Elephant Beetle: Uncovering an Organized Financial-Theft Operation

By Sygnia

Published: 2022-01-05 · Archived: 2026-04-05 15:04:23 UTC

Sygnia's IR team has identified the Elephant Beetle threat group, an organized, significant financial-theft operation threatening global enterprises.

Amnon Kushnir, Noam Lifshitz, Yoav Mazor, Oren Biderman, Boaz Wasserman, Itay Shohat and Arie Zilberstein

For the past two years, Sygnia's Incident Response (IR) team has been methodically tracking the Elephant Beetle threat group, an organized, significant financial-theft operation threatening global enterprises.

Key points

The Sygnia Incident Response team identified an organized and experienced threat group siphoning off funds from businesses in the financial sector in Latin America. Sygnia refers to this threat actor as 'Elephant Beetle' or TG2003, also known as FIN13.

- This group operates undetected for long periods of time, patiently studying target financial systems, creating fraudulent transactions hidden among regular activity, and ultimately stealing millions of dollars.
- Elephant Beetle is highly proficient with Java based attacks and, in many cases, targets legacy Java applications running on Linux-based machines as a means of initial entry to the environment.
- While primarily focused in the Latin American market, Elephant Beetle can expand its attacks to organizations worldwide, with our IR team already discovering a breach in the Latin American operations of a U.S. company.

The full report includes the threat actor's modus operandi, in-depth analysis of its capabilities, and provides actionable insights, IOCs and guidelines for defending against the attacks.

Overview

For the past two years, Sygnia's Incident Response (IR) team has been tracking a **financially motivated threat group targeting and infiltrating organizations from the finance and commerce sectors in Latin America**. The attack is relentless, relying on simplicity to hide in plain sight, without the need to develop sophisticated tools or exploits.

Using an arsenal of over 80 unique tools & scripts, the group executes its attacks patiently over long periods of time, blending in with the target's environment and going completely undetected while it quietly liberates organizations of large amounts of money.

Elephant Beetle seems to primarily focus on Latin American targets, but that doesn't mean that organizations not based there are safe. For example, our IR team discovered that the Latin American operations of a U.S. company had been breached. As such, both regional and global organizations should be on their guard.

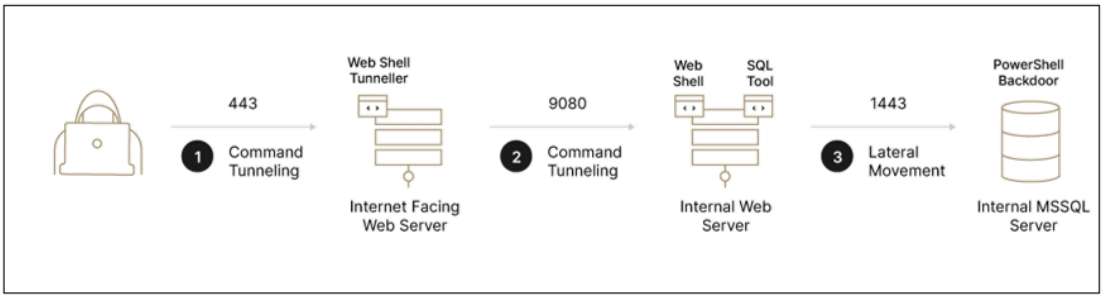
The group is highly proficient with Java based attacks and, in many cases, **targets legacy Java applications running on Linux-based machines as a means of initial entry to the environment**. Beyond that, the group even deploys their own complete Java web application on victim machines to do their bidding while the machine also runs legitimate applications.

Elephant Beetle operates in a well-organized and stealthy pattern, efficiently executing each phase of its attack plan once inside a compromised environment:

1. During the first phase, which can span up to a month, the group focuses on **building operational cyber capabilities** in the compromised environment. The group studies the digital landscape and plants backdoors while customizing its tools to work within the victim environment.
2. The group then spends several months studying **the victim's environment, focusing on the financial operation** and identifying any flaws. During this stage, they observe victim software and infrastructure to

understand the technical process of legitimate financial transactions.

3. The group then **creates fraudulent transactions** in the environment. These transactions mimic legitimate behavior and siphon off incremental amounts of money from the victim. Although the amount of money stolen in a single transaction may seem insignificant, the group stacks numerous transactions to what amounts to millions of dollars.
4. If during its efforts any theft activity is discovered and blocked, the group **then simply lays low** for a few months only to return and target a different system.



Lateral movement flow chart of the threat actor

Defending against an elephant beetle attack

This report is a technical play-by-play of the Elephant Beetle attack as detected, observed and mitigated by Sygnia's IR team. **We share the threat actor's modus operandi, in-depth analysis of its capabilities, and provide actionable insights, IOCs and guidelines for defending against the attacks.**

Source: https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation