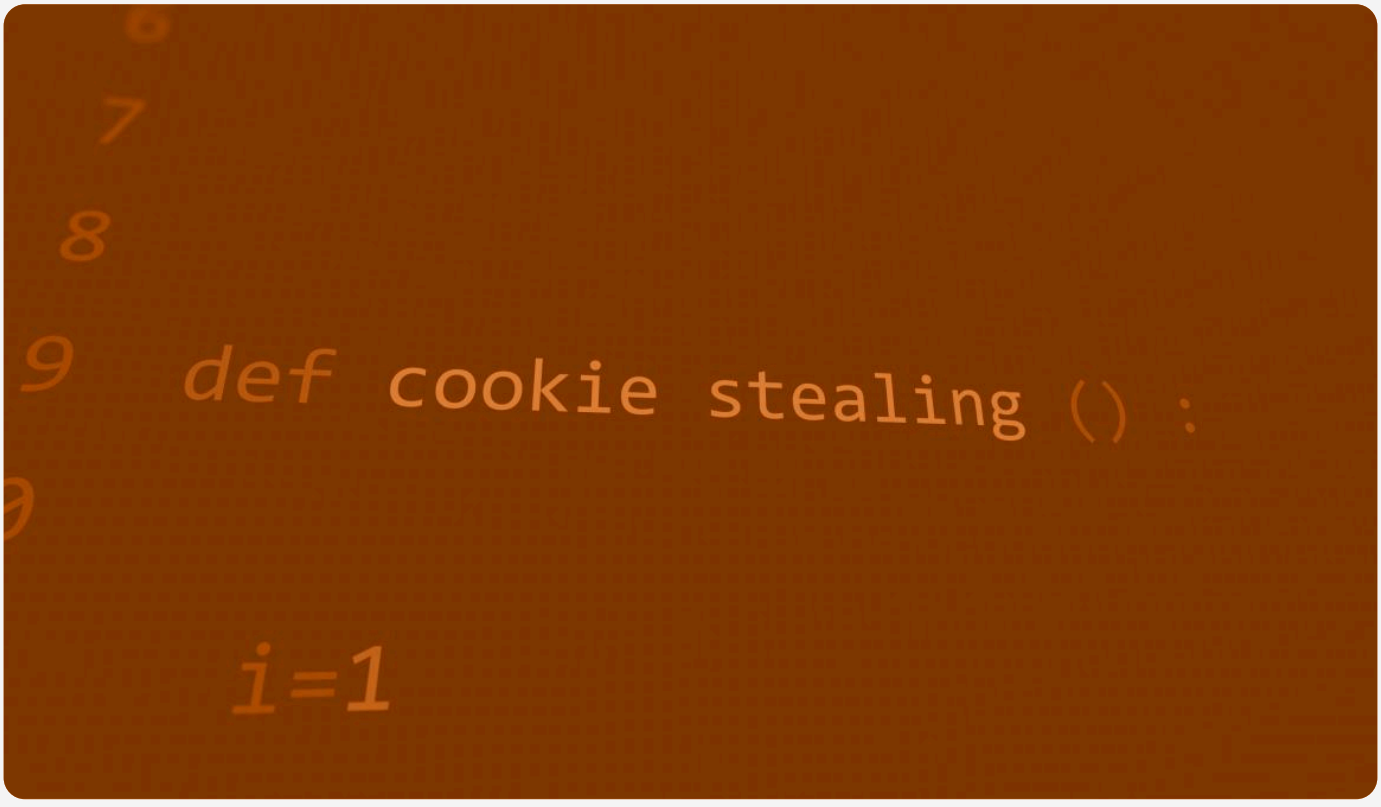
magix

Malware and its Development in South Africa

The Magix R&D Lab



Floyd Tshoma (Primary)
Tim Butler (Co-Author)
Hlayisani Shondlani (Co-Author)

magix

Malware and its Development in South Africa

The Magix R&D Lab

Authors

Floyd Tshoma (Primary)

Tim Butler (Co-Author)

Hlayisani Shondlani (Co-Author)

Abstract

South Africa has become one of the most targeted nations for cyberattacks, with malware campaigns growing in both sophistication and frequency across critical sectors including logistics, healthcare, financial services, and government.

