Chinese Espionage Campaign Expands to Target Africa and The Caribbean

blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/

May 23, 2024

Check Point Research (CPR) sees an ongoing cyber espionage campaign focuses on targeting governmental organizations in Africa and the Caribbean. Attributed to a Chinese threat actor Sharp Dragon (formerly Sharp Panda), the campaign adopts Cobalt Strike Beacon as the payload, enabling backdoor functionalities like C2 communication and command execution while minimizing the exposure of their custom tools. This refined approach suggests a deeper understanding of their targets.

Key Findings

- *Sharp Dragon’s (formerly referred to as Sharp Panda) operations continues, expanding their focus now to new regions – Africa and the Caribbean.*
- *Sharp Dragon 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.*

Since 2021, Check Point Research has closely monitored the activities of Sharp Dragon, a Chinese threat actor formerly known as Sharp Panda. Their historical tactics primarily involve highly-targeted phishing emails, which have previously resulted in the deployment of malware such of VictoryDLL or the Soul framework.

However, a significant shift has been observed in recent months. Sharp Dragon redirected its focus towards governmental organizations in Africa and the Caribbean, demonstrating a clear expansion of their operations beyond their original scope. These activities are consistent with Sharp Dragon’s established modus operandi, characterized by the compromise of high-profile email accounts to disseminate phishing documents leveraging a remote template weaponized using RoyalRoad. However, unlike previous tactics, these lures now deploy Cobalt Strike Beacon, indicating a strategic adaptation to enhance their infiltration capabilities.

