Sharp Dragon Expands Towards Africa and The Caribbean

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

May 23, 2024

Key Findings

- Sharp Dragon's (Formerly referred to as Sharp Panda) operations continue, expanding their focus now to new regions – Africa and the Caribbean.
- Sharp Dragon, a Chinese threat actor, utilizes trusted government entities to infect new ones and establish initial footholds in new territories.
- The threat actors demonstrate increased caution in selecting their targets, broadening their reconnaissance efforts, and adopting Cobalt Strike Beacon over custom backdoors.
- Throughout their operation, Sharp Dragon exploited 1-day vulnerabilities to compromise infrastructure later used as Command and Control (C2) infrastructure.

Introduction

Since 2021, Check Point Research has been closely monitoring the activities of Sharp Dragon (Formerly referred to as Sharp Panda*), a Chinese threat actor. Historical activities mostly consist of highly-targeted phishing emails, previously leading to the deployment of VictoryDLL or Soul framework.

While the final payloads Sharp Dragon operators have deployed overtime changed, their modus operandi has been persistent, and more so, their targets, who have remained within the confines of South-East Asia in the years we were tracking them, up until recently.

In recent months, we have observed a significant shift in Sharp Dragon's activities and lures, now targeting governmental organizations in Africa and the Caribbean. Those activities very much align with known Sharp Dragon modus operandi, and were characterized by compromising a high-profile email account to spread a phishing word document that leverages a remote template weaponized using RoyalRoad. Unlike previous activities, those lures were used to deploy Cobalt Strike Beacon.

***** As part of an ongoing effort to avoid confusion with other vendors naming conventions, the name was changed.***

Inter-Government Relations as an Attack Vector

Starting November 2023, we observed Sharp Dragon's increased interest in governmental entities in Africa and the Caribbean. This interest manifested by directly targeting government organizations within the two regions, by exploiting previously compromised entities in Southeast Asia. Utilizing highly-tailored lures that deal with relations between countries in South-East Asia and the two regions, Sharp Dragon threat actors have established their first footholds in two new territories.

