KPMG Cyber Threat Intelligence Platform

Sharp Dragon – Setting Ablaze Government Organizations

TLP : Clear

KPMG. Make the Difference.

Sharp Dragon, previously known as Sharp Panda, is a Chinese threat actor identified in 2021. They have consistently used highly targeted phishing emails to deploy VictoryDLL or the Soul framework. Initially focused on Southeast Asia, they have recently expanded their targets to include high-level officials and government entities in Africa and the Caribbean, consistent with their modus operandi but showing a significant evolution in their operations.

Initial access is achieved by phishing email containing a malicious attachment that appears to be a legitimate document. Previously, they relied on weaponized RTF files utilizing the RoyalRoad exploit, but they have shifted towards executable files in recent campaigns. Upon opening the executable file, it initiates the download and executes the “5.t DLL loader”. A scheduled task is created to maintain persistence on the infected system, allowing it to run malicious programs at set times or intervals. The 5.t downloader scans the infected system to gather details about the operating system and running processes, identifying valuable targets for exploitation. Sharp Dragon exploits vulnerabilities (CVE-2023-0669) in the GoAnywhere platform, to facilitate command injection and privilege escalation. The use of obfuscated executables and dynamic payloads, such as Cobalt Strike Beacon, helps evade detection by security tools and blends in with legitimate traffic to communicate with the C2 server. The 5.t downloader retrieves and installs additional malicious files, including custom tools, from remote systems to enhance attack capabilities. Stolen data from compromised machines is secretly transmitted to a disguised URL masquerading as a legitimate GoAnywhere service, effectively concealing their activities.

Sharp Dragon’s highly targeted and cautious approach makes it easy for government organizations to fall prey to their tactics, highlighting the urgent need for cyber resilience and awareness.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Sharp Dragon – Setting Ablaze Government Organizations

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
38.54.96[.]97	45.91.225[.]139
38.54.50[.]182	45.121.146[.]88
45.76.193[.]171	185.239.226[.]91
45.251.241[.]12	107.148.165[.]151
103.56.17[.]192	

Indicators of Compromise: Domains	
dueog[.]xyz	schemas.openxmlformats[.]shop

Indicators of Compromise: Hashes
09bf850be5da44a1c3629a1f62813a83
7e168e58f27d5cc684c5b45cb1551f46
92d994be99ea43c121ac4f4ddfacbf75
9b99f9fe7fa43f391eda1dfef1a0c3a6
ea889308acb4249af92807cc7d70f084
37e8ba415702f9f24e497bf6111e3e0c
b85316f68d9f1dbac481e3f397ebf1b0
f3acc63df9f08e217077b0acc690d539
36a3128df1ecf7c3640f76603443f8f6
cb646e35c7a262e8d22ca721a37b2202
d60e2aadaabdbb59c01128d54f4d3cef
70b27d5f201519d0d9d28f4274e8fe80
4c4f89b9a64dce3dd39695b0356eb285
35b0dfbcc269e403aaae48d562327475
ea176a4e93f1ed89c3e493572955cf00
c5f9630e7e82b6461f15ac3567777d7e

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Sharp Dragon – Setting Ablaze Government Organizations

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
c06350a11011e2acff1a64784ee292d8
e1ebf9e6f772ca35bf44311f504715cc
dde388e83c6c85fde975f1246eb1635f
1e9f1746c2dbea0df5017afdf8b94189
d598749a8c86b1cdd313ff6c86626c86
d843b58f31c687d22de09a6765b3ba3b
e5b228d75b3b8796e1a6efeeb6ee9277f6816db9
a4e89d1f060e4dfd5f0fd4e7ba8be96967b39ac7
659b8a50bc4d381c95bdbd4b977700f9fcd8e52c
f14afd2856dab6183150f6e269f5bb6f4a2e3f50
474d3238f78fcdb4f41a429786961938586a132c
92c8f9ea9b6555e1b9c42cd7302f7caf62eb83e6
1e002159ac17ba3380053107862a19b72c8a1c1e
0bdba9af734c7b54f730a237ec20660cd539fcca
6a37c533b9ff57bb50157d243ba6b373fc13392a
f7bd869acf142d8654b50c6132b82331805d8f05
cc165ef3f4e309d810a726571657ebfe44708d6e
0a588f02e60de547969d000968a458dcdc341312
01e1913b1471e7a1d332bfc8b1e54b88350cb8ad
03a57262a2f3563cf0faef5cde5656da437d58ce
388b7130700dcc45a052b8cd447d1eb76c9c2c54
fefec06620f2ef48f24b2106a246813c1b5258f4
548bbf4b79eb5a173741e43aa4ba17b92be8ed3a
278c4fc89f8e921bc6c7d015e3445a1cc6319a66
42be0232970d5274c5278de77d172b7594ff6755
da78602c2a4490d445706f8f111daba9519fece8

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Sharp Dragon – Setting Ablaze Government Organizations

