**Mamadou Bah**

**Pcap analysis**

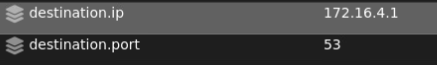
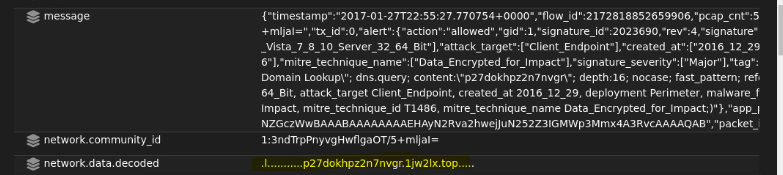
**11/12/2024**

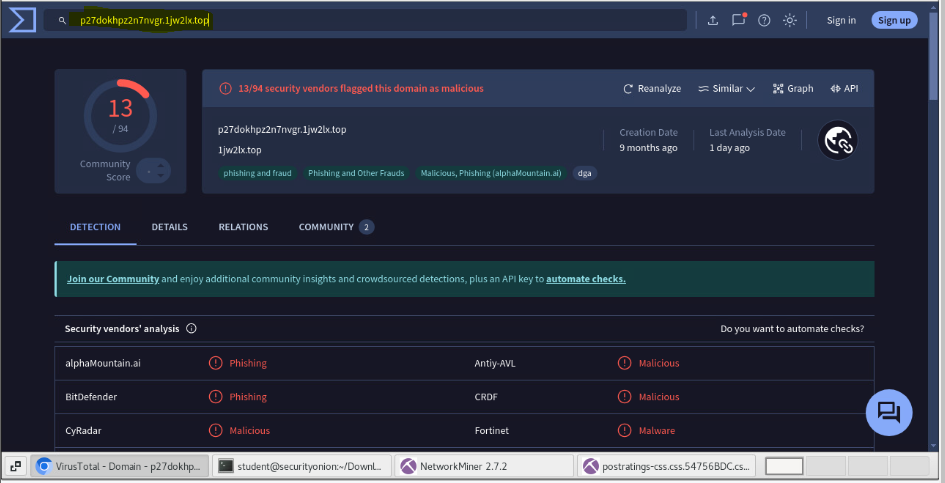
**Things to consider.**

* + **What files have been downloaded via HTTP and what do the malicious ones indicate?**
  + **What C2 is visible**
  + **What data about the infected PC has been exfiltrated?**
  + **What do the rules triggered for the infections tell you about likelihood of accurate identification of malware or a false positive?**
  + **How did the adversary identify the external IP address use to access this internal network?**

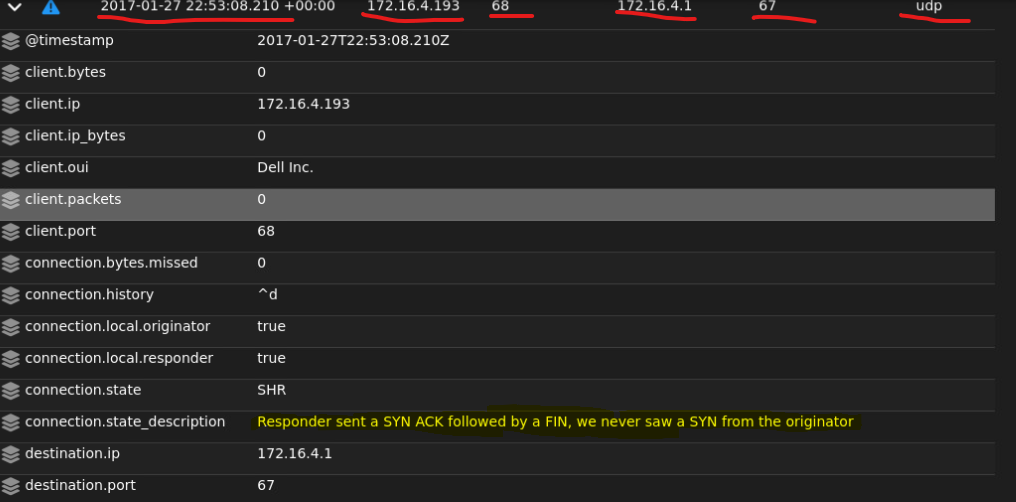






The alert **"ET MALWARE Ransomware/Cerber Onion Domain Lookup"** in Security Onion indicates that network traffic is attempting to resolve or access an .onion domain associated with **Cerber ransomware**. Cerber is a type of ransomware that encrypts files on an infected system and demands payment in cryptocurrency for the decryption key. In virus total it tells us the domain is malicious.

