Incident Report

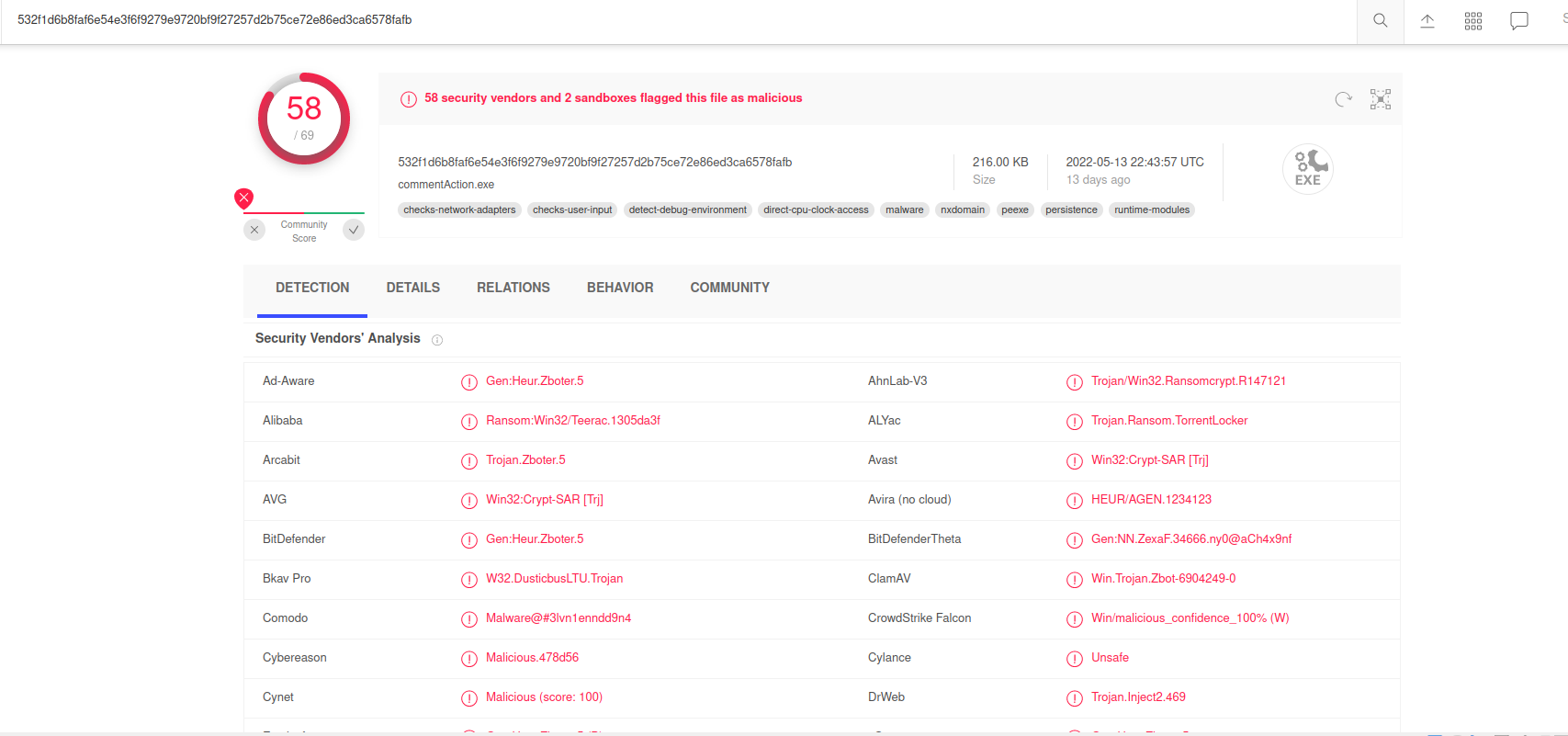
13108 Defensive: Malware Traffic

Date: 5-26-2022 (DS)

# Executive Summary:

On 5/26/2022, a client reported their computer encrypted by a malicious program and are requesting assistance in locating what was responsible for the attack.

**Results**:



**Victim Details:**

IP address: 62.75.195.236

Mozilla/4.0 Windows NT 6.1

**Indicators of Compromise: (IOCs)**

SHA 256 hash: 532f1d6b8faf6e54e3f6f927939720bf9f27257d2b75ce72e86ed3ca6578fafb

File size: 216KB

File Type: PE32 Executable for MS Windows (GUI) intel 80386 j32-bit

File Description/Name: known as commentAction.exe, it contains multiple trojans, viruses and malware. It was requested under ?b514ee6f0fe486009a6d83b035a4c0bd.

**Malicious HTTP Traffic hosts:**

188.165.164.184 -**(ip-addr.es)**

204.152.254.221 -**(runlove.us)**

72.152.254.221 -**(comarksecurity.com)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_