Phishers Cast a Wider Net in the African Banking Sector

cofense.com/phishers-cast-wider-net-african-banking-sector/

Cofense

May 29, 2020

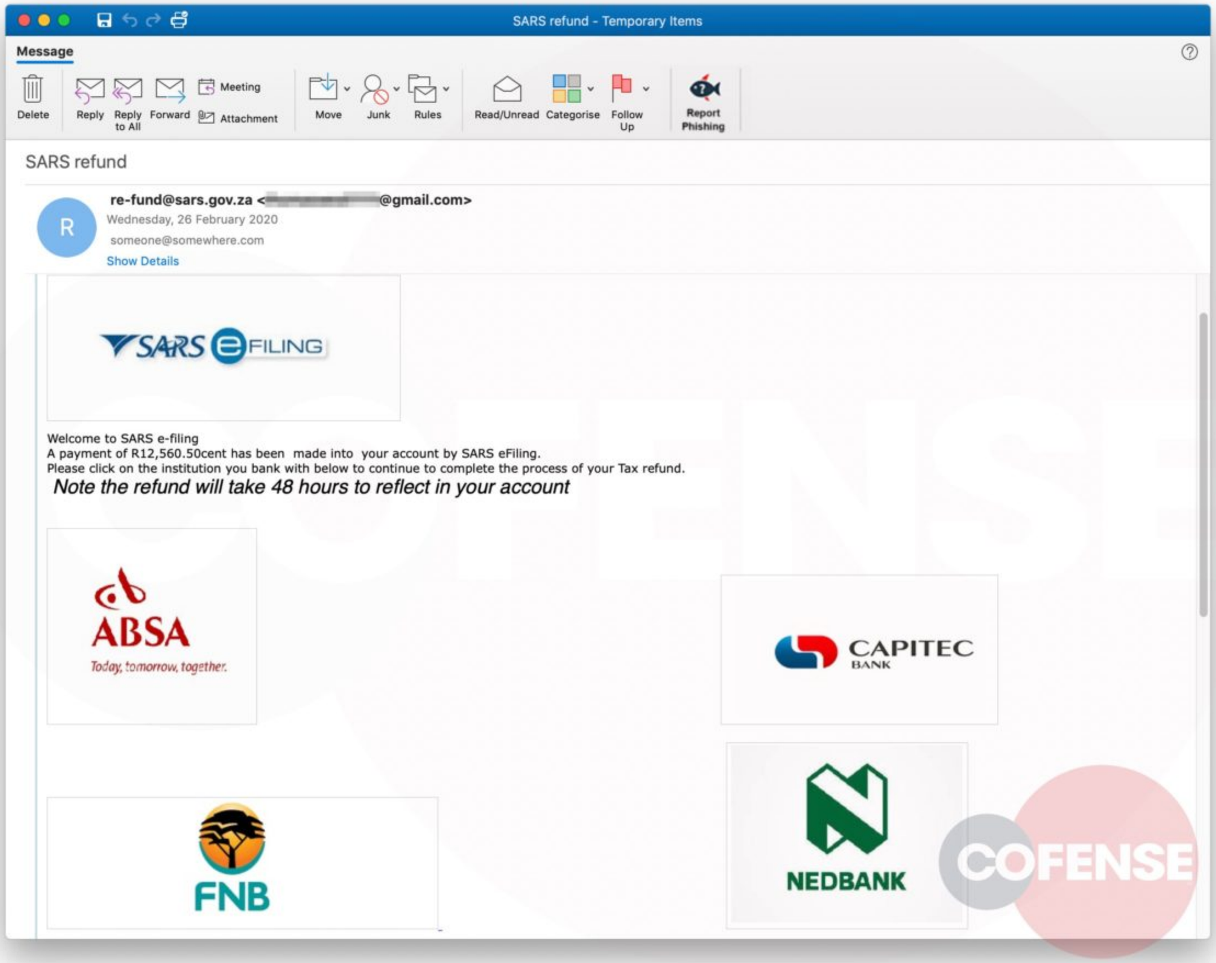
Phishes Found in Environments Protected by SEGs

Proofpoint
Microsoft 365

By Elmer Hernandez, *Cofense Phishing Defense Center (PDC)*

The Cofense Phishing Defence Center (PDC) has uncovered a wide-ranging attempt to compromise credentials from five different African financial institutions. Posing as tax collection authorities, adversaries seek to collect account numbers, user IDs, PINs and cell phone numbers from unsuspecting customers.

