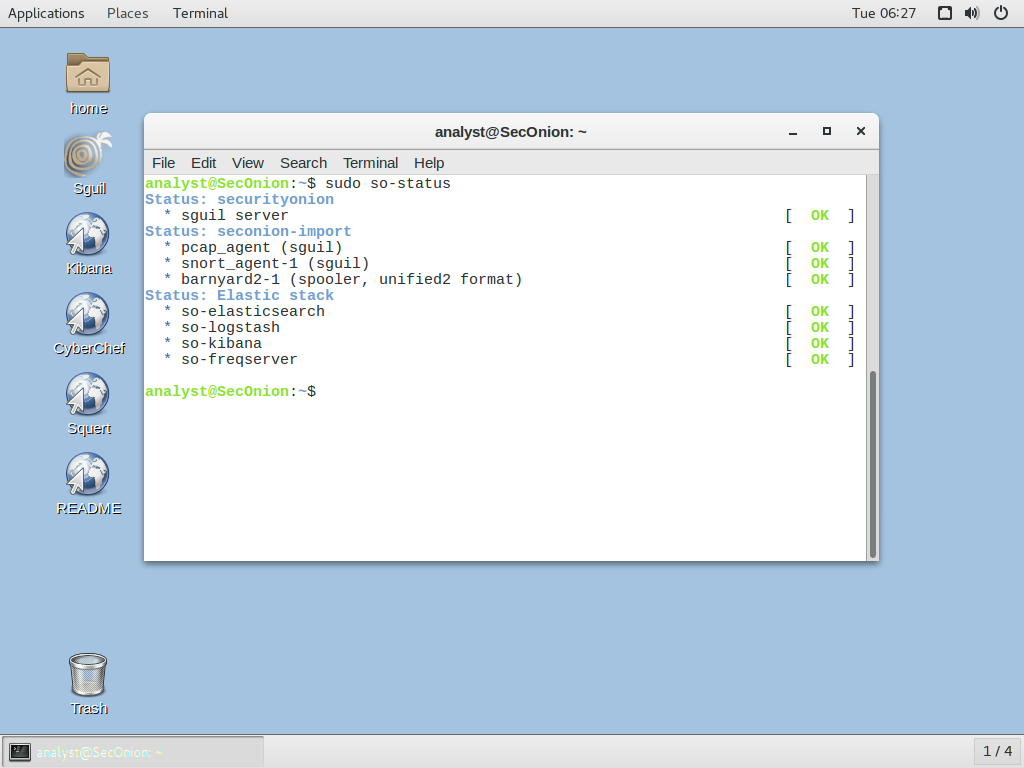
**CyberOps Associate v1.0 - Skills Assessment**

**Part 1: Gather the Basic Information**

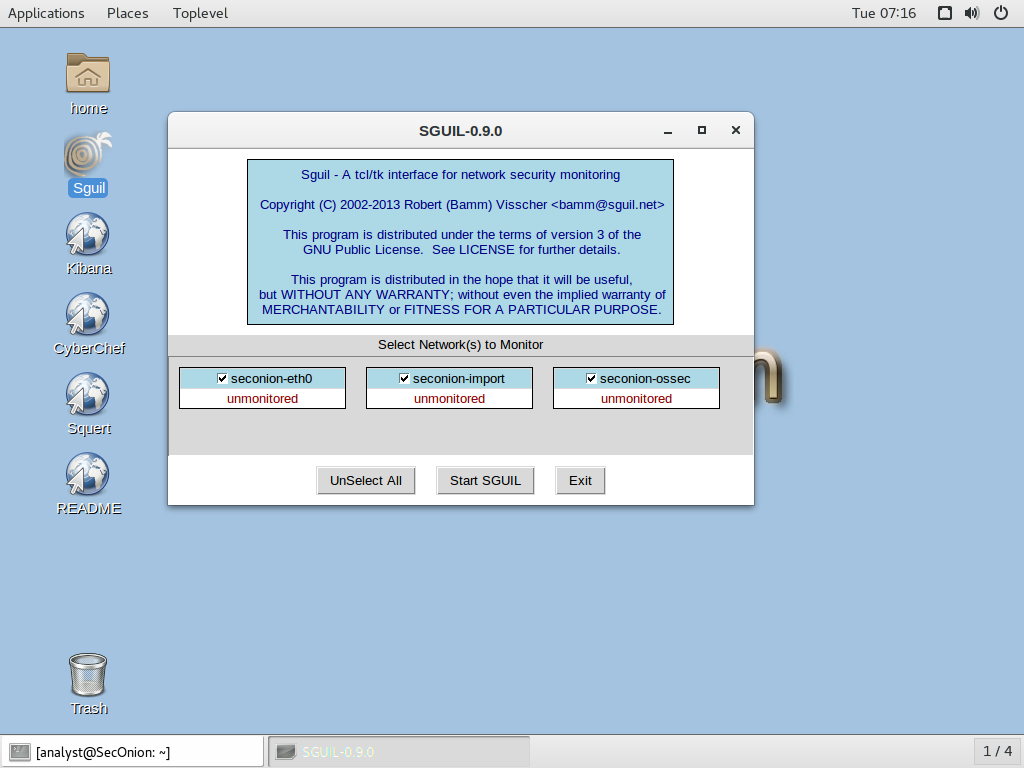
In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

