SOCRadar®
Your Eyes Beyond

SOUTHERN AFRICA

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

In recent years, the expansion and sophistication of cyber threats have accelerated globally, posing an ever-increasing challenge to businesses across the world. No region, including Southern Africa, is exempt from this upward trend. The SOCRadar Southern Africa Threat Landscape Report serves as a pivotal resource, offering organizations deep insights into the evolving cyber threats and identifying the unique risks pertinent to their specific locale.

Leveraging cutting-edge intelligence on the tactics of dark web threat actors, ransomware incidents, and phishing schemes, this report emerges as an indispensable tool for organizations intent on developing comprehensive security strategies. It enables them to allocate their resources more judiciously and accurately identify their critical cybersecurity needs. The meticulous inquiry into cyber incidents by SOCRadar's Cyber Threat Intelligence Analysis (CTIA) Team ensures a profound exploration of dark web threats, the employment of open-source intelligence, and detailed threat analysis.

This summary encapsulates the essence of our findings, underscoring the importance of staying ahead in a rapidly evolving cyber threat landscape. By equipping organizations in Southern Africa with the knowledge to anticipate and mitigate these threats, the SOCRadar Southern Africa Threat Landscape Report aims to fortify their cybersecurity postures significantly.

Top Takeaways

In 2023, 24 distinct threat actors were identified targeting the Southern Africa region, collectively posting 73 times on the dark web, with Public Data Exposure being the predominant type of post by 69.44%.

Additional examination reveals that Compromised User Data Sales accounted for a substantial 27.78% of all dark web posts, while Hack Announcement posts constituted a mere 2.78% of the total.

Threat actors primarily targeted the Public Administration sector, accounting for 18.37% of all incidents, making it the most vulnerable industry.

Following closely behind were the Retail Trade industry at 12.24% and the Information Technology industry at 9.18%, indicating the diverse range of industries vulnerable to cyber threats.

In 2023, the Southern Africa region experienced 93 different ransomware attacks.

The industries most affected by these ransomware attacks were primarily Manufacturing, Information Technology, and Chemical Manufacturing.

Top Ransomware Groups targeting Southern African countries were LockBit 3.0, Cl0p and ALPHV BlackCat.

In 2023, Southern Africa was targeted by a total of 26 different Ransomware Groups.

Throughout 2023, Stealer Logs facilitated the compromise of critical information from thousands of Southern African users.

The critical information compromised through Stealer Logs includes data such as user ID/Email address, password, credit card data, password hash, and victim IP Address information.

The Southern Africa Region was affected by 669 distinct instances of phishing attacks in 2023.

While the primary focus of these phishing attacks was on the Telecommunications industry; National Security & International Affairs and Cryptocurrency & NFT industries were also commonly targeted.

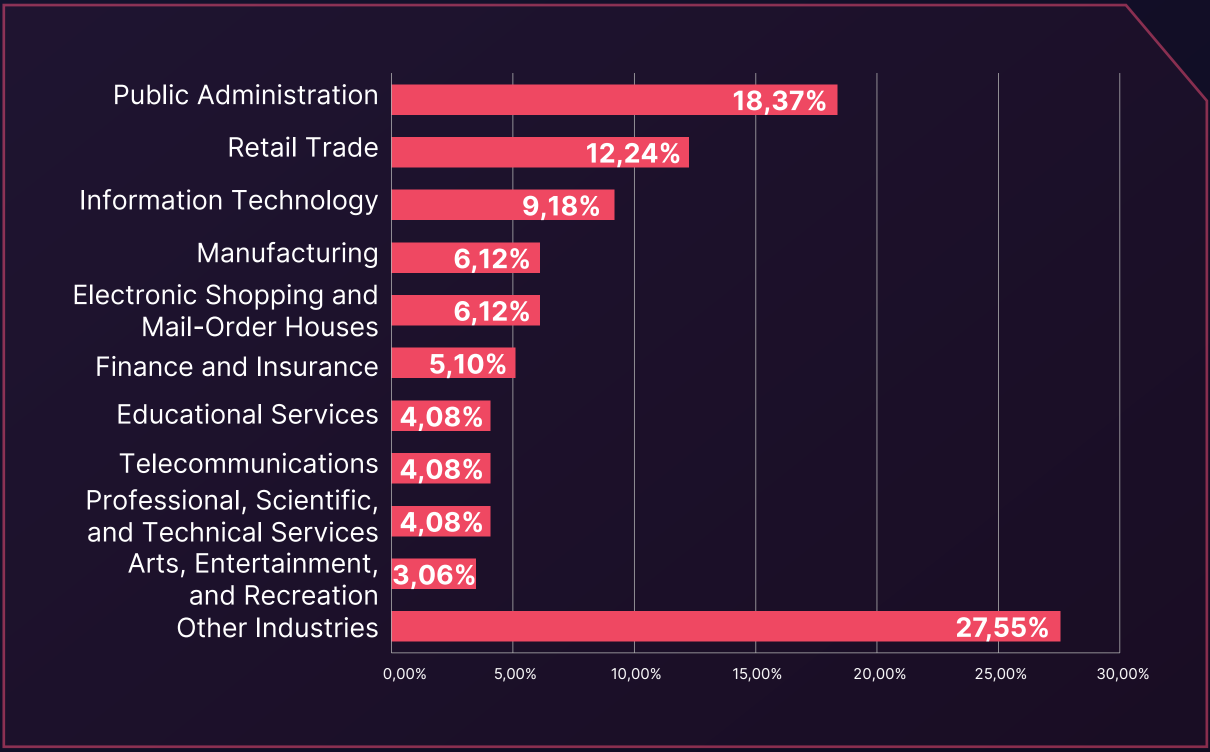
Technical Details

Dark Web Threat Statistics Targeting Industries in Southern Africa

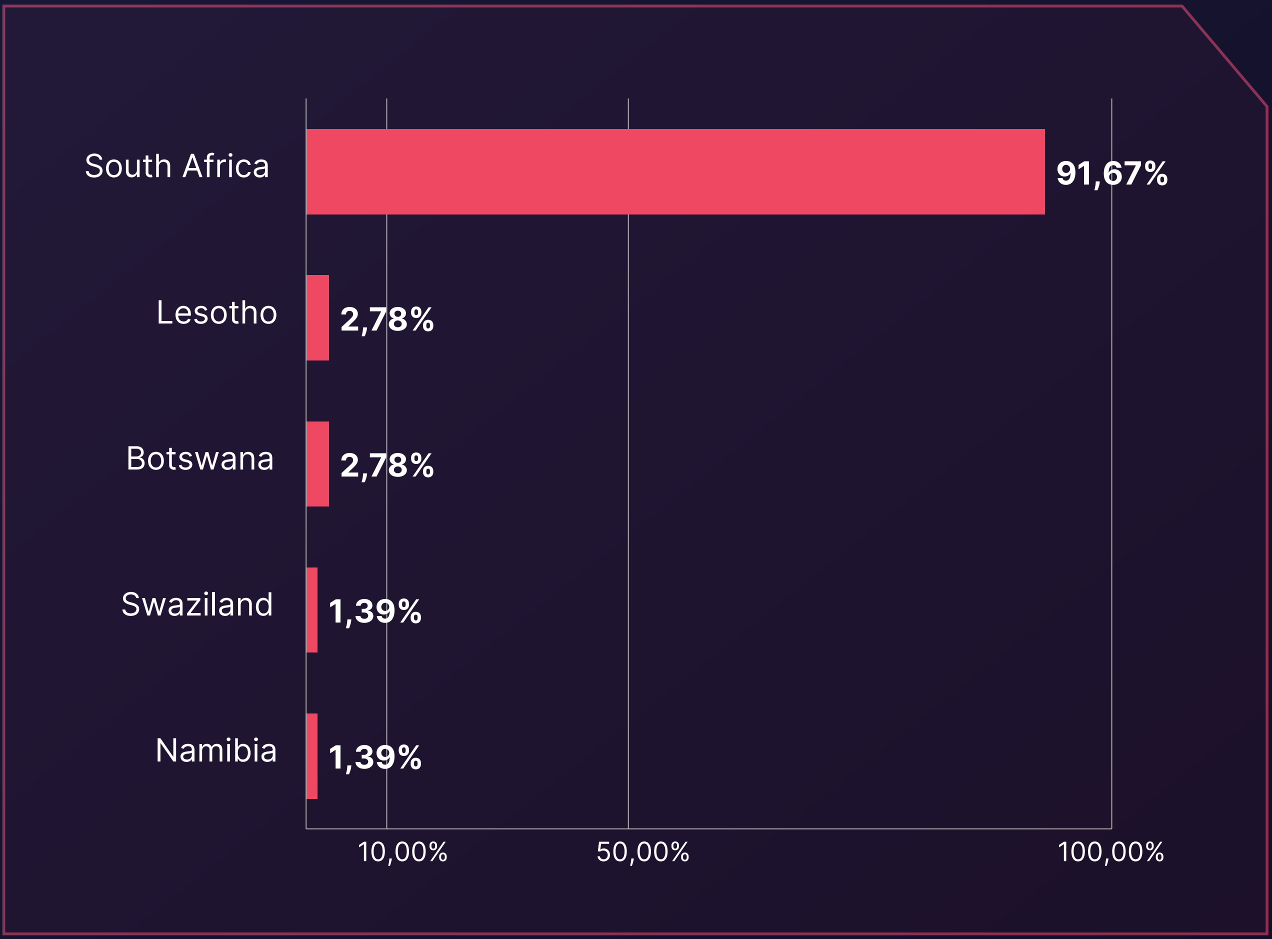
Throughout the preceding year, SOCRadar's Dark Web Analysts maintained vigilant oversight of the dark web, uncovering pivotal trends and establishing crucial links between enterprises in the Southern Africa Region and the clandestine threat actors operating within its depths. In the span of 2023, enterprises encountered an unrelenting onslaught of cyber attacks. A diverse array of threat actors sought to exploit and, on occasion, trade the gains from their successful cyber intrusions within dark web forums

During this period, SOCRadar detected 93 dark web forum posts attributed to 24 distinct threat actors. The industries most frequently targeted included Public Administration, Retail Trade and Information Technology. Public Data Exposure posts dominated the dark web threat landscape.

