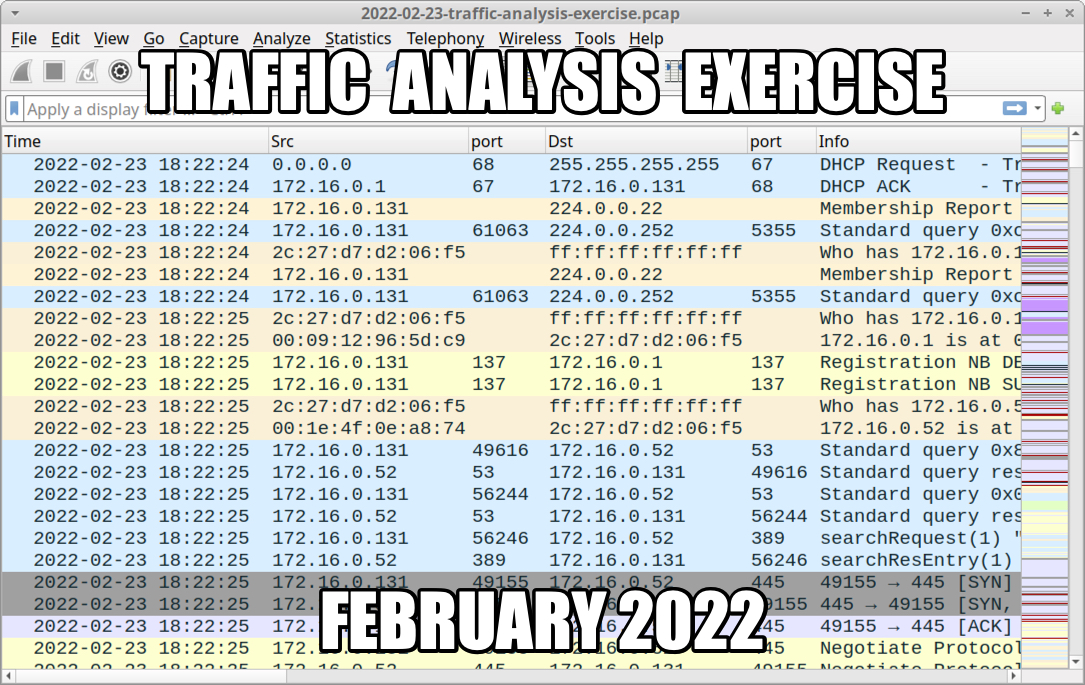
**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

[**Malware Traffic Analysis - Sunnystation**](https://www.malware-traffic-analysis.net/2022/02/23/index.html)

**Pod 6**

**Aayushi Bhatia, Frances Brandofino, Elsa Gilsdorf, Amogh Patel**



**Question:** What hosts/user account names are active on this network?

**Help used:** <https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/>

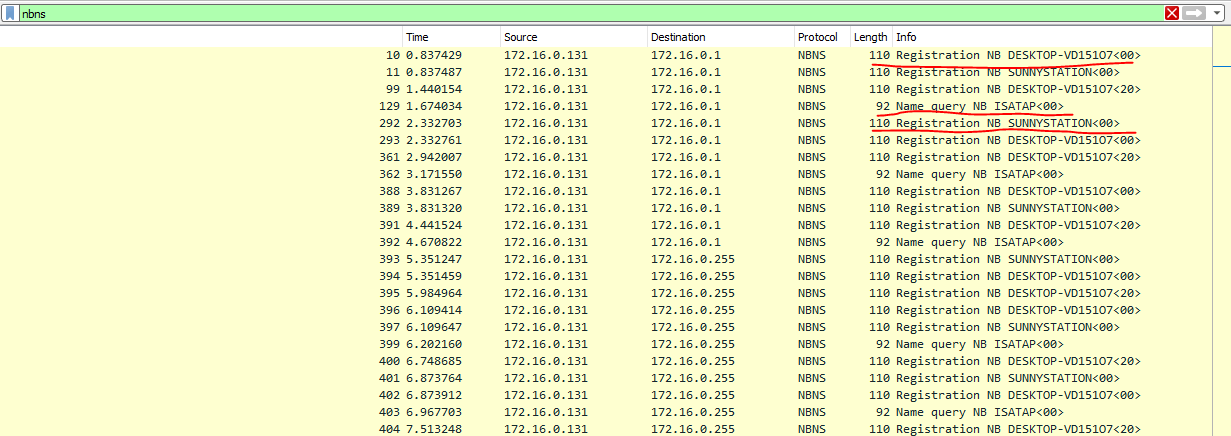
**Answer:**

The following listed below are the active hosts/user accounts found during the analysis of the exercise’s pcap.zip file by Wireshark:

