Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

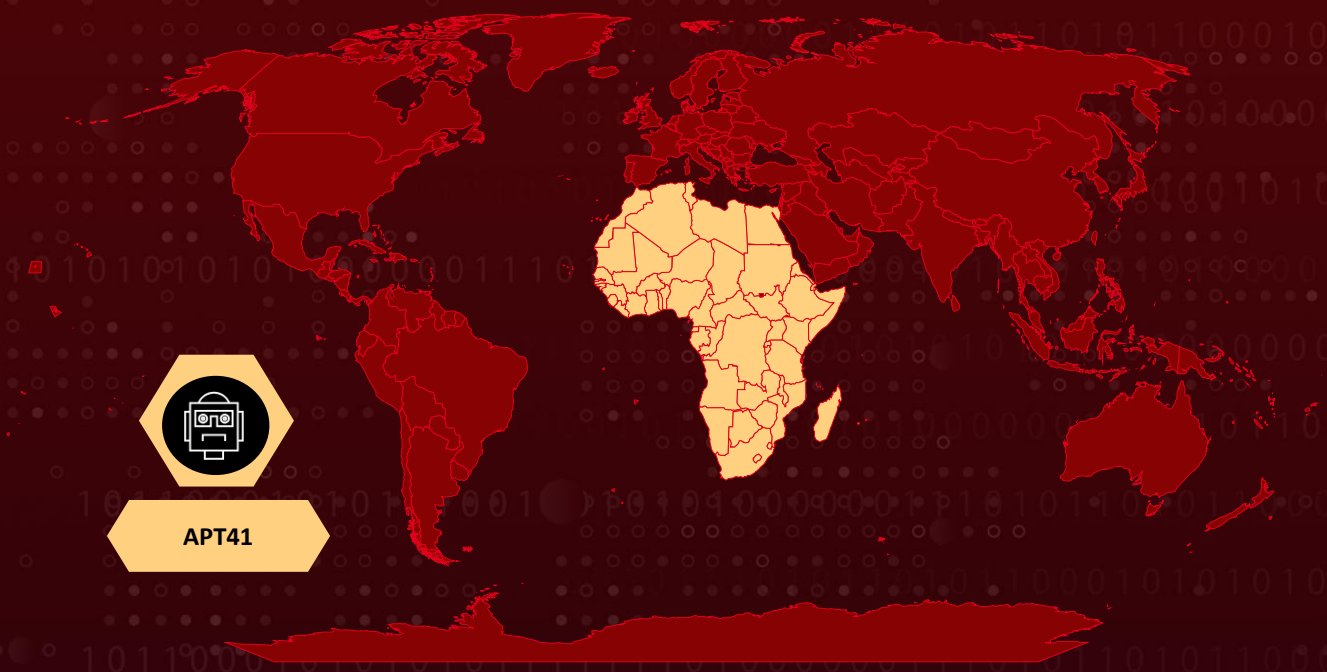
APT41 Targets African Government IT Services

Date of Publication	Admiralty Code	TA Number
July 24, 2025	A1	TA2025230

Summary

First Seen: July 2025
Targeted Region: Africa
Targeted Platforms: Windows
Threat Actor: APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)
Targeted Industries: Government IT Services
Attack: APT41, a Chinese state-linked cyberespionage group, launched a sophisticated attack on a Southern African government IT provider, gaining access via an exposed web server and harvesting privileged credentials. They used tools like Cobalt Strike and Impacket, alongside stealthy techniques such as DLL sideloading and internal SharePoint-based C2, to maintain persistence and evade detection. Sensitive data including credentials, emails, and financial details were exfiltrated using custom stealers and post-exploitation tools. The attack highlights critical gaps in endpoint monitoring and privileged account security.

Attack Regions



Attack Details

#1

APT41, a well-known Chinese-speaking cyberespionage group, executed a sophisticated attack on a Southern African government IT services provider, marking a significant escalation in their previously limited African operations. The group infiltrated the network through an exposed web server, using credential harvesting techniques to obtain privileged domain accounts. These credentials granted them broad access across the organization, enabling lateral movement and helping them remain undetected for an extended period.

#2

Once inside, APT41 deployed a combination of custom and open-source tools, including the Impacket toolkit and Cobalt Strike for command and control (C2), while leveraging legitimate administrative utilities to mimic authentic administrator behavior. They established persistence by sideloading malicious DLLs into legitimate applications and creating scheduled tasks and custom Windows services. Their use of the target's internal SharePoint server as a C2 channel helped disguise malicious communications as normal internal traffic, making detection significantly harder.

