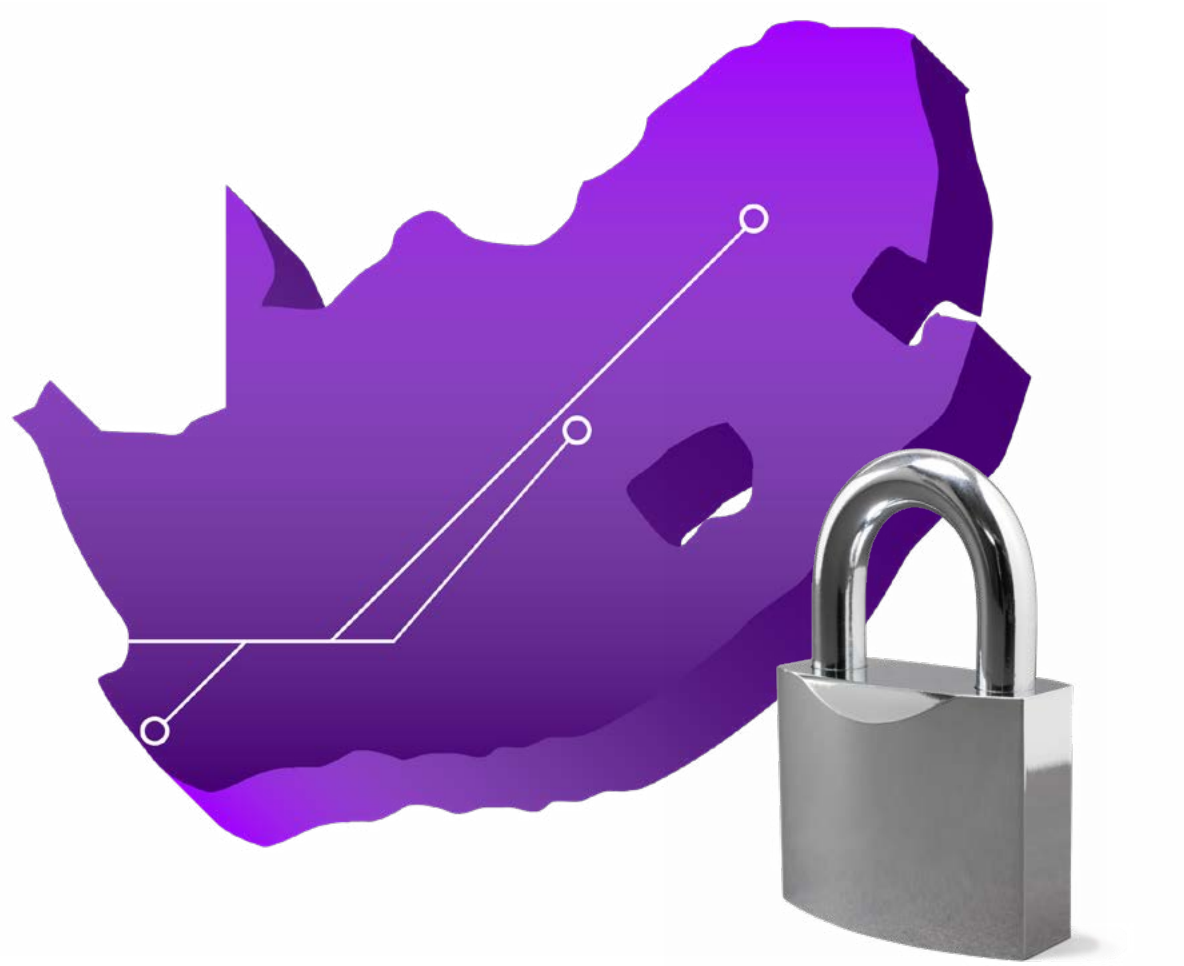
accenture

INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA



EXECUTIVE SUMMARY

As use, and reliance on technology, the Internet and smartphones grows in South Africa, so does the attack surface and the opportunity for cyberthreat actors. In 2019, South Africa saw a spike in cyberattacks on all fronts—banks, Internet service providers (ISPs), utilities and ecommerce platforms were hit, as were consumers.

In this report, iDefense, an Accenture security intelligence company, looks at the trends and incidents from 2019, identifying the reasons for these attacks, and suggesting ways in which businesses in South Africa can better prepare themselves to defend against them.

OVERVIEW

South Africa experienced a cross-industry spike in cyber attacks in 2019. The following facts and figures, taken from a variety of sources over the past 12 months, indicate the scale of the problem:

- Cybersecurity company Kaspersky has noted that malware attacks in South Africa **increased by 22 percent**[1] **in the first quarter of 2019** compared to the first quarter of 2018, which translates to just under 577 attempted attacks per hour.