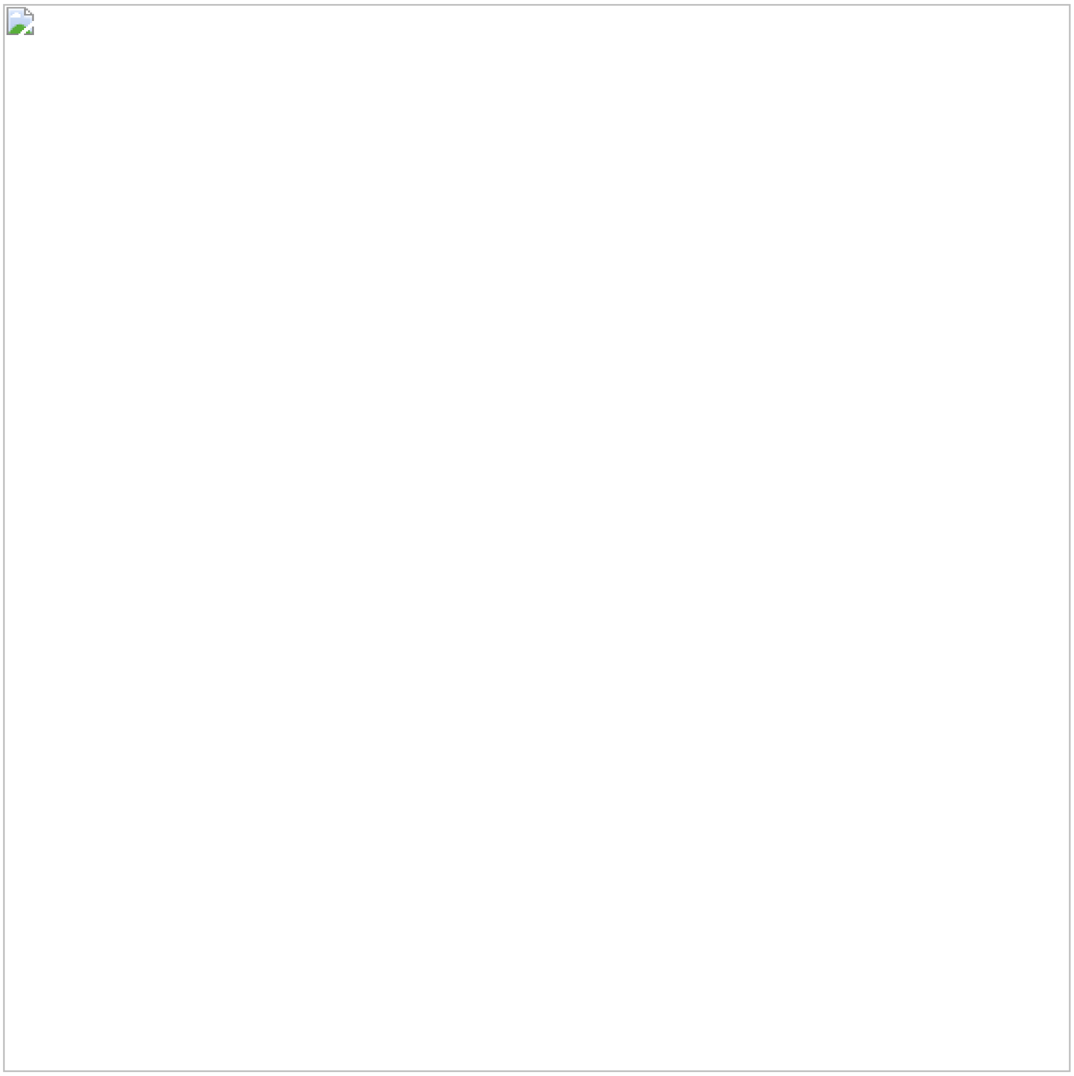

Figure 1 : Sharp Dragon’s shift to target Africa and the Caribbean

Infection Chain

First, the threat actors leverage highly tailored phishing emails, often disguised as legitimate correspondence, to entice victims into opening malicious attachments or clicking on malicious links. These attachments or links execute payloads, which have evolved over time from custom malware like VictoryDLL and the Soul framework to more widely used tools such as Cobalt Strike Beacon. Upon successful execution, the malware establishes a foothold on the victim’s system, allowing the threat actors to conduct reconnaissance and gather information about the target environment. This reconnaissance phase enables Sharp Dragon to identify high-value targets and tailor their attack strategies accordingly.