#3

For data harvesting and exfiltration, the group deployed modified versions of Pillager and Checkout stealers, alongside well-known tools such as Mimikatz and RawCopy. These tools were used to collect system credentials, emails, chat logs, browser data, Wi-Fi passwords, internal source code, and even financial data stored in browsers. Exfiltration was performed via bundled payloads and, in some cases, through web shells installed on internal servers, further blending malicious activity with legitimate operational flows.

#4

The intrusion exposed key weaknesses in the target's cybersecurity posture, particularly insufficient endpoint visibility and inadequate privileged access controls. APT41's use of stealthy, "living off the land" techniques made detection difficult and amplified the impact. This campaign highlights the growing reach and operational maturity of APT41, and it signals the urgent need for stronger cyber defenses across African digital infrastructure.

Recommendations

Enhance Endpoint Detection and Response: Deploy comprehensive endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions across all systems, including previously unmonitored hosts. Ensure that all endpoints are reporting telemetry and that agent software coverage is complete, especially for critical infrastructure.

Strengthen Privileged Account Management: Regularly audit and minimize privileged accounts, applying the principle of least privilege throughout the organization. Enforce robust authentication requirements, such as multi-factor authentication (MFA), for all administrative and sensitive accounts. Routinely review and restrict cross-domain account permissions to limit lateral movement possibilities.

Improve Monitoring and Logging: Implement centralized logging for all critical systems, ensuring logs cannot be tampered with by attackers. Regularly review and analyze logs for unusual activity, such as the use of administrative tools (e.g., Impacket, reg.exe, PowerShell, wmic) and anomalous process chains. Set up alerts for behaviors associated with credential dumping, registry hive access, and new or unauthorized scheduled tasks and Windows services.

Harden Network and Application Security: Patch and monitor exposed web servers and applications to prevent exploitation of public-facing vulnerabilities. Segment the network to limit the spread of lateral movement, with strict controls between different internal zones. Regularly scan for and rapidly remediate vulnerabilities on internet-facing infrastructure.

Potential MITRE ATT&CK TTPs

TA0008 Lateral Movement	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0009 Collection	TA0006 Credential Access	TA0001 Initial Access
TA0010 Exfiltration	TA0040 Impact	TA0007 Discovery	T1574.001 DLL
T1078 Valid Accounts	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter
T1078.002 Domain Accounts	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1047 Windows Management Instrumentation
T1190 Exploit Public-Facing Application	T1567 Exfiltration Over Web Service	T1543.003 Windows Service	T1614.001 System Language Discovery
T1505.003 Web Shell	T1505 Server Software Component	T1505.004 IIS Components	T1543.003 Windows Service
T1543 Create or Modify System Process	T1055 Process Injection	T1140 Deobfuscate/Decode Files or Information	T1070.004 File Deletion
T1070 Indicator Removal	T1036 Masquerading	T1555 Credentials from Password Stores	T1003.002 Security Account Manager
T1003 OS Credential Dumping	T1552 Unsecured Credentials	T1555.003 Credentials from Web Browsers	T1046 Network Service Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1570 Lateral Tool Transfer
T1021.002 SMB/Windows Admin Shares	T1021 Remote Services	T1560.001 Archive via Utility	T1560 Archive Collected Data

T1119 Automated Collection	**T1005** Data from Local System	**T1071.001** Web Protocols	**T1071.004** DNS
T1071 Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1090.001** Internal Proxy	**T1090** Proxy
T1572 Protocol Tunneling	**T1048** Exfiltration Over Alternative Protocol		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2F9D2D8C4F2C50CC4D2E156B9985E7CA, 9B4F0F94133650B19474AF6B5709E773, A052536E671C513221F788DE2E62316C, 91D10C25497CADB7249D47AE8EC94766, C3ED337E2891736DB6334A5F1D37DC0F, 9B00B6F93B70F09D8B35FA9A22B3CBA1, 15097A32B515D10AD6D793D2D820F2A8, A236DCE873845BA4D3CCD8D5A4E1AEFD, 740D6EB97329944D82317849F9BBD633, C7188C39B5C53ECBD3AEC77A856DDF0C, 3AF014DB9BE1A04E8B312B55D4479F69, 4708A2AE3A5F008C87E68ED04A081F18, 125B257520D16D759B112399C3CD1466, C149252A0A3B1F5724FD76F704A1E0AF, 3021C9BCA4EF3AA672461ECADC4718E6, F1025FCAD036AAD8BF124DF8C9650BBC, 100B463EFF8295BA617D3AD6DF5325C6, 2CD15977B72D5D74FADEDFDE2CE8934F, 9D53A0336ACFB9E4DF11162CCF7383A0
IPv4	47[.]238[.]184[.]9, 38[.]175[.]195[.]13