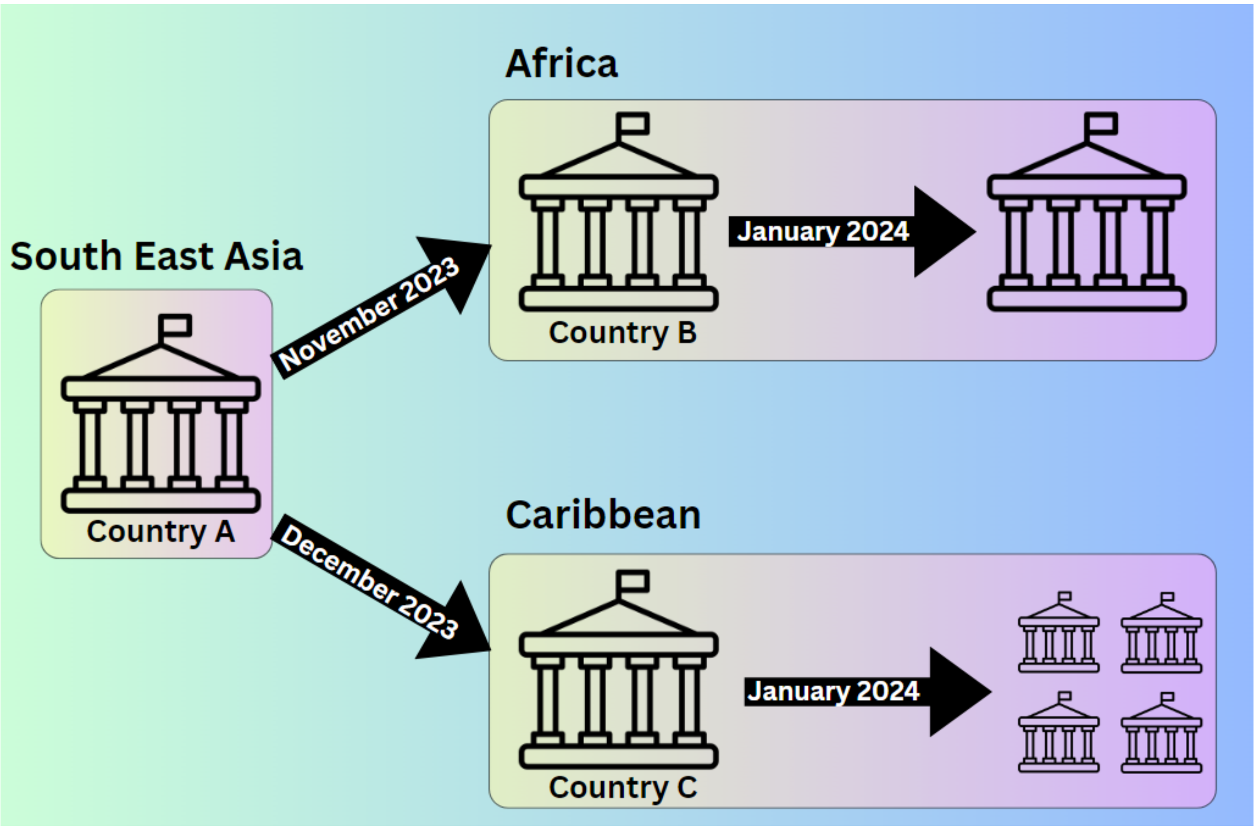
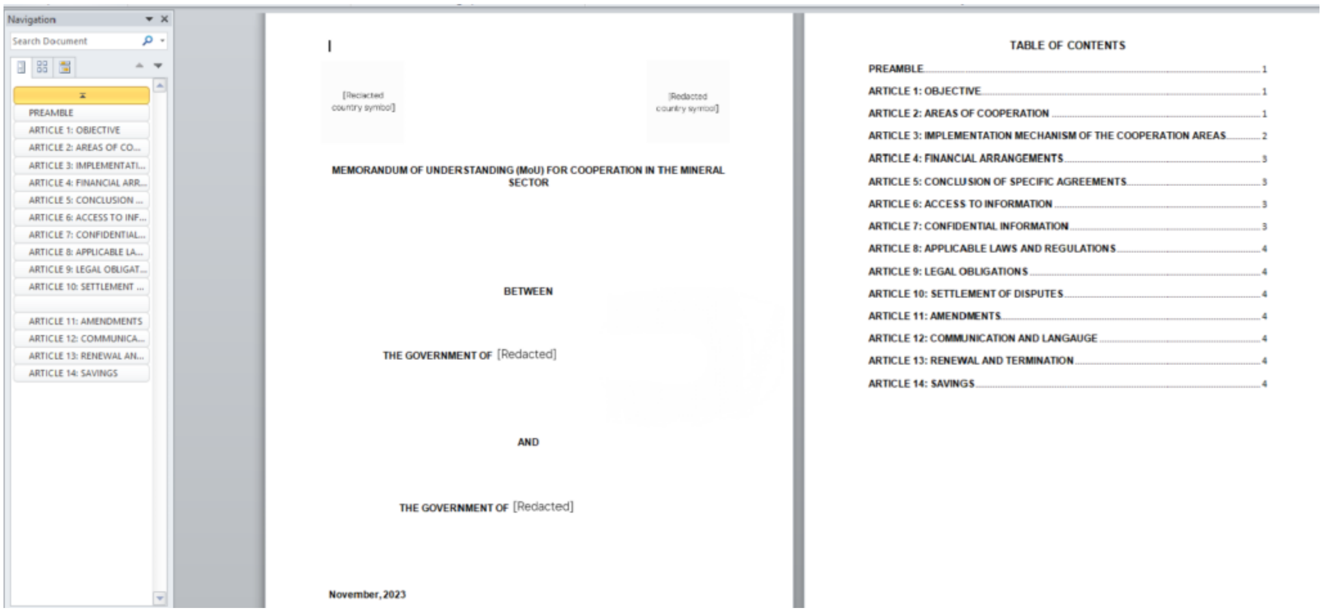


Figure 1- Sharp Dragon’s shift to target Africa and the Caribbean

Sharp Dragon’s Cyber Activities in Africa

The first identified phishing attack targeting Africa was sent out from **Country A (**South-East Asia) to **Country B** (Africa) in November of 2023, using a lure about industrial relations between countries in South-East Asia and Africa. The document is very thorough, and its contents were likely taken from an authentic correspondence between the two countries.


