Incident Report

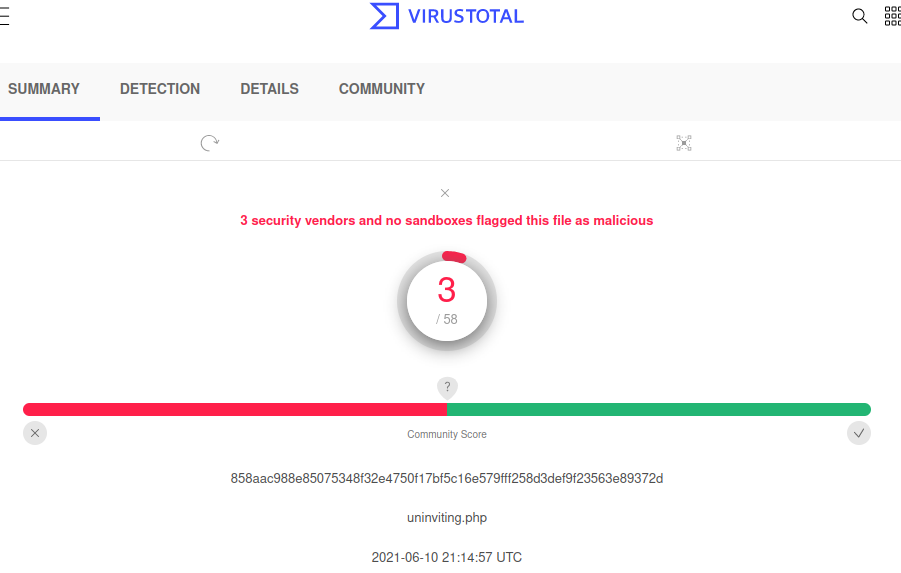
13146 Defensive: Malware Analysis

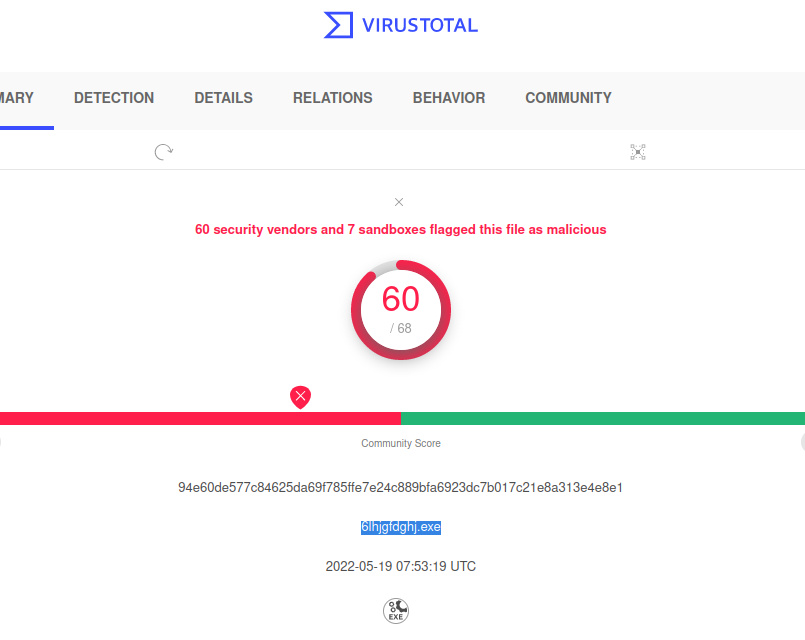
Date: 5-30-2022 (DS)

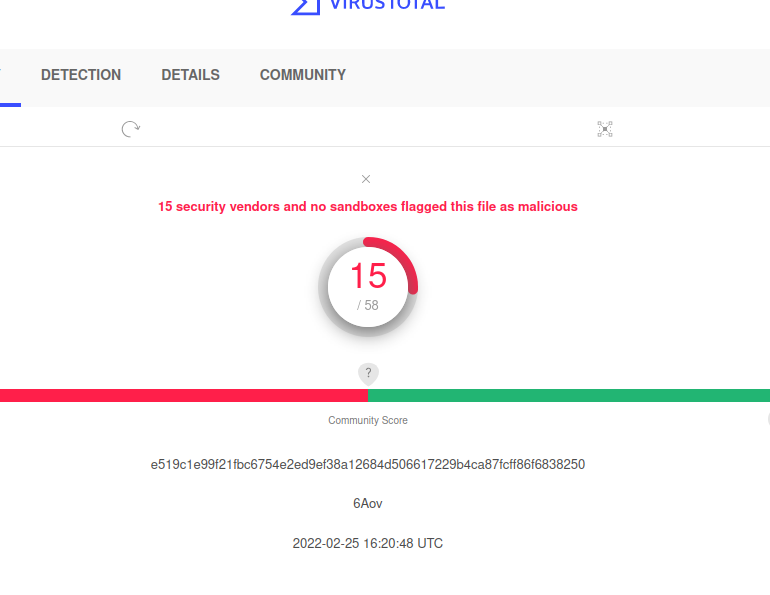
# Executive Summary:

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**:







**Methodology / Steps Taken:**

* In Wireshark I decided it was the most simplistic way to work backwards by first scanning the objects and files for malicious programs that may be in the pcap file.
* After finding the three culprits, I was then able to find the exact packets that they were associated with.
* I then analyzed the packets by following the TCP stream, and found identified who they were going to (which was the clients information, such as IP MAC address and hostname)
* I then was able to filter out the IPs to the point where the user made the request, where it had set off a chain of events and then lead to the infections.

**Victim Details:**

Time: 7:59am

HostName: DESKTOP-MGVG60Z$

UserName: bill.cook

IP address: 10.2.8.101

MAC Address: 00:12:79:41:c2:aa

Hewlett Packard

**Indicators of Compromise: (IOCs)**

**Malicious File Name:**

Uninviting.php

**SHA 256 hash:** 858aac988e85075348f32e4750f17bf5c16e579fff258d3def9f23563e89372d

**File Size:** 1.05 MB

**Malicious File Name:**

6lhjgfdghj.exe

**SHA 256 hash:**

94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1

**File Size:** 267.01 KB

**Malicious File Name:**

6aov

**SHA 256 hash:**

e519c1e99f21fbc6754e2ed9ef38a12684d506617229b4ca87fcff86f6838250

**File Size:** 203.56 KB

**Malicious HTTP Traffic hosts:**

Tonmatdoanminh.com/uninviting.php **(45.124.85.55.)**

Http://198.211.10.238:8080/6Aov **(198.211.10.238)**

Roanoakemortgages.com **(8.208.10.147)**

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