**Question 4**

An organization’s SOC analyst, through examination of the company’s SIEM, discovers what she believes is Chinese-state sponsored espionage activity on the company’s network. Management agrees with her initial findings given the forensic artifacts she presents are characteristics of malware, but management is unclear on why the analyst thought it was Chinese-state sponsored. You have been brought in as a consultant to help determine 1) whether the systems have been compromised and 2) whether the analyst’s assertion has valid grounds to believe it is Chinese state-sponsored. What steps would you take to answer these questions given that you have been provided a MD5 hashes, two call back domains, and an email that is believed to have been used to conduct a spearphishing attack associated with the corresponding MD5 hash. What other threat intelligence can be generated from this information and how would that help shape your assessment?

**Question 19**

What can be factually said about the following VirusTotal submission and what can be inferred based off of this data (SHA-256 == 2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525)

**Question 23**

APT 34 uses the following series of commands strung together in a batch file that it runs on a victim’s computer. Explain what each of these commands does and how the results would benefit APT 34?
whoami & hostname & ipconfig /all & net user /domain 2>&1 & net group /domain 2>&1 & net group "domain admins" /domain 2>&1 & net group "Exchange Trusted Subsystem" /domain 2>&1 & net accounts /domain 2>&1 & net user 2>&1 & net localgroup administrators 2>&1 & netstat -an 2>&1 & tasklist 2>&1 & sc query 2>&1 & systeminfo 2>&1 & reg query "HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1

**Question 28**

Describe what an advanced persistent threat (APT) is, how the term was derived i.e. what it originally meant, what it currently means, and an example, including the APT name, company that identified the APT, the actor the company believes is behind the activity, and who the APT targeted and what tools, techniques, and procedures they used during their operations.

**Question 29**

Your boss has come to you, a strong performing junior security analyst, with a newly released FireEye report on APT 29, known as "Hammer Toss". He claims that your company's business profile fits into the bucket described in the report to be targeted by APT 29, which allegedly has ties to the Russian Government. He presents you with the following graphic and indicators of compromise from the report and asks you to write a YARA signature to identify if your systems have been compromised and to prevent potential future compromise. Please write a YARA signature based on the following information.

* The malware can be identified by MD5 hash value d3109c83e07dd5d7fe032dc80c581d08 or SHA1 hash value 42e6da9a08802b5ce5d1f754d4567665637b47bc
* HammerToss uses the following PowerShell command on a victim's system: Powershell.exe -ExecutionPolicy /bypass -WindowStyle hidden –encodedCommand
* The uploader HammerToss uses the following preconfigured to use a hard-coded URL for its command and control: hxxps://www.twitter.com/1abBob52b
* HammerToss uses a hashtag, in this case #101docto to indicate that the encrypted data begins at an offset of 101 bytes in command and control image file and that the characters "docto" should be added to the encryption key to decrypt the data.