Navigation
Search Document
PREAMBLE
ARTICLE 1: OBJECTIVE
ARTICLE 2: AREAS OF CO...
ARTICLE 3: IMPLEMENTATI...
ARTICLE 4: FINANCIAL ARR...
ARTICLE 5: CONCLUSION ...
ARTICLE 6: ACCESS TO INF...
ARTICLE 7: CONFIDENTIAL...
ARTICLE 8: APPLICABLE LA...
ARTICLE 9: LEGAL OBLIGAT...
ARTICLE 10: SETTLEMENT ...
ARTICLE 11: AMENDMENTS
ARTICLE 12: COMMUNICA...
ARTICLE 13: RENEWAL AN...
ARTICLE 14: SAVINGS

[Redacted country symbol] [Redacted country symbol]

MEMORANDUM OF UNDERSTANDING (MoU) FOR COOPERATION IN THE MINERAL SECTOR

BETWEEN

THE GOVERNMENT OF [Redacted]

AND

THE GOVERNMENT OF [Redacted]

November, 2023

TABLE OF CONTENTS

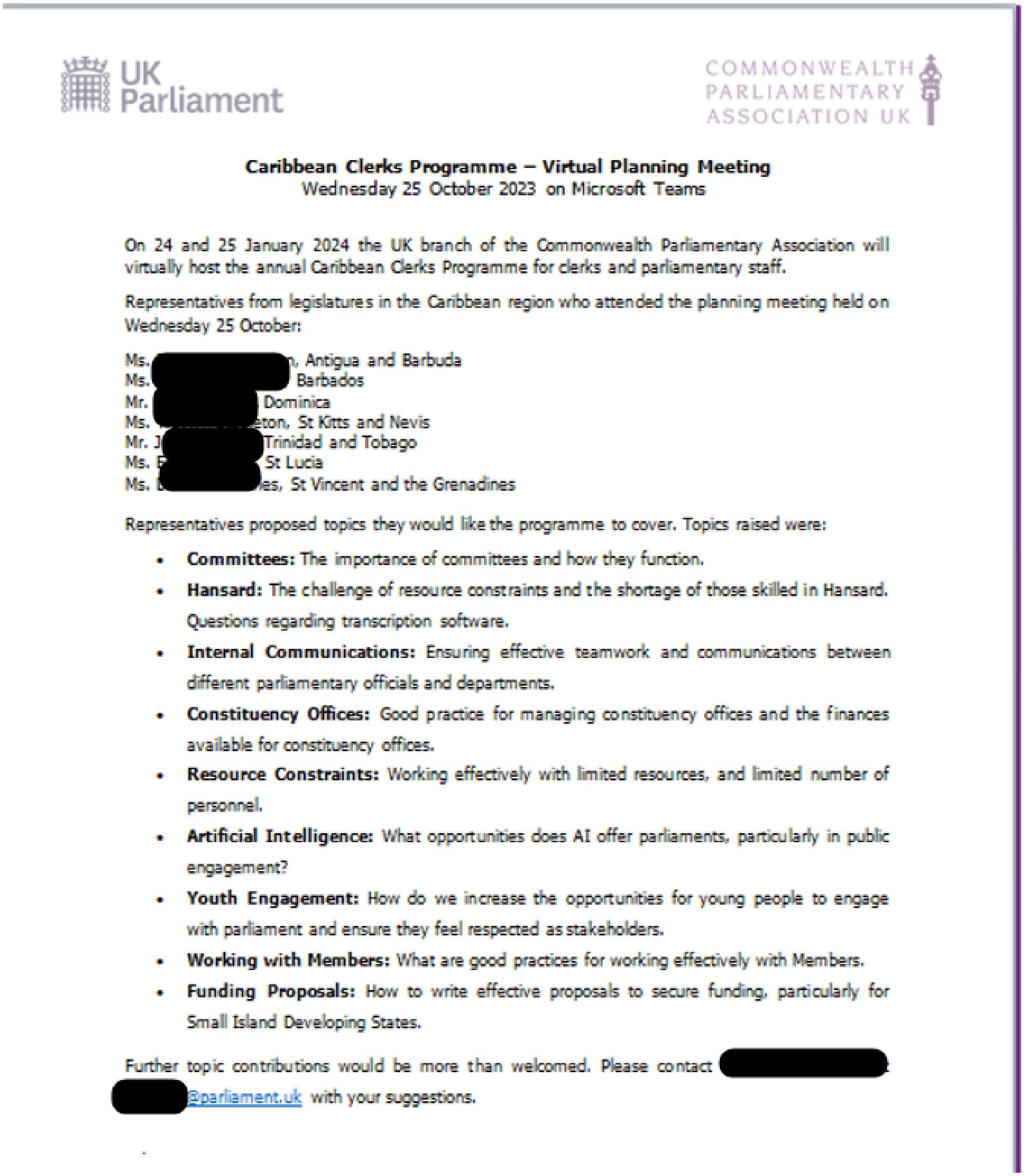
Figure 2 – Lure document targeting Country B in Africa

Following those lures, we’ve also observed direct targeting within Africa in January of 2024, originating from **Country B**, originally targeted in November, likely indicating some of the phishing attacks were successful.

