Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Cybercrime Surge Targets Africa's Financial Hubs

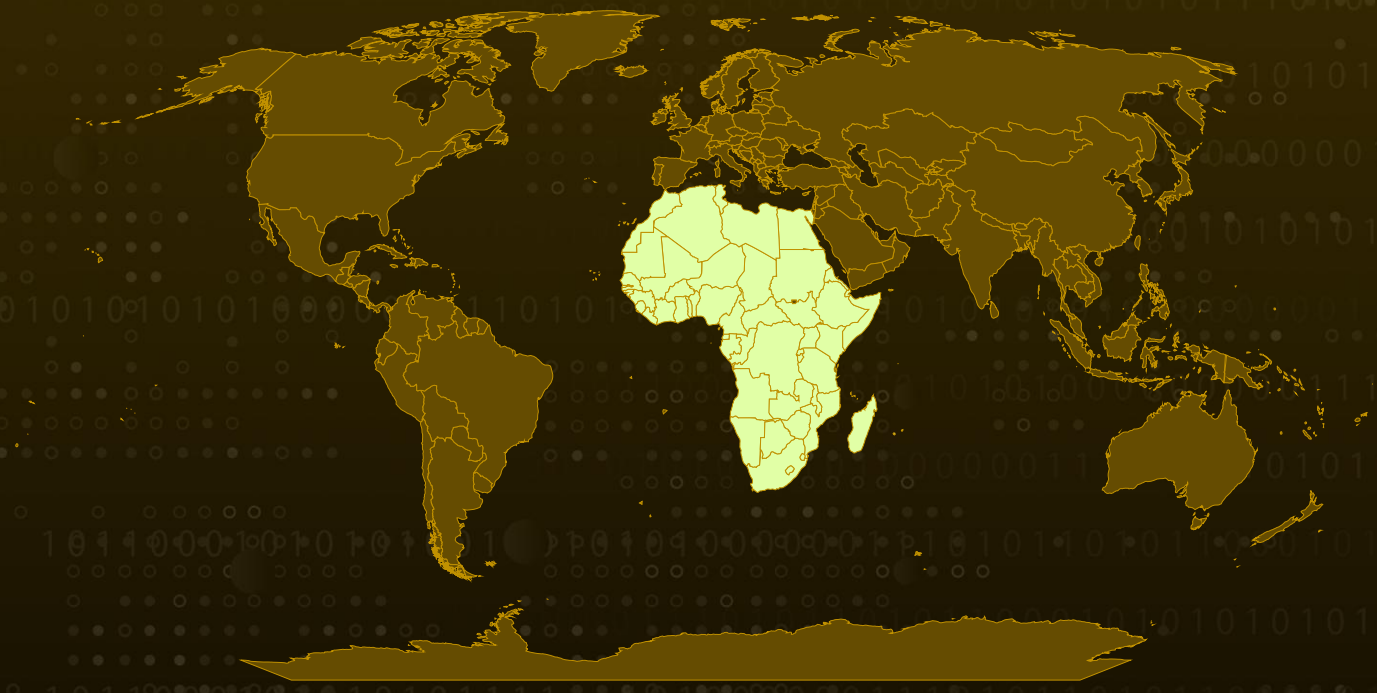
Date of Publication	Admiralty Code	TA Number
June 26, 2025	A1	TA2025200

Summary

Active Since: July 2023
Cluster: CL-CRI-1014
Targeted Region: Africa
Targeted Industry: Finance
Open-Source Tools: PoshC2, Chisel, Classroom Spy

Attack: Africa's financial sector faces a growing, discreet threat. A sophisticated threat cluster, identified as CL-CRI-1014, is targeting institutions with open-source tools cleverly disguised as legitimate software, aiming to establish covert access and monetize it through darknet markets. This campaign mirrors a broader surge in cybercrime activity across the region, with INTERPOL warning that Africa's cybersecurity landscape is under mounting pressure from increasingly organized and persistent threat groups.

Attack Regions



Attack Details

#1

A threat cluster identified as CL-CRI-1014 is actively targeting financial institutions across Africa, following a consistent and calculated attack pattern. The group relies heavily on a blend of open-source and publicly available tools to build its attack infrastructure, establishing covert tunnels for network communication and deploying remote administration utilities to maintain persistent access.

#2

Among the tools in their arsenal are PoshC2, an open-source command-and-control framework, Chisel, a lightweight tunneling tool, and MeshAgent, an open-source remote device management utility, which served as their primary payload in earlier campaigns. In recent activity, however, the group has begun shifting to Classroom Spy, a remote administration tool with both free and commercial versions available for multiple operating systems, including Windows, macOS, Linux, iOS, and Android.