One such email, which was found in environments protected by Proofpoint and Microsoft, alleges to come from the South African Revenue Service's (SARS) eFiling service. It claims a tax return deposit of R12,560.5 (South African Rands), approximately $700 USD, has been made to the user's account and urges them to click on their financial institution in order to claim it. The real sender of the email, however, appears to be a personal Gmail address that may have been created or compromised by the adversaries.



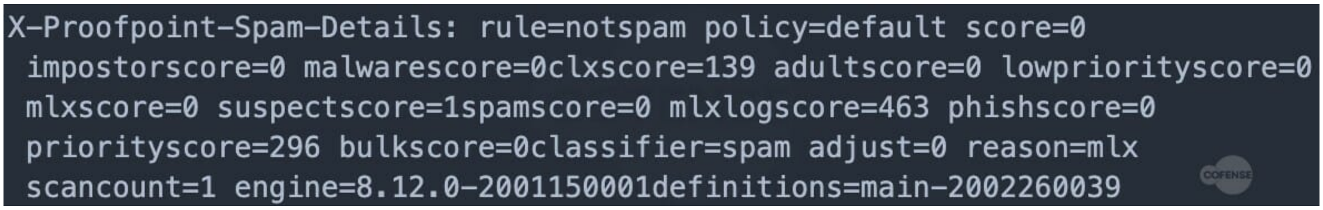
SARS refund

re-fund@sars.gov.za <[redacted]@gmail.com>
Wednesday, 26 February 2020
someone@somewhere.com
Show Details

Welcome to SARS e-filing
A payment of R12,560.50cent has been made into your account by SARS eFiling.
Please click on the institution you bank with below to continue to complete the process of your Tax refund.
Note the refund will take 48 hours to reflect in your account

Figure 1 – (Partial) Email Body

As seen in Figure 2, it is erroneously assigned a score of zero in Proofpoint's "phishscore" metric.



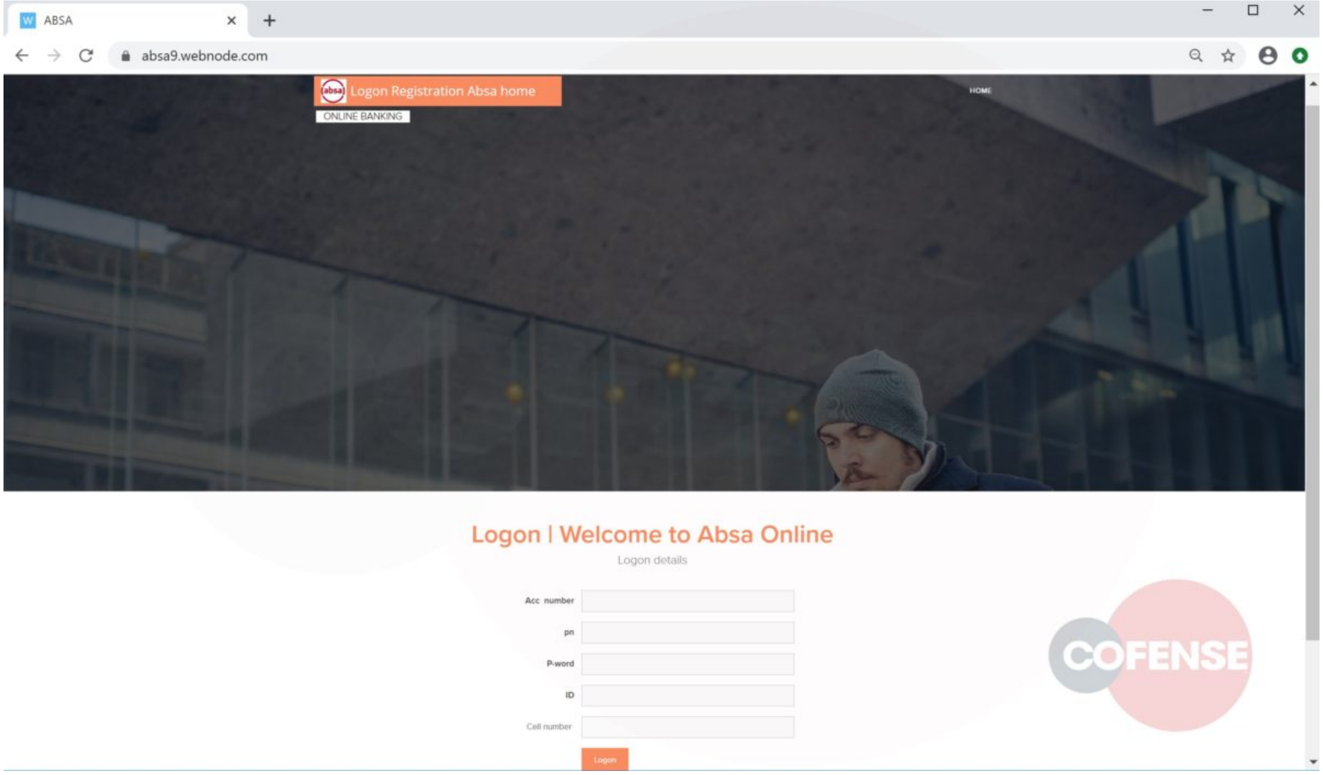
```
X-Proofpoint-Spam-Details: rule=notspam policy=default score=0
 impostorscore=0 malwarescore=0clxscore=139 adultscore=0 lowpriorityscore=0
 mlxscore=0 suspectscore=1spamscore=0 mlxlogscore=463 phishscore=0
 priorityscore=296 bulkscore=0classifier=spam adjust=0 reason=mlx
 scancount=1 engine=8.12.0-2001150001definitions=main-2002260039
```