Sharp Dragon’s interest in Africa does not come in a vacuum, as we’ve observed a set of Chinese affiliated threat actors targeting the region lately. This is also correlated with observations made by other vendors, who observe sustained tasking toward targeting in the region. It appears that Sharp Dragon’s activities are part of a larger effort carried out by Chinese threat actors.

Sharp Dragon’s Activity in the Caribbean

In a similar manner to Africa, Sharp Dragon’s operators have utilized their previous access to compromised governmental entities in South-East Asia **Country A** to target governmental organizations in **Country C,** which is in the Caribbean. The first set of identified malicious documents sent out from the compromised network was sent out in December of 2023 and used a Caribbean Commonwealth meeting lure, named “Caribbean Clerks Programme”. This lure was sent out to a Foreign Affairs ministry of **Country C**.



UK Parliament

COMMONWEALTH PARLIAMENTARY ASSOCIATION UK

Caribbean Clerks Programme – Virtual Planning Meeting
Wednesday 25 October 2023 on Microsoft Teams

On 24 and 25 January 2024 the UK branch of the Commonwealth Parliamentary Association will virtually host the annual Caribbean Clerks Programme for clerks and parliamentary staff.

Representatives from legislatures in the Caribbean region who attended the planning meeting held on Wednesday 25 October:

Ms. [redacted], Antigua and Barbuda
Ms. [redacted] Barbados
Mr. [redacted] Dominica
Ms. [redacted], St Kitts and Nevis
Mr. [redacted] Trinidad and Tobago
Ms. [redacted] St Lucia
Ms. [redacted], St Vincent and the Grenadines

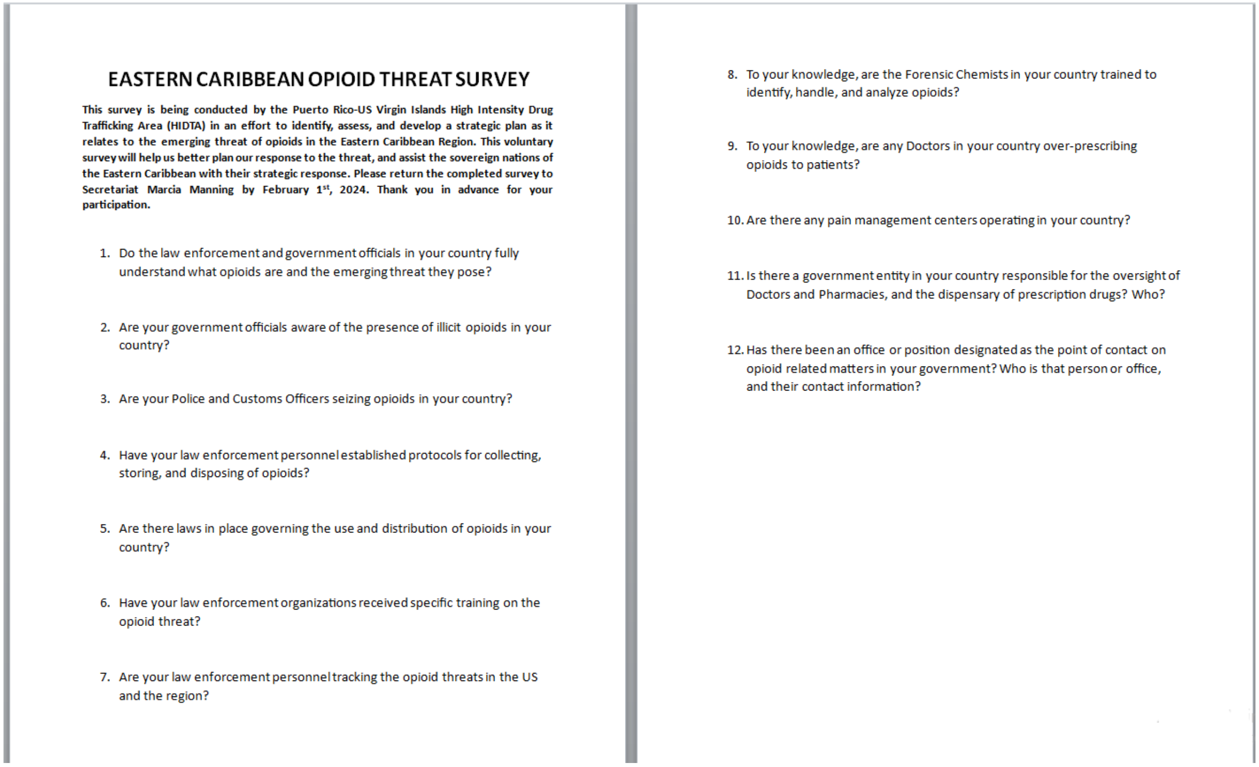
Representatives proposed topics they would like the programme to cover. Topics raised were:

- **Committees:** The importance of committees and how they function.
- **Hansard:** The challenge of resource constraints and the shortage of those skilled in Hansard. Questions regarding transcription software.
- **Internal Communications:** Ensuring effective teamwork and communications between different parliamentary officials and departments.
- **Constituency Offices:** Good practice for managing constituency offices and the finances available for constituency offices.
- **Resource Constraints:** Working effectively with limited resources, and limited number of personnel.
- **Artificial Intelligence:** What opportunities does AI offer parliaments, particularly in public engagement?
- **Youth Engagement:** How do we increase the opportunities for young people to engage with parliament and ensure they feel respected as stakeholders.
- **Working with Members:** What are good practices for working effectively with Members.
- **Funding Proposals:** How to write effective proposals to secure funding, particularly for Small Island Developing States.

Further topic contributions would be more than welcomed. Please contact [redacted] [redacted]@parliament.uk with your suggestions.

Figure 3 – Caribbean-themed lure sent to a Southeast Asian government.

Not long afterwards, in January of 2024, much like in Africa, **Country C** compromised governmental email infrastructure was used to send out a large-scale phishing campaign targeting a wide set of governments in the Caribbean, this time, using a lure of a legitimate –looking survey around the Opioid threat in the Eastern Caribbean.



EASTERN CARIBBEAN OPIOID THREAT SURVEY

This survey is being conducted by the Puerto Rico-US Virgin Islands High Intensity Drug Trafficking Area (HIDTA) in an effort to identify, assess, and develop a strategic plan as it relates to the emerging threat of opioids in the Eastern Caribbean Region. This voluntary survey will help us better plan our response to the threat, and assist the sovereign nations of the Eastern Caribbean with their strategic response. Please return the completed survey to Secretariat Marcia Manning by February 1st, 2024. Thank you in advance for your participation.

1. Do the law enforcement and government officials in your country fully understand what opioids are and the emerging threat they pose?
2. Are your government officials aware of the presence of illicit opioids in your country?
3. Are your Police and Customs Officers seizing opioids in your country?
4. Have your law enforcement personnel established protocols for collecting, storing, and disposing of opioids?
5. Are there laws in place governing the use and distribution of opioids in your country?
6. Have your law enforcement organizations received specific training on the opioid threat?
7. Are your law enforcement personnel tracking the opioid threats in the US and the region?
8. To your knowledge, are the Forensic Chemists in your country trained to identify, handle, and analyze opioids?
9. To your knowledge, are any Doctors in your country over-prescribing opioids to patients?
10. Are there any pain management centers operating in your country?
11. Is there a government entity in your country responsible for the oversight of Doctors and Pharmacies, and the dispensary of prescription drugs? Who?
12. Has there been an office or position designated as the point of contact on opioid related matters in your government? Who is that person or office, and their contact information?

Figure 4 – One of the lures sent to governmental entities in the Caribbean region

