TLP: WHITE — Unrestricted Distribution

THREAT INTELLIGENCE REPORT · G0083

Threat Actor Profile: SilverTerrier

Nigerian Business Email Compromise (BEC) Collective

ACTIVE THREAT

PREPARED BY
Grace Funmilayo Smith

DATE
May 2026

CLASSIFICATION
TLP: WHITE

PRIMARY SOURCES
MITRE ATT&CK, Unit 42, CISA, Interpol

1 EXECUTIVE SUMMARY

> **Key Finding:** SilverTerrier represents one of the most persistent and financially damaging cybercrime collectives globally. For organizations operating in Africa's financial sector — particularly fintech platforms serving mass-market users — BEC attacks represent a direct, credible, and immediate threat to operational integrity and customer trust.

SilverTerrier is the designation assigned by Palo Alto Networks Unit 42 to a collective of Nigerian cybercriminals who have been conducting Business Email Compromise (BEC) campaigns and malware-enabled fraud since at least 2014. Unlike traditional nation-state APT groups, SilverTerrier is not a single organized entity — it is a loosely affiliated ecosystem of over 480 tracked individual actors and groups who share tools, techniques, and infrastructure.

Since 2014, SilverTerrier actors have collectively produced over 81,300 malware samples linked to more than 2.1 million attacks worldwide. BEC schemes attributed to this collective have contributed to billions of dollars in global losses, with the FBI reporting BEC as the second most costly form of cybercrime in 2024 — generating nearly $2.8 billion in losses. For fintech organizations operating in Nigeria, this threat is not theoretical; it is an existential operational risk.

2 THREAT ACTOR OVERVIEW

MITRE ATT&CK ID	G0083
ALSO KNOWN AS	TMT, Nigerian BEC Collective
ORIGIN	Nigeria (West Africa)
ACTIVE SINCE	2014 – Present
MOTIVATION	Financial Gain
SOPHISTICATION	Low to Medium (evolving)
ATTRIBUTION CONFIDENCE	High (Unit 42, Interpol, Group-IB)

LAST KNOWN ACTIVITY
2025 (ongoing)

SilverTerrier actors began their criminal evolution with simple advance-fee (419) scams before rapidly adopting commodity malware tools to conduct large-scale BEC operations. By 2019, the collective was executing an average of 92,739 BEC attacks per month — a 172% increase from the previous year. Law enforcement actions, including Interpol's Operation Delilah in 2022, have resulted in multiple arrests; however, the collective continues to grow, fueled by low barriers to entry and readily available commodity malware.

3 TARGETS & VICTIMOLOGY

SilverTerrier actors demonstrate broad targeting but have shown consistent preference for sectors with high-value financial transactions and large email-dependent workflows. Per MITRE ATT&CK (G0083), primary target sectors include:

Sector	Targeting Rationale	Risk to Fintechs
High Technology	Vendor impersonation, invoice fraud	⚠ High
Financial Services	Wire fraud, account takeover	Critical
Higher Education	Payroll diversion, grant fraud	⚠ Medium
Manufacturing	Supply chain BEC, payment redirection	⚠ Medium
Healthcare / Government	COVID-themed campaigns (2020)	⚠ Medium

Geographically, victims are concentrated in the United States, Australia, Canada, United Kingdom, and Italy — however, as African fintech platforms expand to serve millions of users and process increasing transaction volumes, they represent a growing and increasingly attractive target surface.

4 TACTICS, TECHNIQUES & PROCEDURES (TTPS)

The following TTPs have been documented for SilverTerrier based on MITRE ATT&CK (G0083), Unit 42 research, and CISA advisories:

Tactic	Technique	ID	Description
Initial Access	Spearphishing Attachment	T1566.001	Malicious Office documents or archives sent via targeted phishing emails
Initial Access	Spearphishing Link	T1566.002	Links to credential harvesting pages mimicking legitimate login portals
Execution	User Execution	T1204.002	Victims execute malicious attachments disguised as invoices or HR documents
Persistence	Registry Run Keys	T1547.001	Malware adds entries to ensure execution on system startup
Defense Evasion	Obfuscated Files or Information	T1027	Payloads compressed, encrypted, or AutoIT-obfuscated to evade AV detection
Credential Access	Input Capture / Keylogging	T1056.001	AgentTesla and PredatorPain log keystrokes and steal stored credentials
Credential Access	Credentials from Web Browsers	T1555.003	LokiBot and AZORult extract saved passwords from Chrome, Firefox, etc.
Collection	Email Collection	T1114	Actors harvest email credentials to conduct internal BEC from trusted accounts
C2	Web Protocols (HTTP)	T1071.001	C2 communications conducted over HTTP to blend with normal web traffic
Exfiltration	Exfiltration Over C2 Channel	T1041	Stolen credentials and data exfiltrated via SMTP or HTTP to attacker-controlled servers

