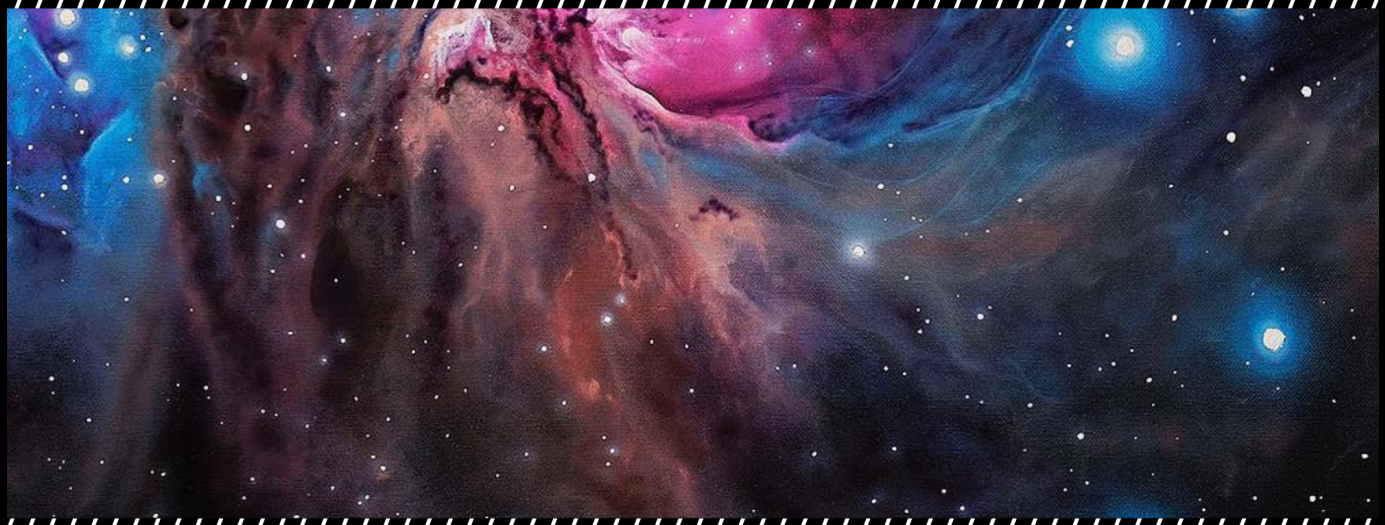
SILVER TERRIER

AXIAL



SILVER TERRIER

NIGERIA

TECH , EDUCATION
MANUFACTURING

RAT

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SILVER TERRIER : ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Assigned the name SilverTerrier, these actors have now collectively produced more than 81,300 samples of malware linked to 2.1 million attacks. In five years (from 2014 to 2019), SilverTerrier actors have evolved from being novice threat adversaries to mature cybercriminals.

II.TARGETS

Countries:
Russia, Belgium, China, Iran, Sweden, and Rwanda.

III. ATTRIBUTION

In 2014, Unit 42 published its first research identifying a small group of Nigerian threat actors employing malware for financial gain. Over the past five years, the number of actors involved in this activity has grown substantially. As of this publication, we have attributed attacks to more than 480 Nigerian threat actors and groups.

IV. TOOLS USED

AgentTesla, AzoRult, Lokibot, Pony, and PredatorPain.

V. METHODS USED

- Since 2014, Nigerian actors have been linked to various popular malware tools,
including Zeus, DarkComet and others.

- SilverTerrier actors have consistently adopted new malware families and shifted to the latest packing tools available i.e. Predator Pain, ISR Stealer, Keybase, ISpySoftware
and Pony malware families.

- Each tool produces malicious executable files that are designed either to provide remote access to a system
or to steal credentials from a victim, with the majority of these variants targeting
Microsoft Windows operating systems.

- These actors routinely rely on packing
software or “crypters” in order to obfuscate the code so that it won’t be identified
by traditional antivirus solutions.

AX1AL

VI. IOCS

1. C537E41126E8E73FD54CEBE580FAB2F9
2. 8B22E8FE34147041B76BFBC9A36B5F0D
3. AD31D2A536287F15345919D69A6C4D0E
4. FD47B2108857C4F55ABF7FF4B55F5C80

C&C

1. 123meka.com
2. 128bitsecured.com
3. 185.165.29.25
4. 2015reunionstudents.com
5. 2tyte.com
6. 46.183.222.15
7. 4sproduct.com
8. 8gs7e8.com
9. abbottt.com
10. abdul-abu2017.com

VII. REFERENCES

1. https://unit42.paloaltonetworks.com/silverterrier-2019-update/
2. https://raw.githubusercontent.com/pan-unit42/iocs/master/silverterrier/domains19.csv
3. https://unit42.paloaltonetworks.com/unit42-silverterrier-update-increasingly-sophisticated-nigerian-cybercriminals-take-bigger-part-3b-bec-related-losses/
4. https://www.computerweekly.com/news/252480923/Nigerian-email-attacks-evolving-into-credible-dangerous-threat
5. https://www.infopoint-security.de/medien/silverterrier-next-evolution-in-nigerian-cybercrime.pdf