Contents

[**G0083 Silver Terrier** 2](#_Toc179359478)

[**I. Introduction** 2](#_Toc179359479)

[**II. Tactics** 2](#_Toc179359480)

[**III. Techniques** 2](#_Toc179359481)

[**IV. Procedures** 3](#_Toc179359482)

[**V. Summary** 5](#_Toc179359483)

[**References** 6](#_Toc179359484)

## **G0083 Silver Terrier**

## **I. Introduction**

G0083 Silver Terrier, also known as SilverTerrier or SA Cybercrime, is a prolific Nigerian cybercriminal group that has been active since at least 2014. Unlike many APT groups that are typically associated with nation-state activities, Silver Terrier is primarily motivated by financial gain. Their operations have evolved from simple 419 scams to sophisticated Business Email Compromise (BEC) attacks and malware campaigns, targeting a wide range of industries globally.

## **II. Tactics**

Silver Terrier's tactical approach is characterized by

***High-volume Attacks***

The group conducts large-scale campaigns, often targeting thousands of potential victims simultaneously.

***Social Engineering***

Heavy reliance on manipulating human psychology to trick victims into taking desired actions.

***Credential Harvesting***

Focused efforts on obtaining login credentials for various services, particularly email accounts.

***Malware Distribution***

Deployment of various malware families to establish persistence and facilitate data theft.

Financial Focus: Primary goal of monetary gain through fraud, theft, and extortion.

## **III. Techniques**

Silver Terrier employs a range of techniques in their operations

|  |  |
| --- | --- |
| Technique | Description |
| **Phishing Campaigns (T1566)** | Use of large-scale email phishing operations for financial theft (T1566.001).  Employment of spear-phishing attachments (T1566.002) targeting specific individuals or organizations. |
| **Malware Deployment** | Use of commodity malware such as AgentTesla, Loki, and Pony (T1204.002).  Deployment of custom-built information stealers (T1555) |
| **Command and Control(C2) Infrastructure** | Utilization of Dynamic DNS services for C2 communication (T1071.004).  Implementation of HTTP-based C2 protocols (T1071.001). |
| **Credential Access** | Employment of keyloggers for capturing user input (T1056.001).  Use of web browsers to harvest saved passwords (T1555.003). |
| **Defense Evasion** | Obfuscation of malicious executables (T1027).  Use of legitimate penetration testing tools to blend with normal activity (T1588.002). |
| **Persistence** | Addition of programs to the startup folder (T1547.001).  Creation of scheduled tasks for periodic malware execution (T1053.005). |
| **Exfiltration** | Use of automated exfiltration scripts (T1020).  Compression of stolen data before exfiltration (T1560). |

## **IV. Procedures**

The group’s typical attack sequence follows this order

1. ***Initial Access***

a. Large-scale phishing campaigns are launched, often impersonating legitimate businesses or using topical lures.

b. Emails contain malicious attachments (often .doc or .pdf files) or links to credential harvesting sites.

1. ***Execution***

a. If a malicious attachment is opened, it typically contains macros that, when enabled, download and execute the main payload.

b. For credential harvesting, victims are directed to convincing phishing sites that mimic legitimate login pages.

1. ***Persistence and Privilege Escalation***

a. Once executed, malware like AgentTesla establishes persistence through startup folder entries or scheduled tasks.

b. The malware may attempt to elevate privileges by exploiting known vulnerabilities or through social engineering tactics.

1. ***Credential Access and Collection***

a. Information stealers begin harvesting credentials from web browsers, email clients, and FTP programs.

b. Keyloggers are deployed to capture user input, including passwords and financial information.

1. ***Command and Control***

a. Malware communicates with C2 servers, often using HTTP protocols to blend with normal traffic.

b. Dynamic DNS services are used to maintain flexible C2 infrastructure.

1. ***Exfiltration***

a. Stolen data is compressed and encrypted before exfiltration.

b. Data is typically exfiltrated in small chunks to avoid detection.

1. ***Impact***

a. Compromised email accounts are used for BEC attacks, attempting to redirect financial transactions.

b. Stolen credentials are used for further compromise or sold on dark web marketplaces.

## **V. Summary**

Silver Terrier or G0083 has appeared on the stage of IT criminals as an interesting example of their gradual development and improvement of technical experience. Before, it was involved in some basic 419 types of scams and is now involved in malware attacks and more recently the BEC.

Why Silver Terrier stands out is that it is not an APT group in the organizational sense – it is more of a digital bazaar of hackers. Such organizational structure has shown ability to avoid the law enforcement actions localizing the capacities of this group even after arresting its leaders. Their methods are changing over the recent past they have been using the ordinary commercial malware and have in the recent past been using living off the land strategies which harnesses the legitimated system utilities for his/her/its evil gains. Priding itself as an English speaking dog, Silver Terrier has ventured a little to Southeast Asia and the middle East for its international outlook.

The economic loss is vast and is in the billions due to BEC scams and other activities by tertiary associations such as Silver Terrier. To counter this increasing threat, an organization needs to develop a complex Security post-control. This involves proper spam and virus checking, periodic security champions’ parade, identity and access management, ideal Endpoint Protection System, good update management, and network zoning.

## **References**

MITRE ATT&CK. (2023). "SilverTerrier" <https://attack.mitre.org/groups/G0083/>