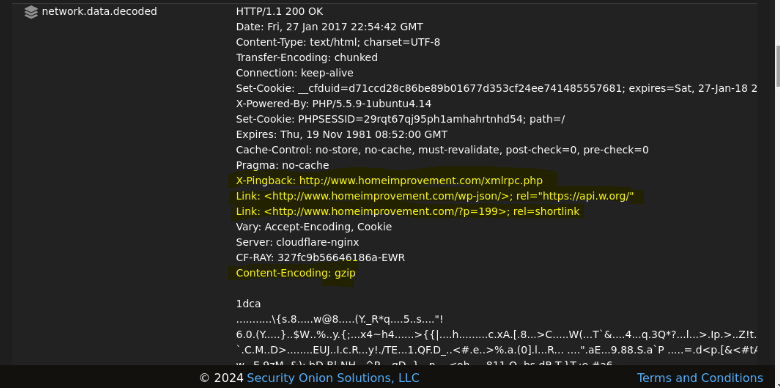


This connection state indicates that the server(172.16.4.1) sent a SYN-ACK as if responding to a connection attempt, followed by a FIN to close the connection, but the initial SYN from the client(172.16.4.193) was never seen.





The source IP is 104.28.18.74 port 80 and destination IP is 172.16.4.193 (internal machine)



Network.data.decoded shows the link to be “www.homeimprovement.com” and the content was enconded as a gzip.

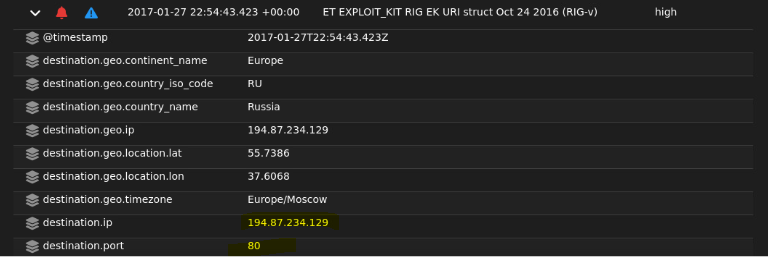
**Summary:** The alert highlights that an internal machine with IP 172.16.4.193 connected to an external IP 104.28.18.74 on port 80. The decoded network data shows that the request was directed to “www.homeimprovement.com”, but the content was encoded as gzip. This connection aligns with the ET EXPLOIT\_KIT Evil Redirector alert, which suggests that this site could be acting as a redirector, forwarding the user to a secondary malicious site associated with an exploit kit (EK). This redirection process is often used by exploit kits to deliver malware payloads by exploiting vulnerabilities on the targeted system. The gzip encoding is common in web traffic but may also indicate an attempt to obscure the content, making it harder to analyze directly.





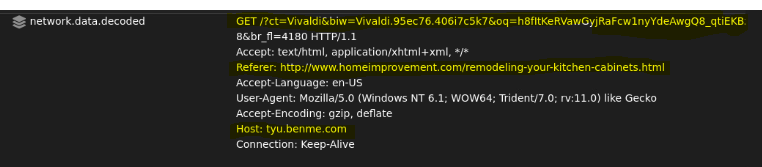


**Summary:** Just like the previous alert this alert, ET EXPLOIT\_KIT Evil Redirector Leading to EK March 15 2017, indicates that network traffic was detected which matches patterns associated with an exploit kit (EK) redirector.

