CYBERSOCAFRICA

Threat Analysis: Phishing Attack Targeting Absa Bank Customers

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

By Victor Mumo

Table of Contents

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 has been identified as a high-risk threat. The attacker leveraged infrastructure such as **Cloudflare** and **Contabo Storage** to host phishing pages and exfiltrate stolen credentials to **loranto[.]com**. Key tactics included credential harvesting, exfiltration, and redirection to a fake loading page. The campaign poses significant financial, reputational, and regulatory risks to Absa Bank and its customers.

- This report is highly relevant to the organization as it highlights the need for immediate action to mitigate risks, including blocking malicious domains, notifying affected parties, and enhancing security measures like user awareness training and email filtering. It also supports compliance efforts by addressing threats to customer data.

- The biggest takeaway is the urgency to act against this phishing campaign, which targets sensitive banking information. New intelligence includes the identification of attacker infrastructure, exfiltration endpoints, and WHOIS data for yu3[.]io. The findings align with existing assumptions about phishing threats and reinforce ongoing security initiatives while highlighting potential misconfigurations that attackers may exploit.

2. Key Takeaways

This report is intended for C-Suite executives, security teams, legal/compliance teams, and Absa Bank's fraud department to address a high-risk phishing campaign. Data was collected from the phishing URL (api[.]yu3[.]io/5ctkkw), the exfiltration endpoint (loranto[.]com/wp-content/update/send_login.php), and the hosting provider (eu2.contabostorage.com).

The attacker is an unknown threat actor leveraging Cloudflare and Contabo Storage to host phishing infrastructure, targeting South African Absa Bank customers for credential theft. This report matters because it highlights a high-risk phishing campaign with potential financial losses, reputational damage, and regulatory implications for Absa Bank and its customers. The main takeaway is that immediate action is required to block malicious domains, notify affected parties, and prevent further attacks.

Key Intelligence Summary Table

Intelligence Metrics	Details
Intelligence Requirements Addressed	Identification of phishing infrastructure, TTPs, and impact assessment.
Data Sources	VirusTotal, URLscan.io, ThreatYeti, WHOIS, AbuseIPDB, BurpSuite, Shodan.
Threat Actor	Unknown threat actor leveraging Cloudflare and Contabo Storage.
Victim Location	South Africa Absa Bank customers.
Sectors	Banking and financial services.
Actor Motivation	**Cybercrime** (financial gain through credential theft).

Model Component	Details
Adversary	Unknown threat actor using phishing tactics.
Capability	Use of Cloudflare, Contabo Storage, Fake banking landing pages and exfiltration endpoints.
Infrastructure	**Domain** yu3[.]io https[:]//api[.]yu3[.]io/5ctkkw https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html loranto[.]com)

	loranto[.]com/wp-content/update/send_login.php. **IPs** 104.21.21.5 172.67.195.69.
Victim	South African Absa Bank customers.
Impact	Financial losses, reputational damage, and regulatory risks.

3. Intelligence Assessment

This phishing campaign demonstrates a **highly targeted and sophisticated approach** to stealing banking credentials, posing significant financial, reputational, and regulatory risks to Absa Bank and its customers. Therefore, we recommend the following actions:

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.
4. **Conduct user awareness training**: Educate employees and customers on identifying phishing attempts.
5. **Monitor for new campaigns**: Use threat intelligence feeds to detect similar phishing activities.

New Information

- **New Exfiltration Endpoint**: The attacker uses loranto[.]com/wp-content/update/send_login.php to exfiltrate stolen credentials.
- **Use of Cloudflare and Contabo Storage**: The attacker leverages these services to host phishing pages and mask their infrastructure.
- **Fake Login Page**: The phishing URL (api[.]yu3[.]io/5ctkkw) redirects to a fake login page hosted at https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html

Key Evidence

- **Phishing URL**: api[.]yu3[.]io/5ctkkw redirects to a fake Absa Bank login page.
- **FakeLoginPage**:Hostedat https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html.
- **Exfiltration**: Credentials are sent to loranto[.]com/wp-content/update/send_login.php.
- **Hosting Infrastructure**: Phishing pages are hosted on eu2.contabostorage.com (Contabo Storage).
- **MITRE ATT&CK Techniques**: T1192 (Spear Phishing Link), T1056 (Input Capture), T1041 (Exfiltration Over C2 Channel).