This white paper provides a comprehensive technical examination of modern malware, from its modular architecture and development lifecycle to the advanced techniques attackers use to evade endpoint detection and response (EDR) solutions. Drawing on real-world South African case studies, including the 2021 Transnet ransomware attack and breaches across retail, healthcare, and municipal infrastructure, it maps the financial and operational impact of these threats on local organisations.

The paper further explores how artificial intelligence is accelerating malware development, the rise of Ransomware-as-a-Service (RaaS) criminal business models, and the evolution of EDR bypass methods from early hooking techniques to AI-driven evasion. It concludes with practical defensive strategies, regulatory context under POPIA and the Cybercrimes Act, and conceptual malware engineering insights that equip security teams to anticipate and counter the threats shaping South Africa's cybersecurity landscape.

Malware in South Africa: Key Threat Statistics

R300M+
estimated cost of the Transnet ransomware attack

72hrs
average downtime from healthcare ransomware

85%
of attacks use phishing as entry point

What Is Malware?

Malware, a shortened form of malicious software, refers to any program or file intentionally designed to infiltrate, damage, disrupt, or exploit computers, networks, or digital devices. It is typically created and distributed by cybercriminals with the goal of gaining unauthorised access to systems or extracting valuable information.

Malware can take many different forms, each with its own method of infection and impact:

- Viruses – Malicious programs that attach themselves to legitimate files and spread when executed.
- Worms – Self-replicating malware that spreads automatically across networks.
- Trojan horses – Malware disguised as legitimate software to trick users into installing it.
- Spyware – Software that secretly monitors user activity and collects sensitive information.
- Adware – Programs that display unwanted advertisements and may track browsing behaviour.
- Ransomware – Malware that locks or encrypts a victim's files and demands payment to restore access.

What Is Malware Used For?

Malware is developed with harmful intent. Its primary purpose is to infiltrate computer systems, compromise security, and exploit resources for financial gain, disruption, espionage, or sabotage.

Intelligence Gathering and Unauthorised Access

Some malware is designed to secretly collect sensitive data including:

- Emails and internal communications

- Business plans and confidential documents
- Login credentials and passwords
- Financial information

Data Exfiltration

Malware often enables attackers to transfer large amounts of confidential information out of a system without detection, severely impacting organisations by exposing trade secrets, customer records, and private data.

Disruption and Extortion

Certain types of malware are created to disrupt operations:

- Systems and networks may be locked or rendered unusable.
- Files may be encrypted to prevent access.

When attackers demand payment in exchange for restoring access, the malware is classified as ransomware. This is commonly used for financial extortion.

Destruction and Vandalism

Some malware is intended purely to cause damage. It may delete files, corrupt operating systems, or completely disable hardware and network infrastructure.

Theft of Computing Resources

- Operating botnets (networks of infected devices controlled remotely)
- Conducting distributed attacks
- Mining cryptocurrency (cryptojacking)
- Sending spam emails

Financial Profit

Many malware campaigns are driven by monetary gain. Stolen intellectual property, financial records, and personal data are sold on illegal marketplaces.

Malware: A Deep Technical Overview

Redefining Malware

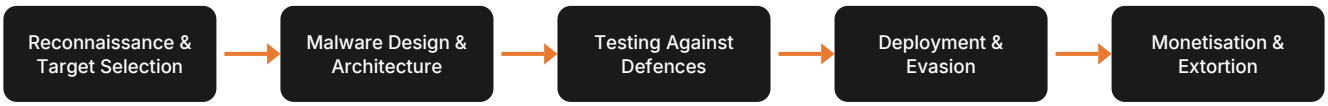
Modern malware is not a single executable but a modular ecosystem. Initial access mechanisms deliver phishing payloads, malicious documents, or exploits. Loaders and droppers deploy additional components. Payloads execute the primary objective, whether ransomware, credential stealers, keyloggers, or remote access trojans. Persistence mechanisms such as registry keys, scheduled tasks, or services ensure survival across reboots. Command and Control (C2) infrastructure provides multi-jurisdictional remote control and updates.