5 MALWARE ARSENAL

SilverTerrier actors rely predominantly on commodity malware tools, lowering the barrier to entry while maintaining operational effectiveness. The following tools have been consistently observed across campaigns:

LokiBot INFOSTEALER

Widely used credential stealer targeting browsers, FTP clients, and email clients. Also capable of creating backdoor access. One of the most consistently deployed tools across SilverTerrier campaigns since 2015. C2 infrastructure used by a prominent SilverTerrier actor included over 50 LokiBot command-and-control domains.

AgentTesla RAT / KEYLOGGER

A .NET-based Remote Access Trojan with keylogging, screenshot capture, and credential theft capabilities. Exfiltrates data via SMTP using attacker-controlled email accounts. Highly prevalent in SilverTerrier spearphishing campaigns.

AZORult INFOSTEALER

Stealer malware targeting cryptocurrency wallets, browser credentials, and system data. Particularly dangerous in fintech environments where digital asset accounts may be targeted.

PredatorPain KEYLOGGER

A commodity keylogger that captures credentials and screenshots, exfiltrating data via email. Regularly observed in SilverTerrier campaigns and requires minimal technical expertise to deploy.

6 DIAMOND MODEL ANALYSIS

The Diamond Model provides a structured framework for mapping the four core features of this intrusion activity:

7 INDICATORS OF COMPROMISE (IOCS)

> **Note:** The following IOCs are representative examples documented in public threat intelligence sources. Organizations should enrich these with live feeds from ThreatFox, AlienVault OTX, and VirusTotal for current indicators. All domains are defanged for safety.

Type	Indicator	Associated Malware	Source
Domain	`agenttesla[.]xyz`	AgentTesla C2	Public Research
IP	`185.62.189[.]43`	AgentTesla C2	Public Research
Registry Key	`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`	AgentTesla Persistence	MITRE ATT&CK
SMTP String	`smtp.gmail[.]com (exfil relay)`	AgentTesla Exfiltration	Unit 42
Behavior	`HTTP POST to /gate.php`	LokiBot C2 Pattern	CISA AA20-266A
File Pattern	`Malicious .xls/.doc with macros`	Initial delivery vector	Unit 42

8 RECOMMENDATIONS FOR FINTECH ORGANIZATIONS

Based on the TTPs and tooling documented above, the following mitigations are recommended for financial technology organizations — particularly those operating in or targeting the Nigerian/African market:

✉ **Deploy Advanced Email Security Controls**
Implement DMARC, DKIM, and SPF policies to reduce email spoofing. Deploy email gateway solutions capable of sandboxing attachments before delivery. Flag external emails with visual banners to reduce user deception.

Enforce Multi-Factor Authentication (MFA)
Even when credentials are stolen via LokiBot or AgentTesla, MFA breaks the kill chain at the credential access stage, preventing account takeover and lateral movement.

Monitor for C2 Beaconing Patterns
Deploy network monitoring to detect HTTP POST requests to known malicious patterns (e.g., /gate.php). Block outbound SMTP from non-mail servers to prevent credential exfiltration via AgentTesla.

Ingest Threat Feeds & Hunt for IOCs
Subscribe to ThreatFox, AlienVault OTX, and Abuse.ch feeds for real-time SilverTerrier IOCs. Proactively hunt for known malware hashes and C2 domains across endpoint and network logs.

Conduct Regular Security Awareness Training
SilverTerrier's primary entry point is human error. Simulate phishing campaigns quarterly. Train staff — especially finance and executive teams — to verify wire transfer requests through out-of-band channels.

Establish a Verified Payment Callback Process
Implement a mandatory voice call verification protocol for any change in vendor banking details or executive-initiated payment requests above a defined threshold. This directly neutralizes the BEC social engineering vector.

9 REFERENCES

1. Palo Alto Networks Unit 42 — SilverTerrier Report Series (2016–2021)
2. MITRE ATT&CK — SilverTerrier Group Profile (G0083) — attack.mitre.org/groups/G0083
3. CISA Advisory AA20-266A — LokiBot Malware (September 2020)
4. Interpol — Operation Delilah Press Release (May 2022)
5. FBI Internet Crime Complaint Center (IC3) — 2024 Internet Crime Report
6. Group-IB — Threat Intelligence Support for Operation Delilah (2022)
7. KrebsOnSecurity — SilverTerrier Coverage (2025)