DESKTOP-VD15107, SUNNYSTATION, DESKTOP-W5TFTQY, DESKTOP-KPQ9FDB, ISATAP, WWW.KRPANO.PRO, WWW.JMTMJZ.COM

**Explanation:**

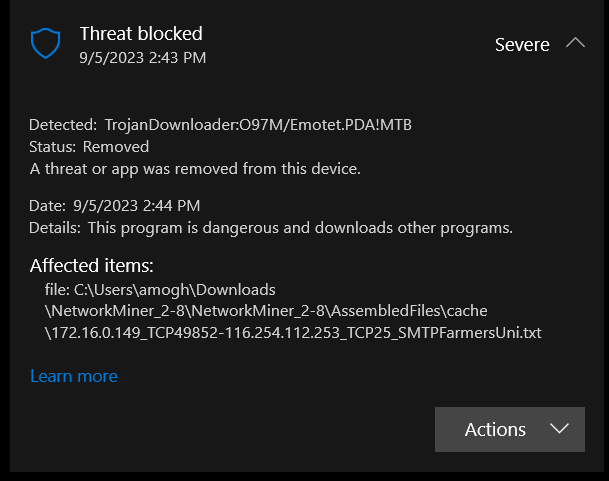
In Wireshark, the command **“nbns”** is used in the filter field and then the hostnames/user accounts are displayed in the “**Info**” column. The command “**nbns**”, or **NetBIOS Name Service**, is a process that converts the IP addresses of human-readable names such as websites and host names to other processes for proper communication. When used in the context of using it as a filter, it shows all traffic using **“nbns”**.