#3

The attack chain begins with the attacker using PsExec from a controlled system to connect to a compromised intermediary host, deploying Chisel to establish a proxy and bypass network firewalls. Through this foothold, the attacker delivers PoshC2 implants to internal systems, executes reconnaissance commands, and uses Chisel for covert network tunneling. In parallel, PsExec is used on additional endpoints to run PowerShell scripts that install Classroom Spy, enabling persistent remote surveillance, keylogging, and control within the compromised infrastructure.

#4

To evade detection, CL-CRI-1014 carefully forges file signatures, icons, process names, and file paths to mimic legitimate software, effectively disguising malicious payloads as trusted applications. It's suspected their broader objective is to establish covert footholds within financial networks and later monetize this access through darknet marketplaces.

#5

Notably, this activity unfolds against the backdrop of a sharp rise in cybercrime across Africa, as highlighted in INTERPOL's 2025 cybercrime assessment. The report confirms a surge in phishing scams, ransomware incidents, business email compromise, and digital extortion campaigns affecting multiple sectors.

Recommendations

Enhance File and Process Integrity Monitoring: Regularly monitor for unauthorized or suspicious file signature modifications, process names, and file paths mimicking legitimate applications. Use whitelisting or allow-listing solutions to block unapproved remote administration and tunneling tools.

Digital Supply Chain Security Audits: Proactively vet third-party software vendors and service providers for the presence of dual-use or open-source tools that could be exploited. Mandate transparency from vendors on their software bill of materials (SBOM) and incident response readiness.

Audit Administrative Accounts and Credentials: Immediately review and reset privileged account credentials. Look for suspicious or recently created admin accounts, especially those enabled for remote access tools.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0042** Resource Development	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1505 Server Software Component	**T1569** System Services	**T1569.002** Service Execution	**T1083** File and Directory Discovery
T1036 Masquerading	**T1036.005** Match Legitimate Name or Location	**T1018** Remote System Discovery	**T1021** Remote Services
T1021.001 Remote Desktop Protocol	**T1570** Lateral Tool Transfer	**T1572** Protocol Tunneling	**T1219** Remote Access Tools

T1071 Application Layer Protocol	**T1048** Exfiltration Over Alternative Protocol	**T1027** Obfuscated Files or Information	**T1056** Input Capture
T1056.001 Keylogging	**T1548** Abuse Elevation Control Mechanism	**T1113** Screen Capture	**T1588** Obtain Capabilities
T1588.002 Tool	**T1090** Proxy		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3bbe3f42857bbf74424ff4d044027b9c43d3386371decf905a4a1037ad468e2c, 9149ea94f27b7b239156dc62366ee0f85b0497e1a4c6e265c37bedd9a7efc07f, a41e7a78f0a2c360db5834b4603670c12308ff2b0a9b6aeaa398eeac6d3b3190, 0bb7a473d2b2a3617ca12758c6fbb4e674243daa45c321d53b70df95130e23bc, 14b2c620dc691bf6390aef15965c9587a37ea3d992260f0cbd643a5902f0c65b, 9d9cb28b5938529893ad4156c34c36955aab79c455517796172c4c642b7b4699, e14b07b67f1a54b02fc6b65fdba3c9e41130f283bfea459afa6bee763d3756f8, a61092a13155ec8cb2b9cdf2796a1a2a230cfadb3c1fd923443624ec86cb7044, 7e0aa32565167267bce5f9508235f1dacbf78a79b44b852c25d83ed093672ed9, d81a014332e322ce356a0e2ed11cffddd37148b907f9fdf5db7024e192ed4b70, d528bcbfef874f19e11bdc5581c47f482c93ff094812b8ee56ea602e2e239b56, f1919abe7364f64c75a26cff78c3fcc42e5835685301da26b6f73a6029912072, 633f90a3125d0668d3aac564ae5b311416f7576a0a48be4a42d21557f43d2b4f, bc8b4f4af2e31f715dc1eb173e53e696d89dd10162a27ff5504c993864d36f2f, 9a84929e3d254f189cb334764c9b49571cafcd97a93e627f0502c8a9c303c9a4,

