Petya ransomware: Like WannaCry, but more ferocious

What is Petya?

- A new strain of ransomware called “Petya” is sweeping across the globe as of Tuesday, June 27th, 2017. It is very similar to the WannaCry ransomware.
- More than 2,000 organizations have been impacted within a day (mostly in Europe)
- Petya and newer iterations called “NotPetya” or “GoldenEye” use stronger encryption keys than WannaCry. More difficult to reverse engineer and decrypt.
- It avoids the design flaws of WannaCry by not encoding a “kill switch” that allowed security analysts to stop the spread of WannaCry around the world. Petya shows no signs of being contained.
- Once inside the network, Petya steals administrative credentials, giving it control over powerful system management tools like Windows PsExec and Windows Management Instrumentation to instruct all PCs to run the malware.

Why do you need ASK Live Security Monitoring- Powered b Arctic Wolf Networks CyberSoc?

- Artic Wolf Security Engineers have seen several instances of Petya targeting customers; each time they have been able to notify the users within 5 mins and help them take appropriate action.
- Arctic Wolf Networks is able to detect new strains of ransomware because we look at endpoint behavior and do not rely on signatures only
- We are able to detect new strains of ransomware because we continuously monitor your network 24/7, apply customized rules (CRulE) to detect indicators of compromise (IOCs), and alert you on anomalous network traffic associated with Petya and WannaCry
- Arctic Wolf can help remediate any infections like Petya if customer is infected:
  - ⇒ Identify which endpoints are or are not infected by this new strain of ransomware
  - ⇒ Identify how the ransomware entered the customer’s environment so future infections can be mitigated
  - ⇒ Expert Security Engineers advise customers step by step until they are free of ransomware