Sep 21 2023

NETMANAGEIT

Intelligence Report

Unveiling the Shadows: The Dark Alliance between GuLoader and Remcos

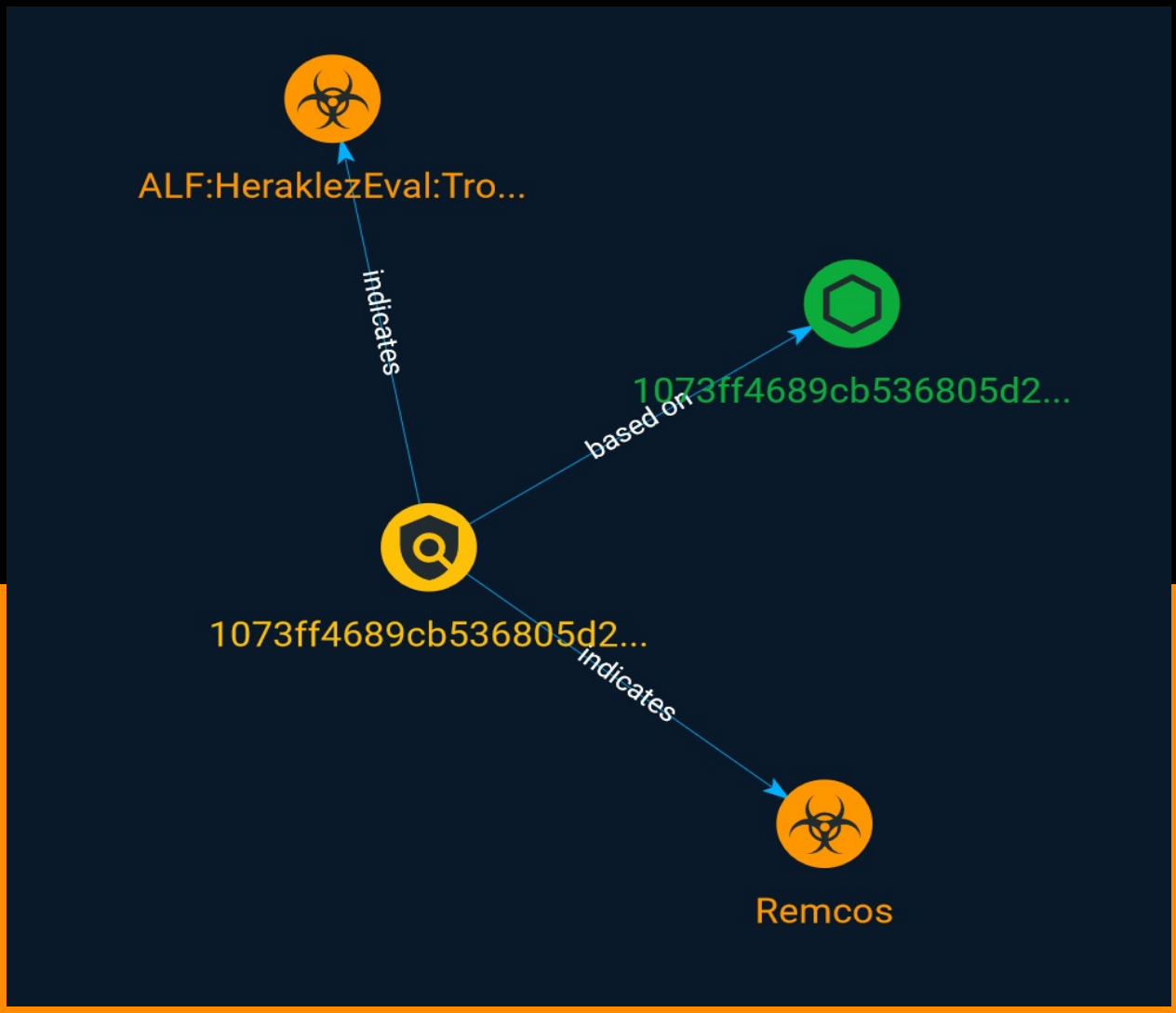

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4
- Malware 5

Observables

- StixFile 6

External References

- External References 7

Overview

Description

Remcos and GuLoader are tools that were once exclusively sold on hacking forums and are now publicly available on e-commerce, masquerading as legitimate products. These tools have become popular among individuals with malicious intentions. Check point Research has discovered that an individual operating under the alias EMINəM administers the websites BreakingSecurity and VgoStore that openly sell Remcos and GuLoader under a new name, TheProtect. This Threat actor is also involved in distributing malware, including the notorious Formbook info stealer and Amadey Loader. At the same time, EMINəM employs TheProtect for his own malicious purposes, exploiting its ability to bypass antivirus software.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
1073ff4689cb536805d2881988b72853b029040f446af5ced18d1bc08b2266e1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1073ff4689cb536805d2881988b72853b029040f446af5ced18d1bc08b2266e1']

Malware

Name
ALF:HeraklezEval:Trojan:Win32/Guloader

Name
Remcos

StixFile

Value
1073ff4689cb536805d2881988b72853b029040f446af5ced18d1bc08b2266e1

External References

- https://otx.alienvault.com/pulse/650aa3ab041adbbc2943d556
- https://research.checkpoint.com/2023/unveiling-the-shadows-the-dark-alliance-between-guloader-and-remcos/