

CYBERSOCAFRICA

Threat Analysis: Phishing Attack Targeting Absa Bank Customers

C-SUITE / LEGAL REPORT

Report	A001
Date	27 TH FEB 2025
Priority	High
Source and Information Reliability	A1
Sensitivity	Confidential

By Victor Mumo

Table of Contents

CYBERSOCAFRICA	1
<i>Threat Analysis: Phishing Attack Targeting Absa Bank Customers.....</i>	1
C-SUITE REPORT	1
1. Executive Summary.....	3
2. Key Takeaways.....	3
3. Intelligence Assessment	4
4. Recommendations	5
5. Key Intelligence Gaps.....	5
6. Supporting Evidence	6
7. Next Steps	9
8. Conclusion.....	9

1. Executive Summary

Campaign Name: Phishing Campaign Targeting Absa Bank Customers

Threat Level: High

Primary URL: https[:]//api[.]yu3[.]io/5ctkkw

Objective: Steal banking credentials and personal information.

Key Findings:

- The phishing campaign targeting Absa Bank customers using api[.]yu3[.]io/5ctkkw. The attacker uses a **shortened URL** (api[.]yu3[.]io/5ctkkw) to mask the malicious link, making it appear less suspicious to victims.
- When clicked, the shortened URL redirects to a **fake Absa Bank login page** hosted on eu2.contabostorage.com.
- Victims are tricked into entering their **account number** and **PIN**, which are then sent to an exfiltration endpoint (loranto[.]com/wp-content/update/send_loginphp).
- The attacker uses **Cloudflare** to hide their infrastructure and **Contabo Storage** to host the phishing page.
- This campaign poses **significant financial, reputational, and regulatory risks** to Absa Bank and its customers.

2. Key Takeaways

- **Who is this report for?**
 - **C-Suite executives, security teams, legal/compliance teams, and Absa Bank's fraud department.**
- **Where was the data collected?**
 - Phishing URL: api[.]yu3[.]io/5ctkkw (shortened URL).
 - Fakeloginpage: eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html.
 - Exfiltration endpoint: loranto[.]com/wp-content/update/send_loginphp.
- **Who was the attacker?**
 - Unknown threat actor leveraging **Cloudflare** and **Contabo Storage**.

- **Who was the victim?**
 - **Absa Bank customers** from South Africa targeted via phishing emails containing the shortened URL.
- **Why does this report matter?**
 - Highlights a **high-risk phishing campaign** designed to steal sensitive banking information, with potential financial losses, reputational damage, and regulatory implications.
- **What is the main takeaway?**
 - Immediate action is required to **block malicious domains, notify affected parties, and prevent further attacks.**

3. Intelligence Assessment

- **Threat Overview:**
 - The attacker uses a **shortened URL** (api[.]yu3[.]io/5ctkkw) to disguise the malicious link, which is sent to victims via **phishing emails**.
 - When clicked, the shortened URL redirects to a **fake Absa Bank login page** hosted on eu2.contabostorage.com.
 - Victims are prompted to enter their **account number** and **PIN**, which are then sent to the attacker's exfiltration endpoint (loranto[.]com/wp-content/update/send_loginphp).
 - The attacker uses **Cloudflare** to mask their infrastructure and **Contabo Storage** to host the phishing page, making it harder to trace.
- **Impact:**
 - **Financial Loss:** Stolen credentials could lead to unauthorized transactions.
 - **Reputational Damage:** Absa Bank's reputation could be harmed if customers lose trust.
 - **Regulatory Risks:** Potential fines for failing to protect customer data.
- **Confidence Level:**
 - **High certainty** that this campaign will impact Absa Bank and its customers if not mitigated promptly.

4. Recommendations

1. **Block Malicious Domains:**

- Add api[.]yu3[.]io, loranto.com, and eu2[.]contabostorage[.]com to blocklists.

2. **Notify Affected Parties:**

- Inform Absa Bank's fraud department and customers about the campaign.

3. **Enhance Email Security:**

- Implement advanced email filtering to detect and block phishing emails containing shortened URLs.

4. **Conduct User Awareness Training:**

- Educate employees and customers on identifying phishing attempts, especially those using shortened URLs.

