NETMANAGEIT

Intelligence Report

MMRat Carries Out Bank Fraud Via Fake App Stores

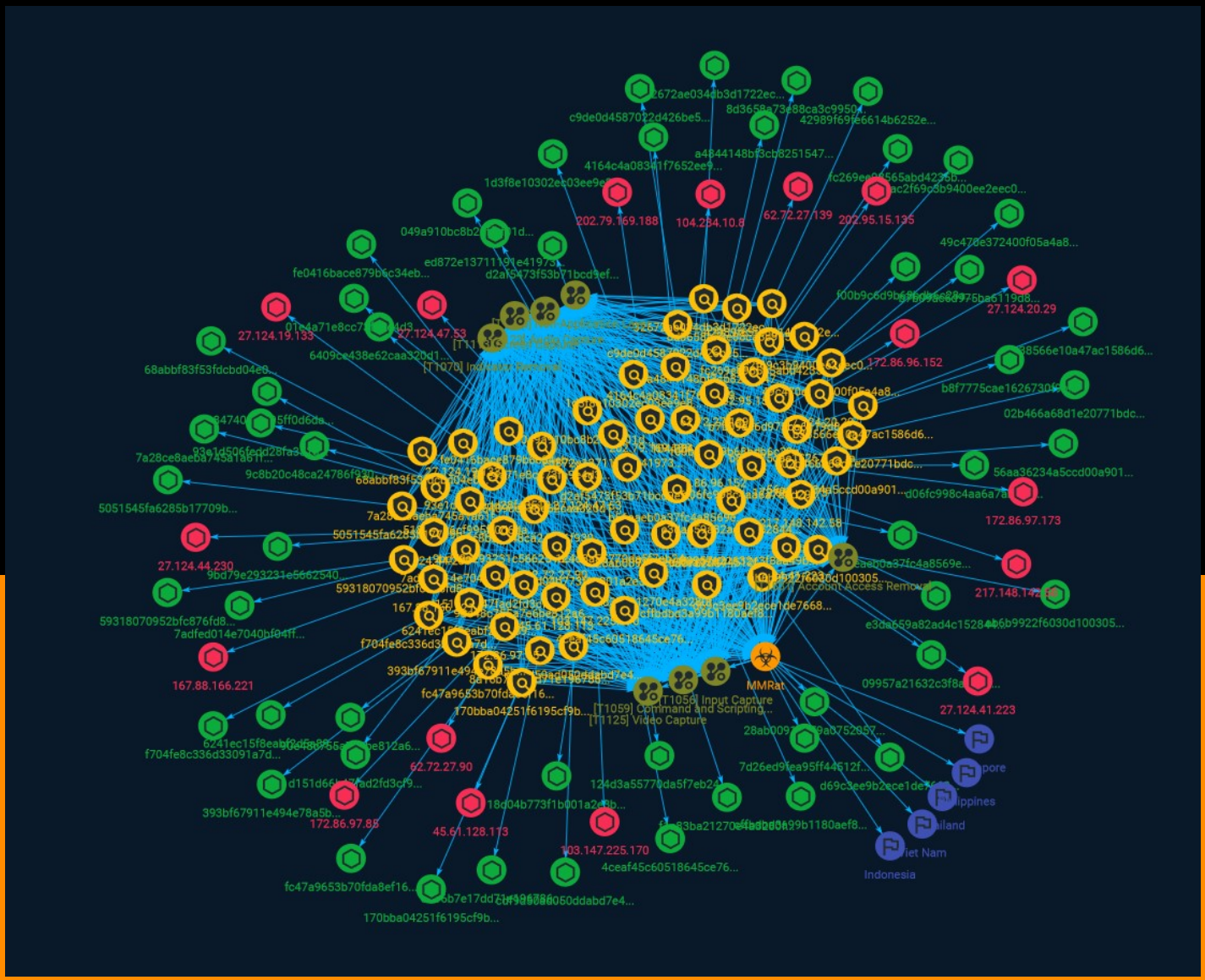

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Confidence

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

15 / 100

Indicator

Name

f00b9c6d9b68bdb6c28a85bdf91780b0da14cab3e6aa350e45650ffc7c886b0b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f00b9c6d9b68bdb6c28a85bdf91780b0da14cab3e6aa350e45650ffc7c886b0b']

Name

9c8b20c48ca24786f930167976abf8c003697d0409f98c5072a83a613057e345

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c8b20c48ca24786f930167976abf8c003697d0409f98c5072a83a613057e345']

Name

18d04b773f1b001a2e3b7d716f0a742d33197c0ea7af4e171ab25f86b4297141

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18d04b773f1b001a2e3b7d716f0a742d33197c0ea7af4e171ab25f86b4297141']

Name

27.124.47.53

Description

ISP: BGPNET Global ASN **OS:** None ---------- Hostnames: - default.zlmediakit.com ---------- Domains: - zlmediakit.com ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 19:34. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421 Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV SPSV ESTP 211 End. ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: openresty Date: Sat, 26 Aug 2023 15:34:04 GMT Content-Type: text/html Content-Length: 544 Last-Modified: Thu, 12 Jan 2023 09:10:35 GMT Connection: keep-alive ETag: "63bfce8b-220" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 400 Bad Request Server: openresty Date: Sat, 26 Aug 2023 17:03:58 GMT Content-Type: text/html Content-Length: 252 Connection: close

400 Bad Request

The plain HTTP request was sent to HTTPS port

---

openresty

``` ---------- **8088:** ``` HTTP/1.1 200 Vary: Origin Vary: Access-Control-Request-Method Vary: Access-Control-Request-Headers X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Type: text/html;charset=UTF-8 Content-Length: 92 Date: Wed, 09 Aug 2023 08:57:01 GMT ``` ---------- **8181:** ``` HTTP/1.1 200 OK Server: nginx/1.25.1 Date: Sat, 12 Aug 2023 04:51:47 GMT Content-Type: text/html Content-Length: 13411 Last-Modified: Wed, 02 Aug 2023 09:50:35 GMT Connection: keep-alive ETag: "64ca26eb-3463" Accept-Ranges: bytes
```