Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

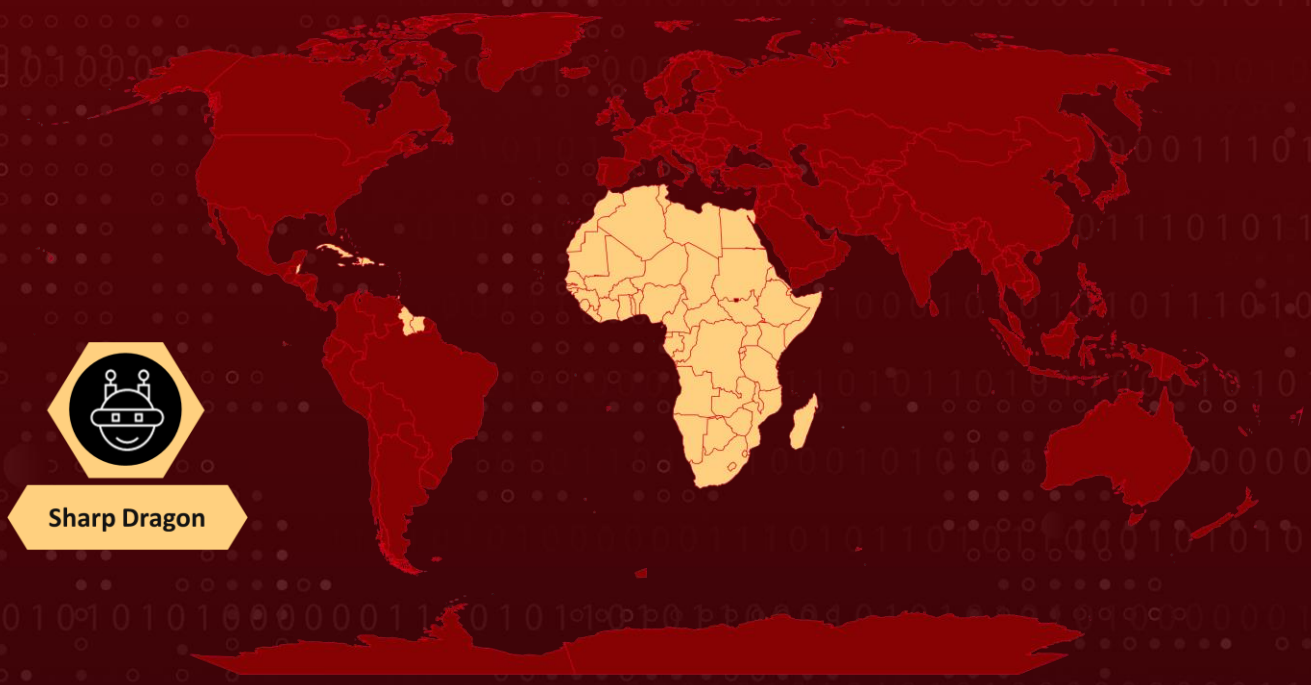
Sharp Dragon's Foray into African and Caribbean Governance Networks

Date of Publication	Admiralty Code	TA Number
May 24, 2024	A2	TA2024205

Summary

Attack Commenced: November 2023
Threat Actor: Sharp Dragon
Malware: 5.t Downloader
Attack Region: Africa and the Caribbean
Targeted Industry: Government
Attack: The China-linked threat actor Sharp Dragon, previously known as Sharp Panda, has expanded its cyber espionage campaign to target governmental organizations in Africa and the Caribbean.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-0669	Fortra GoAnywhere MFT Remote Code Execution Vulnerability	Fortra GoAnywhere MFT	✓	✓	✓

Attack Details

#1 The China-linked threat actor known as Sharp Dragon, formerly referred to as Sharp Panda, has broadened its focus to include governmental organizations in Africa and the Caribbean as part of an ongoing cyber espionage campaign.

#2 Sharp Dragon is notorious for deploying extensive phishing attacks, malicious RTF files, DLL loaders, and more recently, executable loaders disguised as documents. The group has also been reported to exploit the CVE-2023-0669 RCE vulnerability affecting Fortra GoAnywhere in their attacks.