Cyber Kill Chain		
Stage	**Description**	**IOCs / TTPs**
S1: Reconnaissance	The attacker gathers information about Absa Bank and its customers to craft a convincing phishing campaign.	- Research on Absa Bank's login page design. - Identification of customer email addresses.
S2: Weaponization	The attacker creates the phishing page and exfiltration infrastructure.	- Phishing page hosted at https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html. - Exfiltration endpoint: loranto[.]com/wp-content/update/send_login.php.
S3: Delivery	The attacker delivers the phishing link to victims via email or other communication channels.	- Phishing URL: api[.]yu3[.]io/5ctkkw. - Use of Cloudflare to mask the origin server.
S4: Exploitation	The victim interacts with the phishing page, entering their credentials.	- Fake login form on https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html. - JavaScript used to capture user input.
S5: Installation	The attacker installs no malware but establishes a mechanism to collect stolen credentials.	- Exfiltration script sending credentials to loranto[.]com/wp-content/update/send_login.php.
S6: Command & Control (C2)	The attacker uses the exfiltration endpoint to receive stolen credentials.	- C2 communication over HTTPS to loranto[.]com/wp-content/update/send_login.php.
S7: Actions on Objectives	The attacker uses stolen credentials for financial gain or further attacks.	- Unauthorized access to victim accounts. - Potential financial theft or data breaches.

Attack Flow

- **Victim Visits Phishing URL:**
  - The victim accesses the phishing URL: https[:]//api[.]yu3[.]io/5ctkkw.
  - The server responds with an HTTP 302 Redirect, sending the victim to the next stage.

- **Victim Redirected to Fake Login Page:**

- The victim is redirected to the fake login page: https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html
- This page mimics Absa Bank's login page and is designed to trick the victim into entering their credentials.

- **Victim Enters Credentials**:
  - The victim enters their account number and PIN into the fake login form.
  - The credentials are submitted via a POST request to the exfiltration endpoint: https://loranto[.]com/wp-content/update/send_login.php
- **Victim Redirected to Fake Loading Page:**
  - After submitting credentials, the victim is redirected to a fake loading page (if applicable).
  - This page may use client-side redirects (e.g., JavaScript or Meta fields) to further distract the victim.
- **Access Denied Error:**
  - The victim encounters a 403 Forbidden or 421 Misdirected Request error on the fake loading page.
  - This error may indicate:
    - Misconfiguration by the attacker.
    - IP filtering to restrict access to the page.
    - A deliberate tactic to prevent further interaction with the phishing infrastructure.

VirusTotal Analysis

- **https[:]//api[.]yu3[.]io/5ctkkw**:
  - **Community Score**: > 21/96 (indicating malicious activity).
  - **Serving IP**: 173.249.62.85 (Cloudflare).
  - **Flagged**: Yes.
- **yu3[.]io**: URL Shortener
  - **Community Score**: > 13/94 (indicating suspicious activity).
  - **Cisco Umbrella:** 91812
  - **Last DNS Records:** 172.67.195.69 (Cloudflare)
  - **Flagged**: Yes.
- **eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa /index[.]html**:
  - **Community Score**: > 13/96 (indicating malicious activity).
  - **First Submission**: 2025-02-24 17:15:20 UTC
  - **Serving IP**: 173.249.62.85 (Contabo GmbH).
  - **Flagged**: Yes.

- **Loranto[.]com**:
  - **Community Score**: > 1/94 (indicating malicious activity).
  - **Serving IP**: 94.217.255.43 (Amazon Web Services).
  - **Flagged**: Yes.
- **Loranto[.]com/wp-content/update/send_login[.]php**:
  - **Community Score**: > 2/96 (indicating highly malicious activity).
  - **First Submission:** 2025-02-27 08:54:26 UTC
  - **Serving IP**: 104.21.32.41 (Cloudflare).
  - **Flagged**: Yes.

URLScan.io

- eu2.contabostorage.com
- https://loranto.com/wp-content/update/send_login.php

4. Key Intelligence Gaps

Threat Actor Identification

- **Gap**: The identity and motivation of the threat actor are unknown.
- **Action Needed**: Conduct further attribution analysis using:
    - WHOIS data for yu3[.]io and loranto[.]com.
    - Historical threat intelligence to identify similar campaigns or TTPs.
    - Collaboration with industry peers or law enforcement for additional insights.

Infrastructure Details

- **Gap**: Limited visibility into the full infrastructure used by the attacker.
- **Action Needed**: Investigate:
    - Additional domains or IPs associated with api[.]yu3[.]io, loranto[.]com, and eu2.contabostorage.com.
    - Cloudflare logs or Contabo Storage usage patterns to identify other malicious activities.

