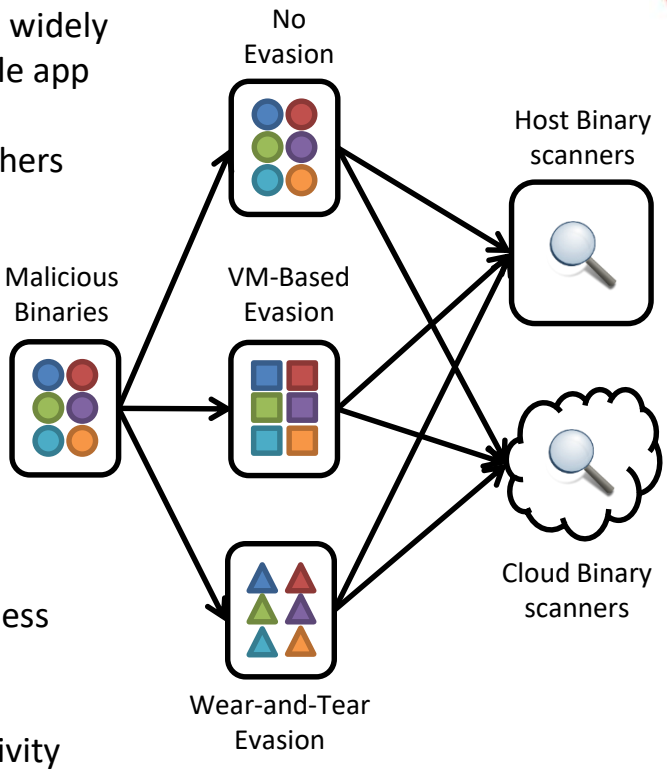
TWC: Small: Combating Environment-aware Malware

Challenge

- Malware analysis sandboxes are widely used by antivirus vendors, mobile app marketplaces, threat detection appliances, and security researchers
- Current sandboxes are prone to evasion by environment-aware malware that alters its behavior once it detects that it is being executed on a monitored environment



Solution

- Study new environment-awareness techniques that evade existing countermeasures by relying on artifacts related to past user activity
- Assess the evasion potential of these techniques against dynamic malware analysis systems
- Develop methods for automatically introducing realistic past user activity artifacts in dynamic analysis systems to counter next-generation, environment-aware malicious code

Award Number: 1617902
(2016 – 2019)

Stony Brook University
Michalis Polychronakis
(mikepo@cs.stonybrook.edu)
Nick Nikiforakis
(nick@cs.stonybrook.edu)

Stony Brook University

Scientific Impact

- Investigation of a novel class of malware evasion techniques
- Systematic analysis of a vast space of artifacts across different devices, operating systems, and software
- Automated generation of artificial but realistic analysis environments robust to evasion

Broader Impact

- Raise awareness by assessing the magnitude of the threat posed by environment-aware malware
- Software prototypes to help practitioners identify weaknesses of existing sandboxes and deploy proactive countermeasures