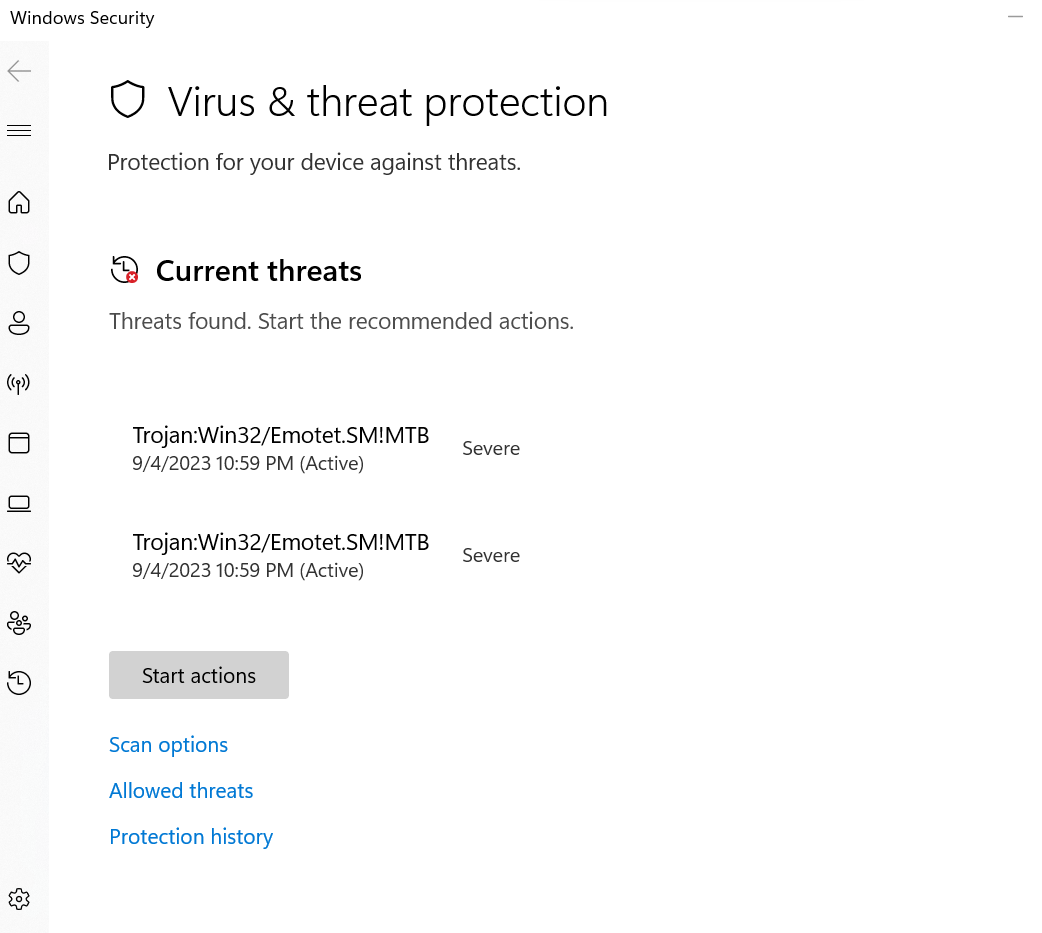


**Question:** What type of malware are they infected with?

**Answer:**

This pcap file is infected with an active emotet trojan horse malware with phishing and media sharing properties.





