Damsky
tech

Training:

DNS intelligence

Instructor
Irena Damsky

Duration
Full day.

Description
DNS is the one of the basic layers that holds the Internet together. Without it, not much else works... even malware. In this training we will focus on how to use DNS to the advantage of defending networks. With good techniques it is possible to find a great deal of misuse based on DNS such as DGAs, fast/double flux networks, phishing, and brand impersonation. Tools like passive DNS, whois, and active probing allow defenders to proactively search for malicious indicators before they are operationalized so defenders can get ahead of the attack cycle.

This is a training on the usage of DNS for malware hunting, detection of new infrastructure, discovery of new network assets and other "research" type of products. In this training we will focus on hands on labs while covering also some theory and history of DNS.

Course modules:
- RECAP - DNS overview
- Gathering data using DNS
- Overview of whois information and effects of GDPR
- Overview of passive DNS (pDNS)
- Tools
- Advanced "Research" Topics
  - Pivoting
  - DGAs
  - Malicious domain detection
  - And more

Pre-requisites
Basic scripting (Bash/Python)
Basic understanding of networking and malware life cycle

Technical requirements (from students)
Laptop capable of
- Running bash / connecting to ssh
- Running VMs

Technical requirements (from venue)
- Stable internet connection

contact@damsky.tech +972-52-329-4417

- Audio Video
- Flipchart / Whiteboard

Intended audience:

Network analysts and defenders, SOC analysts, Incident responders
Red teamers and pen testers
LE
Anyone who is interested in learning a new skillset that will allow them to get ahead of their adversaries

About the instructor

Irena Damsky is the founder of Damsky.tech – CTI Research, Training and Consulting. She is a security and intelligence researcher and developer based in Israel. Her focus is on threat intelligence, networking, malware & data analysis and taking out bad guys as she is running the company and provides the different services.

Prior to starting Damsky.tech, Irena held different roles in the industry from ranging from Threat intelligence leader to VP of Security Research and served over six years in the Israeli Intelligence Forces, where she now holds the rank of Captain in the Reserve Service. She is a frequent speaker at security events, holds a BSc and MSc in Computer Science, and is fluent in English, Russian, and Hebrew.

Website: https://damsky.tech

Twitter: @DamskyIrena

LinkedIN: https://www.linkedin.com/in/irenadam/

contact@damsky.tech +972-52-329-4417