Exfiltration Endpoint Analysis

Gap: Limited understanding of the exfiltration endpoint loranto[.]com/wp-content/update/send_login.php and https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html.
Action Needed: Analyze:
    - Server logs to identify the volume of stolen credentials.
    - The destination of exfiltrated data (e.g., attacker-controlled server or third-party storage).

Victim Impact

- **Gap**: The number of affected victims and the extent of the damage are unknown.
- **Action Needed**: Collaborate with Absa Bank to:
    - Identify affected customers.
    - Assess the impact of stolen credentials (e.g., unauthorized transactions, account takeovers).

Phishing Email Analysis

- **Gap**: The delivery mechanism (e.g., phishing emails) has not been analyzed.
- **Action Needed**: Obtain and analyze:
    - Phishing email samples used to distribute the phishing URL.
    - Email headers to identify sender information and email infrastructure.

Client-Side Behavior

- **Gap**: Limited understanding of client-side behavior (e.g., JavaScript or Meta redirects).
- **Action Needed**: Perform dynamic analysis of the phishing page to:
    - Identify any client-side scripts used for redirection or data capture.
    - Determine if additional malicious behavior (e.g., malware download) is present.

Historical Context

- **Gap**: Limited historical context on similar campaigns targeting Absa Bank or other financial institutions.
- **Action Needed**: Research:
    - Previous phishing campaigns targeting Absa Bank.
    - Threat intelligence feeds for similar TTPs or infrastructure.

Mitigation Effectiveness

- **Gap**: The effectiveness of current mitigations (e.g., blocking domains, email filtering) is unknown.
- **Action Needed**: Monitor:
    - Blocked domains and IPs for signs of new activity.
    - Email filtering logs to detect bypass attempts.