**Step 1: Verify the status of services**

1. Log in to Security Onion VM using the username analyst and password cyberops.
2. Open a terminal window. Enter the sudo so-status command to verify that all the services are ready.



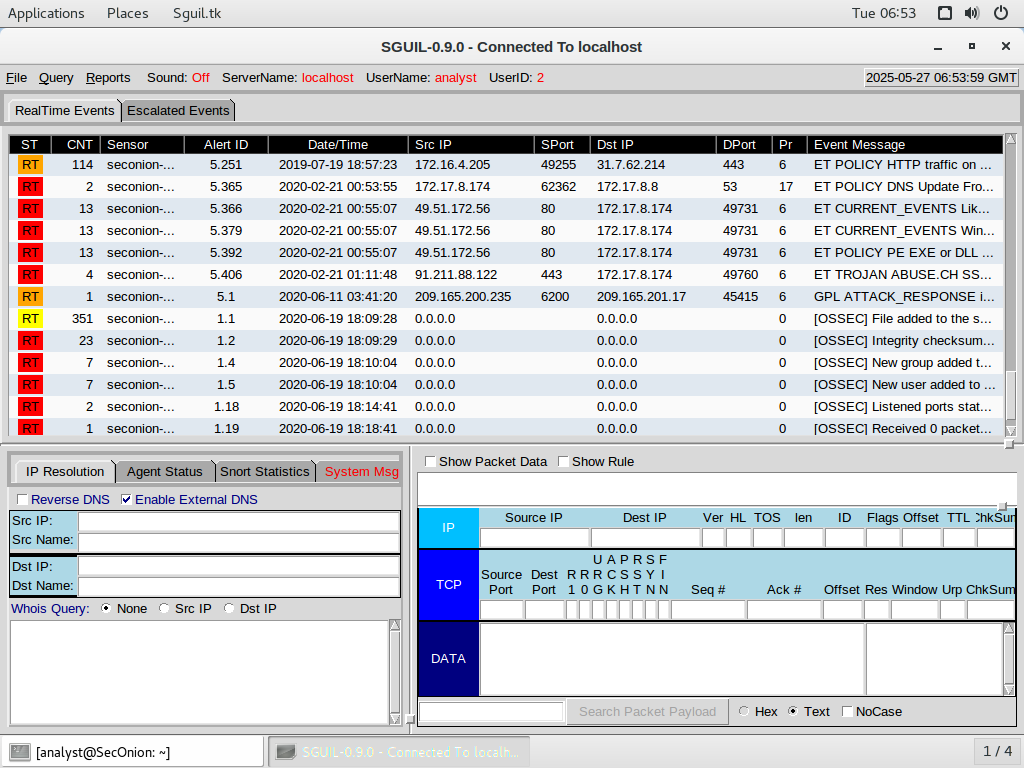
1. When the NSM service is ready, log in to Sguil or Kibana with the username analyst and password cyberops.

Open Sguil using the shortcut on the Desktop. Log in with the username analyst and password cyberops. Click Select All to select the interfaces and then Start SGUIL.  