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6
b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab339214f4e57
180f5a0f9210698b54dcafb9a230b12e3eaf199889e5377a2acb7124c2d48d69
59a9d10eba81d62337f38d8f72a15f283e1f4bc9daa99fe0c08f780f3e4da839
57b64a1ef1b04819ca9473e1bb74e1cf4be76b89b144e030dc1ef48f446ff95b
0373ef0a7874bd8506dc64dd82ef2c6d7661a3250c8a9bb8cb8cb75a7330c1d2
2faf9615227728b2e7b9cfc548d4210452adc08b3ec500c1b46f2e04fa165816
362b9f497fce52a3f14ad9de2a027d974cc810473c929fed7c37526d2f13f83a
42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc
20a4256443957fbae69c7c666ae025522533b849e01680287177110603a83a41
bff674439ea8333b227f6d05caa05b2e3fe592825abd63272d4f1e4c2dfa88ea
c1e403dd787f197f928960c723866424e343789a0422dbe8c98ed2214500d151
cc805511e106a9b5302a4db4bfbb98609aca3dcbd2f709aee8ae316f479dfd49
cd737ac8d66a47d341dd4a3c98ab0d2c77c7558d9a0161f7d08a4ab310d440ba
e6faf05234ceaaba3bdcca60285a7ba83eea229a0ca241e94fb314a73ad98d87
e848355359de1e59901aa387f2d208889c368663438909fd3bb0a97566de2b2d
ea72011929dece4684a2dcb5b76f34cef437dbe50306f19c531d632bf26e7f32
ff35cfed656c0cac5571beae7170a2fec007e75417c1d0c4fd7af4185759ec38
6783545b9fa8dd14890644c166a35f3cee78329f9522c6ee53149698e5889695
708722bafe35a9fdc94ac33b1970776c464f1bb4e9c2ea1c1dba3a9e1ba03ab3
7575ebdd90aa0ab66c4eeaecd628c475e406ac9bcc54de5e01a3d372a050aec7
7b21b95c4256308e8089bff38d5d20845f2dc28fa9e536de979ceab9b7962afa
8e72c9517b0220f8ed6973cfc36f478fc7837fe536c5859554661bc1e7ee4254
941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbca23e209
9885b220b9654ac4743fe907e67da38d723fee2abf2dcd5944aa3a00c4a59c31
1c2a10f282f1a24d88c74d8d324fb59b172cee4ee2e3e3996d9a62ba979812a6

KPMG

KPMG Cyber Threat Intelligence Platform

Sharp Dragon – Setting Ablaze Government Organizations

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
2faf9615227728b2e7b9cfc548d4210452adc08b3ec500c1b46f2e04fa165816
0373ef0a7874bd8506dc64dd82ef2c6d7661a3250c8a9bb8cb8cb75a7330c1d2
bff674439ea8333b227f6d05caa05b2e3fe592825abd63272d4f1e4c2dfa88ea
362b9f497fce52a3f14ad9de2a027d974cc810473c929fed7c37526d2f13f83a
708722bafe35a9fdc94ac33b1970776c464f1bb4e9c2ea1c1dba3a9e1ba03ab3
42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc
941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbca23e209
1db1cf2df0551762eaef0a92923da2f3d032663fdcb331d9474f5398b8ae4398
04f7ae8042e0ed457dd6b86d6e8a40bd361357724b38d3aac7358f5e643299c6
2c7e52eb8290d76780b6ac15a134b58a74c95bc616fd0d91a3f9514409a12846
928f540c9658a458edc649371e178a7c83e2a9291f5b23ae326c3d64bfa902c6
4cc521b470d08c9684cd15ffac032accd50439b81873ee2d87897ab8c495744b
0e8fb748cd58ab2fa754e2fa16e4390327a10593ca72bb6a3b90a1885cbe5387
2d18300d1e8f56c340ed4d4b04e2dcbd6f3eb63436e9f95f2c2c07673a7647f9
674238469f6efd8a284c62df33d44734459dc66e7b0c223fd6a2fed97bc1c3a9
15d011ecee762c383f81930dad741426993910fd9939de1742f786a5aea2ba50
a13b6aa6882e82860ff7b10ab6fe1a3d259aa63e9ed97239572a9a2ba16bc791
b40476638c83b8800413cf1fe88e28c2486367b79d1ddae7eb1ddcfa75ceb0e3
e1105e0aea484f5a3b37ff5143ba2d7be9d1eb17ef1da5c4725be0c415513289
ec7237bc31b59204bd543b76677cd16007237cab6fbf22e266e1e3361849a4ba
0f7ff0a977d69421f1e06b5a44b5bdaeab2b15ee768127d200c1b5cc366e0968
5732cefa7ac96b2aa76ccd5849bbc1e47cb3e76c0d44f8491c47b1b1793604b4
0752c24ded7cc434a56fdd10c4f2c45144ca53252192e21cfa4cee3a5ad68796
d198c4d82eba42cc3ae512e4a1d4ce85ed92f3e5fdff5c248acd7b32bd46dc75
0c346972a2ccebb2642ced34213f43595896da233f06f6251967517ae342908f
6f66faf278b5e78992362060d6375dcc2006bcee29ccc19347db27a250f81bcd