TYPE	VALUE
SHA256	5e4511905484a6dc531fa8f32e0310a8378839048fe6acfeaf4dda2396184997, e788f829b1a0141a488afb5f82b94f13035623609ca3b83f0c6985919cd9e83b, 2ce8653c59686833272b23cc30235dae915207bf9cdf1d08f6a3348fb3a3e5c1, 831d98404ce5e3e5499b558bb653510c0e9407e4cb2f54157503a0842317a363, f5614dc9f91659fb956fd18a5b81794bd1e0a0de874b705e11791ae74bb2e533, aed1b6782cfd70156b99f1b79412a6e80c918a669bc00a6eee5e824840c870c1, 6cfa5f93223db220037840a2798384ccc978641bcec9c118fde704d40480d050, 831d98404ce5e3e5499b558bb653510c0e9407e4cb2f54157503a0842317a363
Domains	finix[.]newsnewth365[.]com, mozal[.]finartex[.]com, vigio[.]finartex[.]com, bixxler[.]drennonmarketingreviews[.]com, genova[.]drennonmarketingreviews[.]com, savings[.]foothillindbank[.]com, tnn[.]specialfinanceinsider[.]com, ec2-18-140-227-82[.]ap-southeast-1[.]compute[.]amazonaws[.]com, c2-51-20-36-117[.]eu-north-1[.]compute[.]amazonaws[.]com, flesh[.]tabtemplates[.]com, health[.]aqlifecare[.]com, vlety[.]forwardbanker[.]com

References

https://unit42.paloaltonetworks.com/cybercriminals-attack-financial-sector-across-africa/

https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

https://github.com/nettitude/PoshC2

https://github.com/jpillora/chisel

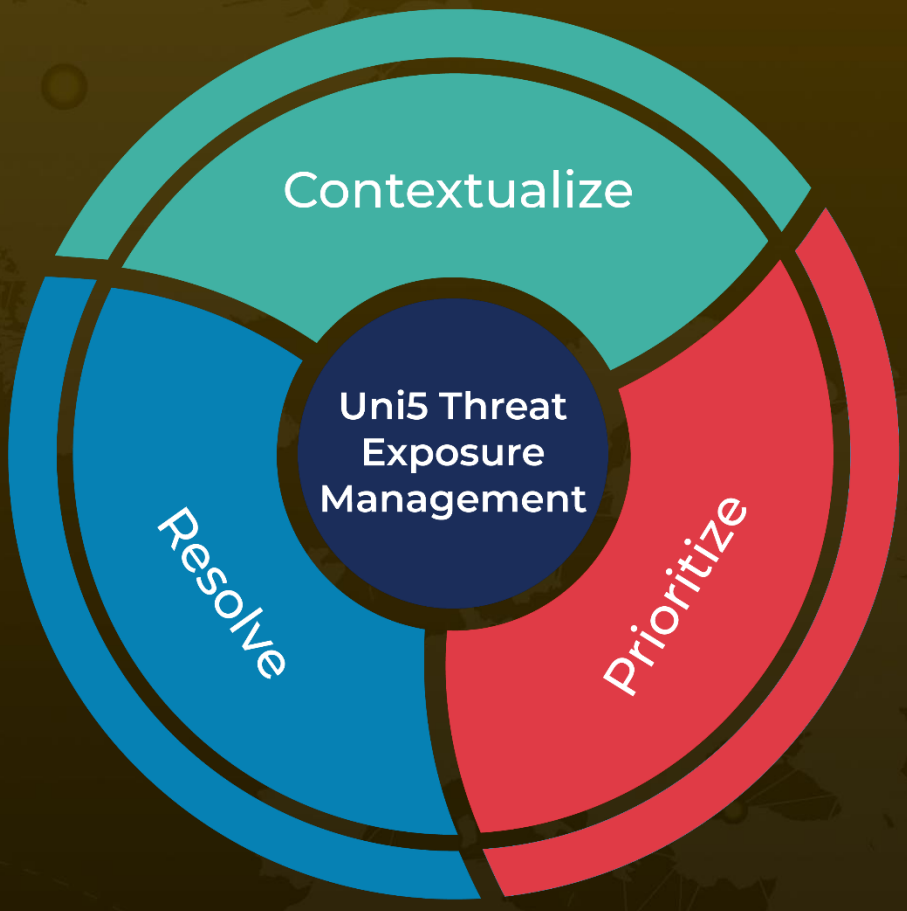
https://hivepro.com/threat-advisory/phantom-enigma-campaign-used-familiar-tools-in-unfamiliar-ways/

https://hivepro.com/threat-advisory/dangerous-savanna-campaign-attacked-african-financial-institutions/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 26, 2025 • 5:30 AM

More at www.hivepro.com