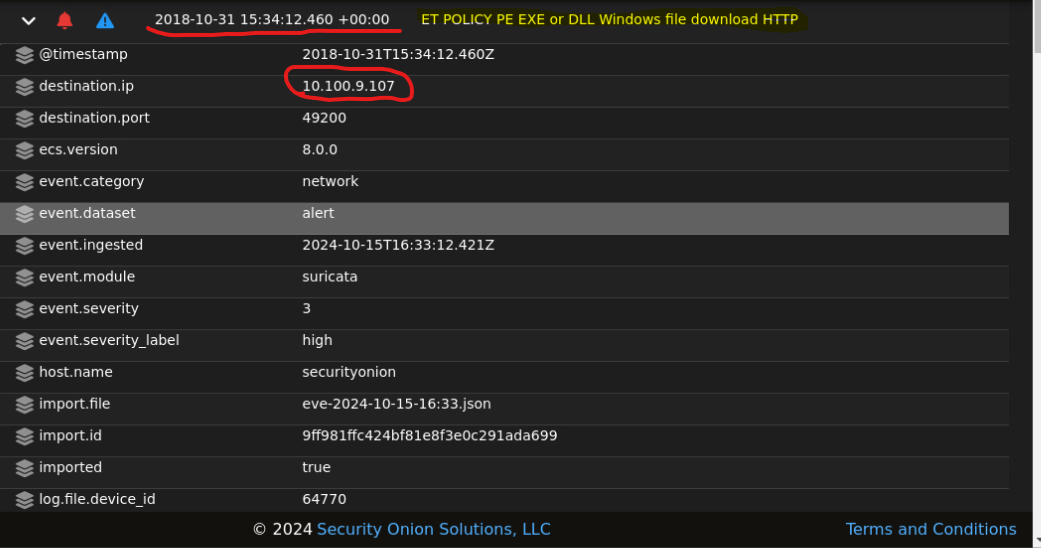
**Mamadou Bah**

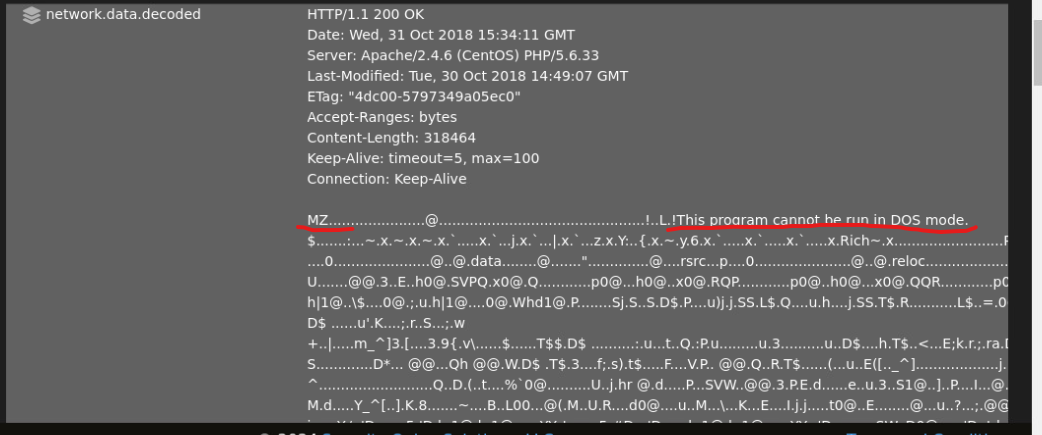
**Pcap Analysis on ET Policy alerts**

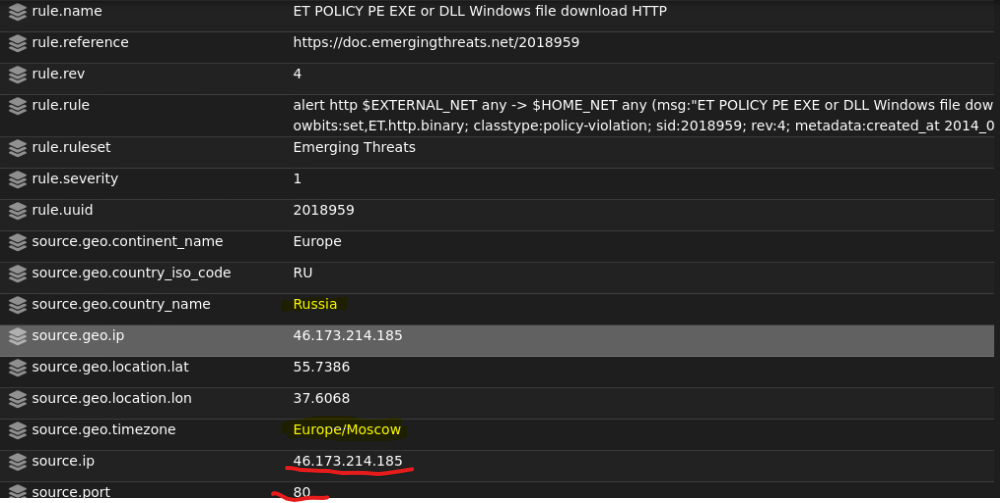
**10/31/2024**

**Things to research:**

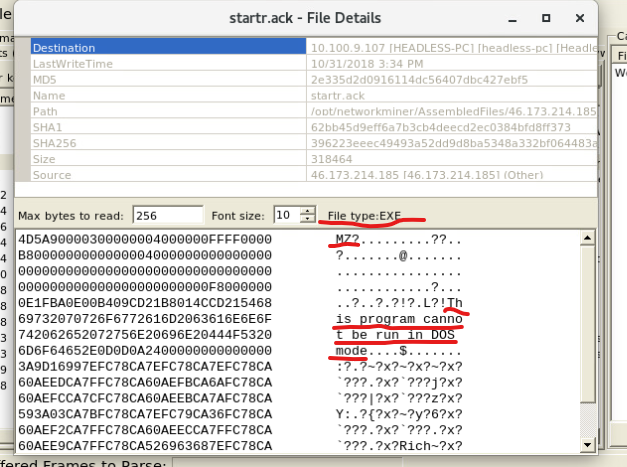
* + **What is the sequence of events from initial contact, through to established C2?**
  + **What was the initial infection traffic and infected PC?**
  + **What is the IP address, port and domain for the C2?**
  + **Are there secondary infections?**
  + **What suspicious indicators are there for certificates used by the C2 servers**



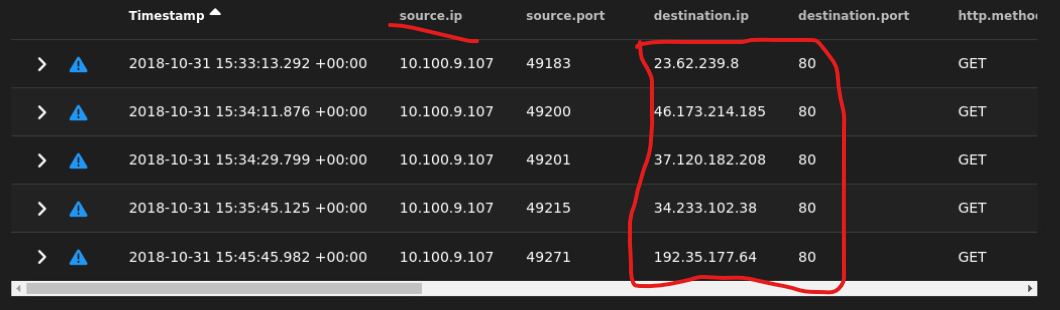




Downloaded a windows executable over HTTP at 15:34:12.460 on 2018-10-31 to 10.100.9.107 from 46.173.214.185

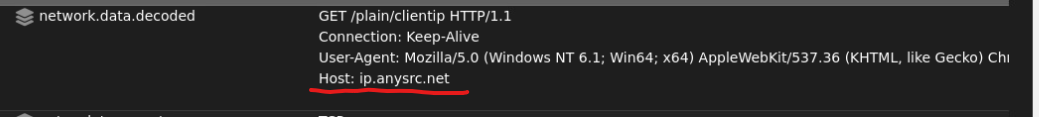


NetworkMiner shows the same things that I found in Security Onion.



The Source and Destination IP Addresses shows who and where things came from





The alert shows that a client is trying to connect to the website ip.anysrc.net, likely to perform an IP lookup or resolve an external IP address. This means it’s looking for a site or domain to load its content or service.



alert indicates that a network connection is using an SSL/TLS certificate issued by the OpenSSL Demo Certificate Authority (CA), specifically from the organization "Internet Widgits Pty Ltd." This type of certificate is typically used for testing or demonstration purposes, not for secure communications in a production environment. The alert suggests a potential security risk, as demo or test certificates should not be used for real, secure connections. This suggests that the connection to ip.anysrc.net is using a test or demo SSL certificate. This is a security risk because it’s not a trusted or valid certificate for real connections.