Technical Analysis

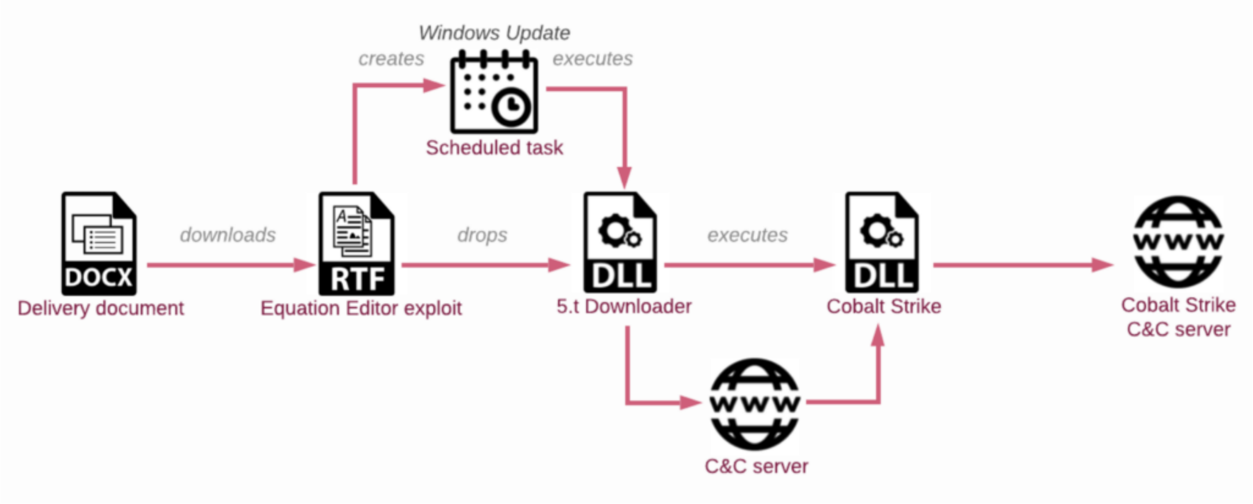


Figure 5 – Sharp Dragon's Infection chain since May 2023 campaign

In our ongoing efforts to track Sharp Dragon activities, we've identified various minor changes in their Tactics, Techniques, and Procedures (TTPs), while the core functionality remains consistent. Those changes reflect a more careful target selection and operational security (OPSEC) awareness. Among those changes are:

Wider Recon Collection

The 5.t downloader now conducts more thorough reconnaissance on target systems, this includes examining process lists and enumerating folders, leading to a more discerning selection of potential victims.

```
HTN:<hostname>
OSN:<os name>
OSV:<os version>
URN:<username>
ITF:NetworkCard:1 <Network card info> NetworkCard:2 <Network card info> ... ;
PGF:[Program Files]-><list of subfolders>|[Program Files (x86)]-><list of subfolders>
PSL:([System Process])<list of running processes>
```

Cobalt Strike Payload

Additionally, we observed a change in the delivered payload: if the machine is deemed attractive by the attackers, a payload is sent. When Check Point Research first exposed this operation in 2021, the payload was VictoryDll, a custom and unique malware enabling remote access and data collection from infected devices. Subsequently, as we continued tracking Sharp Dragon's operations, we observed the adoption of the SoulSearcher framework.

Presently, we are witnessing the use of Cobalt Strike Beacon as the payload of the 5.t downloader. This choice provides backdoor functionalities, such as C2 communication and command execution, without the risk of exposing their custom tools. However, we assume that the Cobalt Strike beacon serves as their primary tool for assessing the attacked environment, while their custom tools come into play at a later stage, which we have yet to witness. This refined approach indicates a deeper understanding of their targets and a desire to minimize exposure, likely resulting from public disclosures of their activities.

Cobalt Strike Configuration:

```
{
"config_type": "static",
"spawnto_x64": "%windir%\\sysnative\\Locator.exe",
"spawnto_x86": "%windir%\\syswow64\\Locator.exe",
"uses_cookies": "True",
"bstagecleanup": "True",
"crypto_scheme": 0,
"proxy_behavior": "Use IE settings",
"server,get-uri": "103.146.78.152,/ajax/libs/json2/20160511/json_parse_state.js",
"http_get_header": [
"Const_header Accept: application/*, image/*, text/html",
"Const_header Accept-Language: es",
"Const_header Accept-Encoding: compress, br",
"Build Metadata",
"XOR mask w/ random key",
"Base64 URL-safe decode",
"Prepend JV6_IB4QESMW4TOIQLJRX69Q7LPGNXW594C5=",
"Build End",
"Header Cookie"
]
}
```

EXE Loaders

Another notable change is observed in the 5.t downloaders: some of the latest samples deviate from the usual DLL-based loaders, incorporating EXE-based 5.t loader samples. While not all the latest samples have shifted to DLLs, this change underscores the dynamic nature of their evolving strategies.

Recently Sharp Dragon has also introduced another executable, altering the initial phase of the infection chain. Instead of relying on a Word document utilizing remote template to download an RTF file weaponized with RoyalRoad, they started using executables disguised as documents. This new method closely resembles the previous infection chain, as the executable writes 5.t DLL loader and executes it, while also creating a scheduled task for persistence.