Common Malware Categories and Real-World Blends

Real-world attacks usually blend multiple malware types. Ransomware and stealer models combine data exfiltration with encryption. Botnet-enabled ransomware uses infected hosts for lateral movement. Living Off the Land (LotL) attacks exploit legitimate tools like PowerShell and WMI to avoid detection.

South Africa has observed a surge in ransomware combined with credential theft, particularly in sectors with on-premise Active Directory environments. The Transnet ransomware attack (2021) disrupted national logistics and exposed how critical infrastructure can be exploited when legacy systems are left exposed.

Malware Development Lifecycle



Reconnaissance and Target Selection

Attackers now treat malware campaigns like market-driven operations, performing pre-deployment analysis. South African attacks have targeted logistics, healthcare, retail, and financial services.

Malware Design and Architecture

Modern malware development mirrors legitimate software engineering. Attackers use version control with private Git repositories, continuous integration to test payloads across environments, configuration management with YAML/JSON configs for rapid re-targeting, and obfuscation frameworks that automate function renaming and control-flow flattening.

Testing Against Defences

- Commercial Antivirus Engines (signature detection and heuristic analysis)
- EDR Platforms (behavioural monitoring, anomaly detection)
- Sandboxes and Detonation Environments (Cuckoo, Hybrid Analysis)

Evading Antivirus and EDR

Modern malware developers intentionally design code to blend into legitimate system activity, taking advantage of trusted processes and built-in administrative tools.

Common Evasion Techniques

Obfuscation changes code appearance through function renaming, control-flow randomisation, and junk instructions. Packing and encryption wrap payloads in layers that decrypt only at runtime, making disk files unrecognisable. Polymorphism and metamorphism cause code to mutate with each execution, rendering signature-based detection ineffective.

Fileless and Memory-Only Execution

Fileless attacks run directly in system memory using PowerShell, WMI, or script interpreters, leaving no disk artefacts and evading traditional AV.

Living-Off-the-Land (LotL)

Attackers use legitimate tools and built-in system utilities to carry out malicious activities, relying on trusted programs to avoid detection.

> Contextual monitoring of legitimate tools is critical for defenders.

Process Injection

Malicious code is inserted into legitimate running processes, inheriting their trust and evading process-based heuristics.

```
Conceptual API flow:
handle = OpenProcess(TARGET_PID, PROCESS_ALL_ACCESS)
alloc_mem = VirtualAllocEx(handle, payload_size)
WriteProcessMemory(handle, alloc_mem, payload)
CreateRemoteThread(handle, alloc_mem)
```

Real-World Examples of Evasion

Conti and Ryuk Operations

Demonstrated fileless lateral movement across enterprise networks using WMI and PSExec.

Kaseya Supply Chain Attack (2021)

Delivered malware through trusted software updates, bypassing antivirus by exploiting vendor-signed update trust.

DarkSide

Employed direct syscalls and memory obfuscation to evade multiple antivirus engines.

The Role of AI in Modern Malware Development

AI is not replacing human attackers but significantly amplifying their capabilities

AI as a Force Multiplier

AI generates loaders, scripts, and polymorphic code variations with minimal human input. It rapidly mutates payloads by adapting encryption schemes and packing methods. Machine learning models craft contextually accurate spear phishing emails. AI also accelerates discovery of misconfigurations and vulnerabilities, reducing skill barriers and allowing lower-tier threat actors to deploy effective campaigns.

AI-Enhanced Social Engineering

AI enables personalised spear phishing that references local events and regulatory updates. Fake invoice and HR communications trigger execution of malicious macros. AI-generated voice cloning and deepfakes can impersonate executives to instruct finance teams to approve transfers.

In South Africa, attackers have impersonated SARS tax communications, courier notifications (DHL, FedEx), and local banking alerts (ABSA, Standard Bank).

