RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HT-R02

Understanding Malware Provenance: A Federal View

MODERATOR: **Dr. Peter Fonash**

Chief Technology Officer
Cybersecurity and Communications, Department of Homeland Security

PANELISTS:

Dr. Phyllis Schneck
Deputy Under Secretary
Cybersecurity and Communications,
Department of Homeland Security

Thomas Ruoff
Director, Technology Innovation and Mission Integration
Cybersecurity and Communications,
Department of Homeland Security

Lisa Kaiser
Computer Scientist
Cybersecurity and Communications,
Department of Homeland Security

#RSAC

Understanding Malware Provenance

- Let's define terms – What is 'Malware Provenance?'
- Who uses this technology? Why do we care?
- Why should you care?
- What are we doing?
- Panel Discussion and Questions

What is ‘Malware Provenance?’

- Malware provenance is the art and science of attributing elements of one object to another, similar to genetics
- This is used every day in many ways: college student papers are analyzed to determine the true author

Who Uses this Technology?

- Education for authorship, industry has this “baked” into many cybersecurity elements
- Cybersecurity industry developing capability to produce actionable reputation scoring information and orchestration
- US-CERT in the malware lab
- DHS/SOC and US-CERT in the end-point detection/protection analytics

Why Should You Care?

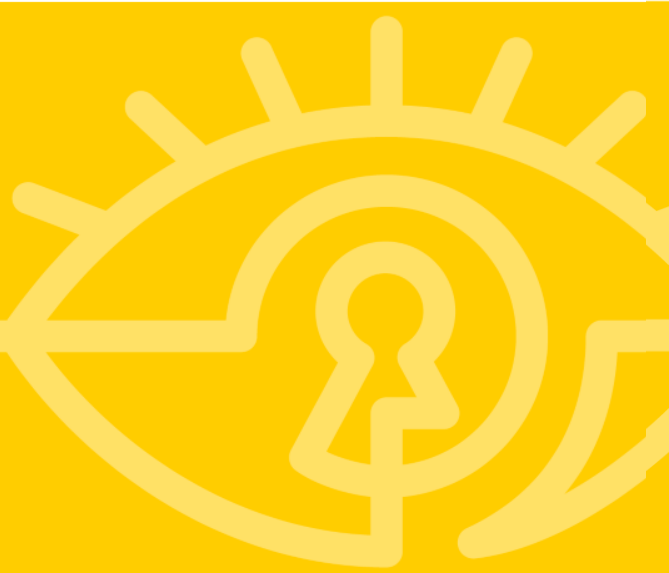
- Malware provenance is a means to enable rapid detection at machine speeds with detection of apparent zero day exploits
- Technique identifies re-packaging of previous exploits with percentages of similarity
- Enables attribution to the real author so they get the credit they deserve
- Makes re-use of code under a different title real hard – polymorphic malware is detected so re-packaging previous exploits not so possible

What Are We Doing?

- DHS is evaluating this technical approach (in the Advanced Malware Analysis Center) to achieve new levels of efficiency in sorting objects into categories of known good, unknown, and known bad as part of the detection and protection capability
- DHS subject experts discussing how passive content is integrated with an emergent taxonomy to produce actionable reputation scoring information and orchestration

What Can You Do Now?

- Get smart on malware provenance – conduct market research
- Advocate for this approach within your organization
- Ask your current vendors to supply this capability as an appliance/bolt on/systems call or functional element



Panel Discussion and Questions

Subhead if needed