### **Step 2: Gather basic information.**:

1. Identify the time frame of the **latest** Trojan attack, including the date and approximate time.

***2020-02-21 from 00:53:55 to 2020-06-11 03:41:20***

******

1. List the alerts noted during this time frame associated with the Trojan.

* ET POLICY DNS Update From External net
* ET CURRENT\_EVENTS Likely Evil EXE download from WinHttpRequest non-EXE extension.
* ET CURRENT\_EVENTS WinHttpRequest Downloading EXE
* ET POLICY PE EXE or DLL Windows file download HTTP
* ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
* GPL ATTACK\_RESPONSE id check returned root

1. List the internal IP addresses and external IP addresses involved.

### **Internal IP Addresses:**

* 172.17.8.174

### **External IP Addresses:**

* 49.51.172.56
* 91.211.88.122
* 209.165.200.235
* 209.165.201.17

**Part 2: Learn about the Exploit**

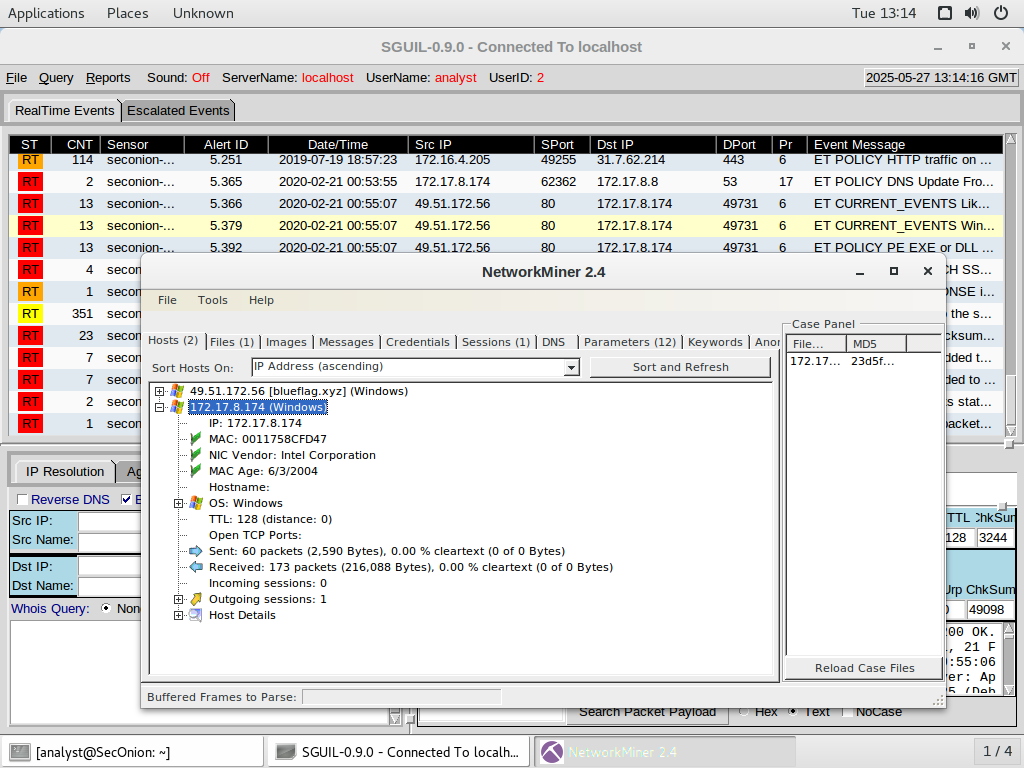
In this part, you will learn more about the exploit.

**Step 1: Infected host**

**Questions:**

1. Based on the alerts, what are the IP and MAC addresses of the infected computer? Based on the MAC address, what is the manufacturer of the NIC chipset? (Hint: Perform an internet search for MAC address lookup vendor to determine the NIC manufacturer based on the MAC address.)