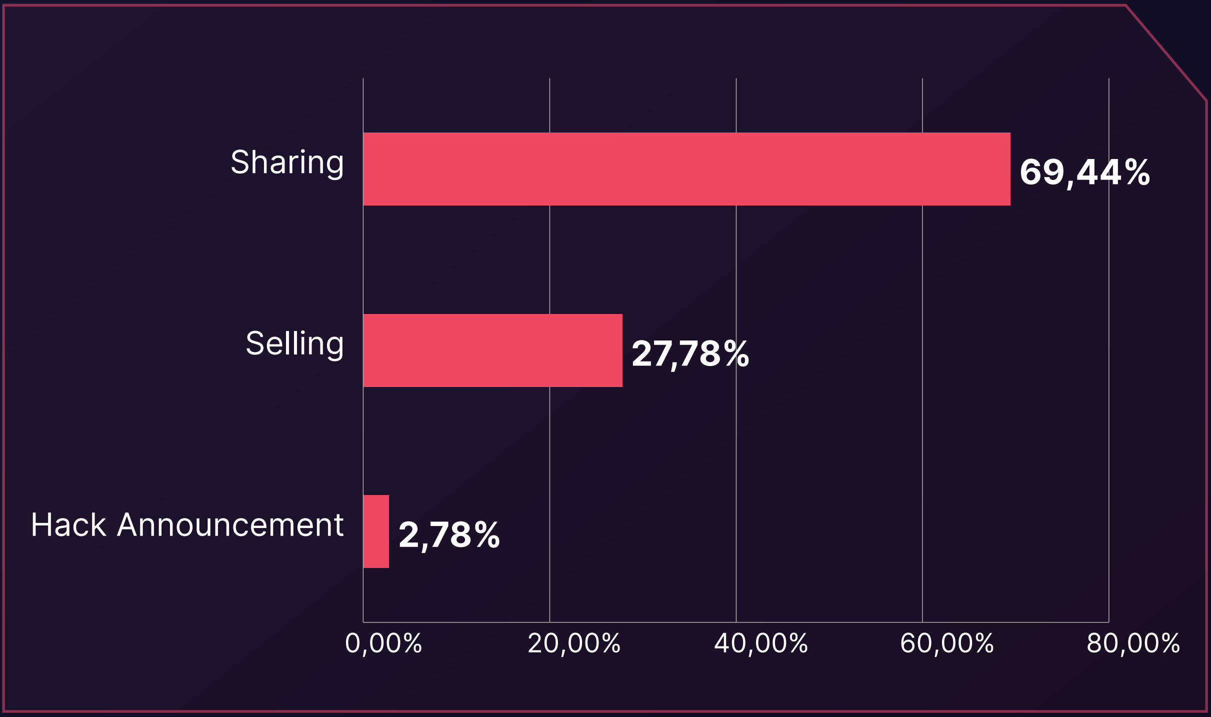
Industry Distribution of Dark Web Threats



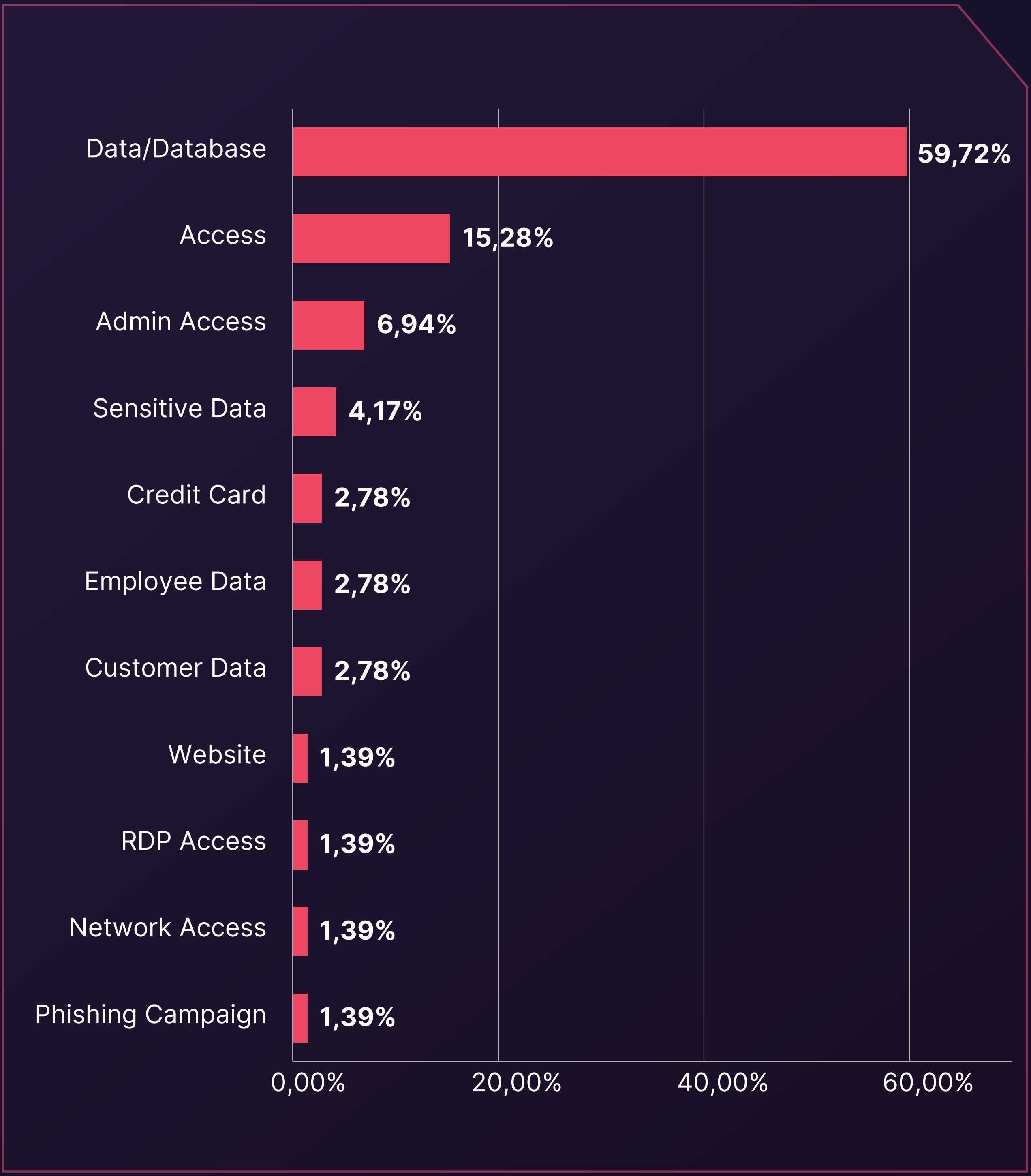
Distribution of Dark Web Threats by Country



Distribution of Dark Web Threats by Threat Categories



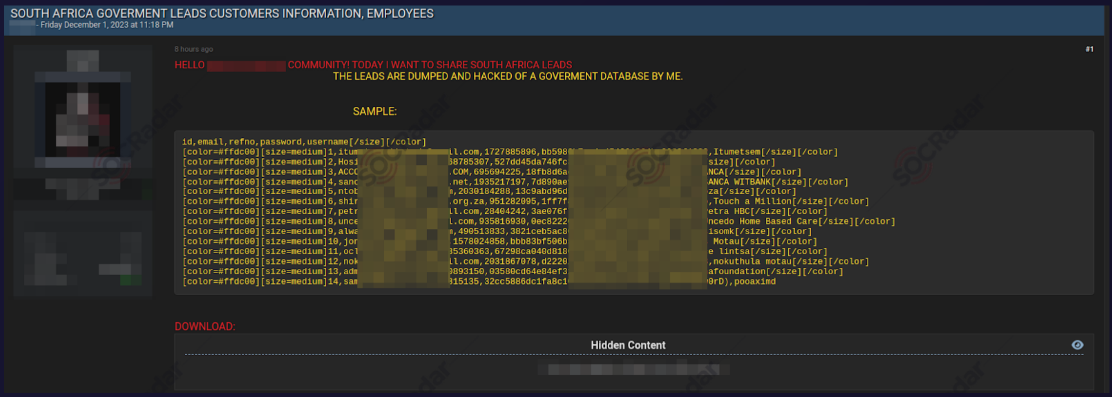
Distribution of Dark Web Threats by Threat Type



Recent Dark Web Activities Targeting Entities in the Southern Africa Region

02 Dec
2023

Data of the South African Government are Leaked



SOUTH AFRICA GOVERMENT LEADS CUSTOMERS INFORMATION, EMPLOYEES
[redacted] - Friday December 1, 2023 at 11:18 PM

8 hours ago

#1

HELLO [redacted] COMMUNITY! TODAY I WANT TO SHARE SOUTH AFRICA LEADS
THE LEADS ARE DUMPED AND HACKED OF A GOVERMENT DATABASE BY ME.