Figure 2 – Proofpoint Header

Dragging and Dropping a Net

Each of the images embedded in the email corresponds to a different bank. Clicking on any of these will take the user to a spoofed login portal corresponding to the selected bank. The spoofed banks include ABSA, Capitec, First National Bank (FNB), Nedbank and Standard Bank, all of which are based in South Africa. The lookalike sites are located at

81[.]0[.]226[.]156 and hosted by Czech hosting provider Nethost. It should be noted that, at the time of analysis, only the site for Standard Bank was unavailable. Figures below -6 show the phishing portals imitating each bank.



Logon | Welcome to Absa Online

Logon details

Acc number

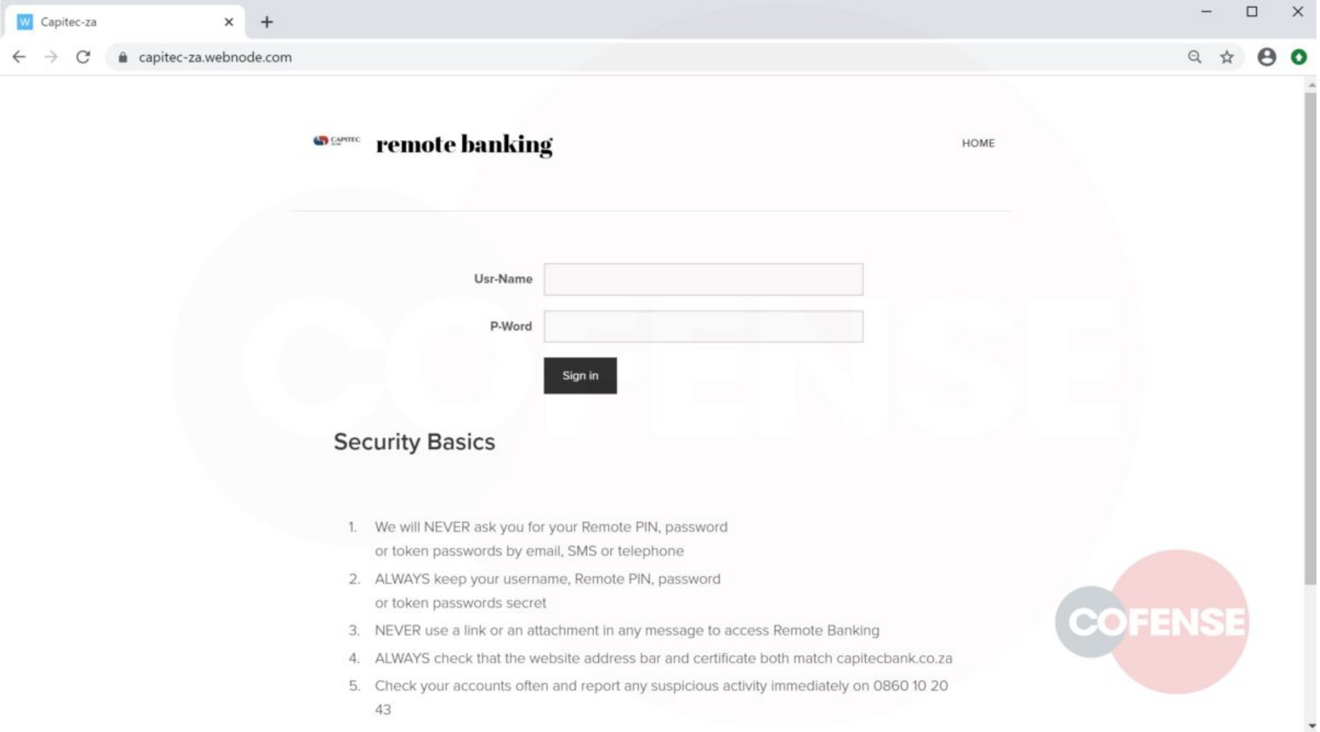
pn

P-word

ID

Cell number

Figure 3 – ABSA



Usr-Name

P-Word

Security Basics

1. We will NEVER ask you for your Remote PIN, password or token passwords by email, SMS or telephone
2. ALWAYS keep your username, Remote PIN, password or token passwords secret
3. NEVER use a link or an attachment in any message to access Remote Banking
4. ALWAYS check that the website address bar and certificate both match capitecbank.co.za
5. Check your accounts often and report any suspicious activity immediately on 0860 10 20 43