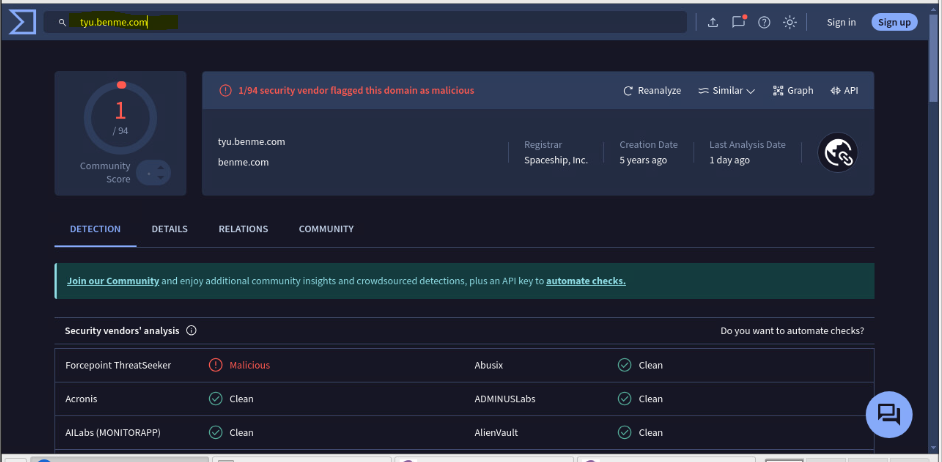




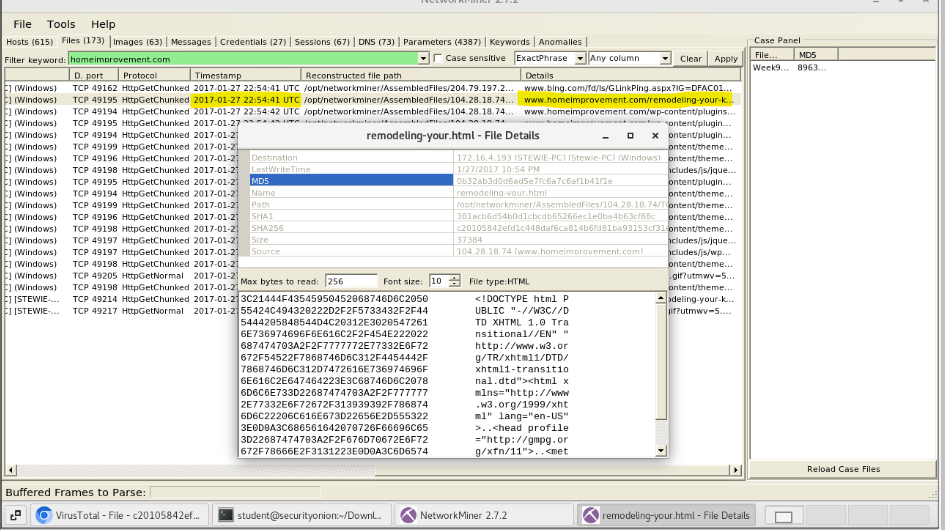
The source IP is 172.16.4.193 (internal machine) and destination IP is 194.87.234.129 port 80

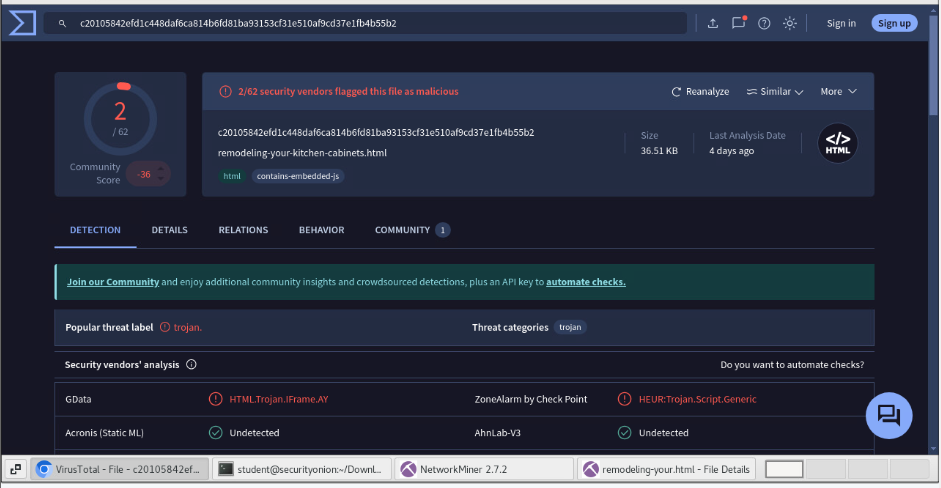


Network.data.decoded shows the GET request URI, the Refer to be “[www.homeimprovement.com](http://www.homeimprovement.com)” again and the host is tyu.benme.com



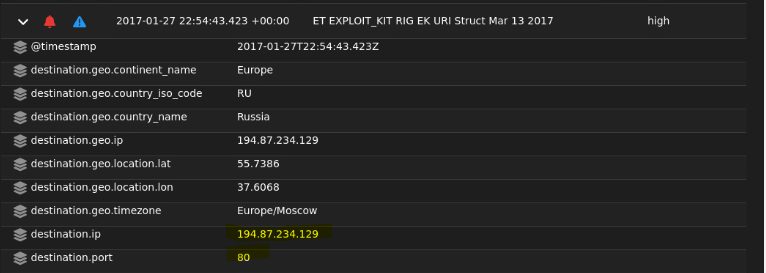
Looking up the host tyu.benme.com on virustotal showed it to be potentially malicious



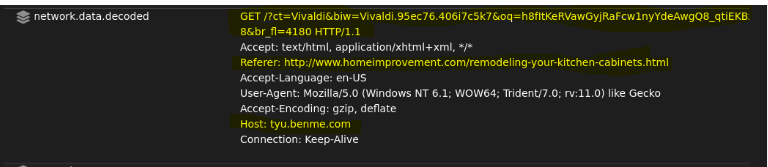


After finding the refer from the network.data.decoded, I put the md5 hash of the file in virustotal and it showed up to be potentially malicious.