SAMPLE:

```
id,email,refno,password,username[/size][/color]
[color=#ffdc00][size=medium]1,itum[redacted]il.com,1727885896,bb598[redacted],Itumetsem[/size][/color]
[color=#ffdc00][size=medium]2,Hosi[redacted]68785307,527dd45da746fc[redacted]size][/color]
[color=#ffdc00][size=medium]3,ACCO[redacted].COM,695694225,18fb8d6a[redacted]NCA[/size][/color]
[color=#ffdc00][size=medium]4,sanc[redacted].net,1935217197,7d890ae[redacted]ANCA WITBANK[/size][/color]
[color=#ffdc00][size=medium]5,ntob[redacted]n,2030184288,13c9abd96d[redacted]za[/size][/color]
[color=#ffdc00][size=medium]6,shir[redacted].org.za,951282095,1ff7f[redacted],Touch a Million[/size][/color]
[color=#ffdc00][size=medium]7,petr[redacted]il.com,28404242,3ae076f[redacted]etra HBC[/size][/color]
[color=#ffdc00][size=medium]8,unce[redacted]l.com,935816930,0ec8222[redacted]ncedo Home Based Care[/size][/color]
[color=#ffdc00][size=medium]9,alwa[redacted]n,490513833,3821ceb5ac8[redacted]isomk[/size][/color]
[color=#ffdc00][size=medium]10,jor[redacted]1578024858,bbb83bf506b[redacted] Motau[/size][/color]
[color=#ffdc00][size=medium]11,ocl[redacted]35360363,67298ca040d818[redacted]e lintsa[/size][/color]
[color=#ffdc00][size=medium]12,nok[redacted]il.com,2031867078,d2220[redacted],nokuthula motau[/size][/color]
[color=#ffdc00][size=medium]13,adm[redacted]0893150,03580cd64e84ef3[redacted]afoundation[/size][/color]
[color=#ffdc00][size=medium]14,sam[redacted]815135,32cc5886dc1fa8c1[redacted]0rD),pooaximd
```

DOWNLOAD:

Hidden Content

[redacted]

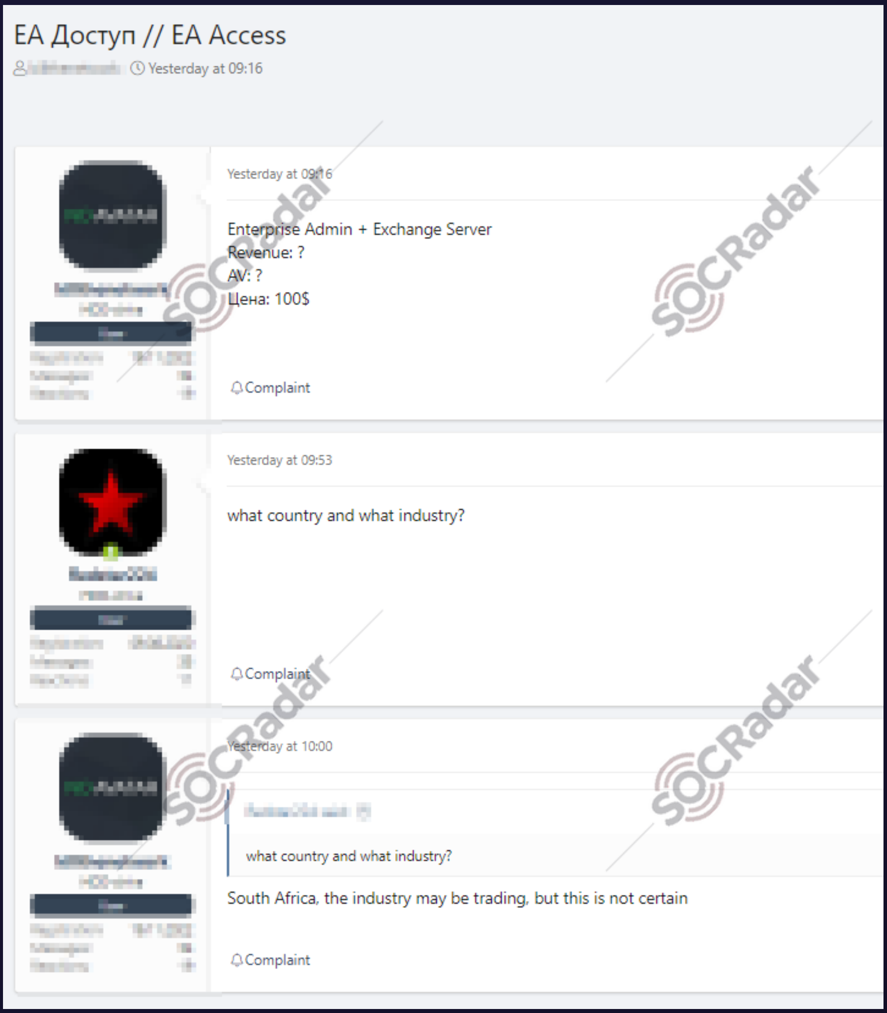
A screenshot from a dark web forum where the data is publicly exposed

In a hacker forum monitored by SOCRadar, a new alleged data leak is detected for the South African Government. The leaked data includes email addresses, reference numbers, passwords, and usernames.

The data breach is aimed directly at government employees, leaving them exposed to potential phishing attacks and other cybersecurity risks. The exposed email addresses and personal details present opportunities for identity theft, financial fraud, and various malicious activities. Such a breach not only jeopardizes the integrity of sensitive information but also poses a significant threat to the reputation of the South African government, undermining public confidence in its capacity to safeguard confidential data.

02 Dec
2023

Unauthorized Admin Access Sale is Detected for a South African Trading Platform



EA Доступ // EA Access

Yesterday at 09:16

Yesterday at 09:16

Enterprise Admin + Exchange Server
Revenue: ?
AV: ?
Цена: 100$

Complaint

Yesterday at 09:53

what country and what industry?

Complaint

Yesterday at 10:00

what country and what industry?

South Africa, the industry may be trading, but this is not certain

Complaint

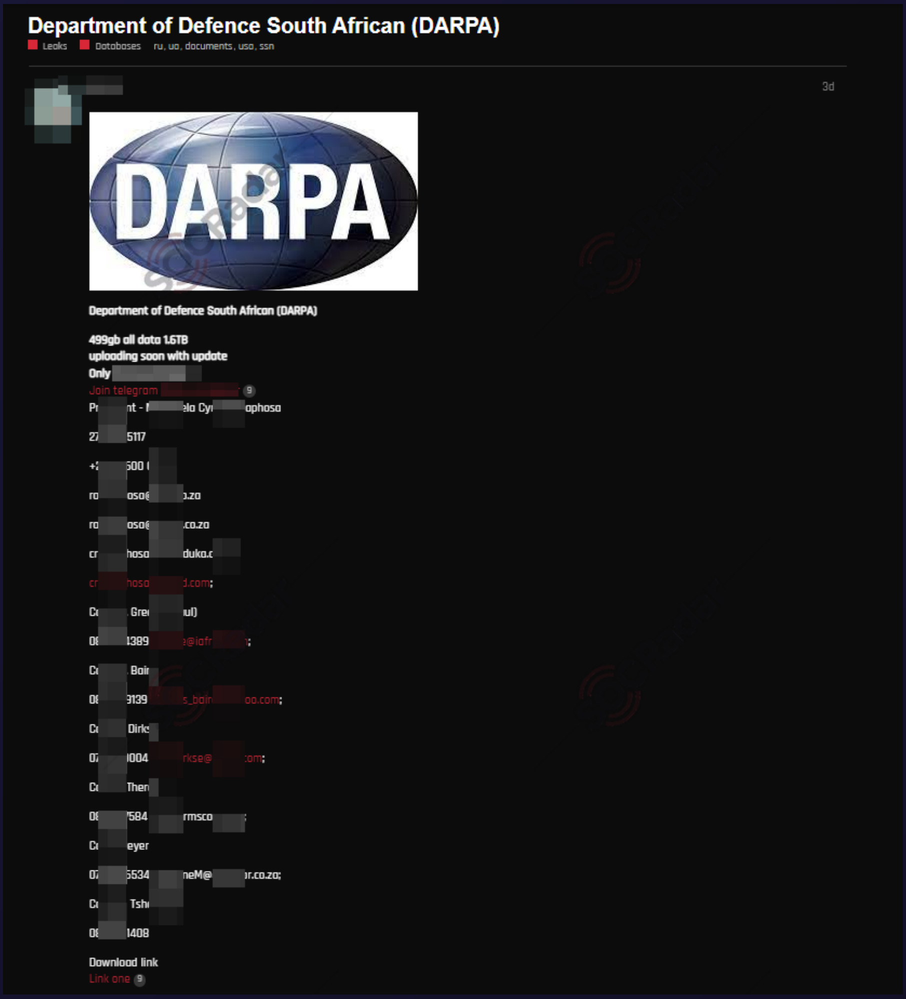
A screenshot from a dark web forum where the data is offered for sale