Supporting Evidence

Screenshots

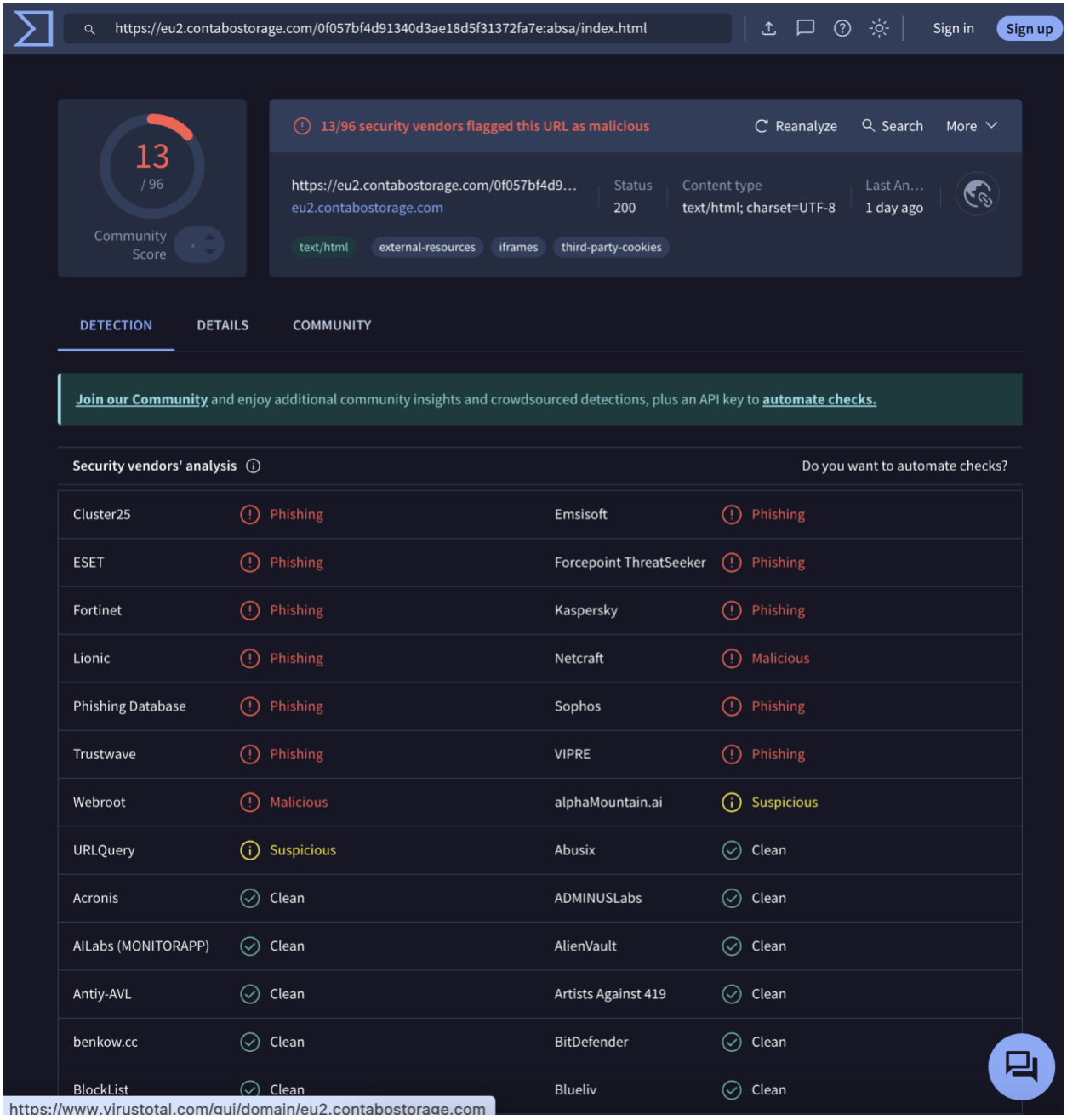

Figure 1. Virus Total (https[:]//eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html