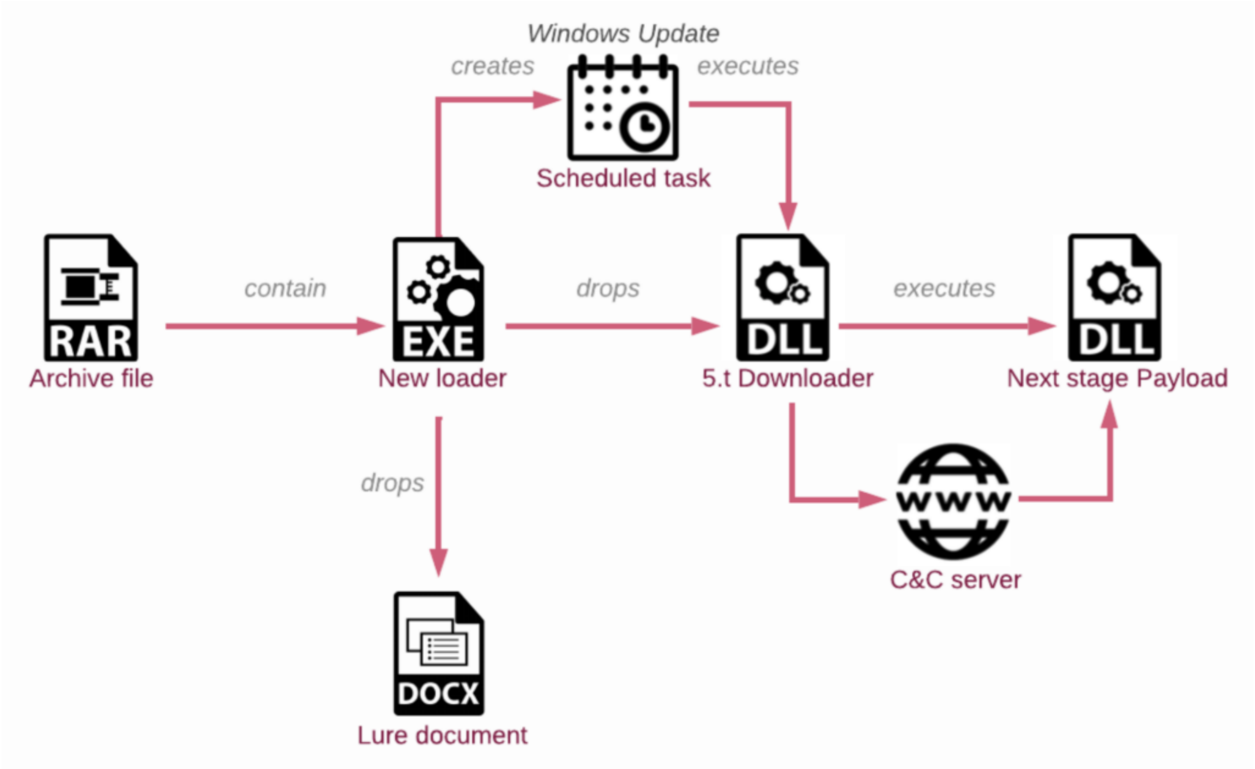


Figure 6 – Sharp Dragon's new infection chain

Compromised Infrastructure

Sharp Dragon not only utilized compromised government infrastructure to target other governments but also shifted from dedicated servers to using compromised servers as C&C servers. During a campaign conducted in May 2023, our team observed that certain servers used by Sharp Dragon as C2 were likely legitimate servers that were compromised. Our suspicion is that Sharp Dragon exploited the CVE-2023-0669 vulnerability, which is a flaw in the GoAnywhere platform allowing for pre-authentication command injection, this vulnerability was disclosed shortly before the incidents occurred.

The data collected from the affected machine was subsequently sent to the following address: `https://<C2_addres>:<port>/GOAnyWhere_up.jsp?Data=`. This address masquerades as belonging to the GoAnywhere service, a file transfer software.

Conclusion

This research highlights Sharp Dragon's strategic shift towards Africa and the Caribbean, suggesting its part in a broader effort carried out by Chinese cyber actors to enhance their presence and influence in these two regions. This move comes after a considerable period of activity in South-East Asia, which was leveraged by Sharp Dragon actors, to establish initial footholds in countries in Africa and the Caribbean.

These changes in Sharp Dragon's tactics, showing more careful selection of targets and the use of publicy and readily available tools, is an indication of a refined approach by this threat actor to target high-profile organizations. These findings bring attention to the evolving nature of Chinese threat actors, especially towards regions that have been somewhat overlooked in global cybersecurity and by the threat intelligence community.

Check Point Customers Remain Protected Against the Threats Described in this Report.