In a hacker forum monitored by SOCRadar, an unauthorized admin access sale is detected allegedly belonging to a trading platform that operates in South Africa. The access includes Enterprise Admin and Exchange Server privileges.

Unauthorized access to administrative accounts poses significant risks, encompassing data theft, system manipulation, and potential ransomware assaults. Given the trading industry's handling of sensitive financial data, it stands as a prime target for cybercriminal activities. Notably, Exchange Server, a widely used email platform, has historically been subjected to numerous cyberattacks. The potential sale of administrative access could signal an impending data breach or forthcoming assault on the trading platform's security infrastructure.

28 Aug
2023

Database of Department of Defence of South Africa is Leaked



Department of Defence South African (DARPA)

Leaks Databases ru, ua, documents, usa, ssn

[redacted] 3d

Department of Defence South African (DARPA)

499gb all data 1.6TB
uploading soon with update
Only [redacted]
Join telegram [redacted] 9
Pr[redacted]nt - [redacted]ela Cy[redacted]aphosa
27[redacted]5117
+[redacted]500 [redacted]
ra[redacted]osa@[redacted].za
ra[redacted]osa@[redacted].co.za
cr[redacted]hosa[redacted]duka.[redacted]
cr[redacted]hosa[redacted].com;
C[redacted] Gre[redacted]ul)
08[redacted]389[redacted]@iafr[redacted];
C[redacted] Bai[redacted]
08[redacted]3139[redacted]s_bain[redacted]oo.com;
C[redacted] Dirk[redacted]
07[redacted]004[redacted]rkse@[redacted]om;
C[redacted] Ther[redacted]
08[redacted]7584[redacted]rmsco[redacted];
C[redacted]eyer
07[redacted]5534[redacted]neM@[redacted]r.co.za;
C[redacted] Tsh[redacted]
08[redacted]1408

Download link
Link one 9

A Screenshot from a dark web forum where the data is publicly exposed

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for the Department of Defence of South Africa, containing sensitive information such as personal data, email addresses, and phone numbers of high-ranking officials.

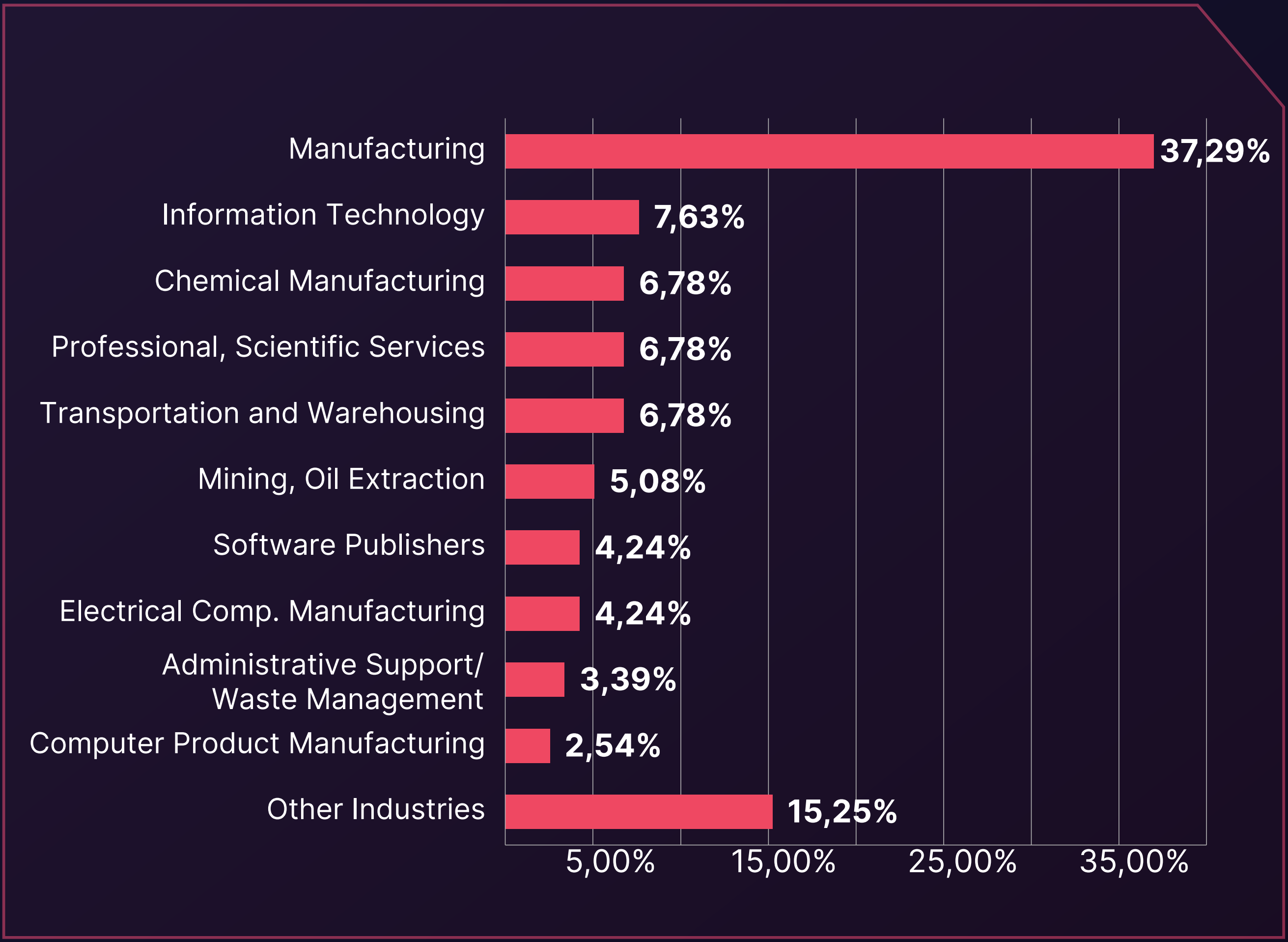
The exposure of sensitive information belonging to key figures within the South African military poses a significant risk to national security. This breach may also hint at an insider threat, indicating that an individual with authorized privileges may have accessed and extracted the data. The leaked data holds the potential for exploitation in cyber espionage activities, offering adversaries valuable insights into South Africa's defense capabilities. Consequently, this breach threatens to tarnish the reputation of the South African military and diminish public confidence in its capacity to safeguard confidential data.

