# DeepSec 2017 Talk: Uncovering And Visualizing Botnet Infrastructure And Behavior – Andrea Scarfo & Josh Pyorre

Posted on **September 28,2017** by **sanna**

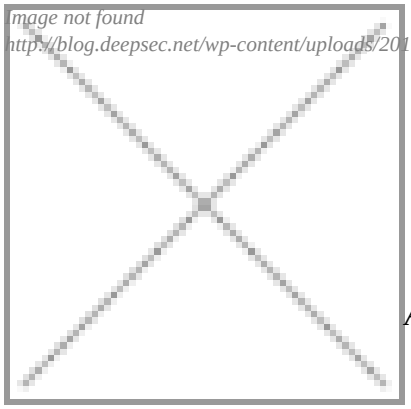
When you read about information security, then you might get the impression that there are lots of nameless threats Out There™. Especially when it comes to networked malicious software, i.e. malware, that forms robot armies, the picture gets a lot more vague and foggy. So you need to get some details to sharpen your view. There are some means how to do this, and you will be told at DeepSec 2017 by Andrea Scarfo and Josh Pyorre.

How much information about a botnet can one find using a single IP address, domain name or indicator of compromise (IOC)? What kind of behavior can be determined when looking at attacker and victim infrastructure?

In an attempt to discover and analyze the infrastructure behind large-scale malware activity, Andrea and Josh began their research with known indicators from popular botnets, such as Necurs.

This presentation will highlight co-occurring malicious activities observed on the infrastructure of popular botnets. Andrea and Josh will demonstrate practical techniques for analyzing botnet and malware traffic to provide context that can be used in identifying actor and victim infrastructure and to discover additional IOC's. They will also show how political and societal world events may influence specific types of malware activity based on locations and times of malware events. Finally, Andrea and Josh will demonstrate a visualization framework that can be used to better understand the connections between infrastructure, threats, victims, and malicious actors.

*Josh and Andrea are Security Researchers with Cisco Umbrella (formerly OpenDNS).*




*Andrea began her career in Support and worked as a Sysadmin for 12 years. She has worked with Hewlett Packard and the Town of Danville, California. Security has always been her passion. She began working with OpenDNS as a Security Researcher on the Security Research team in 2015 and spends her days working to make the Internet a safer place by hunting attackers and malware. She presented at B Sides Las Vegas in 2016 and BSides Amsterdam in 2017.*

*the SOC at Mandiant. His professional interests involve network, computer and data security with a goal of maintaining and improving the security of as many systems and networks as possible. Josh has presented at Defcon, B Sides Austin, Chicago, San Francisco, Los Angeles, Amsterdam and Vienna, Source Boston, Source Seattle, Derbycon, InfoSecurity World Europe, DeepSec Vienna and Qbit Prague. He hosted season 1 of rootaccesspodcast.com.*

Posted in:Conference,Internet | Tagged:Botnet,DeepSec,Malware,Talk | With 0 comments