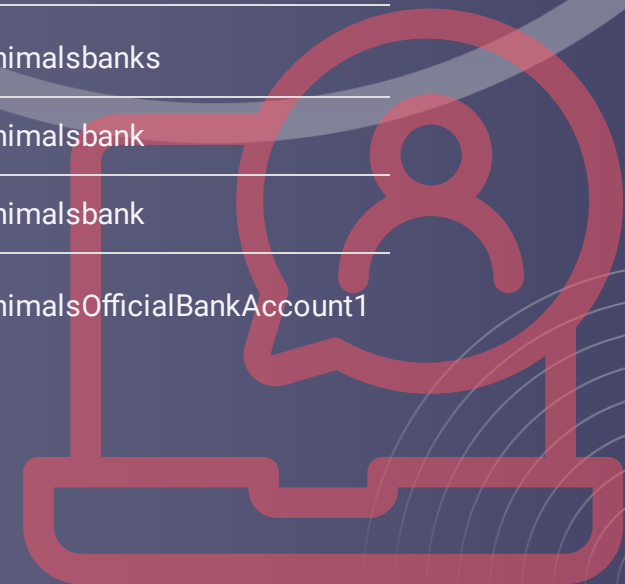
11

Impersonating Social Media Profiles



Recently detected accounts

Social Platform	Account Name
brand_radar	greenanimalsbank
	GreenAnimals
	AnimalsBank
	greenanimalsbanks
brand_radar	greenanimalsbank
brand_radar	greenanimalsbank
	greenanimalsOfficialBankAccount1



The SOCRadar Advantage

Consolidated architecture for operational efficiency and unmatched ROI.

SOCRadar combines attack surface management, digital risk protection, and threat intelligence capabilities to protect your entire business against sophisticated multi-vector cyber attacks.



ThreatFusion
Cyber Threat Intelligence



RiskPrime
Digital Risk Protection



AttackMapper
Attack Surface Management



Power of automation

Skyrocket security team efficiency by reducing mundane tasks.



360° visibility

Gain in-depth visibility into your external-facing digital assets.



Precise API integration

Smooth integration with existing security stack and SIEM solutions.



Immediate start

Hitting the ground in hours, discovering, monitoring and alerting without requiring any input.



Optimized costs

Choose from the discovered assets only you want to monitor to reconcile license costs with real needs.



CTIA support

Ready to work with clients to identify and remediate threats, helping them build in-house skills and expertise.



Trusted by world's leading organizations