IP: 172.17.8.174  
MAC: 0011758CFD47  
NIC Vendor: Intel Corporation



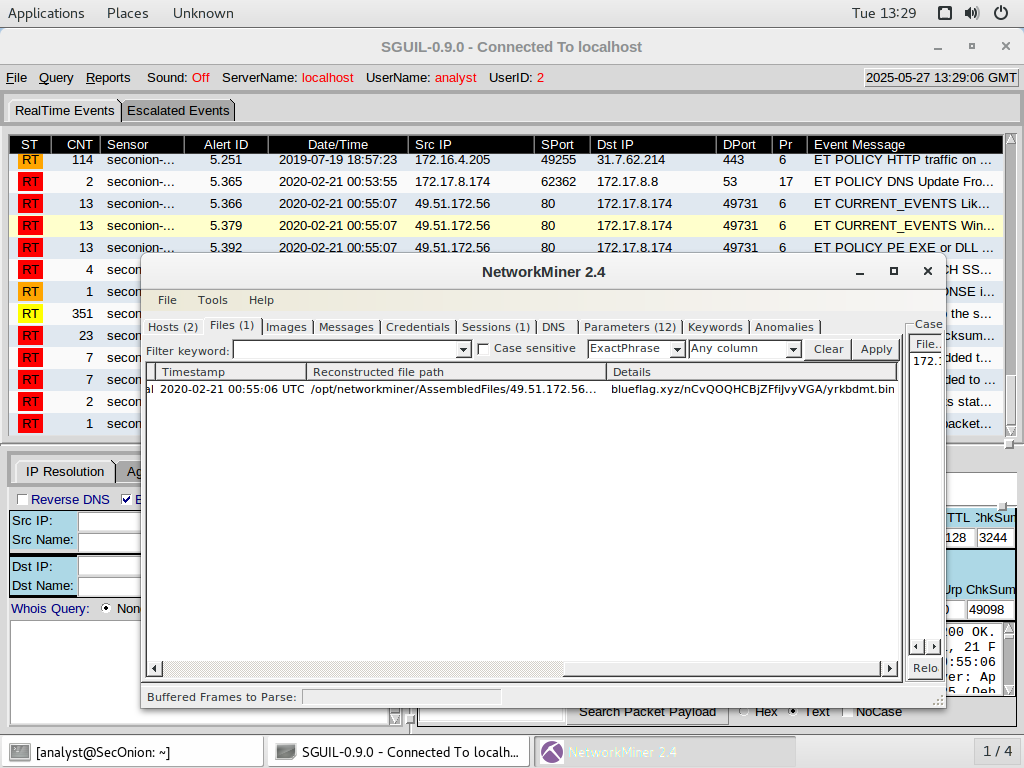
1. What is the hostname of the infected PC? What is the domain and the IP address of the domain controller?

* Hostname of infected PC: 172.17.8.174 (hostname not resolved)
* Domain controller domain: blueflag.xyz
* Domain controller IP address: 49.51.172.56

1. Based on the alerts, when (date and time in UTC), and how was the PC infected? (Hint: Enter the command date in the terminal to determine the time zone for the displayed time.)

2020-02-21 00:55:06 UTC

After downloading and running yrkbdmt.bin from the domain blueflag.xyz, the PC got infected. Security researchers state that the file is associated with the Dridex banking trojan, and the infection commonly occurs when someone visits malicious sites or downloads files via email.



1. How did the malware infect the PC? Use an internet search as necessary.

At 2020-02-21 00:55:06 UTC, the infected device reached the domain blueflag.xyz (at 49.51.172.56) and downloaded a file named yrkbdmt.bin. Sometimes, this happens because the victim opens the file, which was embedded in an e-mail or downloaded on its own from the internet, or because users are tricked into downloading it.

According to our observations, the downloaded file is associated with the Dridex banking trojan, which is often sent out using exploit kits or through malicious spam. Dridex is made to steal your bank login information and can also bring in extra malicious code.

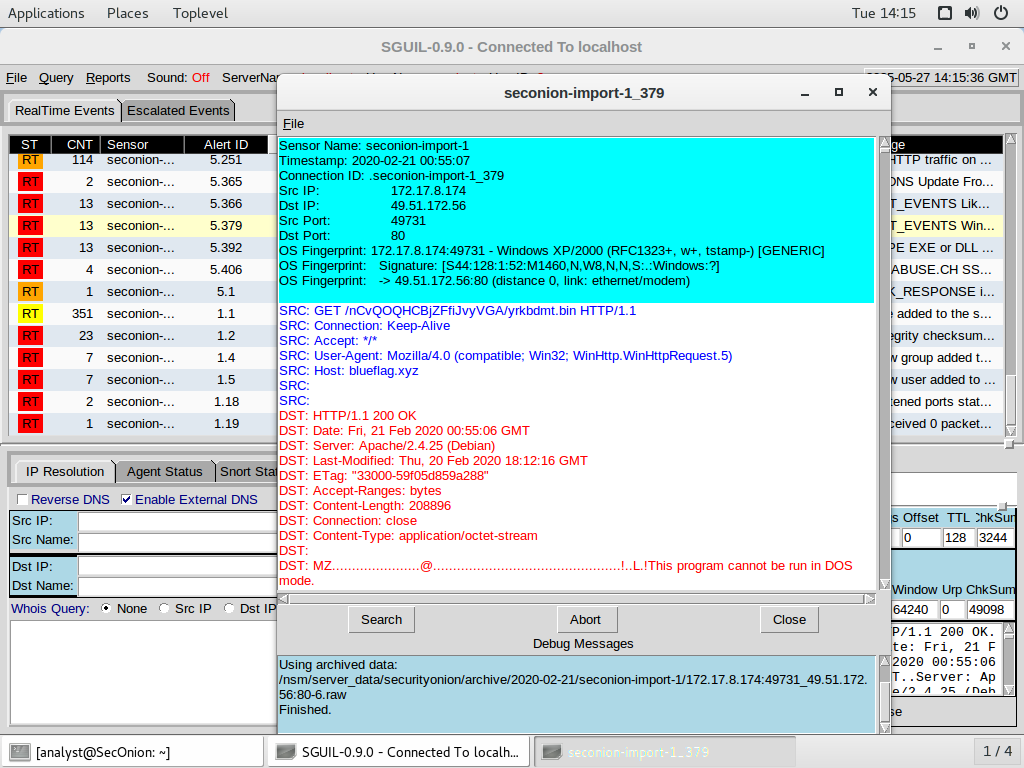
Whereas some attacks use Pushdo to initiate Dridex downloads, this incident shows that the campaign directly downloaded yrkbdmt.bin from the suspicious domain. If only fake HTTP packets on port 80 are seen purporting Pushdo activity, it is most likely that the infection happened through the use of a harmful binary taken from a hacked server.