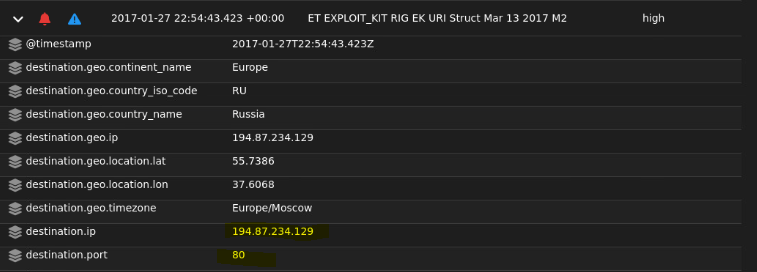
**Summary:** An internal machine with IP 172.16.4.193 made an HTTP GET request to 194.87.234.129 on port 80. The decoded network data reveals that the request's Referer field points to [www.homeimprovement.com](http://www.homeimprovement.com), while the actual Host is tyu.benme.com. Further investigation on VirusTotal flagged tyu.benme.com as potentially malicious, suggesting it may host or distribute harmful content. Additionally, analyzing the file associated with the md5 hash from the traffic revealed that it, too, was marked as potentially malicious. This activity aligns with the signature of the RIG Exploit Kit, where a seemingly legitimate website (homeimprovement.com) might be used to redirect users to a malicious host (tyu.benme.com), which then attempts to exploit the user’s system or download malware.

****

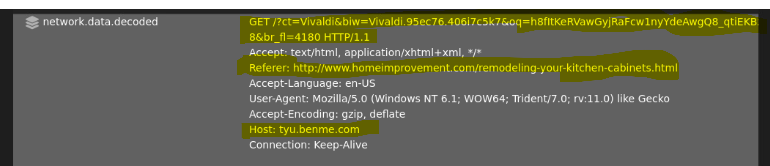
****

****

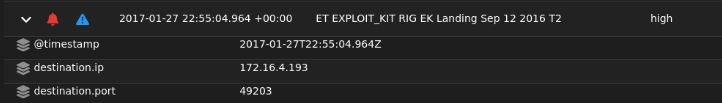
**Summary:** Just like the previous alert this alert reflects another attempt from 172.16.4.193 an internal machine to connect to the malicious server 194.87.234.129, continuing the same suspicious activity associated with the RIG Exploit Kit.

****

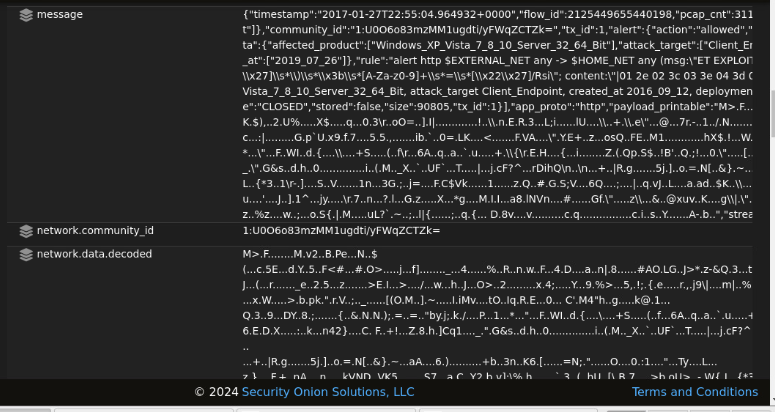
****

****

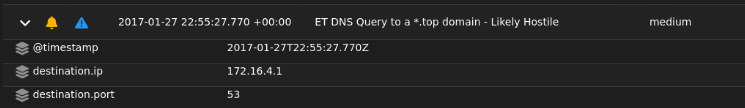
**Summary:** Just like the previous 2 alerts an internal machine 172.16.4.193 made an HTTP GET request to a known malicious IP 194.87.234.129 as part of an attack attempt using the RIG Exploit Kit. Which specifically targets vulnerabilities in browsers and their plugins using URL structure (URI) pattern commonly associated with RIG EK's traffic flow or payload delivery.







