Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

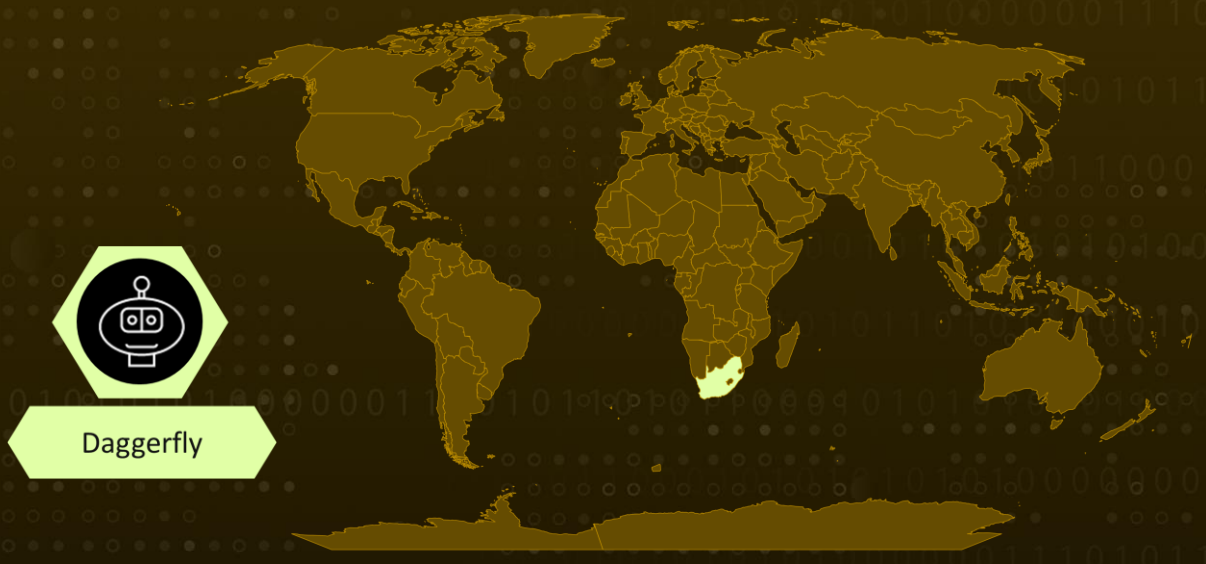
Daggerfly APT Deploys MgBot to Target African Telecoms Organization

Date of Publication	Admiralty Code	TA Number
April 26, 2023	A1	TA2023200

Summary

Attack Began: November 2022
Threat Actor: Daggerfly(Bronze Highland, Evasive Panda)
Attack Country: South Africa
Attack Indutry: Telecommunication
Malware: MgBot
Attack: The Daggerfly advanced persistent threat group has been observed using previously unseen plugins from the MgBot malware framework in a recent campaign, which is believed to have targeted a telecommunications organization in Africa and is linked to their previous activity in 2020 by shared tactics, techniques, and procedures.

Attack Regions



Attack Details

#1

The Daggerfly advanced persistent threat (APT) group, also known as Evasive Panda and Bronze Highland, has been spotted in a recent campaign using previously unseen plugins from the MgBot malware framework. They targeted a telecommunications organization in Africa and the campaign is believed to have started in November 2022. To gain access to the targeted systems, the group used the legitimate AnyDesk remote desktop software and side-loaded the PlugX loader onto victim machines with the help of Rising antivirus software. This activity is linked to Daggerfly, partly due to similarities with a 2020 activity blog attributed to Evasive Panda by Malwarebytes.

#2

The latest campaign and the one from 2020 both involved a renamed Rundll32.exe file and the loader DLL "pMsrvd.dll". The file and folder names used in the most recent activity also support this attribution. Suspicious activity on the victim network was first detected in November 2022, with AnyDesk connections spotted on a Microsoft Exchange mail server. The WannaMine crypto-mining malware was also seen on the same server. The attackers used living-off-the-land tools BITSAdmin and PowerShell to download files onto victim systems and credential dumping tools to retrieve usernames and passwords from web services stored in the credential manager using PowerShell.