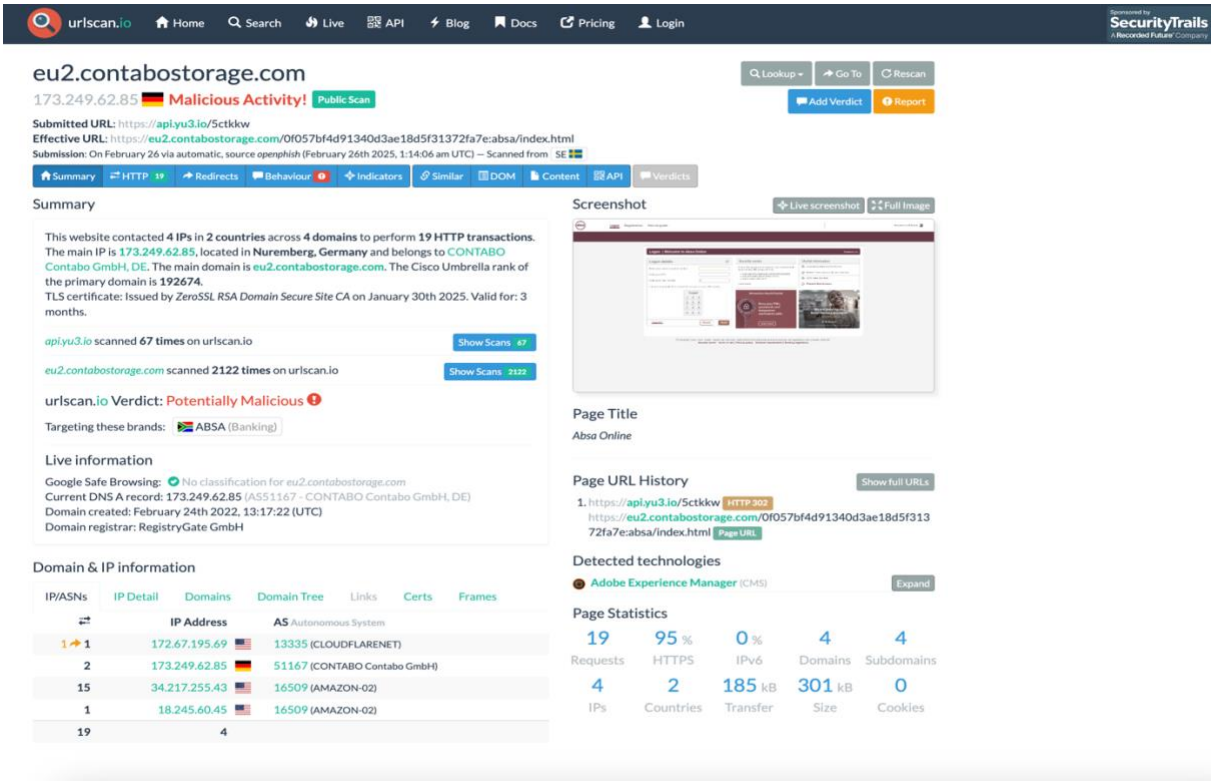

Figure 2 URLScan.io for the malicious URLs

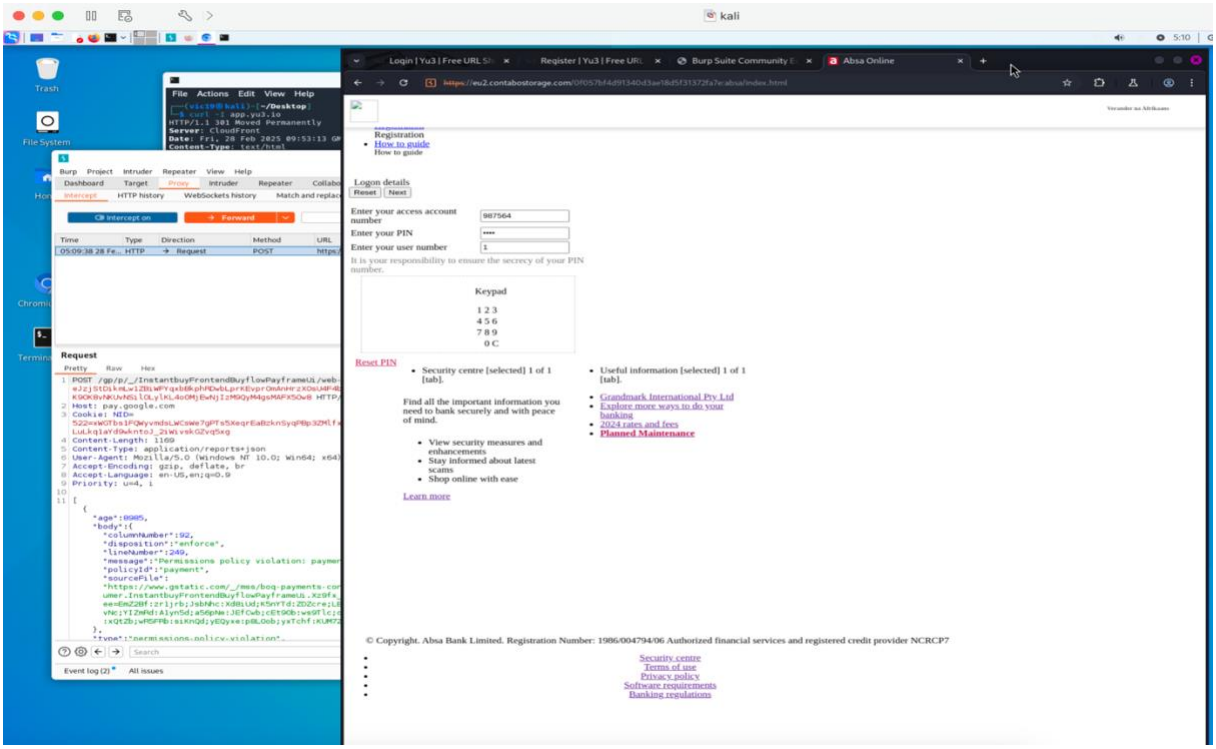

Figure 3 Fake Bank Login Page to fetch credentials

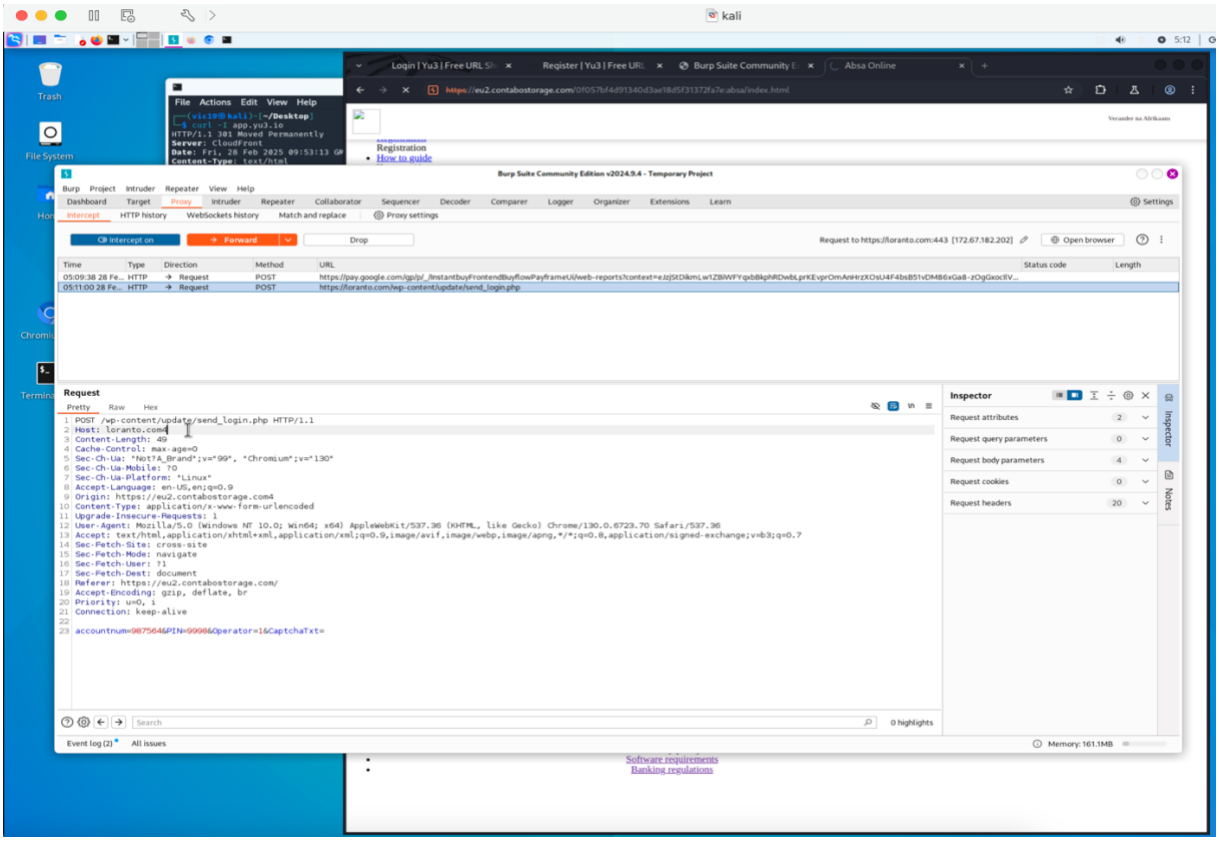

Figure 4 Credentials fetched and redirected to Lorento[.]com

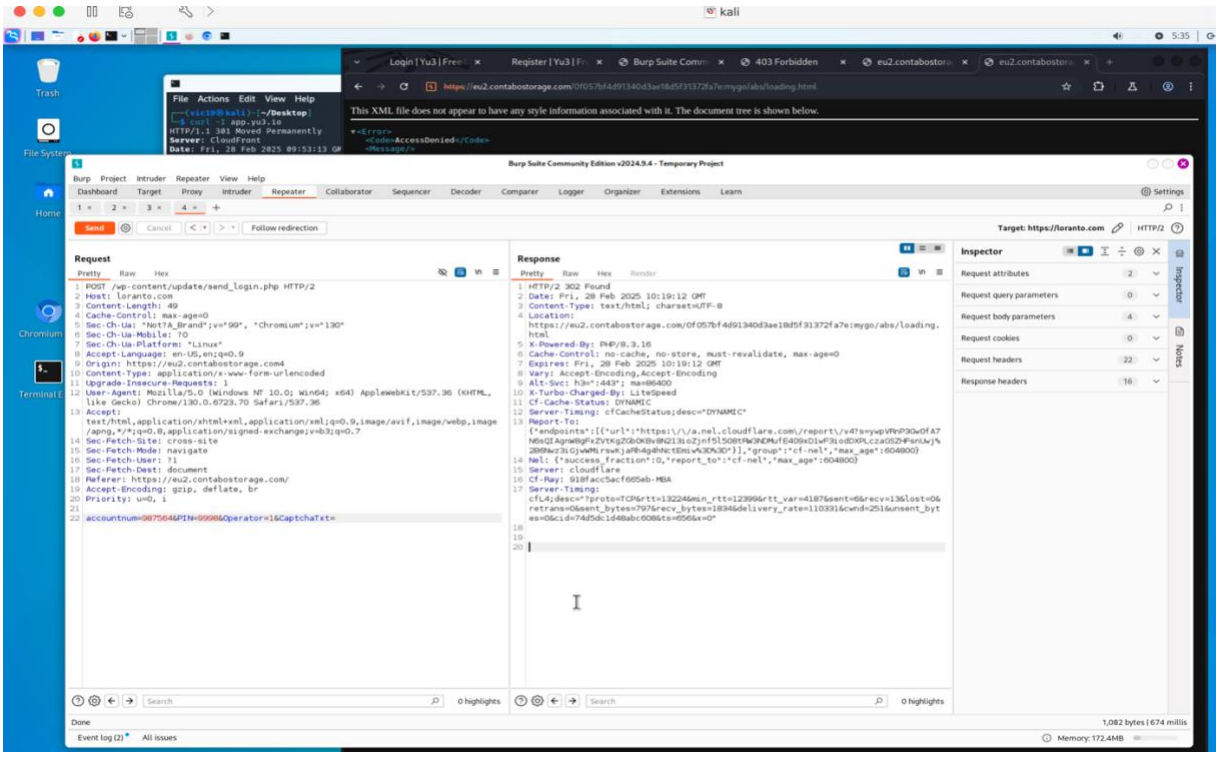

Figure 5 Credentials grabbed and user redirected to fake loading page

5. Indicators of Compromise (IOCs)

Domain/URL	Description
api[.]yu3[.]io/5ctkkw	Shortened URL that redirects to the url where the phishing page is hosted
https[:]//eu2[.]contabostorage[.]com /0f057bf4d91340d3ae18d5f31372fa7e[:]absa/index[.]html	The phishing page with the fake bank login
loranto[.]com/wp-content/update/send_login[.]php	Endpoint for exfiltrating stolen credentials.
eu2[.]contabostorage[.]com /0f057bf4d91340d3ae18d5f31372fa7e[:]mygo /abs/loading[.]html	redirected to a fake loading page

IP Address	Hosting Provider	Description
104.21.21.5	**Cloudflare**	Serving IP for api.yu3.io.
172.67.195.69	**Cloudflare**	Serving IP for api.yu3.io.
173.249.62.85	**Contabo GmbH**	Hosting provider for eu2.contabostorage.com

Common Vulnerabilities and Exposures (CVEs)

To be filled after Incident Response Team has checked the report.

CVE Number	CVSS Score	Patch Available (Y or N)	Remediation	Date Reported	Patch Applied (Y or N or N/A)

6. MITRE ATT&CK Techniques

Tactic	Technique	Procedure	Security Control
Initial Access	T1192: Spear Phishing Link	Phishing URL used to lure victims.	**D3-DFP**: Deceptive Filing (e.g., email filtering to detect phishing emails).