Limitations of AI-Driven Malware

Fully autonomous attacks at scale remain largely theoretical. Human involvement continues to be essential for target selection, strategic deployment, and ransomware negotiations.

Malware Economics and Criminal Business Models

Ransomware as a Service (RaaS)

RaaS has transformed malware into a commercialised, profit-driven ecosystem. Developers create and maintain ransomware engines while affiliates execute attacks, sharing revenue through affiliate agreements.

> LockBit RaaS affiliates targeted South African financial services and retail chains in 2022, encrypting critical systems while exfiltrating data for double extortion.

Data Extortion and Double Extortion

Modern ransomware campaigns frequently use data exfiltration before encryption. Sensitive documents, PII, and financial records are extracted first. Attackers then pressure organisations to pay by threatening public release. In South Africa, POPIA fines enhance extortion leverage, creating additional pressure on victims.

South African Malware Case Studies

Transnet Ransomware Attack (2021)

Targeted national logistics and freight, causing severe disruption to port operations and supply chain activities. Attackers combined ransomware with credential theft, leveraging PowerShell and WMI for lateral movement.

Retail Sector Attacks

Spear-phishing campaigns with macro-enabled Excel documents resulted in customer PII exposure, POS system downtime, and heightened regulatory scrutiny.

Healthcare Sector

Ransomware, credential-stealing malware, and data exfiltration tools targeting legacy medical systems have posed significant risks to patient safety and POPIA compliance.

Municipalities and Government

Exposed RDP, web portals, and weak credential reuse have made municipalities targets for ransomware, wiper malware, and data leaks affecting essential services.

Financial and Operational Impact

Impact of Malware on South African Organisations

R300M+
Transnet attack estimated total cost

48hrs
average mining operations shutdown

R2.5M+
typical retail ransom demand

Immediate Financial Impacts

Direct costs include ransom payments, cybersecurity specialists for forensic investigations, and rebuilding affected systems.

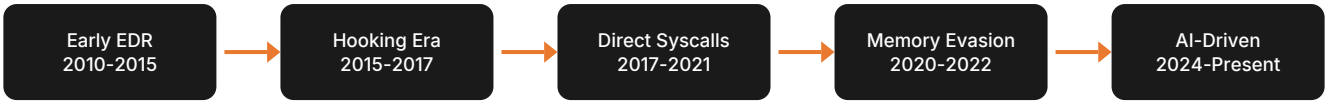
Secondary and Ongoing Impacts

Indirect costs include operational downtime, revenue loss, reputational damage, customer churn, POPIA penalties, and increased cyber insurance premiums.

Why South Africa Is a High-Value Target

South Africa's attractiveness to cybercriminals stems from several structural challenges. Many organisations rely on legacy infrastructure with outdated servers and unpatched systems. A cybersecurity skills shortage limits the pool of professionals available to monitor and respond to threats. Inconsistent patch management leaves known vulnerabilities open. Rapid digital transformation means security is not always integrated at the design stage.

Evolution of EDR Bypass Techniques



Early EDR Solutions (2010–2015)

First-generation EDR relied on signature-based detection. Malware developers used process hollowing, DLL injection, and manual DLL loading to evade monitoring.

The Hooking Era (2015–2017)

EDR platforms expanded API monitoring through hooking. Attackers responded with hook detection, API restoration, and manual mapping methods.

Direct and Indirect Syscalls (2017–2021)

Malware adopted direct kernel calls via SysWhispers, Hell's Gate, and Halos Gate, combined with call-stack spoofing and module stomping.

Advanced Memory and Hardware Evasion (2020–2022)

Sophisticated memory obfuscation, transacted NTFS sections, phantom DLL loading, and hardware-aware evasion exploiting timing discrepancies.