Recommendations

Employ strict access control measures: To prevent the Daggerfly APT group from gaining unauthorized access to critical systems and sensitive information, implement strict access control measures such as multi-factor authentication, strong password policies, and role-based access control.

Use threat intelligence: Keep up-to-date with the latest threat intelligence to identify potential attacks and respond quickly to any suspicious activity. Use this information to monitor for activity associated with Daggerfly APT group and other known threat actors.

Conduct regular security awareness training: Employees should be regularly trained on how to identify and respond to phishing attacks, social engineering tactics, and other common techniques used by threat actors like Daggerfly. This training should emphasize the importance of maintaining good security hygiene practices and reporting any suspicious activity.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	T1012 Query Registry	T1016 System Network Configuration Discovery
T1018 Remote System Discovery	T1027 Obfuscated Files or Information	T1027.005 Indicator Removal from Tools	T1036 Masquerading
T1055 Process Injection	T1056 Input Capture	T1056.001 Keylogging	T1057 Process Discovery
T1070 Indicator Removal	T1070.004 File Deletion	T1070.006 Timestomp	T1082 System Information Discovery
T1083 File and Directory Discovery	T1106 Native API	T1112 Modify Registry	T1125 Video Capture
T1129 Shared Modules	T1497 Virtualization/Sandbox Evasion		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab 90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe 706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36 017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7 cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a

TYPE	VALUE
SHA256	54198678b98c2094e74159d7456dd74d12ab4244e1d9376d8f4d864f6237cd79 d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934 cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5 2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc a16a70b0a1ac0718149a31c780edb126379a0d375d9f6007a6def3141bec6810 0bcdcc0515d30c28017fd7931b8a787feebe9ee3819aa2b758ce915b8ba40f99 c31b409b1fe9b6387b03f7aedeafd3721b4ec6d6011da671df49e241394da154 db489e9760da2ed362476c4e0e9ddd6e275a84391542a6966dbcda0261b3f30a 632cd9067fb32ac8fbbe93eb134e58bd99601c8690f97ca53e8e17dda5d44e0e c1e91a5f9cc23f3626326dab2dcdf4904e6f8a332e2bce8b9a0854b371c2b350 5a0976fef89e32ddcf62c790f9bb4c174a79004e627c3521604f46bf5cc7bea2 7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453 3f75818e2e43a744980254bfdc1225e7743689b378081c560e824a36e0e0a195 1b8500e27edc87464b8e5786dc8c2beed9a8c6e58b82e50280cebb7f233bcde4 03bc62bd9a681bdcb85db33a08b6f2b41f853de84aa237ae7216432a6f8f817e ae39ced76c78e7c2043b813718e3cd610e1a8adac1f9ad5e69cf06bd6e38a5bd f6f6152db941a03e1f45d52ab55a2e3d774015ccb882853365 4e3f3161cfcd21 2f4a97dc70f06e0235796fec6393579999c224e144adcff908e0c681c123a8a2 22069984cba22be84fe33a886d989b683de6eb09f001670dbd8c1b605460d454 7b945fb1bdeb27a35fab7c2e0f5f45e0e64df7821dd1417a77922c9b08acfdc3 e8be3e40f79981a1c29c15992da116ea969ab5a15dc514479871a50b20b10158 b5c46c2604e29e24c6eb373a7287d919da5c18c04572021f20b8e1966b86d585 53d2506723f4d69afca33e90142833b132ed11dd0766192a087cb206840f3692