Ransomware Attack Statistics Targeting Industries in Southern Africa

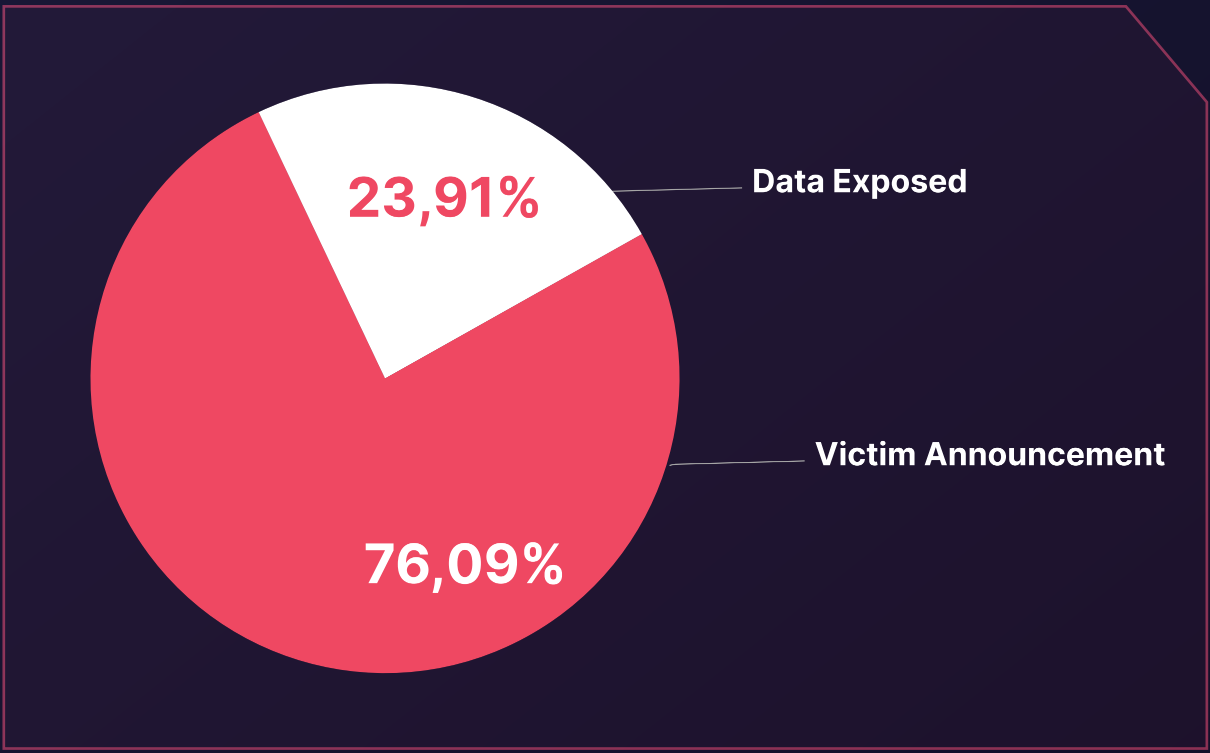
Ransomware attacks present formidable threats to organizations, frequently leading to dire outcomes including substantial data loss and the disclosure of confidential information. Through diligent monitoring, SOCRadar has pinpointed 93 cases of ransomware victim notifications linked to diverse ransomware threat actors and/or groups. Notably, South Africa stands out as the most affected country, accounting for 94.64% of these attacks.

The top three active ransomware groups targeting enterprises in the Southern Africa Region are LockBit 3.0, Cl0p and ALPHV BlackCat. These attacks predominantly target Manufacturing and Information Technology industries.

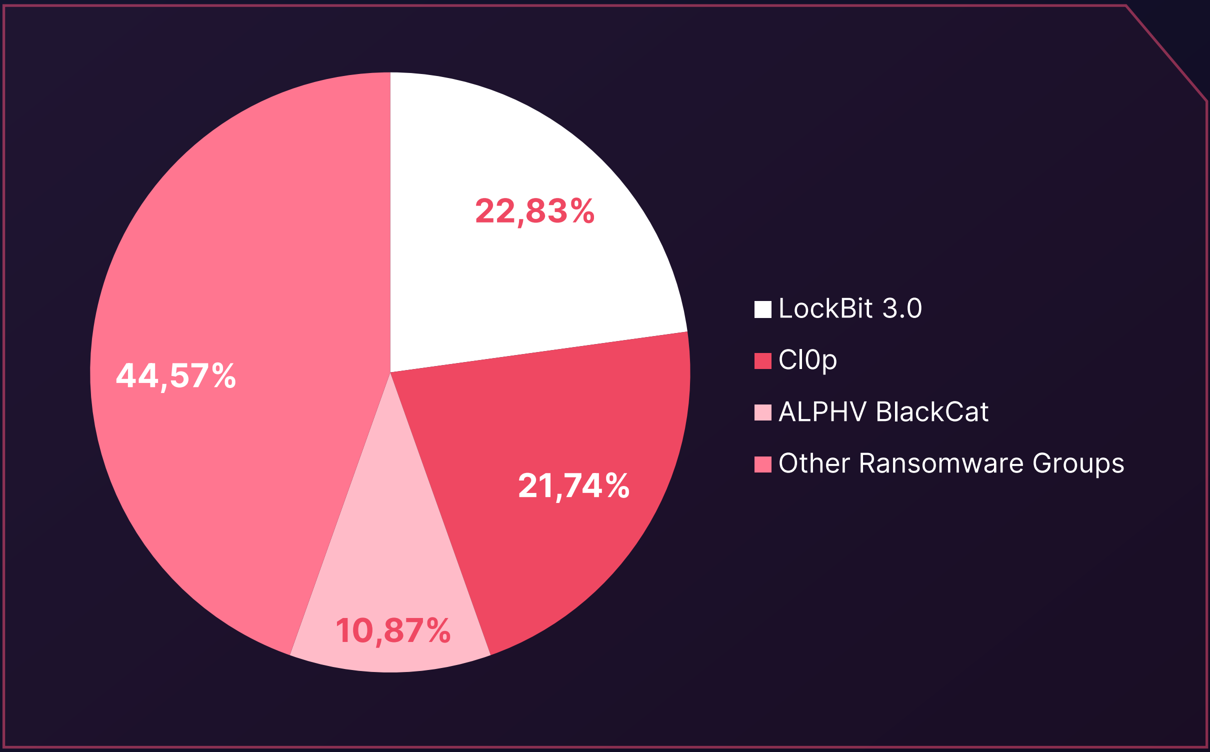
Distribution of Ransomware Attacks by Industry



Distribution of Ransomware Attacks by Share Type



Top Ransomware Groups Targeting Targeting Southern Africa



A Closer Look into The Top 3 Ransomware Groups

Lockbit 3.0 Ransomware Group

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, as well as recruiting insiders and hosting hacker recruitment contests. With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

For more detailed information about the Lockbit 3.0 Ransomware Group, you can visit our blog post.

Cl0p Ransomware Group

Cl0p

Country of Origin: Russia

A Ransomware group that has been active since 2019 and currently brings up its name by exploiting zero-day vulnerabilities that existed in GoAnyWhere MFT and MOVEit MFT software.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	The US, Canada, The UK, Australia, Colombia, Sweden, Germany, India, Mexico, Turkey
Target Sectors:	IT, Healthcare, Finance, Professional Services, Retail, Media, Telecommunication
Attack Type:	Spearphishing, Zero-Day Exploitation, Compromised RDP, Ransomware, Data exfiltration, Double-extortion

-TTPs-

Exploit Public-Facing Application:	T1190
Exploitation for Privilege Escalation:	T1068
Exfiltration Over C2 Channel:	T1041

Clop, also referred to as "Cl0p," stands as a cybercriminal entity recognized for its sophisticated extortion tactics and widespread dissemination of malware across the globe. The word clop comes from the Russian word “klop,” which means “bed bug,” a Cimex-like insect that feeds on human blood at night (mosquito). A distinguishing feature of CLOP is the string “Don’t Worry C|0P” found in the ransom notes.

With a track record of extorting over $500 million in ransom payments, the group focuses on major organizations on a global scale. Gaining infamy in 2019, Clop has executed notable attacks, employing extensive phishing initiatives and advanced malware to breach networks and coerce ransom payments, leveraging the threat of data exposure if demands remain unmet.

For more detailed information about the Cl0p Ransomware Group, you can visit our blog post.

ALPHV BlackCat Ransomware Group

BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

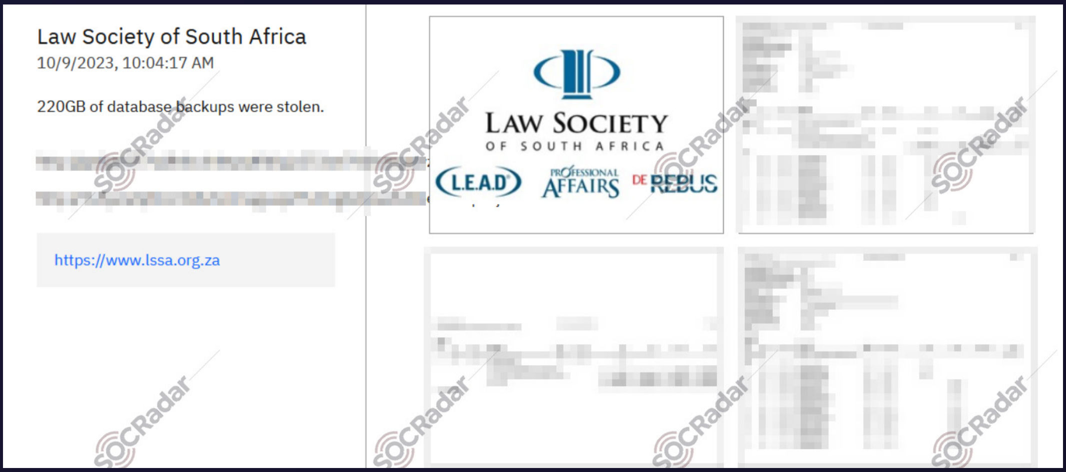
BlackCat, or ALPHV, is a ransomware group known for being the first to use Rust -a cross-platform language programming language that allows for easy malware customization for different operating systems, such as Windows and Linux- successfully. The group has been able to evade detection and successfully encrypt their victims' files by using Rust, which allows them to target multiple operating systems and bypass security controls that are not designed to analyze malware written in Rust.