Harmony Endpoint provides comprehensive endpoint protection at the highest security level and protects with the following:

- Trojan.Win.SharpDragon.B
- Trojan.Win.SharpDragon.C

Threat Emulation:

- Trojan.Wins.Royalroad.ta.A
- APT.Wins.SharpPanda.*

Indicators of Compromise

Hashes:

Archives

- da78602c2a4490d445706f8f111daba9519fece8
- 6783545b9fa8dd14890644c166a35f3cee78329f9522c6ee53149698e5889695
- cd737ac8d66a47d341dd4a3c98ab0d2c77c7558d9a0161f7d08a4ab310d440ba

Docx

- 57b64a1ef1b04819ca9473e1bb74e1cf4be76b89b144e030dc1ef48f446ff95b
- 2faf9615227728b2e7b9cfc548d4210452adc08b3ec500c1b46f2e04fa165816
- 0373ef0a7874bd8506dc64dd82ef2c6d7661a3250c8a9bb8cb8cb75a7330c1d2
- bff674439ea8333b227f6d05caa05b2e3fe592825abd63272d4f1e4c2dfa88ea
- 362b9f497fce52a3f14ad9de2a027d974cc810473c929fed7c37526d2f13f83a

RTF

- 180f5a0f9210698b54dcafb9a230b12e3eaf199889e5377a2acb7124c2d48d69
- c1e403dd787f197f928960c723866424e343789a0422dbe8c98ed2214500d151
- ff35cfed656c0cac5571beae7170a2fec007e75417c1d0c4fd7af4185759ec38
- 9885b220b9654ac4743fe907e67da38d723fee2abf2dcd5944aa3a00c4a59c31
- 708722bafe35a9fdc94ac33b1970776c464f1bb4e9c2ea1c1dba3a9e1ba03ab3

- 9885b220b9654ac4743fe907e67da38d723fee2abf2dcd5944aa3a00c4a59c31

5.t loader DLL

- 21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6
- 7575ebdd90aa0ab66c4eeaecd628c475e406ac9bcc54de5e01a3d372a050aec7
- b952a459dac430d006a4d573612ca8474a410310792ea8141f9ab339214f4e57
- 42095521622c055db8d79441317952c0899c34d7b776f6f45855581fb86522dc
- 941e52ce5ce89b7307bdfe1b88657dfd76892b475971b86683cfc6fbca23e209
- e848355359de1e59901aa387f2d208889c368663438909fd3bb0a97566de2b2d
- cc805511e106a9b5302a4db4bfbb98609aca3dcbd2f709aee8ae316f479dfd49
- ea72011929dece4684a2dcb5b76f34cef437dbe50306f19c531d632bf26e7f32
- 7b21b95c4256308e8089bff38d5d20845f2dc28fa9e536de979ceab9b7962afa
- e6faf05234ceaaba3bdcca60285a7ba83eea229a0ca241e94fb314a73ad98d87

5.t loader EXE

- 20a4256443957fbae69c7c666ae025522533b849e01680287177110603a83a41
- 1c2a10f282f1a24d88c74d8d324fb59b172cee4ee2e3e3996d9a62ba979812a6

New EXE Loader

- 8e72c9517b0220f8ed6973cfc36f478fc7837fe536c5859554661bc1e7ee4254
- 59a9d10eba81d62337f38d8f72a15f283e1f4bc9daa99fe0c08f780f3e4da839
- 1db1cf2df0551762eaef0a92923da2f3d032663fdcb331d9474f5398b8ae4398

Cobalt-Strike

- 04f7ae8042e0ed457dd6b86d6e8a40bd361357724b38d3aac7358f5e643299c6
- 2c7e52eb8290d76780b6ac15a134b58a74c95bc616fd0d91a3f9514409a12846

C&C servers

- 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
- schemas.openxmlformats[.]shop
- dueog[.]xyz
- http://13.236.189[.]80:8000/res/translate.res
- https://13.236.189[.]80:8001/G0AnyWhere_up.jsp?Data=
- http://52.236.140[.]86:8000/res/translation.res

- https://52.236.140[.]86:8001/G0AnyWhere_up.jsp?Data=

Cobalt-Strike path

> https://<c2 addres>/ajax/libs/json2/20160511/json_parse_state.js

Mutex

> mt_app_http_get_zed2vsp

PDB

- D:\Project\0_new_plain\0_start\01_XXX_64bit\01_XXX\x64\Release\01_XXX.pdb
- d:\project\downloader\dll_rls\downloader.pdb

GO UP
BACK TO ALL POSTS