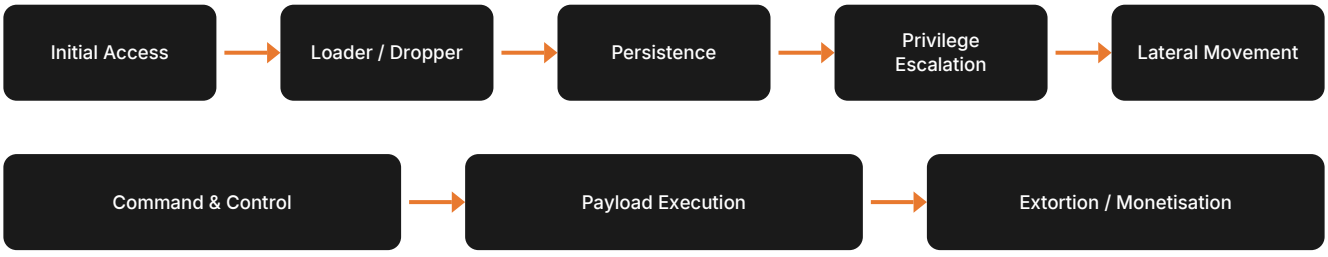
VEH and Kernel Callback Exploits (2022–Present)

VEH exploitation uses controlled exceptions to redirect execution stealthily. Kernel callback and ETW bypasses manipulate kernel objects and event tracing to hide malicious activity. Techniques like Process Doppelgänging and Herpaderping enable stealthy memory writes that evade monitoring.

AI-Driven Evasion (2024–Present)

Behavioural cloning allows malware to mimic legitimate application patterns, evading heuristic detection. Adaptive learning modifies execution strategies in real-time based on EDR feedback. Dynamic evasion adjusts persistence, timing, and memory allocation to continuously avoid detection.

Modern Malware Kill-Chain



Defensive Strategies Against Modern Malware

Technical Controls

EDR platforms continuously monitor endpoint activity, analyse behavioural patterns, and track process relationships. Network segmentation limits lateral movement. Zero trust architecture requires continuous verification rather than implicit trust. Immutable and offline backups provide critical recovery mechanisms against encryption attacks.

Human and Process Controls

Structured cybersecurity awareness programmes train employees to recognise spear-phishing attempts. Phishing simulation campaigns reinforce training with realistic scenarios. Red-team exercises test how well people, processes, and technologies respond to real-world techniques. Incident response plans supported by periodic tabletop drills prepare teams for coordinated containment.

AI for Defence

AI-driven systems analyse large volumes of activity to identify behavioural anomalies, support automated containment, and detect zero-day threats.

> AI-driven anomaly detection flagged unusual PowerShell execution patterns in a South African healthcare network, preventing a ransomware payload from reaching production systems.

Regulatory and Legal Context in South Africa

POPIA has elevated cyber incidents from technical matters to board-level issues. Organisations must report security compromises to the Information Regulator and affected individuals. Regulatory compliance now forms a critical component of cybersecurity strategy.

Future Outlook

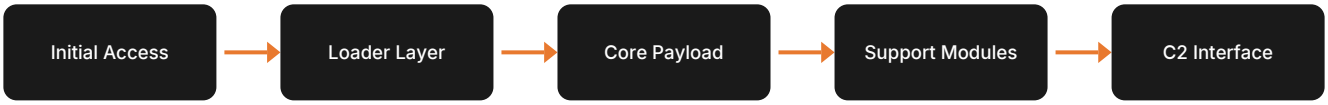
Malware will become more industry-specific. AI will enhance social engineering. Regulatory frameworks will expand. Organisations without unified defence strategies integrating technical controls, AI defence, awareness, and processes will face escalating consequences.

Conceptual Malware Engineering

Malware Design Philosophy

Threat actors approach malware development using software engineering best practices. Reliability ensures consistent execution across OS versions and configurations. Stealth prioritises avoiding detection over execution speed. Modularity allows components to be swapped or upgraded without rewriting the entire programme. Scalability enables the same malware family to target thousands of endpoints with minimal adaptation.