For more detailed information about the ALPHV BlackCat Ransomware Group, you can visit our blog post.

Recent Ransomware Attacks Targeting Entities in Southern Africa

09 Oct
2023

ALPHV BlackCat Ransomware Group Leaked The Data of Law Society of South Africa



Law Society of South Africa
10/9/2023, 10:04:17 AM

220GB of database backups were stolen.

https://www.lssa.org.za

Screenshot of the threat actor share

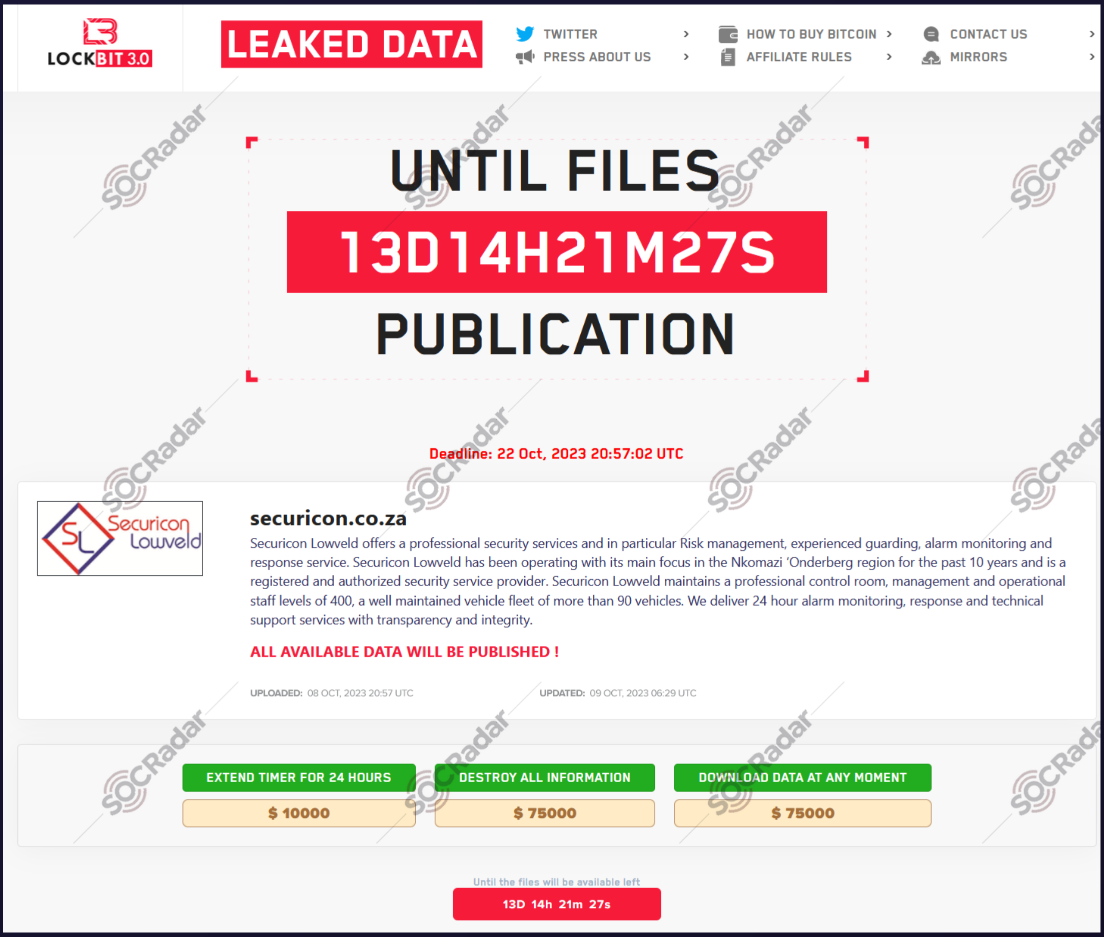
In the ALPHV / BlackCat ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Law Society of South Africa, including 200GBs of database backups.

The Law Society of South Africa is an attractive target for cybercriminals due to its possession of sensitive information concerning its members and clients. The leaked data presents opportunities for cybercriminals to launch phishing attacks, commit identity theft, or engage in other forms of cybercrime targeting the Law Society's stakeholders.

This incident underscores the critical need for organizations to prioritize data protection measures against ransomware attacks. Such measures include the implementation of robust cybersecurity protocols and the establishment of comprehensive data backup and recovery strategies.

09 Oct
2023

The New Ransomware Victim of Lockbit 3.0: Securicon Lowveld



Deadline: 22 Oct, 2023 20:57:02 UTC

securicon.co.za

Securicon Lowveld offers a professional security services and in particular Risk management, experienced guarding, alarm monitoring and response service. Securicon Lowveld has been operating with its main focus in the Nkomazi 'Onderberg region for the past 10 years and is a registered and authorized security service provider. Securicon Lowveld maintains a professional control room, management and operational staff levels of 400, a well maintained vehicle fleet of more than 90 vehicles. We deliver 24 hour alarm monitoring, response and technical support services with transparency and integrity.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 08 OCT, 2023 20:57 UTC
UPDATED: 09 OCT, 2023 06:29 UTC

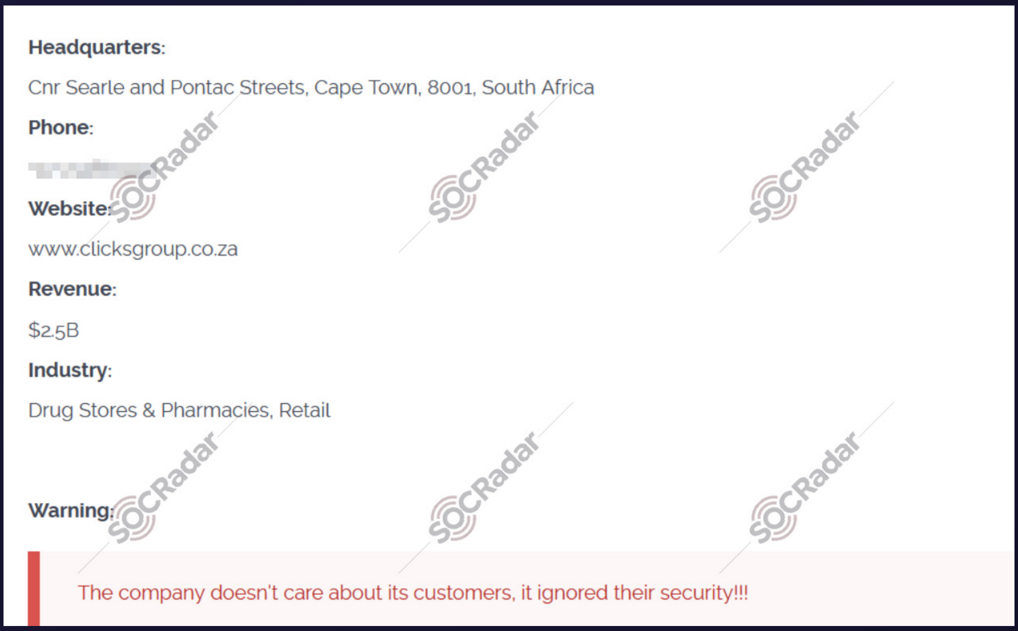
Screenshot of the threat actor share

In the Lockbit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Securicon Lowveld. The group has published the victim's data on its website and is demanding a ransom payment.

The emergence of Lockbit 3.0 underscores the escalating danger posed by ransomware attacks, exemplified by this recent incident. Security firms frequently find themselves in the crosshairs of ransomware groups owing to the sensitive nature of the data under their purview. Such attacks can culminate in the compromise of critical customer and employee data, precipitating reputational damage and eroding trust in the affected entity. Moreover, ransomware attacks exact a heavy toll on victims, encompassing ransom payments, operational downtime, and the financial burdens associated with recovery efforts.

29 Jun
2023

The New Ransomware Victim of Cl0p: Clicks Group



Headquarters:

Cnr Searle and Pontac Streets, Cape Town, 8001, South Africa

Phone:

[redacted]

Website:

www.clicksgroup.co.za

Revenue:

$2.5B

Industry:

Drug Stores & Pharmacies, Retail

Warning:

The company doesn't care about its customers, it ignored their security!!!

Screenshot of the threat actor share and claims

In the Cl0p ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Clicks Group, a South African retail and pharmacy chain.

Cl0p, a notorious ransomware group with a history of targeting multiple organizations, has once again brought attention to the persistent menace of ransomware attacks, particularly when directed at high-profile entities.

These attacks frequently entail data exfiltration, potentially compromising sensitive customer information. Such ransomware incidents risk tarnishing an organization's reputation, undermining customer confidence and often resulting in significant financial repercussions. As stated in the threat actor share concerning Clicks Group, allegations of negligence regarding customer security could further exacerbate reputational damage.

