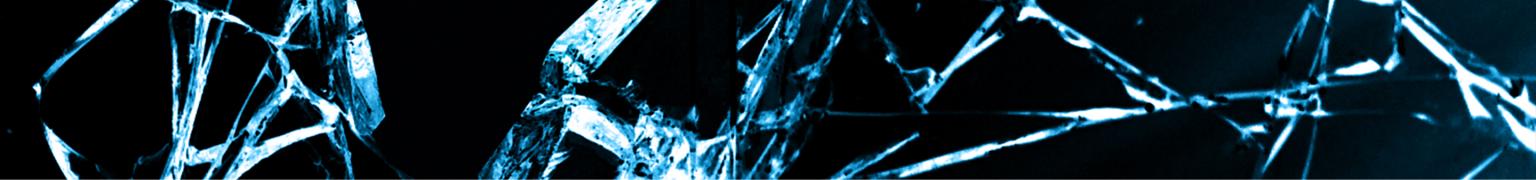




JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS



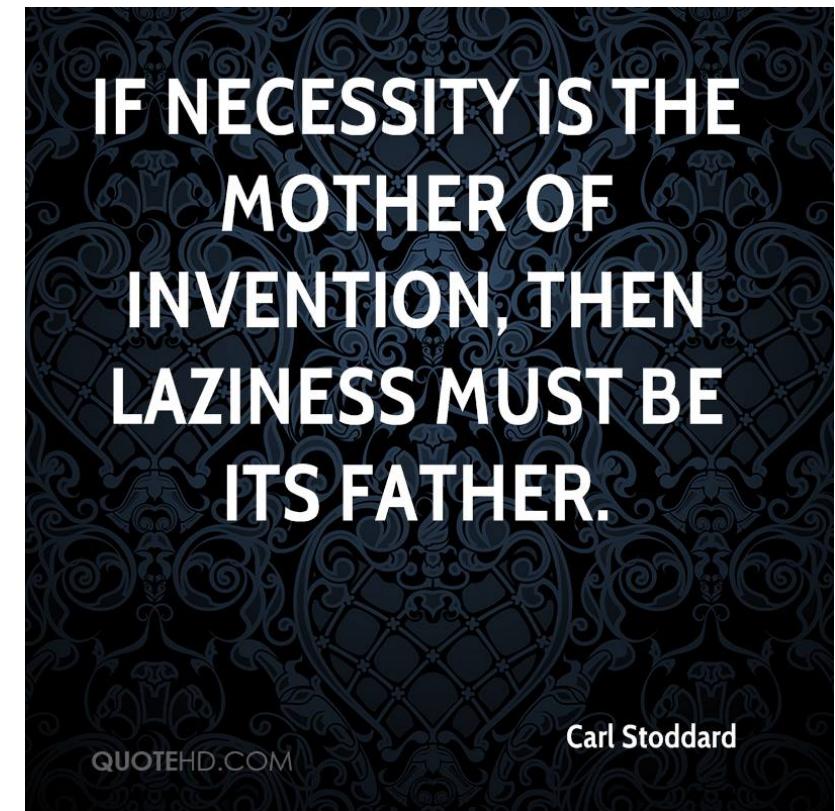
Maltese

Malware Traffic Emulating Software

Sasi Siddharth Muthurajan, Security Researcher
Barak Raz, Security Research Manager

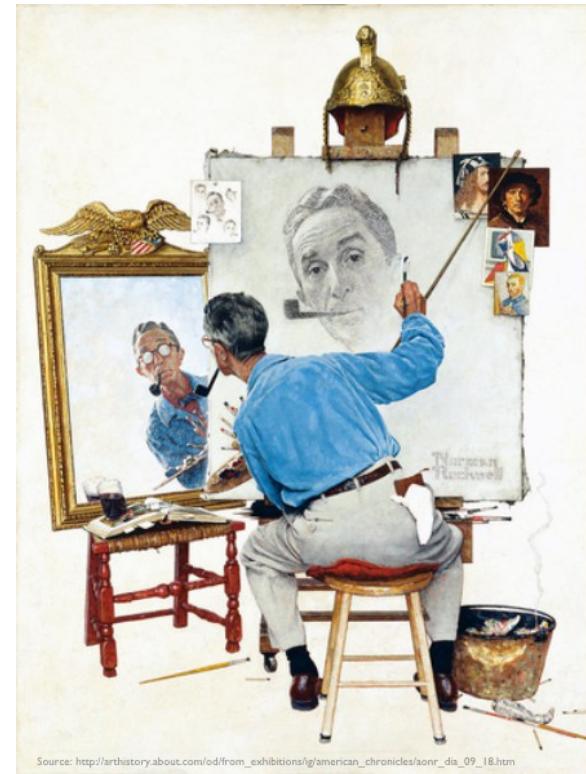
Why

- Verifying the effectiveness of DNS based malware detectors
 - Existing security deployments
 - New security deployment
 - Against new malware outbreaks