TYPE	VALUE
URLs	hxxp[://]github[.]githubassets[.]net/okaqbfk867hmx2tvqxhc8zyq9fy694gf/hta, hxxp[://]chyedweeyaxkavyccenwjvqrsgvyj0o1y[.]oast[.]fun/aaa, hxxp[://]toun[.]callback[.]red/aaa, hxxp[://]asd[.]xkx3[.]callback[.][]red, hxxp[://]ap-northeast-1[.]s3-azure[.]com, hxxps[://]www[.]msn-microsoft[.]org:2053, hxxp[://]www[.]upload-microsoft[.]com
Domains	s3-azure[.]com, *[.]ns1[.]s3-azure[.]com, *[.]ns2[.]s3-azure[.]com, upload-microsoft[.]com, msn-microsoft[.]org
SHA256	E0C81C64B4486C69C1202A3CCCBDDBF2CD271361D1D11C879B7562FD19C7A03E, 22CE240194AF081B58F6EBFBC90D96A1A7BAE9000730E4BCF9CB498C1BC66747, 1EB705643F0F76F7551686FABB54F3B3BDAEB2C285251ABD2B69753393A19140, 9B50E888AAEC0E4D105A6F06DB168A8A2DCF9AB1F9DEEFF4B7862463299AB1CA, D9C34E2248BF47AC4C13C023A42BB6FF18962CFD9BB9143D3D993A7BB0E1B1C4, CB9A14FA6950912B2486706E095FAFC30B33D4DD3639E4151EA1E9C5A04040B5, 7E33C5150CD320FFA1F895B80DE818BFFD987D3BC90BC87124455075B1EBF3E9E, 0320E0824327FB3C81024AEBCF51EAD26DEEFD3DCCCED2EA9269BD0D85A2970B

References

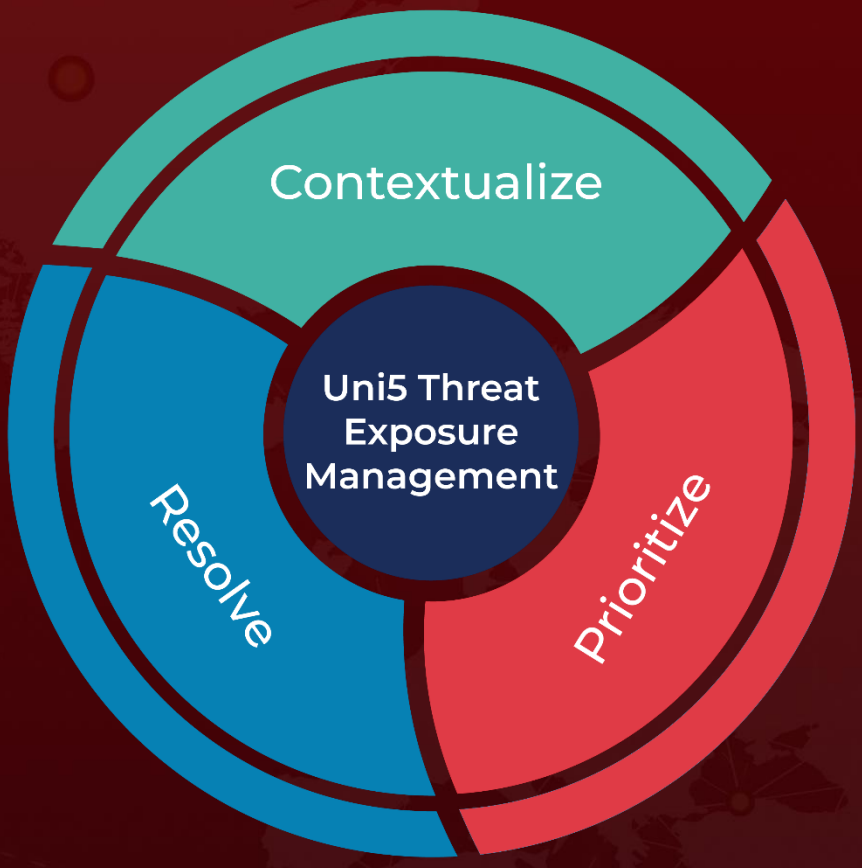
https://securelist.com/apt41-in-africa/116986/

https://hivepro.com/threat-advisory/apt41-leverages-google-calendar-for-command-and-control/

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

July 24, 2025 • 7:30 AM

More at www.hivepro.com