**Step 2: Examine the exploit.**

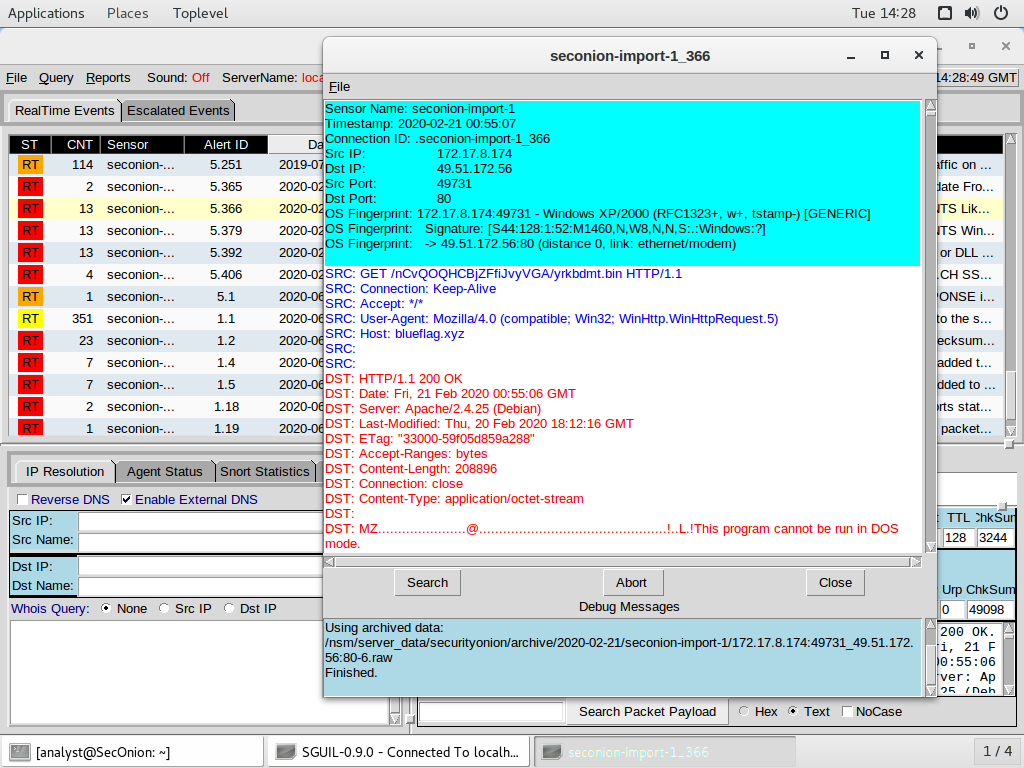
**Questions**:

1. Based on the alerts associated with the HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

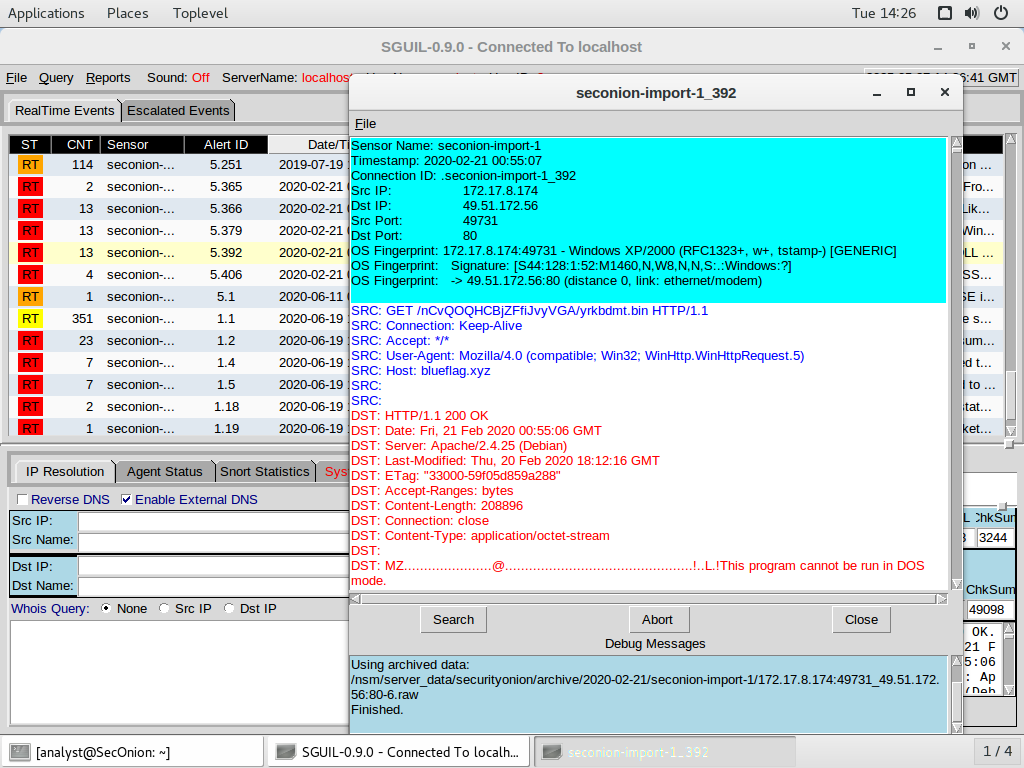
**Alert ID 5.379 Transcript**



**Alert ID 5.366 Transcript**



**Alert ID 5.392 Transcript**



Based on the alerts associated with the HTTP GET request (Alert IDs **5.366**, **5.379**, and **5.392**)

#### **Malicious Domain Observed:**

* blueflag.xyz

#### **Files Downloaded:**

* yrkbdmt.bin

#### **Details:**

At 2020-02-21 00:55:07 UTC, the infected host (172.17.8.174) made an HTTP GET request to the domain blueflag.xyz, hosted on IP 49.51.172.56, requesting the file:

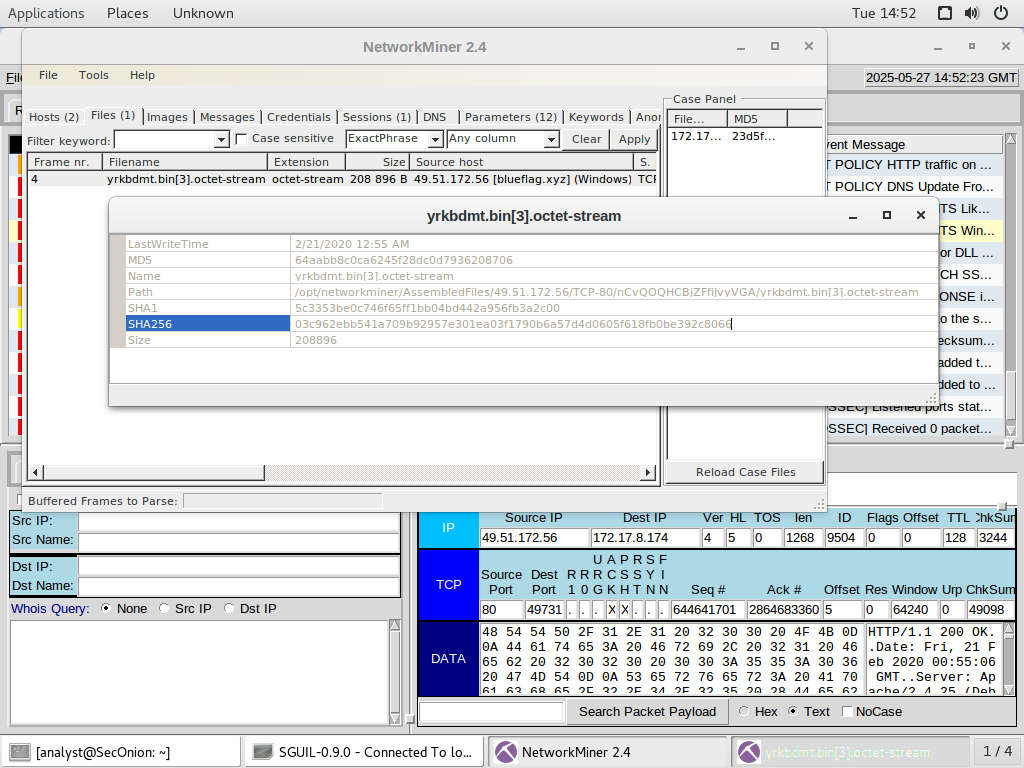
GET /nCvQOQHCBjZFfiJvyVGA/yrkbdmt.bin HTTP/1.1