TYPE	VALUE
SHA256	26d129aaa4f0f830a7a20fe6317ee4a254b9caac52730b6fed6c482be4a5c79d b45355c8b84b57ae015ad0aebfa8707be3f33e12731f7f8c282c8ee51f962292 17dce65529069529bcb5ced04721d641bf6d7a7ac61d43aaf1bca2f6e08ead56 98b6992749819d0a34a196768c6c0d43b100ef754194308eae6aaa90352e2c13 6d5be3e6939a7c86280044eebe71c566b48981a3341193aa3aff634a3a5d1bbd 1cf04c3e8349171d907b911bc2a23bdb544d88e2f9b8fcc516d8bcf68168aede 2dcf9e556332da2a17a44dfceda5e2421c88168aafea73e2811d65e9521c715c a6ed16244a5b965f0e0b84b21dcc6f51ad1e413dc2ad243a6f5853cd9ac8da0b ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024 585db6ab2f7b452091ddb29de519485027665335afcdb34957ff1425ecc3ec4b 29df6c3f7d13b259b3bc5d56f2cdd14782021fc5f9597a3ccece51ffac2010a0 ea2be3d0217a2efeb06c93e32f489a457bdea154fb4a900f26bef83e2053f4fd

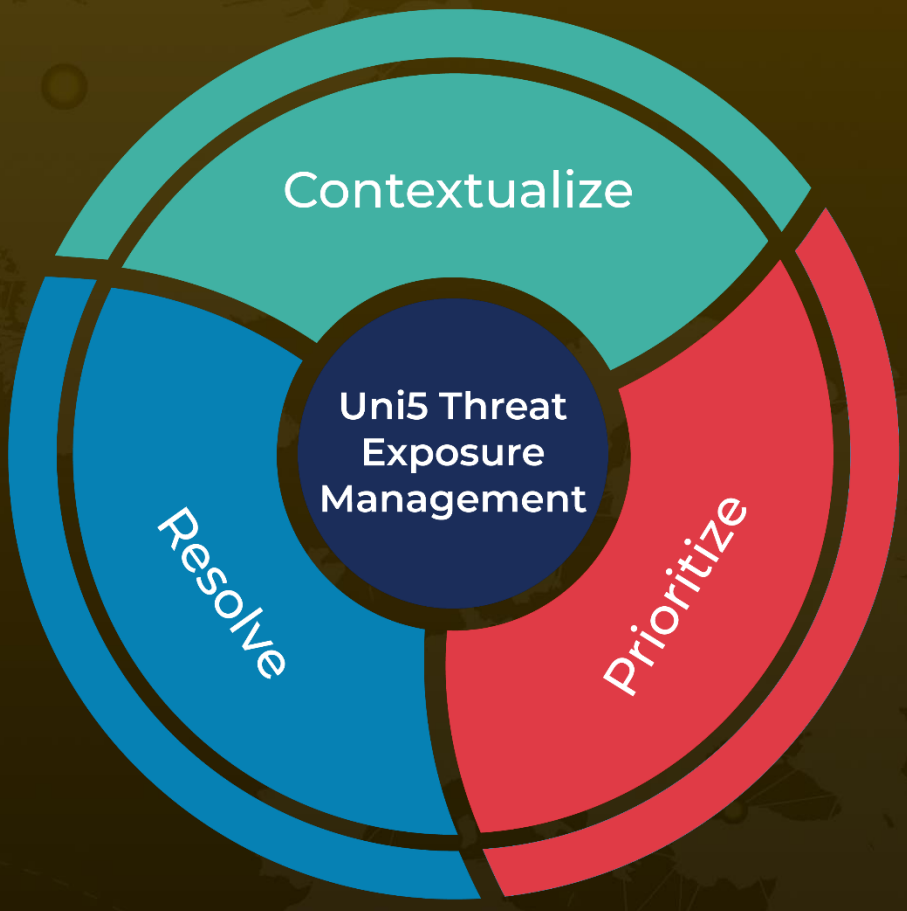
References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot

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

April 26, 2023 • 7:30 AM

More at www.hivepro.com