Stealer Log Statistics Top Domains in the Southern Africa Region

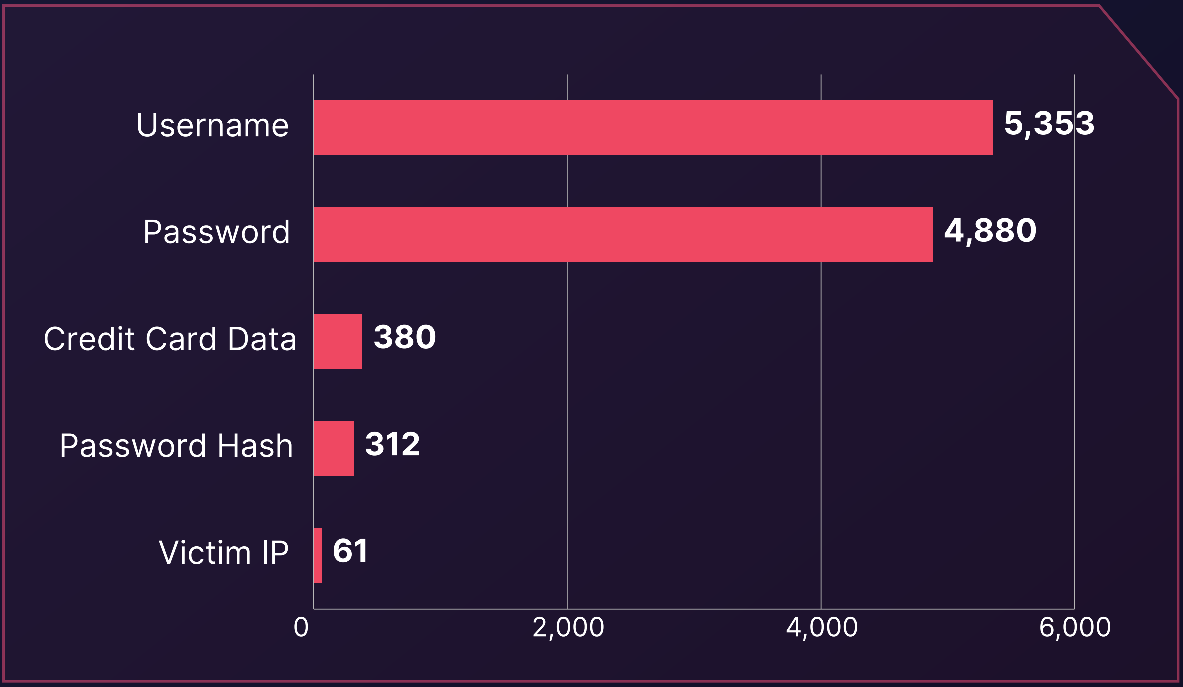
Throughout 2023, thousands of usernames, passwords, credit card data, password hash, and victim IP address information were compromised via Stealer Logs from some of the highest traffic domains in Southern Africa.

The table below lists the domains associated with Southern Africa that have the highest traffic.

- betway.co.za
- iol.co.za
- ourpower.co.za
- dailymaverick.co.za
- fnb.co.za
- unisa.ac.za
- playabets.co.za
- thefuse.co.za
- mtn.co.za
- citizen.co.za
- businesstech.co.za
- autotrader.co.za
- timeslive.co.za
- maroelamedia.co.za

The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with the Southern Africa Region.

Stealer Logs - Distribution of the Compromised Data



The data unveils a notable dissemination of compromised information, encompassing 5,353 usernames, 4,880 passwords, 380 credit card data, 312 password hashes and 61 compromised victim IPs, each signifying distinct instances of breach.

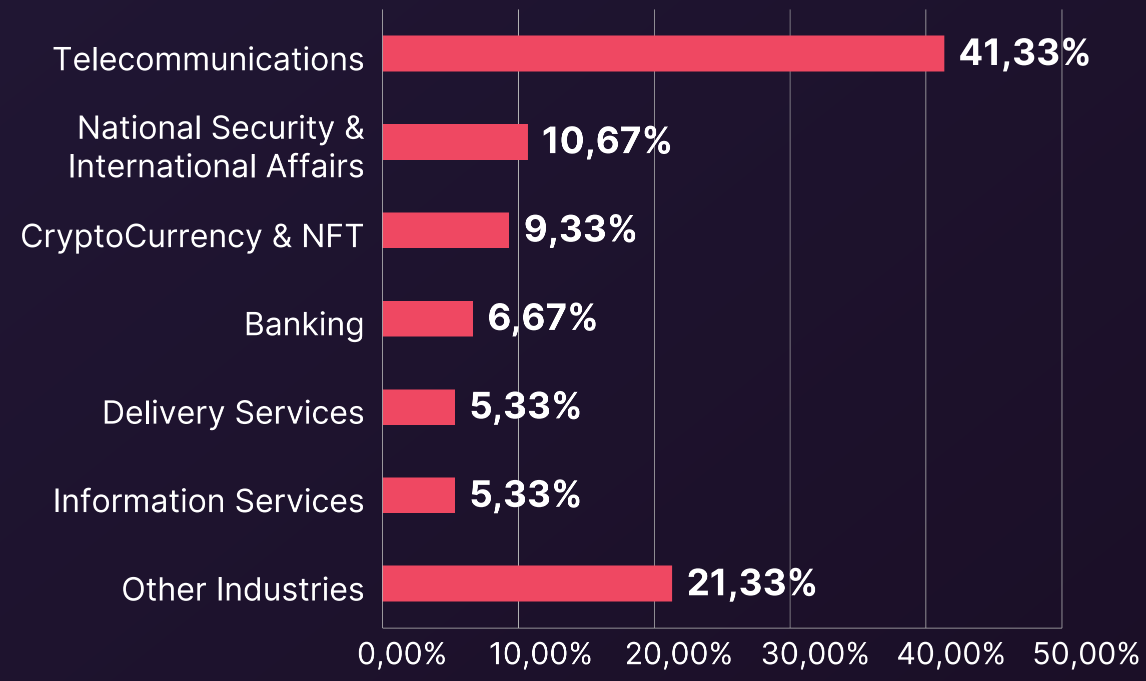
These discoveries emphasize the gravity of data compromise occurrences impacting users in the digital sphere of the Southern Africa Region, emphasizing the urgent necessity for strong cybersecurity protocols to efficiently alleviate such risks.

Phishing Threats Targeting Southern Africa

Phishing is an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

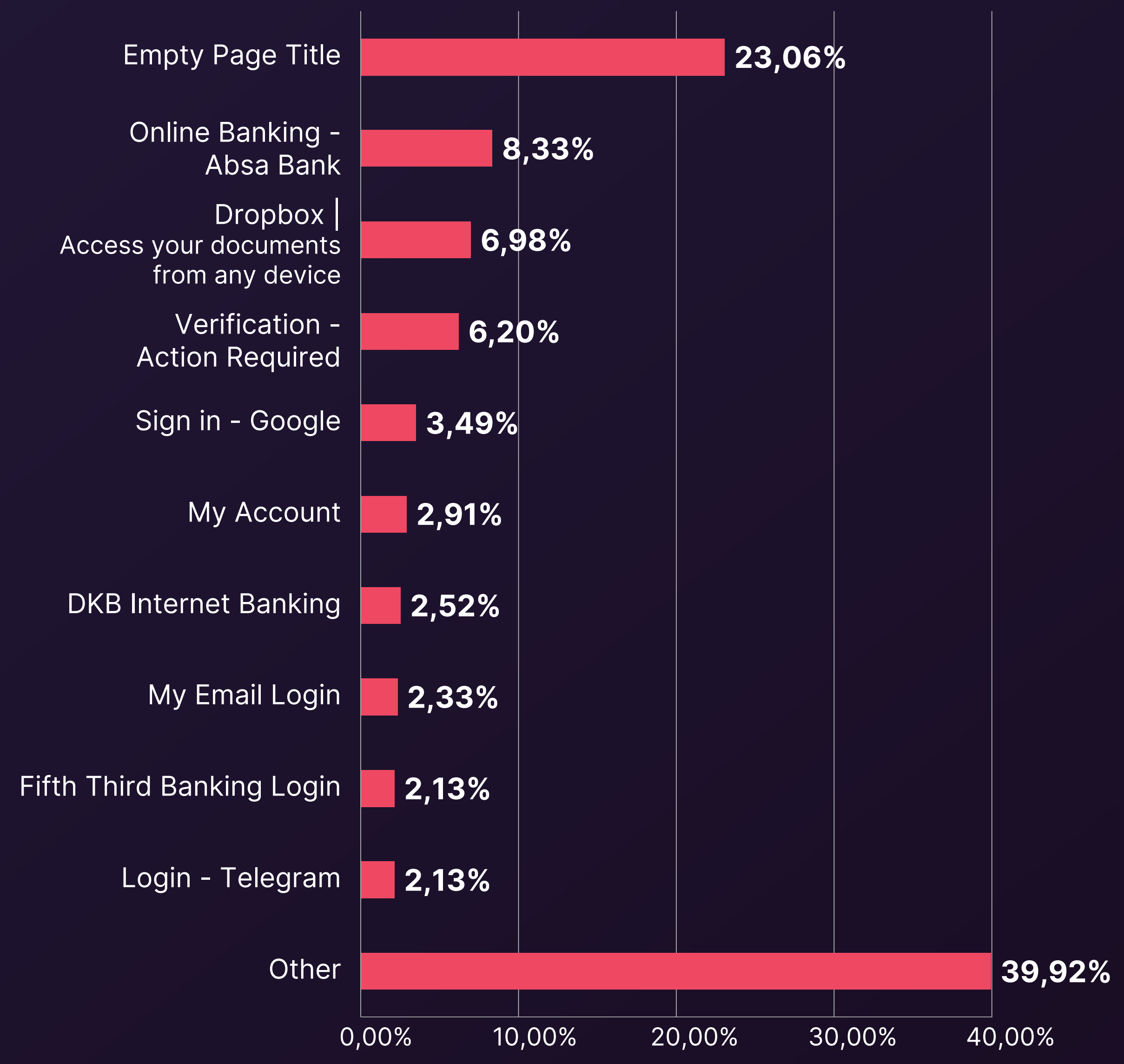
Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, enterprises in the Southern Africa Region encountered 669 distinct instances of phishing attacks, primarily targeting the Telecommunications industry.