#3 Although the final payloads deployed by Sharp Dragon operators have evolved over time, their primary modus operandi remains information theft and espionage. In recent months, Sharp Dragon compromised a high-profile email account. Additionally, Sharp Dragon has transitioned away from dedicated servers and begun utilizing compromised servers as command and control (C&C) servers.

#4 Instead of relying solely on disseminating phishing Word documents that leverage a remote template weaponized via RoyalRoad, they started using executables disguised as documents to drop a downloader named 5.t.

#5 The 5.t downloader is responsible for conducting reconnaissance and launching Cobalt Strike Beacon over custom backdoors, enabling the attackers to gather intelligence about the target environment. Sharp Dragon's strategic pivot towards Africa and the Caribbean indicates a broader initiative by Chinese cyber actors to enhance their presence and influence in these regions.

Recommendations

Regular Vulnerability Assessments: Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses in government networks and systems. Proactive measures can help prevent the exploitation of known vulnerabilities by threat actors like Sharp Dragon.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Network Segmentation: Implement network segmentation to isolate critical systems and sensitive data from less secure areas of your network. This can help contain the spread of malware.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0043 Reconnaissance
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1036 Masquerading	T1012 Query Registry
T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1001 Data Obfuscation	T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer
T1573 Encrypted Channel	T1053 Scheduled Task/Job	T1588.001 Malware	T1588.002 Tool
T1588.006 Vulnerabilities	T1566 Phishing	T1203 Exploitation for Client Execution	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	da78602c2a4490d445706f8f111daba9519fece8
SHA256	6783545b9fa8dd14890644c166a35f3cee78329f9522c6ee53149698e5889695, cd737ac8d66a47d341dd4a3c98ab0d2c77c7558d9a0161f7d08a4ab310d440ba,

TYPE	VALUE
SHA256	57b64a1ef1b04819ca9473e1bb74e1cf4be76b89b144e030dc1ef48f446ff95b, 2faf9615227728b2e7b9cfc548d4210452adc08b3ec500c1b46f2e04fa165816, 0373ef0a7874bd8506dc64dd82ef2c6d7661a3250c8a9bb8cb8cb75a7330c1d2, bff674439ea8333b227f6d05caa05b2e3fe592825abd63272d4f1e4c2dfa88ea, 362b9f497fce52a3f14ad9de2a027d974cc810473c929fed7c37526d2f13f83a, 180f5a0f9210698b54dcafb9a230b12e3eaf199889e5377a2acb7124c2d48d69, c1e403dd787f197f928960c723866424e343789a0422dbe8c98ed2214500d151, ff35cfed656c0cac5571beae7170a2fec007e75417c1d0c4fd7af4185759ec38, 9885b220b9654ac4743fe907e67da38d723fee2abf2dcd5944aa3a00c4a59c31, 708722bafe35a9fdc94ac33b1970776c464f1bb4e9c2ea1c1dba3a9e1ba03ab3, 21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6, 7575ebdd90aa0ab66c4eeaecd628c475e406ac9bcc54de5e01a3d372a050aec7, b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab339214f4e57, 42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc, 941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbca23e209, e848355359de1e59901aa387f2d208889c368663438909fd3bb0a97566de2b2d, cc805511e106a9b5302a4db4bfbb98609aca3dcbd2f709aee8ae316f479dfd49, ea72011929dece4684a2dcb5b76f34cef437dbe50306f19c531d632bf26e7f32, 7b21b95c4256308e8089bff38d5d20845f2dc28fa9e536de979ceab9b7962afa, e6faf05234ceaaba3bdcca60285a7ba83eea229a0ca241e94fb314a73ad98d87, 20a4256443957fbae69c7c666ae025522533b849e01680287177110603a83a41, 1c2a10f282f1a24d88c74d8d324fb59b172cee4ee2e3e3996d9a62ba979812a6, 8e72c9517b0220f8ed6973cfc36f478fc7837fe536c5859554661bc1e7ee4254,

