Alex Smetana

CIS311 – Lab01

02/03/2023

File 1 - 2b5e3fcc801c0d1592eab89bafde34e2.pcap

No malicious or suspicious activity found.

File 2 - 3cfd2b1a67ab3703be3668dad24627ca.pcap

Malicious Activity - ET POLICY PE EXE or DLL Windows file download HTTP

1) Essentially, the alert "ET POLICY PE EXE or DLL Windows file download HTTP" means an executable file was downloads using HHTP (Hyper Text Transfer Protocol) or the internet. It doesn't necessarily mean malware was downloaded, however is probable that is contains some malicious activity. For whatever reason, the computer deems it as suspicious.

   "Someone downloaded a Windows executable file or DLL over HTTP. In most cases this is just noise unless you've prohibited downloading of executable files in your environment." (Security Stack Exchange).

   https://security.stackexchange.com/questions/202654/intrusion-prevention-system-detected-et-policy-pe-exe-should-i-worry

Malicious Activity - ET POLICY HTTP traffic on port 443 (POST)

2.) The alert "ET POLICY HTTP traffic on port 443" is telling the user that unencrypted traffic has gone through the port. Port 443 is a port that is used for network traffic with either HTTP or HTTPS. Port 443 is generally encrypted however the notification is alerting the user that the traffic is the most secure due to it not being encrypted.

"The message is saying, I saw unencrypted HTTP traffic travelling over a port generally reserved for HTTPS encrypted traffic. It is more of a notification/warning as opposed to an alert about truly malicious activity. You could safely disable that rule if you wish" (Forum negate).

https://forum.netgate.com/topic/93479/et-policy-http-traffic-on-port-443-post/3

Malicious Activity - ET POLICY Application Crash Report Sent to Microsoft

3.) The "Application Crash Report Sent to Microsoft" occurs after an application crashes, allowing for a user to report the details of the crash to Microsoft. The reason for the application crashing is unknown however, this feature can help further the crashes from happening the future.

"The error reporting feature enables users to notify Microsoft of application faults, kernel faults, unresponsive applications, and other application specific problems" (Microsoft).

https://learn.microsoft.com/en-us/windows/win32/wer/windows-error-reportin

Suspicious Activity - ProtocolDetector::Protocol_Found

4.) Protocol detection is the ability to determine the connection by inspecting traffic. It was able to identify traffic by using a TCP connection.

"Put simply, protocol detection is the ability to determine the protocol in use on a TCP connection by inspecting the traffic on the connection."

https://linkerd.io/2021/02/23/protocol-detection-and-opaque-ports-in-linkerd/

File 3 - 8e90c2a233049e54b1c6a8ee3d22651e.pcap

Malicious Activity - ET POLICY HTTP traffic on port 443 (POST)

Same error in file 2

Suspicious Activity - ProtocolDetector::Protocol_Found

Same error in file 2

Suspicious Activity - ProtocolDetector::Server_Found

5.) Protocol detection is the ability to determine the connection by inspecting traffic. It was able to identify the sever.

"Put simply, protocol detection is the ability to determine the protocol in use on a TCP connection by inspecting the traffic on the connection."

https://linkerd.io/2021/02/23/protocol-detection-and-opaque-ports-in-linkerd/

File 4 - a28f5c309ba487151009168f333844c2

Malicious Activity - ET TROJAN Loki Bot User-Agent (Charon/Inferno) (x12)

6.) The alert “ET TROJAN Loki Bot User-Agent” is an alert saying that a Trojan (Loki Bot) was detected on the computer. A Loki bot is malware with the intended use of stealing credentials through the use of mal spam.

“Lokibot is a password/info-stealing malware, delivered through malware spam (malspam) campaigns, and notably known for the wide range of applications that it targets.”

https://www.f-secure.com/v-descs/trojan_w32_lokibot.shtml

Suscipious Activity - None

File 5 - c96d086468b9b0f442a84ce5309144bb.pcap

Malicious Activity - ET POLICY External IP Lookup ip-api.com

7.) Used by advertise to test internet access and acquire their IP address to gain access to their IP. Commonly used with Trickbot – Information stealer.

“Identifies domains commonly used by adversaries for post-exploitation IP lookups. It is common for adversaries to test for Internet access and acquire their external IP address after they have gained access to a system. Among others, this has been observed in campaigns leveraging the information stealer, Trickbot.”

https://www.elastic.co/guide/en/security/master/external-ip-lookup-from-non-browser-process.html

Suspicious Activity - None