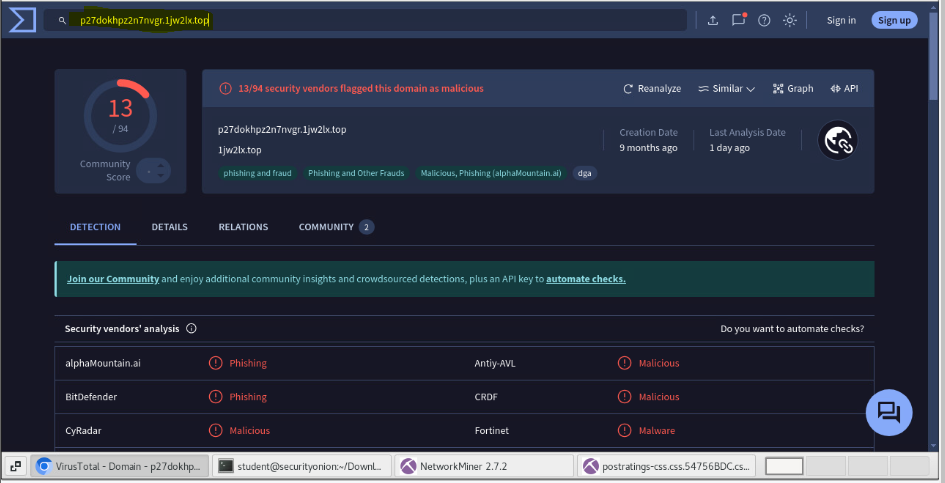
**Summary:** This alert indicates that network traffic matching a known RIG Exploit Kit (EK) landing page was detected. Signaling that a device within the network might have accessed a site or page associated with RIG EK, potentially leading to a malware infection.

****

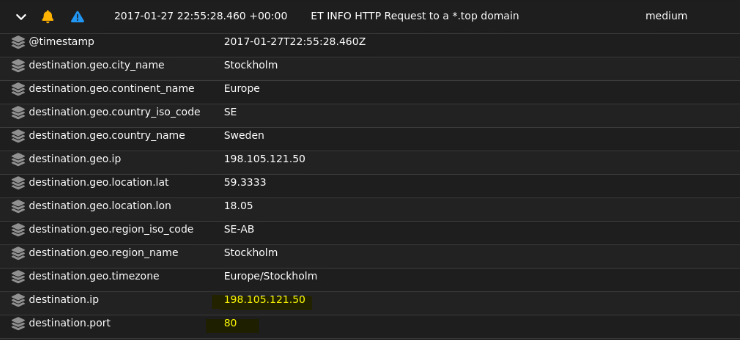
****

The source IP 172.16.4.193 (internal machine) and destination IP 172.16.4.1 (DNS Server)

****

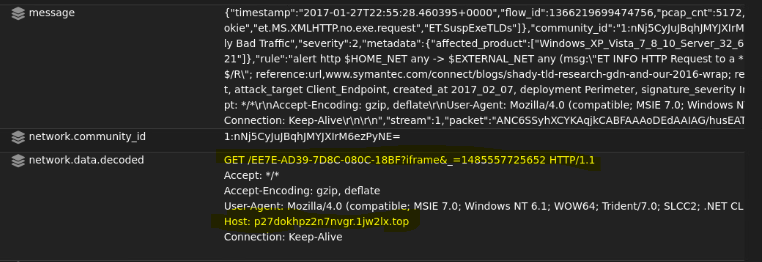


**Summary:** An internal machine with IP 172.16.4.193 attempted a DNS query through its local DNS server at 172.16.4.1 to resolve a .top domain, which is often associated with malicious activities. This query to a .top domain suggests that the internal machine might be attempting to reach a potentially harmful external server. Domains with the .top TLD are commonly used for phishing, malware distribution, and command-and-control (C2) operations. The activity implies that the internal machine may be trying to establish a connection with a Tor-based Onion service or another malicious service used for C2 communications or data exfiltration.





The source IP 172.16.4.193 (internal machine) and destination IP 198.105.121.50 on port 80

****

Network.data.decoded shows the HTTP GET request, the Host to the .top domain and the User-Agent which shows an outdated version of Internet Explorer (IE7)

**Summary:** The alert indicates that an internal machine with IP 172.16.4.193 made an HTTP GET request to a potentially malicious .top domain hosted on 198.105.121.50 over port 80. The HTTP headers reveal that the User-Agent is set to an outdated version of Internet Explorer (IE7), suggesting one of two possibilities: either an old, vulnerable system was used, or a malicious actor is deliberately using an outdated User-Agent to mimic legitimate traffic and avoid detection.