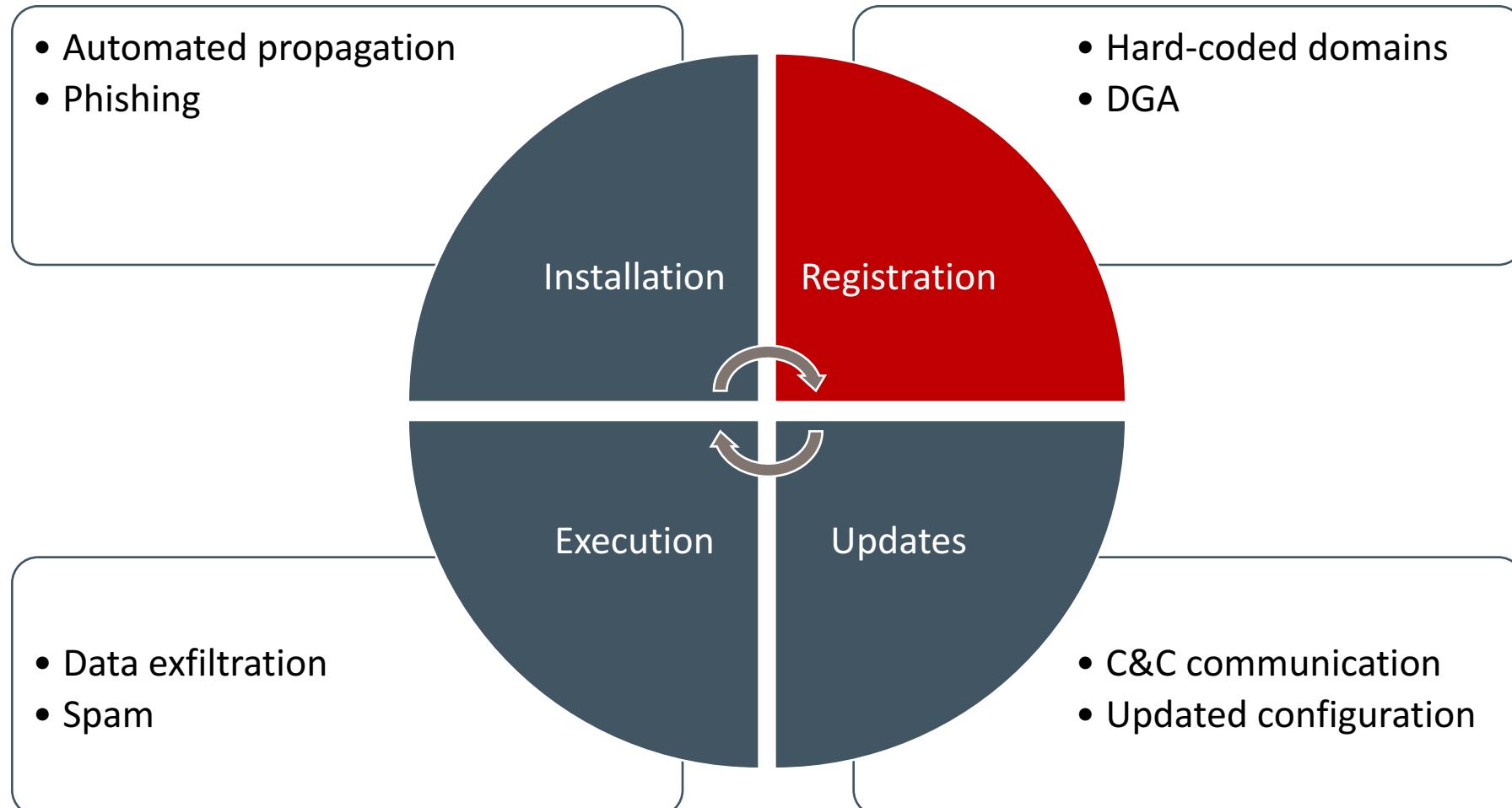
How

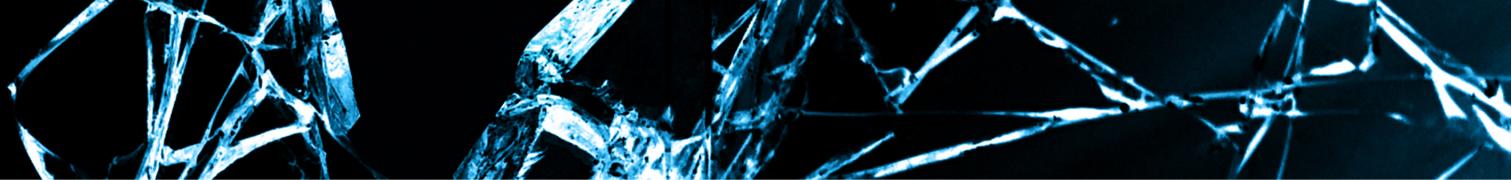
- Emulate malicious DNS traffic of any given malware
 - On demand
 - Without interacting with real malware samples
 - In a safe way without any risk of infection



Emulate
Don't Imitate

Malware Communication Lifecycle





What

- Malicious domains
 - Replay
 - Pre-recorded pcaps
 - List of known domains
 - Create DNS traffic based on a Domain Generation Algorithm (DGA)
- Traffic model
 - Used to accurately emulate the traffic patterns of a malware
 - Modeled based on the probability distribution of malware requests

Where

- GitHub: <https://github.com/HPE-AppliedSecurityResearch/maltese>

Who

- Email: maltese@hpe.com

