Dynamic Analysis: Detecting Malware System Changes

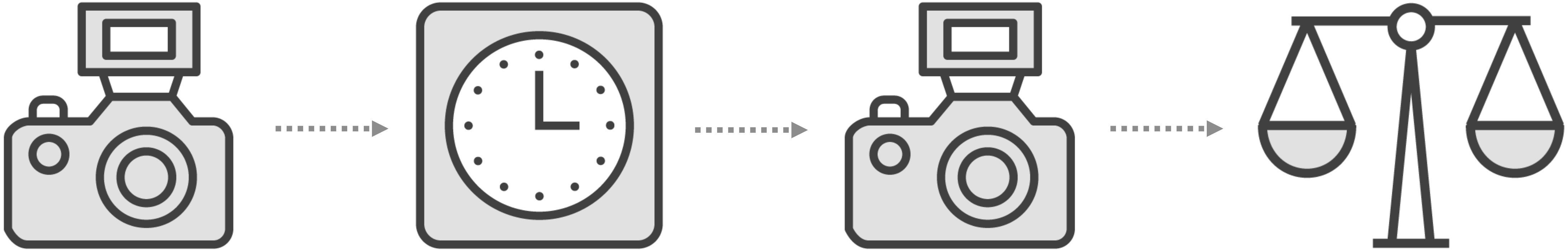
Tyler Hudak
INCIDENT RESPONDER

@secshoggoth

Overview

Detect changes when the malware runs

System Integrity Monitoring



Take initial snapshot

Wait

Take second snapshot

Compare snapshots

System integrity monitoring will detect most file and registry modifications.

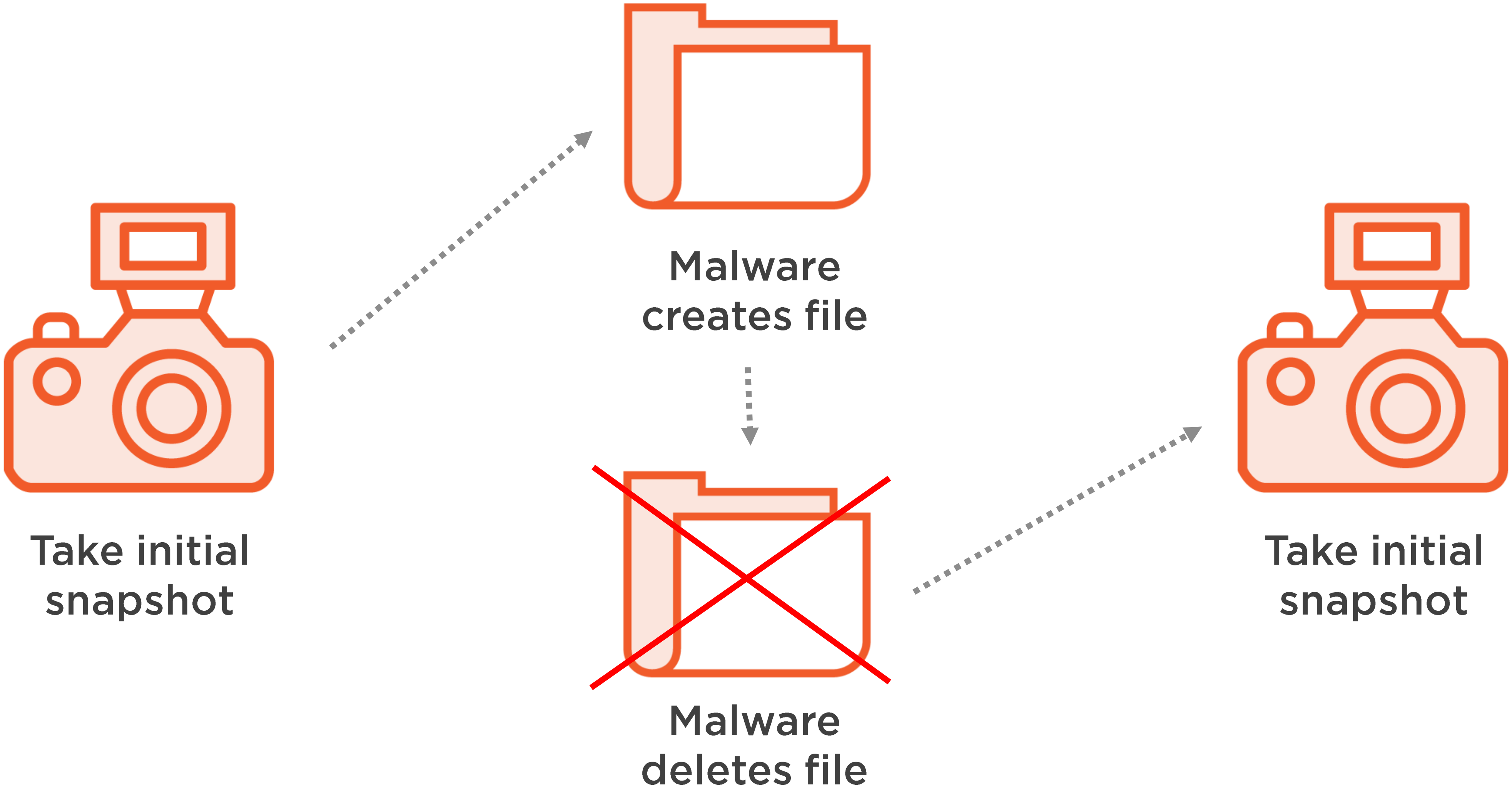
What Does It Not Do?

Tell who made the changes

Rootkit hidden files

Temporary files

Temporary Files



Take initial snapshot

Malware creates file

Malware deletes file

Take initial snapshot

Regshot

Monitors registry and file system

Can save snapshots between boots

Output in text or HTML

https://sourceforge.net/projects/regshot/

Demo

System integrity monitoring

http://bit.ly/malfund-1

budget-report.exe

Created directory

- %USER%\AppData\Roaming\12648430

Created file

- spoolsv.exe

Persistence via RunOnce key

HTTP connection to mbaquyahcn.biz

Summary

Detects most changes when malware runs

Misses

- Who made the changes
- Rootkit hidden files
- Temporary files

Use to see most likely malware change candidates