The server responded with an HTTP 200 OK and sent a binary file (Content-Type: application/octet-stream) with a size of 208,896 bytes, indicating successful download of the file yrkbdmt.bin.

The file starts with the "MZ" header, which is a signature for Windows PE (Portable Executable) files, confirming that it is a Windows executable.

1. Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that are probably infected with the computer.

yrkbdmt.bin = 03c962ebb541a709b92957e301ea03f1790b6a57d4d0605f618fb0be392c8066



1. Navigate to [www.virustotal.com](http://www.virustotal.com), input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and the target machine. You can also include any information that is provided by the community, posted in VirusTotal, or other resources.

**yrkbdmt.bin:**

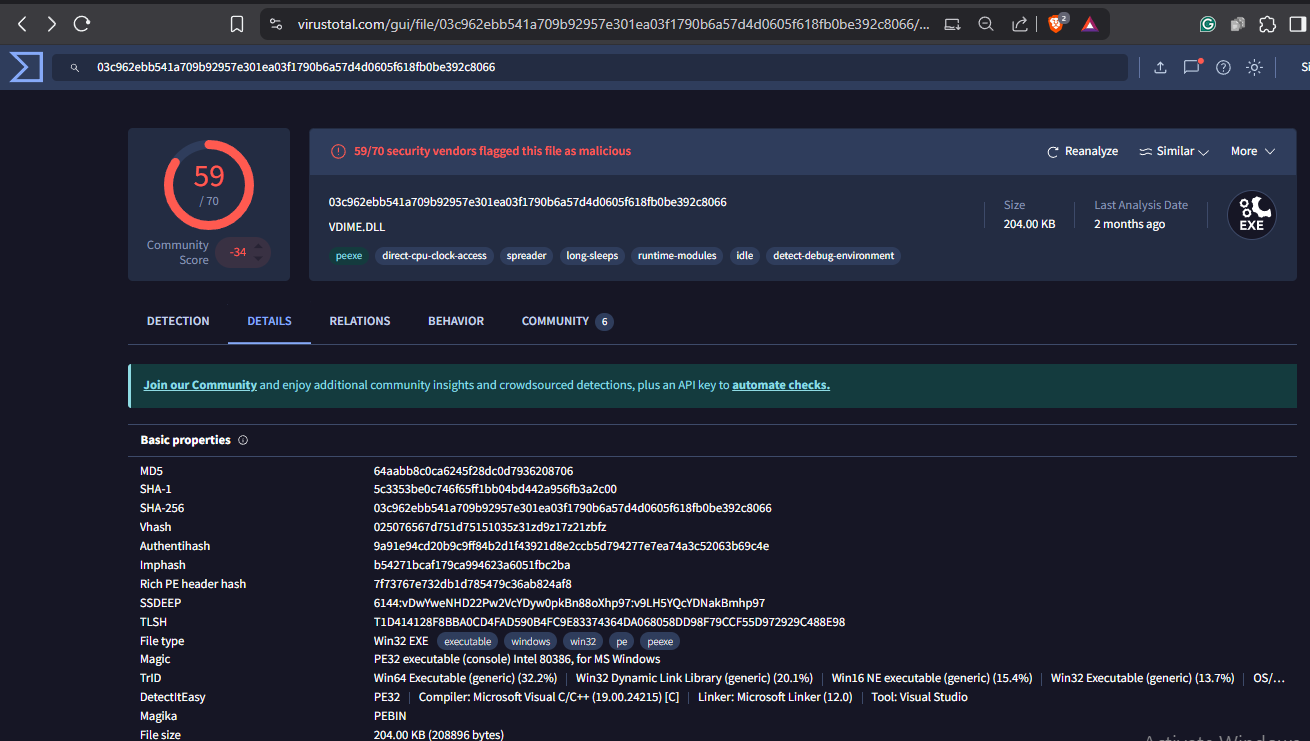
* 58 engines detected this file
* File type: Win32 EXE
* File size: 204.00 KB (208896 bytes)

