Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

DroxiDat Targets Southern African Power Utility

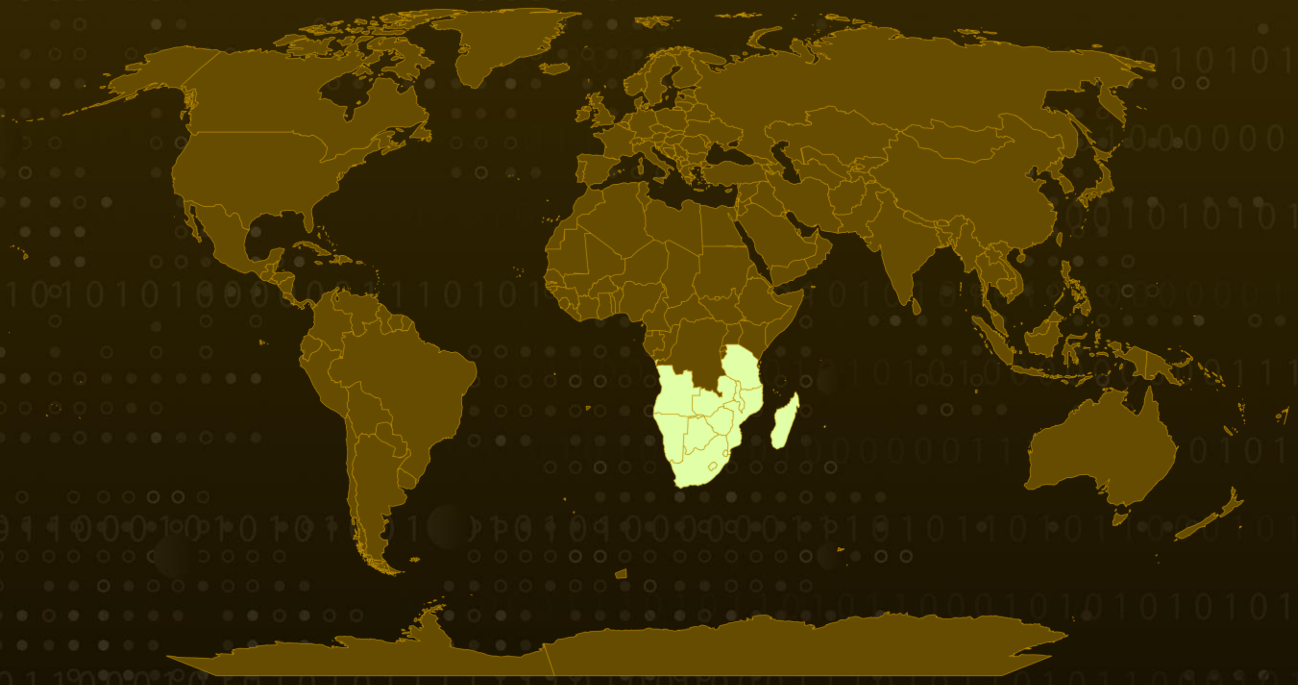
Date of Publication	Admiralty Code	TA Number
August 11, 2023	A1	TA2023331

Summary

First Seen: March 2023
Malware: DroxiDat and SystemBC
Attack Region: Southern Africa
Targeted Sectors: Utility, Healthcare, and Energy

Attack: In a targeted operation, an unidentified actor strategically deployed the advanced DroxiDat proxy-capable backdoor alongside Cobalt Strike beacons. The operation was aimed at a critical power utility within the infrastructure of a Southern African nation.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

An unknown adversary meticulously deployed the sophisticated DroxiDat proxy-capable backdoor in tandem with Cobalt Strike beacons, targeting a vital power utility within the critical infrastructure of a Southern African nation. Simultaneously, a healthcare-related incident involving DroxiDat came to light, accompanied by the malicious launch of Nokoyawa ransomware.

#2

Notably, several additional incidents connected to CobaltStrike unfolded, all united by the same license_id, staging directories, and C2 (Command and Control) infrastructure. This iteration of DroxiDat represents a novel rendition of the SystemBC payload, which has previously been employed in cyberattacks. The aforementioned attack transpired during the third and fourth weeks of March 2023.

#3

SystemBC, at times, referred to as Coroxy, is a proxy-oriented malware that utilizes the SOCKS5 protocol. The notably streamlined nature of this particular DroxiDat variant sets it apart from its predecessors within the SystemBC lineage. The records of identified SystemBC artifacts date back to at least 2018, with their quantity numbering in the thousands. These artifacts have been utilized by an extensive array of ransomware affiliates.

#4

One of the prominent strengths of DroxiDat resides in its ability to simultaneously target multiple objectives, automating tasks and enabling the hands-off execution of ransomware through native Windows utilities, assuming the attackers successfully acquire the necessary credentials.