- Android mobile phones in South Africa were the second most targeted[2] by banking malware, second only to those in Russia.

- Virtual-currency-related crime is on the rise,[3] with hackers increasingly using people's phones to mine cryptocurrencies.

- Card-not-present (CNP) fraud on South African-issued credit cards remained the leading contributor to gross fraud losses in the country, **accounting for 79.5 percent of all losses.** [4]

- South Africa has seen an increase of more than **100 percent in mobile banking application fraud.**[5]

In addition to these worrying general trends, 2019 was a year in which a range of different threat actors found success when attacking **high-profile South African targets**, from ISPs to electricity providers, as the following section shows.

TIMELINE OF NOTABLE ATTACKS

February 2019: A South African energy supplier suffered two security breaches in quick succession.[6] In the first, a staff member incurred an infection from the information stealer AZORult after downloading a game from the Internet. In the second, a security researcher discovered an unsecured database containing sensitive information.

July 2019: The South African Civil Aviation Authority (SACAA) reported a failure of some of its IT systems.[7] A representative announced that "some files had suspicious characteristics", resulting in some servers being disconnected from the network by SACAA.

July 2019: Ransomware infected a provider of pre-paid electricity.[8] The malware encrypted the company's internal network, Web applications and official website, leaving customers without power. The infection occurred on July 24, which is the day before a standard payday for many South Africans when many purchase new electricity packages for the upcoming month.

August 2019: The United Nations announced an investigation into at least 35 instances in 17 countries in which North Korean threat actors used cyber attacks to illegally raise funds.[9] The majority of these countries were developing countries, and South Africa was on the list. These incidents took the form of attacks through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system which is used to transfer money between banks; the theft of cryptocurrency by attacking both exchanges and users; and the mining of cryptocurrency. A bank in Africa was though to have been a victim of a SWIFT-based attack, but South African banks denied any security breaches.

September 2019: Garmin South Africa disclosed that sensitive customer payment data entered into its shopping portal, shop.garmin.co.za, had been stolen.[10] Magecart is a type of cyberattack in which malicious code is implanted on ecommerce sites to steal credit card information as people transact online. This Magecart incident affected 6,700 South African customers. The stolen data contained payment information, including card numbers, expiration dates and CVV codes, first and last names, physical addresses, phone numbers and e-mail addresses.

Such stolen data often finds its way to Dark Web online marketplaces where threat actors purchase it and use it to defraud victims.

September 2019: On September 21, 2019, one of South Africa's largest ISPs suffered a distributed denial of service (DDoS) attack lasting two days.[11] The attack also targeted another South African ISP. The attack resulted in clients losing connectivity or receiving degraded performance throughout the weekend. The attack technique, known as "carpet bombing", sends junk traffic to random IP addresses in a target network, facilitating a DDoS attack. Attackers have used this method for many years but use spiked in 2018 due to the proliferation of stresser and booter (on-demand DDoS attack) services. Threat actors have previously used such services to take down ISPs in other developing countries, such as Cambodia and Liberia.

October 2019: A breach of a major South African city network resulted in unauthorised access to its systems.[12] Officials said the attack affected its call centers, website and online platforms. News sources reported this incident as a ransomware attack, but it was later established that nothing was encrypted. A group calling itself Shadow Kill Hackers claimed responsibility and attempted to extort its victim. The group also claimed to have gained access to the networks of a South African hotel accommodation service. The city noted that the attack was carefully timed to coincide with city month-end processes affecting supplier and customer payments.

October 2019: Also in October, several South African banks, as well as financial institutions in Singapore and Scandinavia, suffered DDoS attacks, resulting in a loss of service.[13] Threat actors issued a ransom note pretending to be Russian threat actor groups Fancy Bear and Cozy Bear. This attack was similar to a 2017 campaign in which threat actors targeted backend servers rather than public websites, knowing that such servers were less likely to have DDoS mitigation protection. The DDoS attacks occurred on payday, resulting in delayed paychecks, which suggests that threat actors planned the attacks to cause maximum disruption.

WHY IS SOUTH AFRICA SUCH AN ATTRACTIVE TARGET?

Threat actors may perceive South African organisations as having lower defensive barriers than companies in more developed economies. They may also believe that they have a lower chance of being caught or prosecuted. iDefense suggests that the increased focus on South Africa by cyberthreat actors is due to the following interconnected factors:

- **Lack of investment in cyber security:** South Africa struggles with high crime rates, inequality and poverty, high unemployment and a shortage of skilled labor. While many developing economies consider cyber security a necessity, businesses often cannot invest sufficient funds. Those that can invest, face shortages of trained cybersecurity practitioners. This hampers South Africa's ability to put measures in place to prevent and mitigate advanced threats.