Phishing Attacks - Distribution by Industry



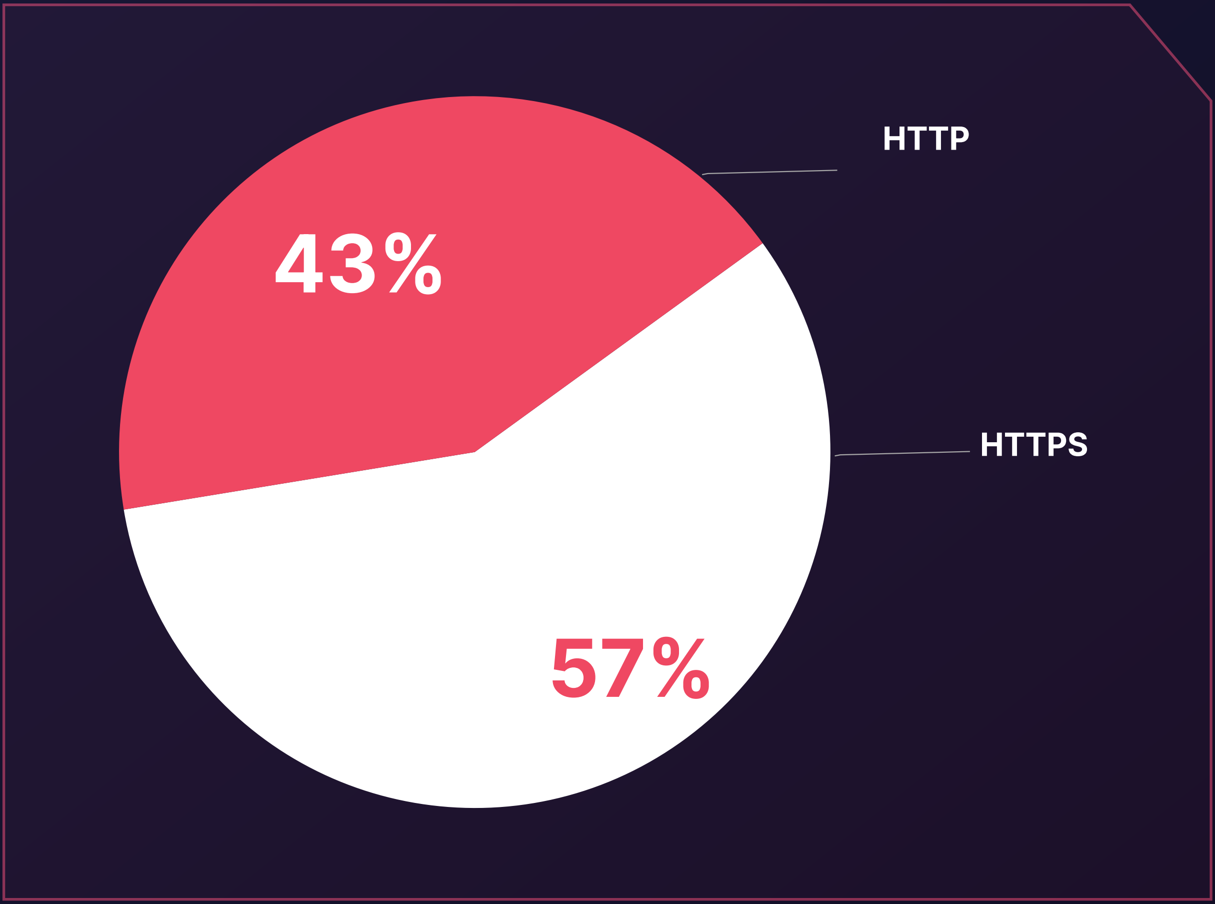
As cyber threats continue to escalate throughout the Southern Africa Region, phishing attacks have become increasingly prevalent, posing substantial risks to businesses and individuals alike. In light of this escalating threat landscape, the graph below provides insight into the page titles of phishing pages meticulously crafted to target entities within the region, shedding light on the evolving tactics employed by malicious actors.

Phishing Attacks - Distribution by Phishing Page Title



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

Phishing Attacks- Distribution by SSL/TLS Protocol



Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in the Southern Africa Region, several pivotal lessons and recommendations emerge. These insights, coupled with the capabilities of SOCRadar, offer a roadmap for enhancing cyber resilience and preserving operational integrity. The following are the top 5 takeaways from our analysis:

Maintain vigilance regarding the evolving cyber threat landscape:

It's evident that the cyber threat landscape is dynamically evolving, as evidenced by the surge in dark web activity related to the Southern Africa Region and the proliferation of ransomware incidents. Organizations must stay abreast of these developments and adapt their security strategies accordingly. Leveraging SOCRadar's Cyber Threat Intelligence provides businesses with real-time insights into emerging threats, enabling them to stay ahead of cyber adversaries.

Emphasize multi-layered security measures:

The diverse range of industries targeted by cyber threats underscores the necessity for multi-layered security measures. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all industries, from Information Technology to Public Administration. SOCRadar can support this effort through proactive threat intelligence and monitoring services.

Maintain vigilance against ransomware:

Ransomware remains a significant threat, highlighting the importance of robust defenses and response plans. SOCRadar's threat intelligence capabilities enable businesses to identify potential ransomware threats and develop effective response strategies.

Educate and train employees:

Given the persistent threat of phishing attacks, continuous education and training for employees are essential. Familiarity with phishing tactics and detection methods is critical. SOCRadar's solutions can assist in this regard by identifying potential phishing domains and raising awareness of the latest phishing techniques.

Ensure defense against Stealers:

With the Southern Africa Region being a primary target country for Stealer malware infections, organizations must enhance their defenses against these malicious software. SOCRadar's advanced threat intelligence aids in detecting and mitigating Stealer threats, bolstering the overall security posture of the organization.

In conclusion, adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, organizations in Southern Africa can fortify their defenses and effectively navigate the evolving cyber threat landscape.

Who is SOCRadar® ?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

21.000+
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

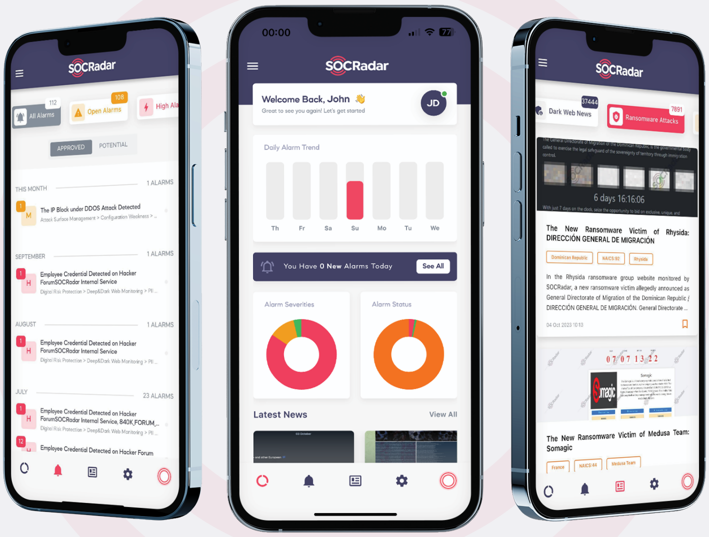
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



GET IT ON Google Play

Gartner Peer Insights™ Customer First

4.8/5 ★★★★★