5. **Monitor for New Campaigns:**

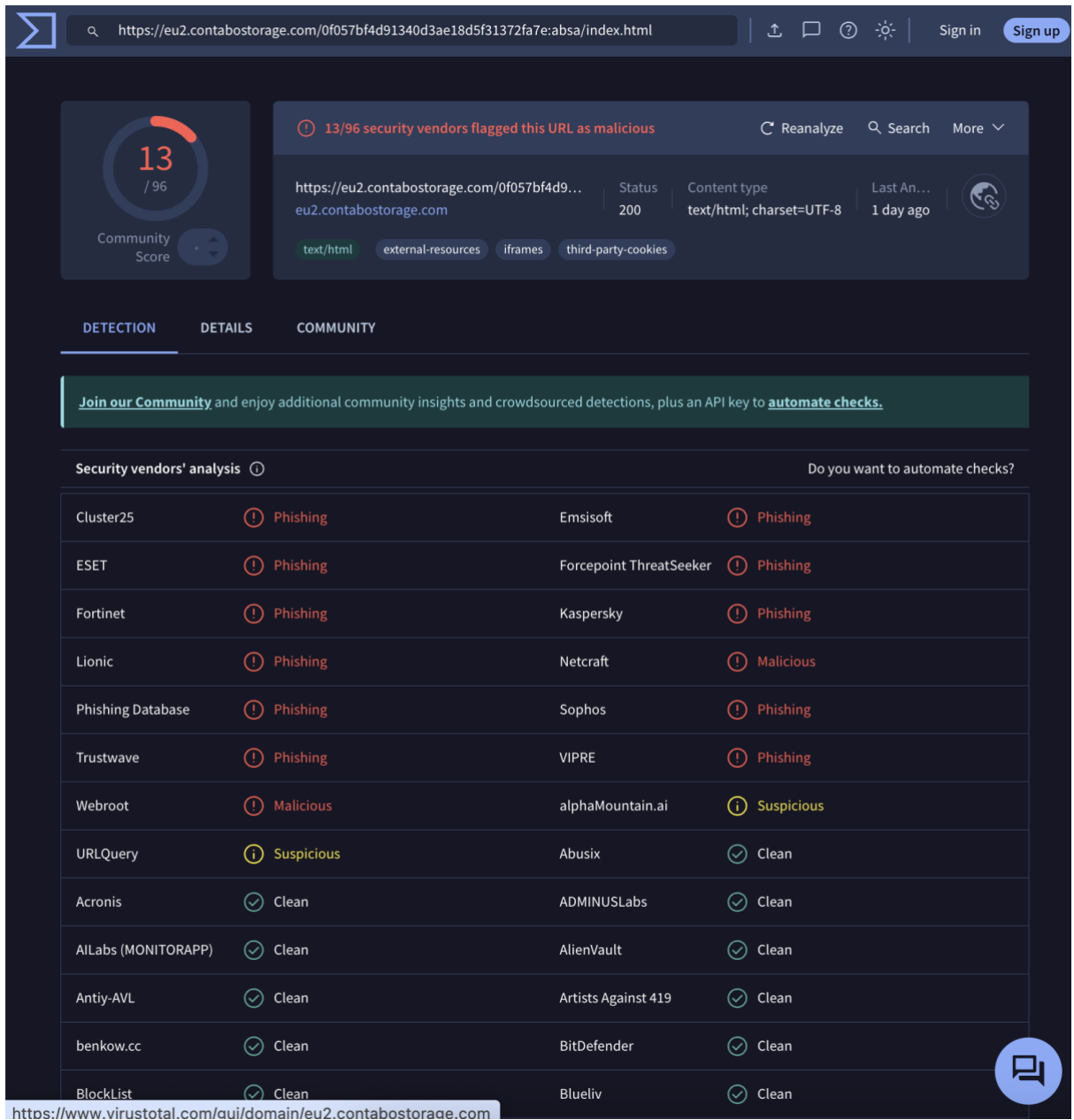
- Use threat intelligence feeds to detect similar phishing activities.

5. Key Intelligence Gaps

- **Threat Actor Identification:** Unknown attacker identity and motivation.
- **Infrastructure Details:** Limited visibility into the full infrastructure used.
- **Victim Impact:** Number of affected customers and extent of damage unknown.
- **Phishing Email Analysis:** Delivery mechanism (e.g., phishing emails) not analyzed.