- **Developing cybercrime legislation and law enforcement training:** Developing countries often lack comprehensive cybercrime legislation[14], making them safe havens for illegal operations. South Africa has been slow to adopt cybercrime legislation. While the National Assembly adopted the Cyber Crimes Bill in January 2020, intense public scrutiny of its impact on privacy and freedom of expression has resulted in delays. In addition, while the South African Police Service is now also empowered to act against such crimes, a lack of cybercrime training may cause challenges in the short term.

- **Poor public knowledge of cyber threats:** South Africa has the second highest GDP[15] and operates the second fastest Internet[16] in Africa. Investment in new tech startups is booming[17] and the country is employing technological solutions to achieve a vast array of business and social needs. However, iDefense analysts note that South African Internet users are inexperienced and less technically alert than users in other nations.

One report concluded that a worrying 31 percent of South Africans thought that a cyber threat that encrypts files and demands payments is a Trojan virus, and that more than 50 percent of respondents were not aware of multi-factor authentication or its benefits.[18] As an increasing proportion of the population begins connecting to the Internet for the first time, this inexperience paired with increased exposure is a potent combination that cyber criminals will try to exploit. While threat actors are still attempting to exploit digital platforms such as banking sites or other places that store financial data, the mitigation strategies these entities deploy are usually robust—it is easier to target individuals, due to their low levels of technical knowledge.

- **The use of shadow IT:** iDefense analysts note that shadow IT—the use of applications and infrastructure without the knowledge of an enterprise's IT department—is rife in South African companies . After conducting a survey of South African IT professionals and senior executives, one recent report concluded that "We have found that organisations have hugely underestimated their exposure to applications, which could have inherent risk to business". The use of personal devices or applications on business networks can pose a significant risk, providing gateways for the deployment of ransomware or other infection vectors on a network.

- **Threat actors are taking notice:** iDefense analysts note that between 2010 and 2014 they rarely saw any Dark Web threat actors mentioning South Africa (see Exhibit 1). However, mentions picked up slightly between 2014 and 2016. Since 2016 there has been a much higher focus on South Africa among the criminal underground.

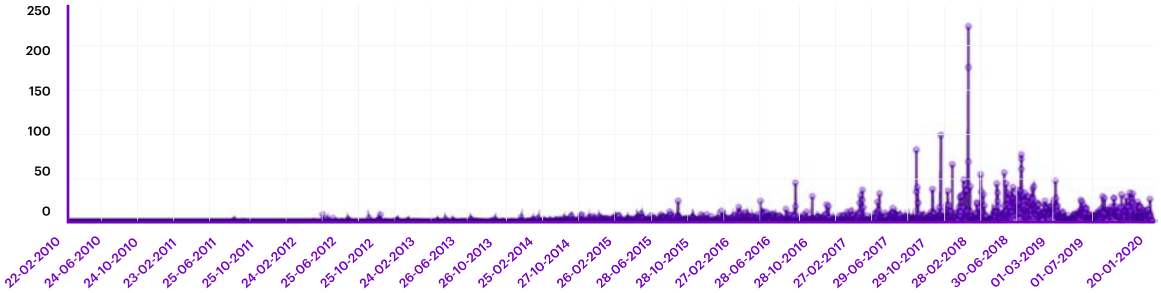


Exhibit 1: Mentions of "South Africa" between 2010 and 2020 on Dark Web

South Africa are consistent with attacks in other world economies. These attacks include the use of ransomware, banking Trojans, business e-mail compromise (BEC) scams and carding fraud. The difference is that South Africa is experiencing these threats in bulk for the first time. When iDefense examined the Scandinavian threat landscape, it found malicious actors could still use rudimentary scams successfully because the targeted businesses and people had not been exposed to them before. This same trend is playing out in South Africa. However, the threat is amplified as South Africans are inherently less aware of cyber threats than the populations of some other nations.

iDefense highlights the following areas noted in the targeting of South African organisations on cybercriminal underground forums:

- The rapid uptake in recent years in the use of mobile financial services (MFS) among South Africans leaves users vulnerable to banking Trojans and Android banking malware, the use of which has been steadily increasing among threat actors since 2017. In particular, LokiBot, RedAlert and Anubis have been under constant development and are widely available among criminal threat actors.

- Malicious actors use rudimentary scams like BEC scams, phishing, vishing and smishing abundantly against South African targets, especially small, underequipped businesses. The use of these scams remains universal, especially against developing countries, as they have less resilience to these scams than more-advanced economies.