Execution	T1059: Command and Scripting Interpreter	JavaScript used to execute malicious actions on the phishing page.	**D3-ASA**: Application Sandboxing (isolate browser sessions to prevent malicious scripts).
Persistence	T1071: Application Layer Protocol	HTTP/HTTPS used for communication with the exfiltration endpoint.	**D3-NTA**: Network Traffic Analysis (monitor for unusual HTTP/HTTPS traffic).
Credential Access	T1056: Input Capture	Fake login form captures user credentials.	**D3-MFA**: Multi-Factor Authentication (prevent unauthorized access with stolen credentials).
Exfiltration	T1041: Exfiltration Over C2 Channel	Stolen credentials sent to the exfiltration endpoint.	**D3-DEE**: Data Loss Prevention (DLP) to block unauthorized data transfers).
Defense Evasion	T1071.001: Web Protocols	HTTPS used to encrypt communication.	**D3-TLSI**: TLS Inspection (decrypt and inspect HTTPS traffic for malicious activity).
Defense Evasion	T1090: Proxy	Cloudflare used to mask the origin server.	**D3-PA**: Proxy Avoidance (block known malicious proxy services like Cloudflare).
Resource Development	T1583: Acquire Infrastructure	Use of third-party services like Cloudflare and Contabo Storage.	**D3-RA**: Reputation Analysis (block known malicious infrastructure).
Resource Development	T1584: Compromise Infrastructure	Possible compromise of legitimate infrastructure (e.g., loranto[.]com).	**D3-CA**: Compromise Analysis (monitor for signs of compromised infrastructure).