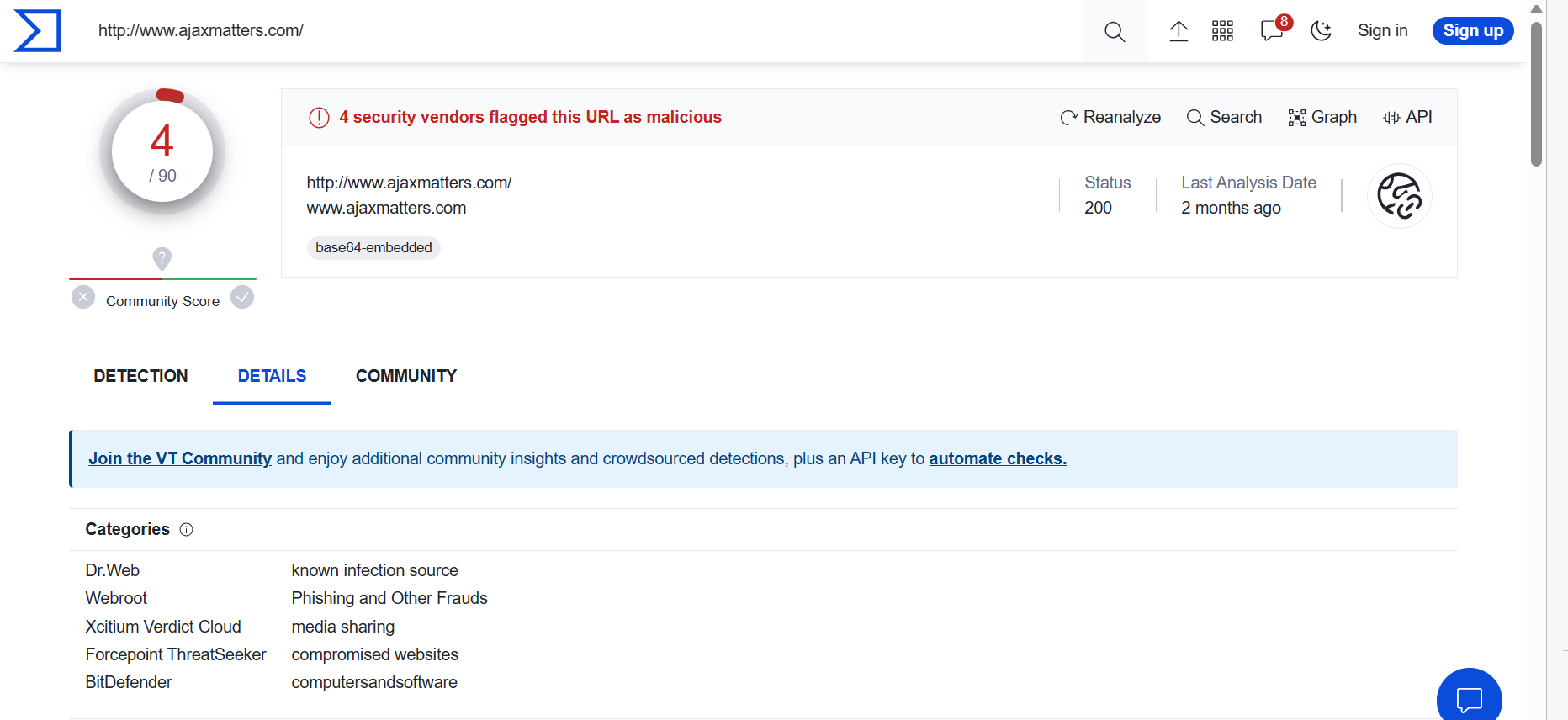
**Explanation:**

When the pcap file was ran using NetworkMiner (NetworkMiner is an open source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files), it prompted the windows defender to alert that the pcap file contains malware.

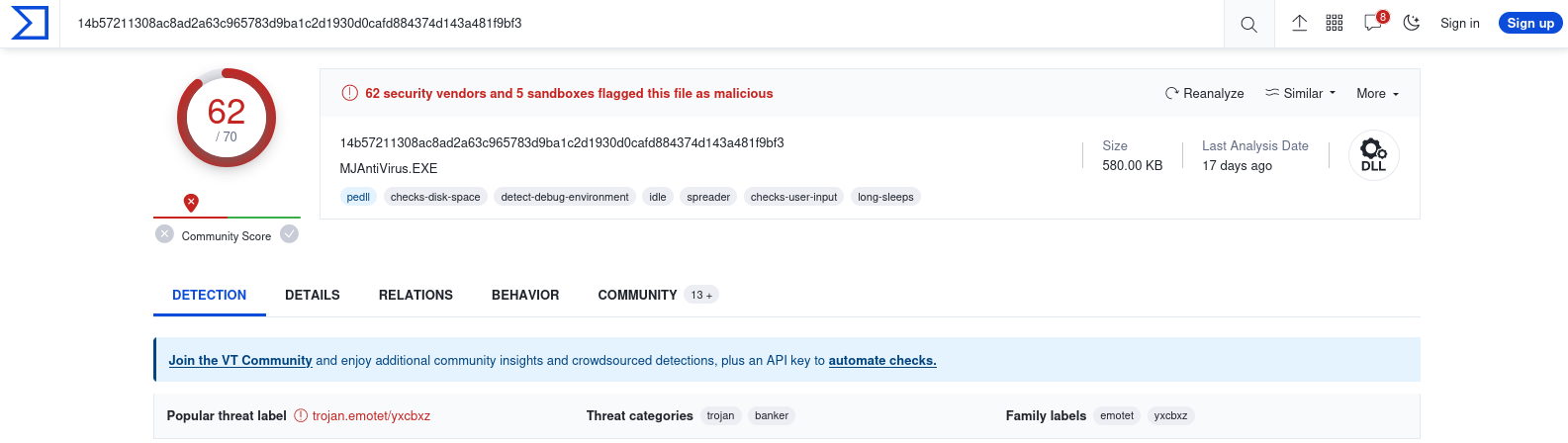
After using the **export objects “http”** option in wireshark under the file tab, the packet #4675 with hostname www.ajaxmatters.com was saved to the desktop. However, the desktop’s Windows Security prevented the file from being opened and informed the user of an emotet trojan horse contained in the file.

* An emotet trojan horse is a dangerous malware which has worm-like capabilities and can detect if it is being run in a virtual machine in which case it will lay dormant. The emotet trojan horse primarily spreads through email spam and then steals private information.

Next, the hostname/address was copied and inserted into the virustotal.com (A site which scans URLs and files for viruses) which then scanned the address and reported that the hostname address was a known infection source with phishing, media sharing properties, as well as containing the ability to compromise websites.



Then the isolated packet #4675 was uploaded to virustotal.com and the following community score was obtained.



**Division of Labor Report:**

**Wireshark operator -** Frances Brandofino, Aayushi Bhatia.

**Write up -** Everyone.

**Formatter -** Elsa Gilsdorf, Amogh Patel.