- The use of ransomware has increased in popularity. Ransomware is widely available for sale across the criminal underground for as little as US$100. This enables unskilled threat actors to conduct malicious activities simply by purchasing the tools they need. iDefense also observed a new trend where advanced threat actor groups target larger entities, such as city administrations, as such targets can pay higher ransoms.

- Some threat actors may consider South Africa a testing ground for malware.[19] As cybersecurity measures are not as robust amongst private and public enterprises in South Africa as they are in other countries globally, some actors may test their tools and techniques against South African targets before deploying them against sophisticated targets.

WHAT CAN BE DONE?

As cybercrime figures continue to rise, South African organisations need to get serious about defending their businesses and protecting their customers. iDefense recommends a number of actions: making use of security and threat intelligence, protecting against internal threats and people-based attacks, and focussing on compliance—applying standards and best practices.

- **Makes use of security and threat intelligence:** This has previously been the reserve of large, well-funded organisations, but is now accessible and affordable to most businesses. Accenture's ninth annual report on "The Cost of Cybercrime"[20], reported that security intelligence and threat sharing provides the greatest cost savings compared with levels of spending (US$2.26 million). Security and threat intelligence is not only an important enabling technology for both discovery and investigation activities, it is a valuable source of information to understand threats and better use resources against anticipated attacks.

- **Prioritise protecting against people-based attacks:** Counteracting internal threats is still one of the biggest challenges business leaders face today. Increases in phishing, ransomware and malicious insider attacks mean that organisations need to place greater emphasis on nurturing a security-first culture. Training and education are essential to reinforcing safe behaviors, both for people within an organisation and across entire business ecosystems.

- **Focus on compliance:** Many organisations already have tools and solutions in place to help them with data compliance. However, these tools are often configured incorrectly. When business tools and services are installed and configured correctly, data compliance follows automatically. Particular attention should be paid to the reduction of shadow IT.

- **Prepare for when, not if:** The previous points all relate to detection, and "pre-breach" preparation. For post-breach incidents, such as those listed in this report, put clear procedures in place, including an incident-response capability, post-incident analysis, backed-up data, anti-DDoS measures and Cloud access security brokers.

REFERENCES

1 https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429

2 https://www.forbes.com/sites/tobyshapshak/2019/05/09/south-africa-has-second-most-android-banking-malware-attacks-as-cyber-crime-increases/#47a6a6d85d77

3 http://www.itwebafrica.com/security/514-south-africa/246610-virtual-currency-crime-spikes-in-south-africa

4 https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/

5 http://www.itwebafrica.com/home-pagex/opinion/246661-counting-the-cost-of-cybercrime

6 https://www.bleepingcomputer.com/news/security/power-company-has-security-breach-due-to-downloaded-game/

7 https://www.fin24.com/Companies/Industrial/sa-civil-aviation-authority-launches-investigation-into-possible-cyber-hack-20190708

8 https://www.zdnet.com/article/ransomware-incident-leaves-some-johannesburg-residents-without-electricity/

9 https://apnews.com/ece1c6b122224bd9ac5e4cbd0c1e1d80

10 https://www.bleepingcomputer.com/news/security/garmin-sa-shopping-portal-breach-leads-to-theft-of-payment-data/

11 https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

12 https://www.zdnet.com/article/city-of-johannesburg-held-for-ransom-by-hacker-gang/

13 https://www.thesslstore.com/blog/cyber-attacks-hit-the-city-of-johannesburg-and-south-african-banks/

14 https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=238

15 https://en.wikipedia.org/wiki/List_of_African_countries_by_GDP_(nominal)

16 https://moguldom.com/220816/10-african-countries-with-the-fastest-broadband-speeds/

17 https://www.forbes.com/sites/tobyshapshak/2020/01/20/african-tech-start-ups-have-record-investment-year-in-2019/#56e6b62832f9

18 https://www.itweb.co.za/content/4r1lyMRoaVAqpmda

19 https://www.itweb.co.za/content/wbrpOMgPAkeqDLZn

20 “Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players”, Fawzia Cassim. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders.

With 505,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at www.accenture.com

AUTHORS

WANDILE MCANYANA
Security Lead, Accenture in Africa
wandile.mcanyana@accenture.com

CLIVE BRINDLEY
Senior Manager, Security, Accenture in Africa
clive.brindley@accenture.com

YUSOF SEEDAT
Head of Global Geographies, Accenture Research
yusof.seedat@accenture.com

MAIN CONTRIBUTORS

PAUL MANSFIELD
Cyber Threat Intelligence Analyst, iDefense
paul.a.mansfield@accenture.com

THOMAS WILLKAN
Cyber Threat Intelligence Analyst, iDefense
thomas.willkan@accenture.com

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, the ideas should not be viewed as professional advice with respect to your business. This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.