Impact	T1531: Account Access Removal	Potential locking of victims out of their accounts.	**D3-AA**: Account Auditing (monitor for

			unauthorized account changes).
Impact	T1657: Financial Theft	Financial gain through stolen banking credentials.	**D3-FM**: Fraud Monitoring (detect and block fraudulent transactions).

7. Detection Opportunities

Rule/Query Name	Type	Description	Reference
Suspicious PowerShell Commands	Vendor-Specific Rule	Detects PowerShell commands used for downloading or executing scripts.	Microsoft Defender Advanced Hunting
HTTP POST to Malicious Domains	Vendor-Specific Rule	Detects HTTP POST requests to known malicious domains (e.g., loranto[.]com).	Splunk Search Reference
HTTP 302 Redirects to Phishing Domains	Threat Hunting Query	Identifies HTTP 302 redirects to known phishing domains (e.g., eu2.contabostorage.com).	Elastic SIEM Documentation
Processes Accessing Phishing URLs	Threat Hunting Query	Detects processes accessing known phishing URLs (e.g., api[.]yu3[.]io).	CrowdStrike Query Syntax
Phishing URL Access	Sigma Rule	Detects access to known phishing URLs.	Sigma GitHub Repository
Credential Exfiltration via HTTP POST	Sigma Rule	Detects HTTP POST requests to known credential exfiltration endpoints.	Sigma GitHub Repository
Phishing HTML Files	YARA Rule	Detects HTML files containing phishing-related keywords (e.g., "Absa Bank").	YARA Documentation
Credential Harvesting JavaScript	YARA Rule	Detects JavaScript files used for credential harvesting.	YARA Documentation

