STIX in the Mud

SCYTHE

NEW CONTEXT

Us

Bryson Bort

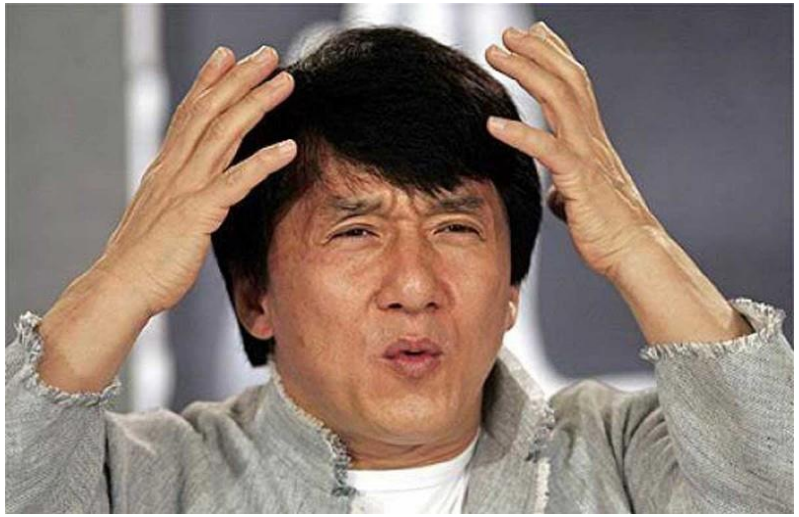
@brysonbort

Daniel Riedel

@riedelinc

Today’s Threat Intel

- Static Identifiers are **Limited**
  - Ch-ch-ch-changes
- Analyst reports...
  - Have to read them…
  - Then. Do. Something.



STIX v2.1

STIX 2.1 Extends STIX 2.0

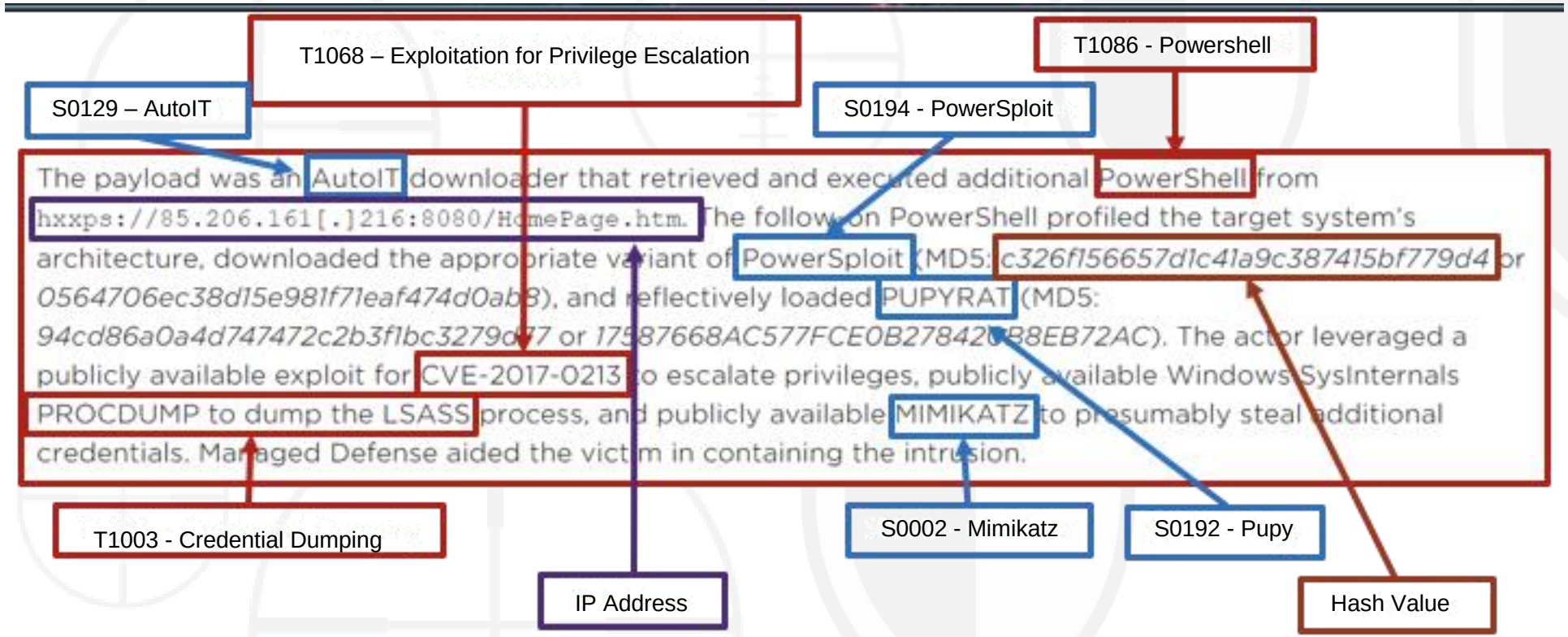
- Course of Action Improvements
- Malware Objects
- Infrastructure Objects
- Grouping Object

Combined with STIX patterning creates even more robust machine readable threat intel

Still Need

- Ability to reduce noise/dedup
- Priority and severity that organizations stand behind.
- ATT&CK/KillChain context

Threat Intelligence for the Machine



Graphic derived from idea by Katie Nickels, MITRE