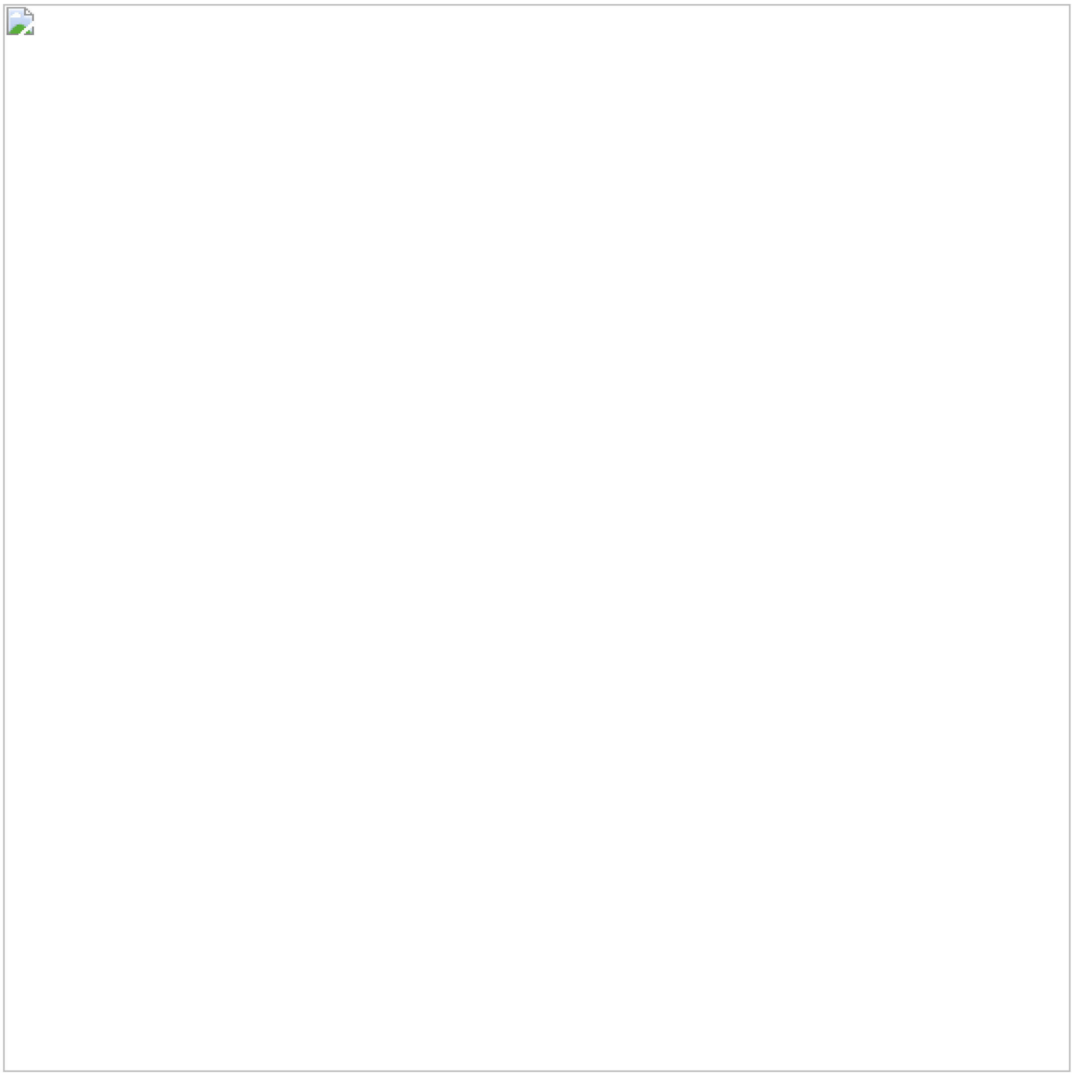

Figure 2 : Infection Chain Example

This infection chain highlights Sharp Dragon’s sophisticated approach to cyber operations, emphasizing careful planning, reconnaissance, and exploitation of vulnerabilities to achieve their objectives while minimizing detection.

Tactics, Techniques, and Procedures

While the core functionality remains consistent, CPR has identified changes in their Tactics, Techniques, and Procedures (TTPs). Those changes reflect a more careful target selection and operational security (OPSEC) awareness. Some changes include:

- **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.
- **Cobalt Strike Payload:** Sharp Dragon has transitioned from using VictoryDll and the SoulSearcher framework to adopting Cobalt Strike Beacon as the payload for the 5.t downloader, providing backdoor functionalities while minimizing exposure of custom tools, suggesting a refined approach to target assessment and minimizing exposure.

- **EXE Loaders:** Recent observations indicate a notable change in 5.t downloaders, with some latest samples incorporating EXE-based loaders instead of the typical DLL-based ones, highlighting the dynamic evolution of their strategies. Additionally, Sharp Dragon has introduced a new executable, shifting from the previous Word document-based infection chain to executables disguised as documents, closely resembling the prior method while enhancing persistence through scheduled tasks.
- **Compromised Infrastructure:** Sharp Dragon shifts from dedicated servers to using compromised servers as Command and Control (C&C) servers, specifically using CVE-2023-0669 vulnerability, which is a flaw in the GoAnywhere platform allowing for pre-authentication command injection

Conclusion

Sharp Dragon's strategic expansion towards Africa and the Caribbean signifies a broader effort by Chinese cyber actors to enhance their presence and influence in these regions. The evolving tactics of Sharp Dragon underscore the dynamic nature of cyber threats, especially towards regions that have been historically overlooked.

These findings emphasize the importance of vigilant cybersecurity measures, with products like Check Point Harmony Endpoint providing comprehensive protection against emerging threats.