**Names:**

* yrkbdmt.bin
* yrkbdmt.bin.octet-stream
* yrkbdmt.bin[3].octet-stream
* yrkbdmt.bin[5].octet-stream
* VDIME
* VDIME.DLL
* HTTP-Fxn5Bv18iRBhpzhfwb.exe
* extracted\_at\_0x0.exe
* Caff54e1.exe
* 17.bin

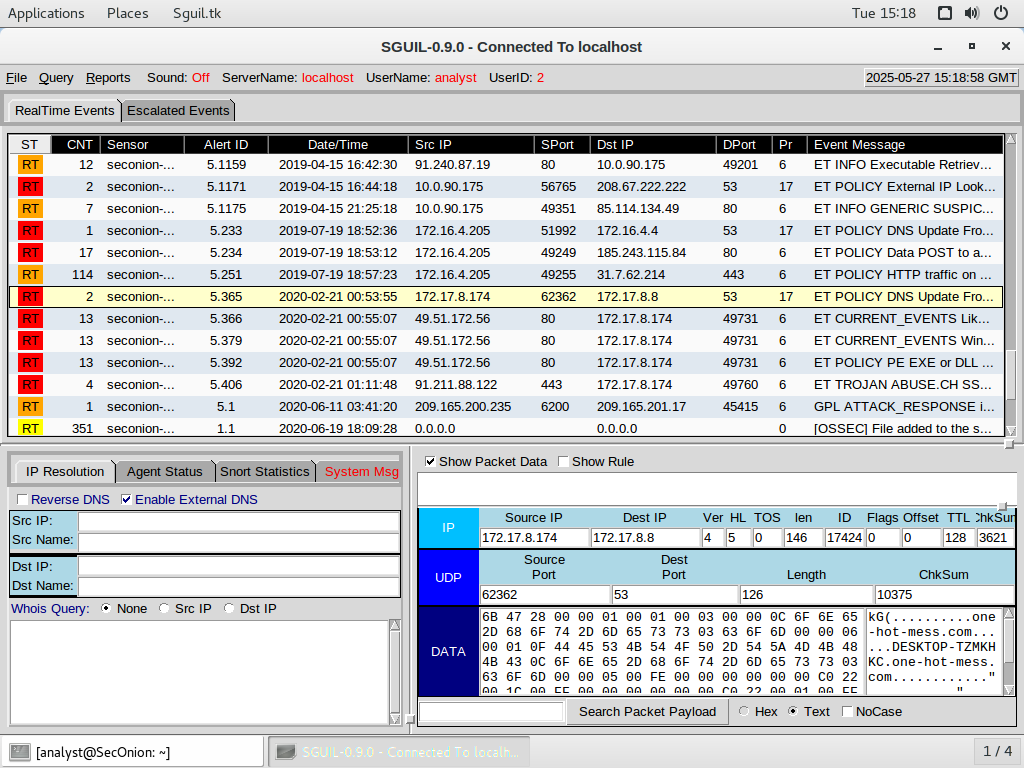
**Target Machine:**

* Intel 386 or later processors and compatible processors



1. Examine other alerts associated with the infected host during this timeframe and record your findings.

ET POLICY DNS Update From External net – infection started when the user of the 172.17.8.174 host performed a DNS update through a suspicious domain – destination IP: 172.17.8.8.



**Step 3: Report your findings.**

After the investigation, it was found that the infected computer had an IP address 172.17.8.174 and a MAC address 0011758CFD47, which shows it was an Intel NIC. The unwanted infection happened on February 21, 2020, at 00:55:06 UTC. That day, the computer downloaded yrkbdmt.bin from the domain blueflag.xyz. Dridex banking trojan is linked to this file, and VirusTotal shows 58 antivirus engines detect it as dangerous. Downloaded binary files come in at 204 KB and are recognized as executable files used by Windows (PE). Certain HTTP requests were picked up, leading to EXE downloads, and the system also detected various updates to its DNS settings. The external IPs that are listed are 91.211.88.122 and 209.165.200.235. We are using BlueFlag.xyz (IP 49.51.172.56) as our domain controller. Experts think the malware got into the system by using faulty downloads or phishing emails. It is confirmed that this is a successful case of a Trojan infection with efforts to steal data and send harmful files.