



STUDYDADDY

Get Homework Help From Expert Tutor

[Get Help](#)

Fordham University

CISC 6680 Intrusion Detection & Network Forensics

Professor: Ravi Tanikella

Packet Analysis Assignment 3

Scenario

You are working as an analyst reviewing suspicious network events at Fictitious Corporations' Security Operations Center (SOC). Things have been quiet for a while. However, you notice several alerts occur within minutes of each other on separate hosts.

Your were able to retrieve a pcap of network traffic, and you have a list of Snort and Suricata events from the activity. You are also able to capture the following image

| ST | CNT | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|-----|----------|---------------|-----------------|-------|-----------------|-------|----|--|
| RT | 1 | 3.8859 | 2016-01-07... | 192.168.122.52 | 49200 | 192.185.21.183 | 80 | 6 | ETPRO CURRENT_EVENTS Possible Evil Redirector Leading to EK Dec 03 2015 M3 |
| RT | 4 | 3.8861 | 2016-01-07... | 92.51.131.150 | 80 | 192.168.122.132 | 49182 | 6 | ET CURRENT_EVENTS Evil Redirector Leading to EK Mon Dec 21 2015 5 |
| RT | 2 | 3.8865 | 2016-01-07... | 192.168.122.132 | 49195 | 89.38.144.75 | 80 | 6 | ETPRO CURRENT_EVENTS Possible Neutrino Landing Oct 20 2015 M9 Landing URI Struct |
| RT | 2 | 3.8868 | 2016-01-07... | 89.38.144.75 | 80 | 192.168.122.132 | 49215 | 6 | ETPRO CURRENT_EVENTS Neutrino EK Payload Dec 06 2015 M2 |
| RT | 2 | 3.8870 | 2016-01-07... | 192.185.21.183 | 80 | 192.168.122.52 | 49200 | 6 | ETPRO CURRENT_EVENTS Evil Redirector Leading to EK Dec 03 2015 M1 |
| RT | 9 | 3.8873 | 2016-01-07... | 192.168.122.132 | 49218 | 188.138.101.154 | 80 | 6 | ET TROJAN CryptoWall Check-in |
| RT | 9 | 3.8880 | 2016-01-07... | 192.168.122.130 | 49220 | 216.158.85.7 | 80 | 6 | ETPRO TROJAN Nemucod Downloading Payload |
| RT | 7 | 3.8884 | 2016-01-07... | 216.158.85.7 | 80 | 192.168.122.130 | 49220 | 6 | ET POLICY PE EXE or DLL Windows file download |
| RT | 6 | 3.8886 | 2016-01-07... | 216.158.85.7 | 80 | 192.168.122.130 | 49220 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe extension M2 |
| RT | 6 | 3.8887 | 2016-01-07... | 216.158.85.7 | 80 | 192.168.122.130 | 49220 | 6 | ET INFO EXE - Served Attached HTTP |
| RT | 4 | 3.8891 | 2016-01-07... | 174.36.186.235 | 80 | 192.168.122.130 | 49223 | 6 | ET POLICY PE EXE or DLL Windows file download |
| RT | 2 | 3.8893 | 2016-01-07... | 174.36.186.235 | 80 | 192.168.122.130 | 49223 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe extension M2 |
| RT | 2 | 3.8894 | 2016-01-07... | 174.36.186.235 | 80 | 192.168.122.130 | 49223 | 6 | ET INFO EXE - Served Attached HTTP |
| RT | 16 | 3.8898 | 2016-01-07... | 184.168.173.1 | 80 | 192.168.122.130 | 49224 | 6 | ET POLICY PE EXE or DLL Windows file download |
| RT | 16 | 3.8906 | 2016-01-07... | 184.168.173.1 | 80 | 192.168.122.130 | 49224 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe extension M2 |
| RT | 16 | 3.8914 | 2016-01-07... | 184.168.173.1 | 80 | 192.168.122.130 | 49224 | 6 | ET INFO EXE - Served Attached HTTP |
| RT | 1 | 3.9032 | 2016-01-07... | 192.168.122.132 | 52568 | 8.8.4.4 | 53 | 17 | ET TROJAN Cryptowall .onion Proxy Domain |
| RT | 1 | 3.9033 | 2016-01-07... | 192.168.122.132 | 52568 | 8.8.4.4 | 53 | 17 | ETPRO POLICY DNS Query to .onion proxy Domain (waytopaytosystem.com) |
| RT | 1 | 3.9034 | 2016-01-07... | 95.128.181.144 | 80 | 192.168.122.132 | 49226 | 6 | ETPRO TROJAN AlphaCrypt Payment Page |

Your Report Submission

You'll need to write a report. Your report should include with detailed screen shots with marking identifying each of the items listed below.

- When did the event take place? E.G. Date and time range of the traffic in question.
- IP address, MAC address, and host name for each of the computers.
- Description of the activity for each of the computers (what happened, if the host became infected, any details, etc.).
- A screenshot for each infected host with filters applied so you only see traffic for that host
- Infection vector and payload if present. Correlate with all files to confirm your findings.
- A conclusion with recommendations for any follow-up actions.



STUDYDADDY

Get Homework Help From Expert Tutor

[Get Help](#)