6. Supporting Evidence

- Screenshots:



https://eu2.contabostorage.com/0f057bf4d91340d3ae18d5f31372fa7e:absa/index.html

13 / 96 Community Score

13/96 security vendors flagged this URL as malicious

Reanalyze Search More

https://eu2.contabostorage.com/0f057bf4d9... Status 200 Content type text/html; charset=UTF-8 Last An... 1 day ago

text/html external-resources iframes third-party-cookies

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Cluster25	Phishing	Emsisoft	Phishing
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	Kaspersky	Phishing
Lionic	Phishing	Netcraft	Malicious
Phishing Database	Phishing	Sophos	Phishing
Trustwave	Phishing	VIPRE	Phishing
Webroot	Malicious	alphaMountain.ai	Suspicious
URLQuery	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean
BlockList	Clean	Blueliv	Clean

https://www.virustotal.com/gui/domain/eu2.contabostorage.com

Figure 1 Virus Total (<https://eu2.contabostorage.com/0f057bf4d91340d3ae18d5f31372fa7e:absa/index.html>)

eu2.contabostorage.com
 173.249.62.85 **Malicious Activity!** [Public Scan](#)

Submitted URL: <https://apiyu3.io/5ctkkw>
 Effective URL: <https://eu2.contabostorage.com/0f057bf4d91340d3ae18d5f31372fa7e-absa/index.html>
 Submission: On February 26 via automatic, source openphish (February 26th 2025, 1:14:06 am UTC) — Scanned from SE

[Summary](#) [HTTP](#) [Redirects](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 4 IPs in 2 countries across 4 domains to perform 19 HTTP transactions. The main IP is 173.249.62.85, located in Nuremberg, Germany and belongs to **CONTABO Contabo GmbH, DE**. The main domain is eu2.contabostorage.com. The Cisco Umbrella rank of the primary domain is 192674.
 TLS certificate: Issued by ZeroSSL RSA Domain Secure Site CA on January 30th 2025. Valid for: 3 months.

[apiyu3.io](#) scanned 67 times on urlscan.io [Show Scans](#) 47
[eu2.contabostorage.com](#) scanned 2122 times on urlscan.io [Show Scans](#) 3123

urlscan.io Verdict: Potentially Malicious
 Targeting these brands: [ABSA \(Banking\)](#)

Live information
 Google Safe Browsing: [No classification for eu2.contabostorage.com](#)
 Current DNS A record: 173.249.62.85 (AS51167 - CONTABO Contabo GmbH, DE)
 Domain created: February 24th 2022, 13:17:22 (UTC)
 Domain registrar: RegistryGate GmbH

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
	IP Address	AS Autonomous System				
1	172.67.195.69	13335 (CLOUDFLARENET)				
2	173.249.62.85	51167 (CONTABO Contabo GmbH)				
15	34.217.255.43	16509 (AMAZON-02)				
1	18.245.60.45	16509 (AMAZON-02)				
19		4				

Screenshot
[Live Screenshot](#) [Full Image](#)

Page Title
 Absa Online

Page URL History [Show Full URLs](#)
 1. <https://apiyu3.io/5ctkkw> [HTTP 200](#)
<https://eu2.contabostorage.com/0f057bf4d91340d3ae18d5f31372fa7e-absa/index.html> [Page URL](#)

Detected technologies
 Adobe Experience Manager (CMS) [Expand](#)

Page Statistics

Requests	HTTPS	IPV6	Domains	Subdomains
19	95 %	0 %	4	4

IPs	Countries	Transfer	Size	Cookies
4	2	185 kB	301 kB	0

Figure 2 URLScan.io for the malicious URLs

Request

```

1 POST /api/v1/instantbuyFrontendBuyFlowPaymentFrame/...
Host: pay.google.com
Cookie: ...
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

```

Response

```

{
  "age": 1000,
  "body": {
    "columnNumber": 102,
    "disposition": "enforce",
    "lineNumber": 240,
    "message": "Permissions policy violation: payment:policy:payment",
    "sourceFile": "https://www.gstatic.com/www/bop-payments-co...
  }
}

```

Browser Window

Login | Yu3 | Free URL | Register | Yu3 | Free URL | Burp Suite Community | Absa Online

[Registration](#)
[How to guide](#)
[How to guide](#)

Login details
 Enter your access account number: 907564
 Enter your PIN: ****
 Enter your user number: 1

It is your responsibility to ensure the secrecy of your PIN number.