TYPE	VALUE
SHA256	59a9d10eba81d62337f38d8f72a15f283e1f4bc9daa99fe0c08f780f3e4da839, 1db1cf2df0551762eaef0a92923da2f3d032663fdcb331d9474f5398b8ae4398, 04f7ae8042e0ed457dd6b86d6e8a40bd361357724b38d3aac7358f5e643299c6, 2c7e52eb8290d76780b6ac15a134b58a74c95bc616fd0d91a3f9514409a12846
IPv4	103[.]146[.]78[.]152, 185[.]239[.]226[.]91, 38[.]54[.]96[.]97, 38[.]54[.]50[.]182, 45[.]76[.]193[.]171, 45[.]251[.]241[.]12, 103[.]56[.]17[.]192
Domains	schemas.openxmlformats[.]shop, dueog[.]xyz
URLs	hxxp[:]//13[.]236[.]189[.]80[:]8000/res/translate[.]res, hxxps[:]//13[.]236[.]189[.]80[:]8001/G0AnyWhere_up[.]jsp?Data=, hxxp[:]//52[.]236[.]140[.]86[:]8000/res/translation[.]res, hxxps[:]//52[.]236[.]140[.]86[:]8001/G0AnyWhere_up[.]jsp?Data= hxxps[:]//<c2, addres>/ajax/libs/json2/20160511/json_parse_state[.]js
Mutex	mt_app_http_get_zed2vsp
File Paths	D:\Project\0_new_plain\0_start\01_XXX_64bit\01_XXX\x64\Release\01_XXX.pdb, D:\project\downloader\dll_rls\downloader.pdb

Patch Details

Upgrade to the version, 7.1.2. or later.
Fortra users require an active account to log in and access the patch.

Link:
https://my.goanywhere.com/webclient/Login.xhtml

References

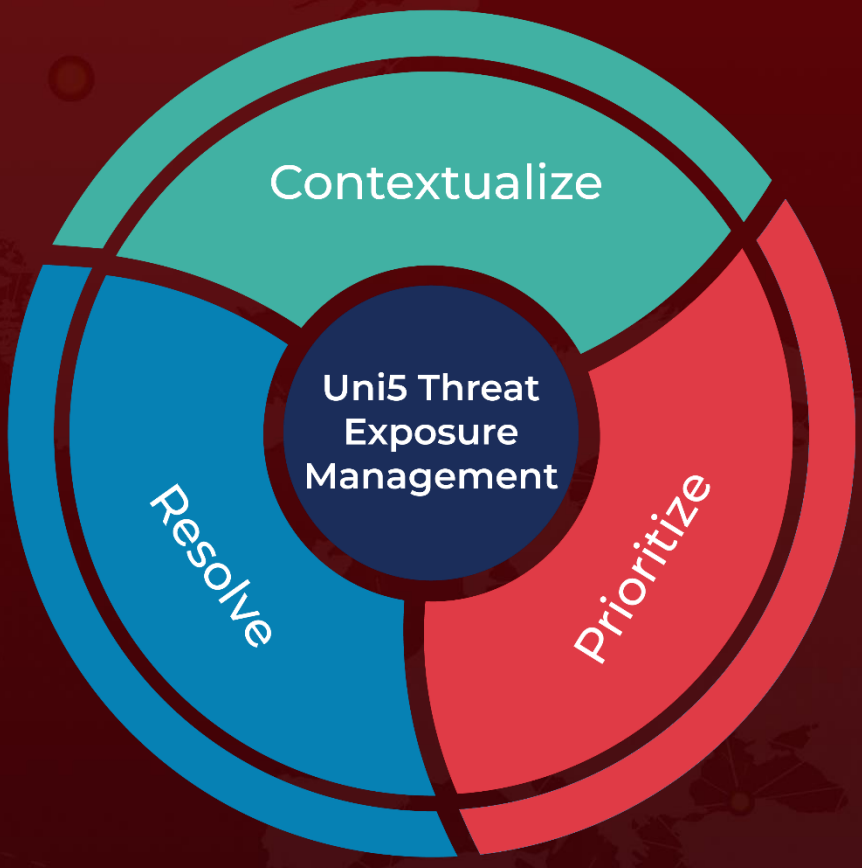
https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/

https://www.hivepro.com/threat-advisory/sharp-panda-a-sophisticated-cyber-espionage-campaign-targeting-governments/

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

May 24, 2024 • 4:30 AM

© 2024 All Rights are Reserved by HivePro

More at www.hivepro.com