Malware Component Layers



Loader Architecture

Key functions include environment profiling, execution control with delays and staged execution, and payload handling from C2 servers.

```
Pseudocode (Defensive Perspective):
if system.is_sandbox() or system.is_virtualized():
    sleep(random_delay)
else:
    decrypt_payload()
    execute_in_memory(payload)
```

Persistence, Escalation, and Lateral Movement

Persistence mechanisms include configuration-based approaches using startup folders and registry Run keys, scheduled tasks that execute at specific times, and service-based persistence that installs as or imitates legitimate system services. Privilege escalation exploits misconfigurations, reuses compromised credentials, and abuses Active Directory trust relationships. Lateral movement modules enumerate reachable systems, identify high-value targets, and reuse harvested credentials to authenticate without deploying additional malware.

C2 Infrastructure and Ransomware Engineering

C2 infrastructure relies on multiple fallback servers and encrypted communications that mimic normal traffic. Modern ransomware prioritises critical systems for encryption first, interferes with backup and restore mechanisms, and applies psychological pressure through carefully crafted extortion messaging that leverages regulatory frameworks like POPIA.

Industry-Specific Malware Threats

Banking and Financial Services

Primary threats include banking trojans, credential stealers, BEC, and ransomware. Banks are targeted for large-value transactions and immediate monetisation opportunities.

> In 2022, a South African financial institution suffered a banking trojan attack allowing fraudulent wire transfers totalling over ZAR 3 million.

Mining and Industrial Operations

Ransomware, industrial espionage malware, and OT/IT crossover attacks target legacy SCADA systems and remote operations with high downtime costs.

Healthcare, Municipalities, and Retail

Healthcare faces ransomware targeting patient records. Municipalities are targeted through exposed RDP/VPN. Retail faces POS malware and fileless execution.

Financial Impact Overview

The financial ramifications of a ransomware attack extend far beyond the immediate crisis. Direct costs include ransom payments, incident response, forensic investigations, and system rebuilding. However, the more substantial burden lies in indirect and long-term costs: business interruption, revenue loss, customer churn, reputational damage, legal fees, POPIA compliance actions, and increased cyber insurance premiums. In the case of the Transnet attack alone, combined direct and indirect costs were estimated at over R300 million.

Conclusion

Today's threats are sophisticated, business-like operations. Developers use professional software engineering practices to build modular, adaptable malware customised for specific industries and targets.

South Africa faces unique challenges. Organisations run on legacy systems, face a cybersecurity skills shortage, and sectors like healthcare, municipalities, banking, and mining have become attractive targets because disruption has real-world consequences.

However, understanding how malware works gives defenders a powerful advantage. The fact that attackers must constantly evolve shows that our defences are working and forcing adaptation.

Organisations that invest in foundational security, keeping systems updated, segmenting networks, implementing MFA, and training employees, will be ahead of most attackers. Those adding EDR, behavioural monitoring, and incident response capabilities will be stronger still.

The future of cybersecurity in South Africa is one of continuous improvement, of learning from each incident, building stronger defences, and developing local expertise that understands both global threats and local context.

magix

This white paper was compiled by the Magix Lab team

Sources

Surge in Cyberattacks Across Various Sectors In South Africa

South Africa’s ransomware reckoning: six trends that demand urgent action

Africa’s cybercrime crisis deepens as scam cases spike 3,000%

Ransomware attackers claim hit on Methodist Church of Southern Africa

Prominent private hospital group in South Africa hacked

South Africa’s national health lab hit with ransomware attack amid mpox outbreak

National Health Laboratory Service hit by cyber attack

Important South African bank hit by ransomware attack

SABS still cannot access its systems after cyber-attack

South Africa a top target for cybercriminals – INTERPOL Africa Cyberthreat Assessment 2025

ESET Threat Report: Phishing and social engineering pose greatest risks to SA organisations

Kaspersky warns of a new credential-stealing campaign via Facebook

Kaspersky uncovers GriffithRAT targeting fintech platforms

Data-stealing malware infections increased sevenfold since 2020

Nclose survey reveals rising ransomware threat to SA businesses

Sophos: SA companies being hit by ransomware hard!

Ransomware hits more than half of SA companies (Sophos 2022)

Transnet ransomware attack (Wikipedia)

https://www.stationx.net/malware-statistics/

https://www.next7it.com/insights/malware-statistics/

https://earthweb.com/malware-statistics/