Keypad

1	2	3
4	5	6
7	8	9
0	C	

[Reset PIN](#)

• Security centre [selected] 1 of 1 [tab]
 Find all the important information you need to bank securely and with peace of mind.
 • View security measures and enhancements
 • Stay informed about latest scams
 • Shop online with ease

[Learn more](#)

• Useful information [selected] 1 of 1 [tab]
 • [Grandmark International Pte Ltd](#)
 • [Explore more ways to do your banking](#)
 • [2024 rates and fees](#)
 • [Planned Maintenance](#)

© Copyright, Absa Bank Limited. Registration Number: 1966/004794/06 Authorized financial services and registered credit provider NCRCP?

• [Security centre](#)
 • [Terms of use](#)
 • [Privacy policy](#)
 • [Software requirements](#)
 • [Banking regulations](#)

Figure 3 Fake Bank Login Page to fetch credentials

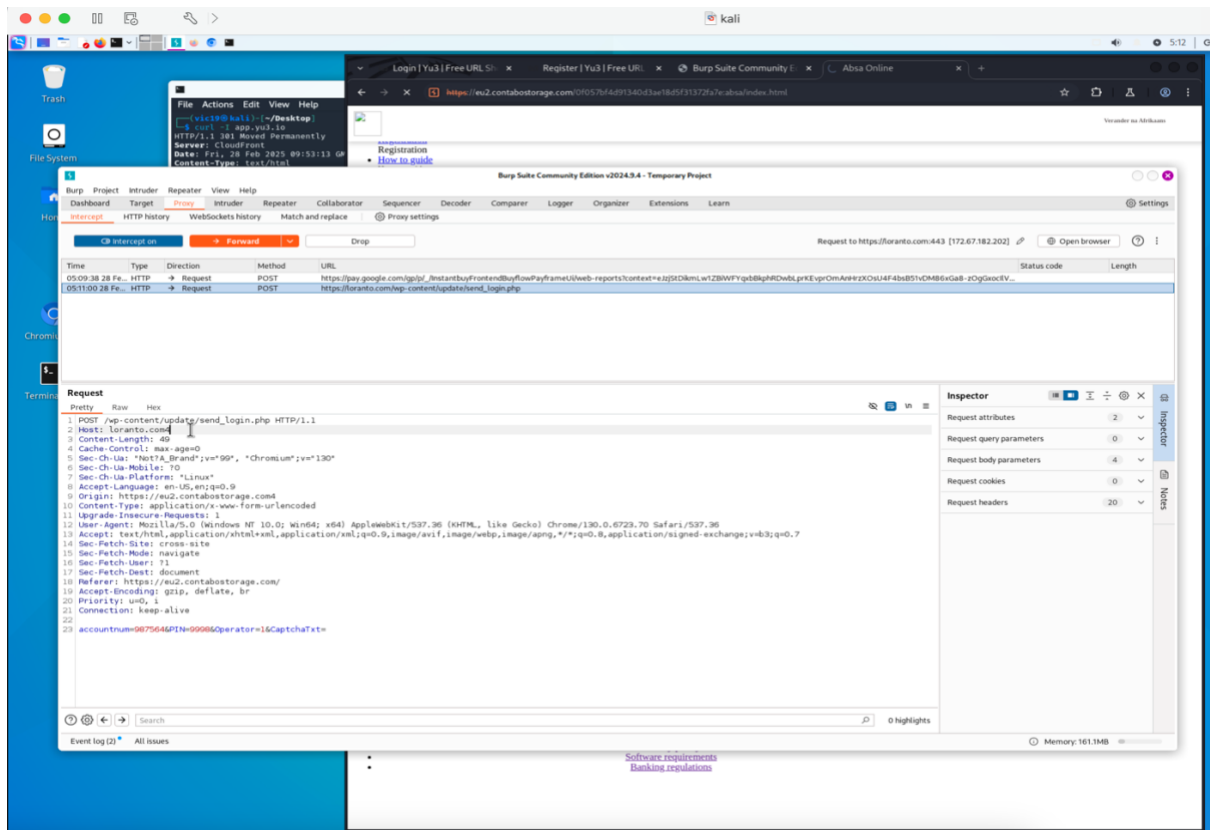


Figure 4 Credentials fetched and redirected to Lorentof.[com

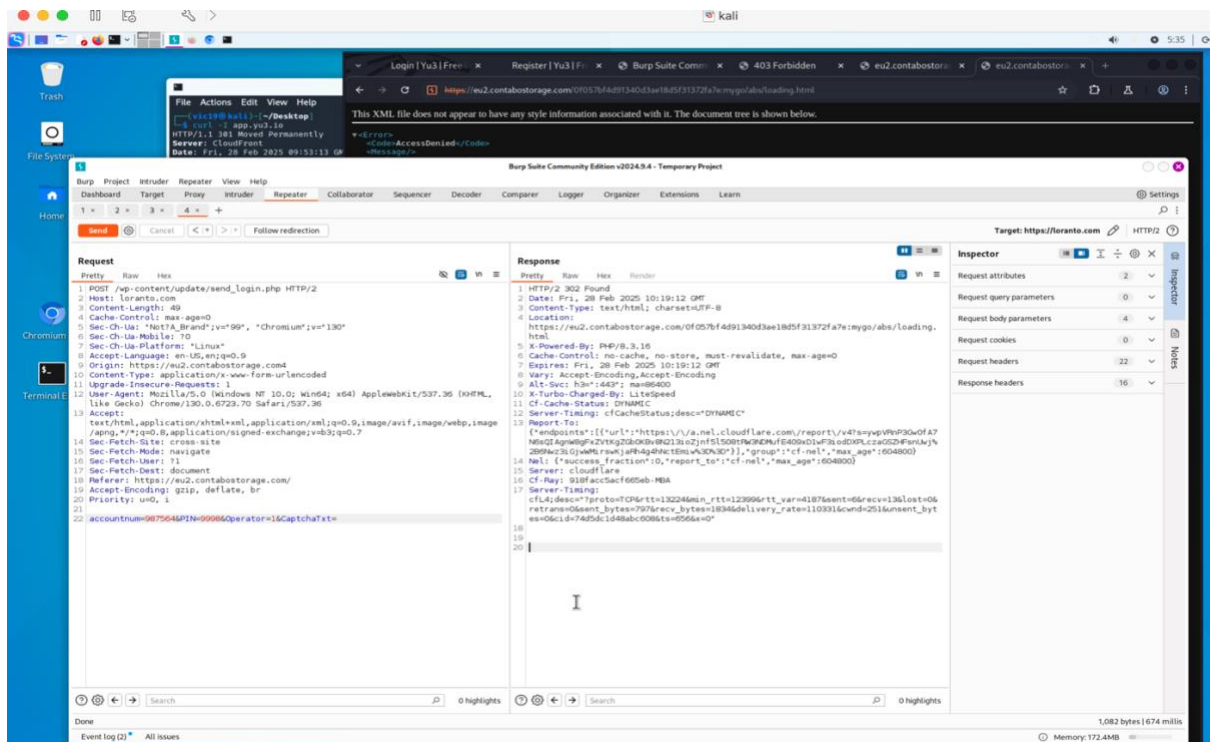


Figure 5 Credentials grabbed and user redirected to fake loading page

- **VirusTotal Analysis:**
 - All URLs and domains flagged as malicious.
 - High community scores for api[.]yu3[.]io, loranto.com, and eu2.contabostorage.com.

7. Next Steps

- **Immediate Actions:**
 - Block malicious domains and notify affected parties.
 - Enhance email security and conduct user awareness training.
- **Further Investigation:**
 - Identify the threat actor and assess the full impact of the campaign.

8. Conclusion

This phishing campaign uses a **shortened URL** to disguise a malicious link, redirecting victims to a **fake Absa Bank login page** designed to steal sensitive banking information. **Immediate action** is required to mitigate the threat, including blocking malicious domains, notifying affected parties, and enhancing security measures. Further investigation is recommended to identify the threat actor and prevent future attacks.