Recommendations

Adopt a zero-trust architecture that advocates the elimination of implicit trust throughout the organization.

Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Configure network infrastructure devices such as firewalls and routers with strict security specifications. Use application whitelisting or control mechanisms to only allow authorized applications to run on systems. This effectively prevents the execution of unauthorized executables, such as the DroxiDat variants.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	T1033 System Owner/User Discovery	T1059 Command and Scripting Interpreter	T1021 Remote Services
T1127 Trusted Developer Utilities Proxy Execution	T1027 Obfuscated Files or Information	T1112 Modify Registry	T1564.003 Hidden Window
T1087 Account Discovery	T1071 Application Layer Protocol	T1573 Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	be9e23e56c4a25a8ea453c093714eed5e36c66d0, f98b32755cbfa063a868c64bd761486f7d5240cc, fd9016c64aea037465ce045d998c1eead3971d35
MD5	1957deed26c7f157cedcbdae3c565cff, 8d582a14279920af10d37eae3ff2b705, 19567b140ae6f266bac6d1ba70459fbd
Domains	powersupportplan[.]com, epowersoftware[.]com

TYPE	VALUE
SHA256	926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732, a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e, a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4
IPv4	93.115.25[.]41, 179.60.146[.]6, 194.165.16[.]63
File Paths	C:\perflogs\syscheck.exe, C:\perflogs\a.dll, C:\perflogs\hos.exe, C:\perflogs\host.exe, C:\perflogs\hostt.exe, C:\perflogs\svch.dll, C:\perflogs\svchoct.dll, C:\perflogs\admin\svcpost.dll, C:\perflogs\admin\syscheck.exe, C:\perflogs\sk64.dll, C:\perflogs\clinic.exe

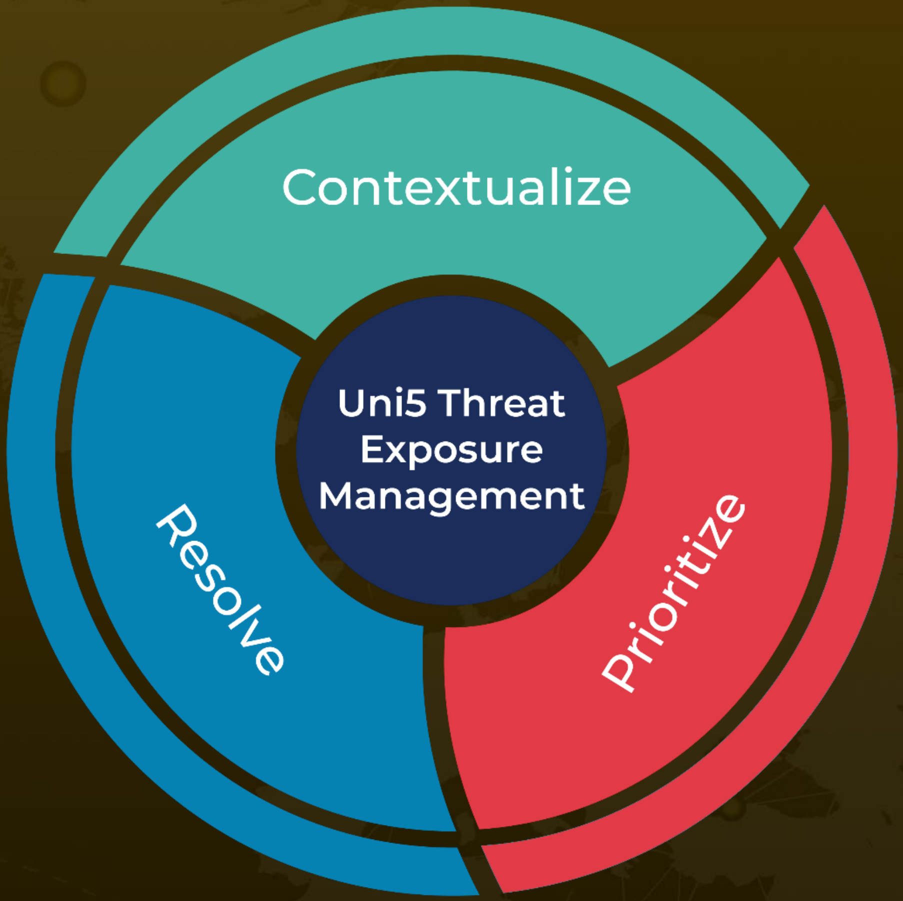
References

https://securelist.com/focus-on-droxidat-systembc/110302/

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

August 11, 2023 • 6:00 AM

More at www.hivepro.com