8. Appendices

Probability Matrix

Almost Impossible	Highly Unlikely	Unlikely	Possible	Likely	Highly Likely	Almost Certain
0-5%	5-25%	25-45%	45-55%	55-75%	75-85%	95-100%

Priority Matrix

Low	The threat requires regular monitoring and should be addressed when possible.
Moderate	The threat needs to be monitored closely and addressed.
High	The threat needs to be addressed quickly and monitored.
Critical	Immediate action is required.

Source and Information Reliability

Source Reliability (A-F)	
A (Completely reliable)	The source has a history of consistently providing accurate information.
B (Usually reliable)	Most of the time, the source provides accurate information.
C (Fairly reliable)	The source has provided accurate information on occasion.
D (Not usually reliable)	The source has provided accurate information infrequently.
E (Unreliable)	The source has rarely or never provided accurate information.
F (Reliability cannot be judged)	The source's reliability is unknown or untested.

Information Credibility (1-6)	
1 (Confirmed)	Other independent sources have confirmed the information.
2 (Probably true)	The information is likely true but has not been confirmed.

3 (Possibly true)	The information might be true, but it is unconfirmed.
4 (Doubtful)	The information is unlikely to be true.
5 (Improbable)	The information is very unlikely to be true.
6 (Cannot be judged)	The credibility of the information cannot be assessed.

Sensitivity Matrix

TLP:CLEAR	TLP:GREEN	TLP:AMBER	TLP:AMBER+STRICT	TLP:RED
There are no sharing restrictions. The information can be publicly shared.	Information can be shared within a community or sector to raise awareness of a threat.	Sensitive information that can be shared on a need-to-know basis within an organization or community	The information is restricted to the organization and should not be shared with its clients or trusted partners.	Highly sensitive information that should only be shared with a limited number of authorized people

Feedback Contacts

Role	Name	Title	Phone	Email
Head of CTI				
CTI Manager				
CTI Lead				
CTI Analyst (author)	Victor Mumo	CTI Analyst	+254726153461	Mumovictor77@gmail.com

Definitions and Acronyms

Key Term	Definition
Actions on Objections (AoO)	The final stage of a cyber attack is where a threat actor achieves their goals. This may include exfiltrating sensitive data, deploying ransomware, or performing espionage.
Admiralty Scale	A method used to evaluate the reliability of sources and the credibility of information in intelligence gathering. Reliability is scored from A to F, and credibility from 1 to 6.
Command and Control (C2)	The communication channel attackers aim to establish between compromised systems and their command infrastructure.
Common Vulnerabilities and Exposures (CVE)	A system and standardized naming convention used to identify and catalog publicly known cybersecurity vulnerabilities and exposures.
Cyber Kill Chain	A structured framework for understanding the different stages a cyber attack must complete to be successful.
Cyber Threat Intelligence (CTI)	The process of gathering, analyzing, and disseminating information about current or potential threats to an organization's digital infrastructure
Diamond Model	A simple framework for analyzing and understanding cyber threats. Defenders use it to organize and structure their intrusion analysis.
Estimative Language	Carefully chosen words that convey the confidence, certainty, or likelihood of an intelligence assessment’s conclusion or judgment.
Indicator of Compromise (IOC)	A piece of data or evidence that indicates a malicious activity has occurred within a network or on a computer system.
Intelligence Requirement (IR)	Specific information needs to guide the collection, analysis, and dissemination of cyber threat intelligence within an organization.
Malware	A term used to define any malicious software designed to harm, exploit, or otherwise

	compromise a computer system, network, or device (e.g., ransomware).
MITRE ATT&CK	A framework that provides a detailed and organized catalog of common tactics, techniques, and procedures (TTPs) threat actors use.
MITRE D3FEND	A framework that provides a detailed catalog of defensive security controls and mitigations against attack techniques.
Sigma Rules	A standardized format for writing and sharing detection rules for identifying suspicious or malicious activity within log data.
Tactic, Technique, Procedure (TTP)	A way to describe and categorize the behavior of adversaries to help organizations anticipate, detect, and respond to cyber threats.
Traffic Light Protocol (TLP)	A classification framework for securely sharing and handling sensitive information in the cyber security community.
YARA Rules	A standardized format for identifying and classifying malware, detecting threats, and analyzing files based on patterns and signatures.