Figure 4 – Capitec

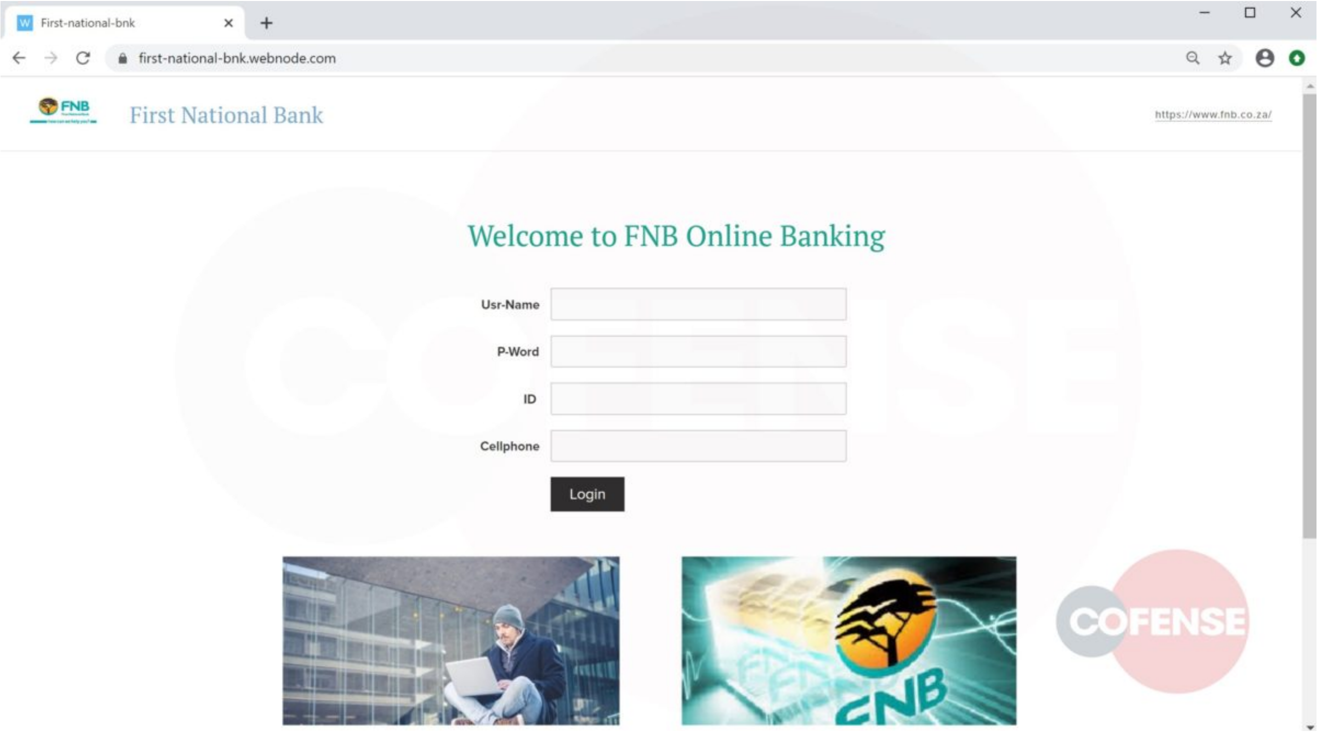


Figure 5 – FNB

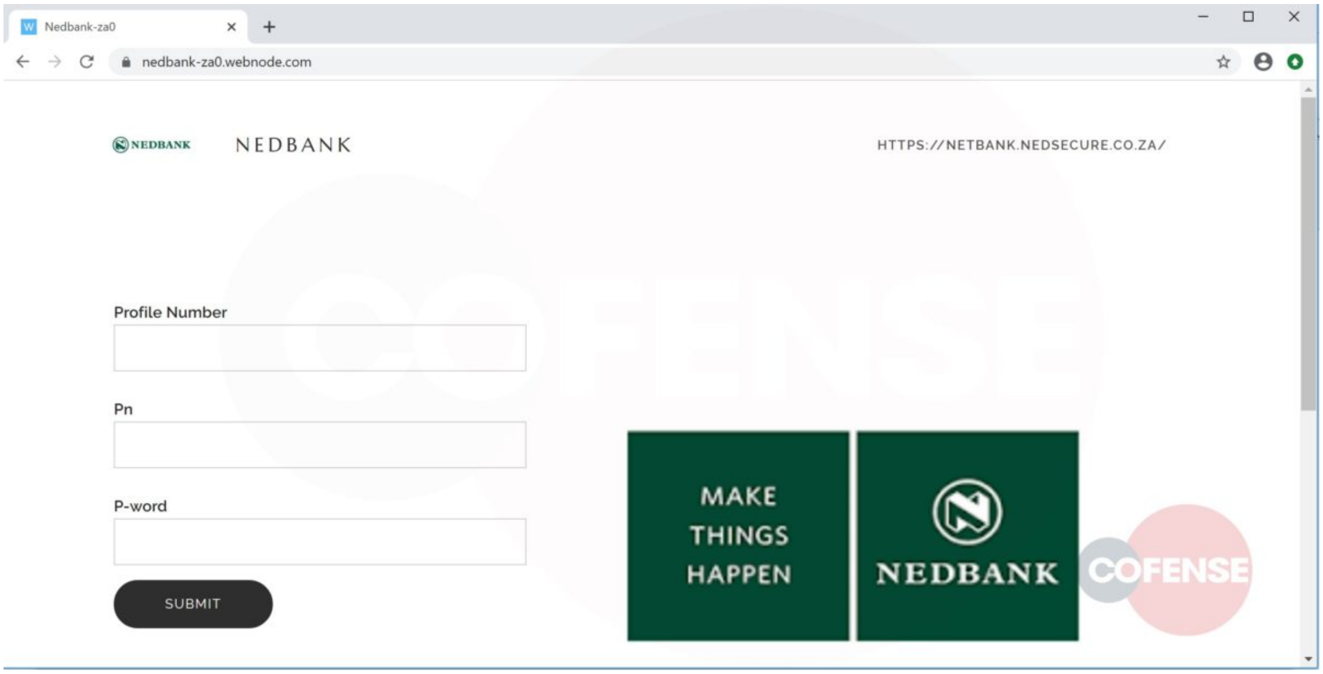


Figure 6 – Nedbank

All spoofed portals were created using Webnode, a website building service known for its friendly drag and drop features. Despite this ease of use, adversaries have kept things rather simple, as all portals are basic forms with a few or no images. The portals ask for a variety of personal information, including account numbers, passwords, PINs and even cell phone numbers.

Adversaries can access all entries directly from the form itself. They can also receive notifications to an email address of their choosing every time a submission is made; the Gmail account used to send the phishing email may also be where adversaries are notified of each and every new victim. Webnode also allows the export of form submission data in xml and csv formats.

Webnode therefore is an optimal way to store and retrieve stolen user data. There is no need for additional infrastructure, nor to compromise any third parties. As in the case of the Standard Bank portal, the risk of discovery and subsequent closure of spoofed sites means adversaries can lose access to any unretrieved information. However, this risk seems to be offset by the ease with which replacement spoofed sites can be created.

IOCs:

Malicious URLs:

- hxxps://absa9[.]webnode[.]com
- hxxps://capitec-za[.]webnode[.]com
- hxxps://first-national-bnk[.]webnode[.]com
- hxxps://nedbank-za0[.]webnode[.]com
- hxxps://standardbnk[.]webnode[.]com

Associated IPs:

81[.]0[.]226[.]156

How Cofense Can Help:

Easily consume phishing-specific threat intelligence in real time to proactively defend your organization against evolving threats with Cofense Intelligence™. Cofense Intelligence customers were already defended against these threats well before the time of this blog posting and received further information in the Active Threat Report 38237 and a YARA rule.

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats.