2015-03-09 - TRAFFIC ANALYSIS EXERCISE

**SCENARIO**

1) What is the host name of the Windows computer that gets infected?

A) WIN-C2KE6N4W3N1 ( Use nbns filter to find the host name)

2) What is the IP address of the Windows computer that gets infected?

A) 172.16.138.158  
3) What is the MAC address of the Windows computer that gets infected?

A) f0:4d:a2:92:e0:a7  
4) What exploit kit infected the computer? (Angler, Fiesta, Nuclear, Neutrino, Rig?)

A) Nuclear Exploit Kit ( Kelihos bot)  
5) What compromised website kicked off a chain of events leading to the exploit kit?

A) fortunet.biz  
6) What is the IP address and domain name of the exploit kit?

A) soquumaihi.co.vu (178.62.142.240)