Title: Mapping Adversary Infrastructure Using DNS  
Proposer: Merike Käo  
Author and Speaker: Merike Käo, CTO Farsight Security  

Description  
Nothing good or bad can happen on the Internet without involving the Domain Name System (DNS). DNS offers a commanding view of both the local and global Internet, and can provide unparalleled intelligence on cybercriminals and their attack methods. During their investigations, incident response professionals are increasingly using DNS to build out Indicators of Compromise (IOC)s and other threat indicators to map the attackers' entry and lateral movement throughout their network. In this presentation, “Mapping Adversary Infrastructure Using DNS,” Farsight Security CTO Merike Käo will provide the latest insights on the value of DNS to today’s cyber investigations as well as real-world examples of how incident responders, SOC analysts and more are using these real-time Global DNS observations to significantly improve response time and accuracy to today's cyberattacks.  

The presentation will cover:  
• Almost all cybercrimes involve IP addresses/domain names – phishing, controlled substance sales, online child abuse materials, knock-off merchandise, malware  
• Why cybercriminals use more than one IP address or domain name to commit crime  
• Why Bad Guys may share their evil online infrastructure  
• Passive DNS and how it can be used to make connections adversary infrastructure and provide examples including:  
  o Example #1: Illegal Controlled Substance  
    In this example, we will show how Passive DNS can be used to work a serious crime involving the sale of Schedule I controlled substance (or online fraud); Demonstrate how one initial lead, easily found in a major search engine, can be used to expose many additional related sites, thereby preventing incomplete or ineffectual action against the criminal actors (e.g., take down one or two sites, leave many others); Illustrate there are major issues with domain WHOIS quality control  
  o Example #2: Counterfeit Merchandise  
    Demonstrate how Passive DNS is a useful tool for those involved in brand protection and the fight against the sale of counterfeit merchandise; Outline how an easily identified starting point can be developed into a large number of related apparently infringing domains and by resolving those domains, demonstrate how we can then find additional IP addresses involved with the apparently infringing behavior, and those IP will often yield additional domains of interest
Example #3: Phishing
Demonstrate how Passive DNS can be used to develop leads relating to phishing, starting from a single example from PhishTank; Discuss how one lead allows us to find many additional related phishing sites, and by expanding the IPs used by those related sites, we've found further phishing sites; Show how blocking the entire network ranges used by the phishing crews would be potentially problematic, since those ranges include what appear to be major government web sites, and educational institutions.