Advanced Malware Analysis: Combating Exploit Kits

INTRODUCTION

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER
@jareddemott www.vdalabs.com

Course Overview

Commercial and Open Tools

Exploit Vector and Obfuscation

Exploit Kit Encryption

Moving Target Communications

Angler in the Wild

Safe Dynamic Analysis

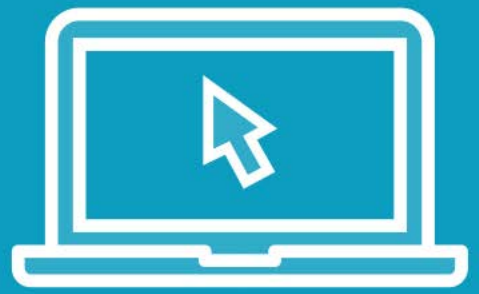
Analyzing Files Statically

Reversing with Debugging Tools

Reversing with IDA pro

Report and Share

Demo



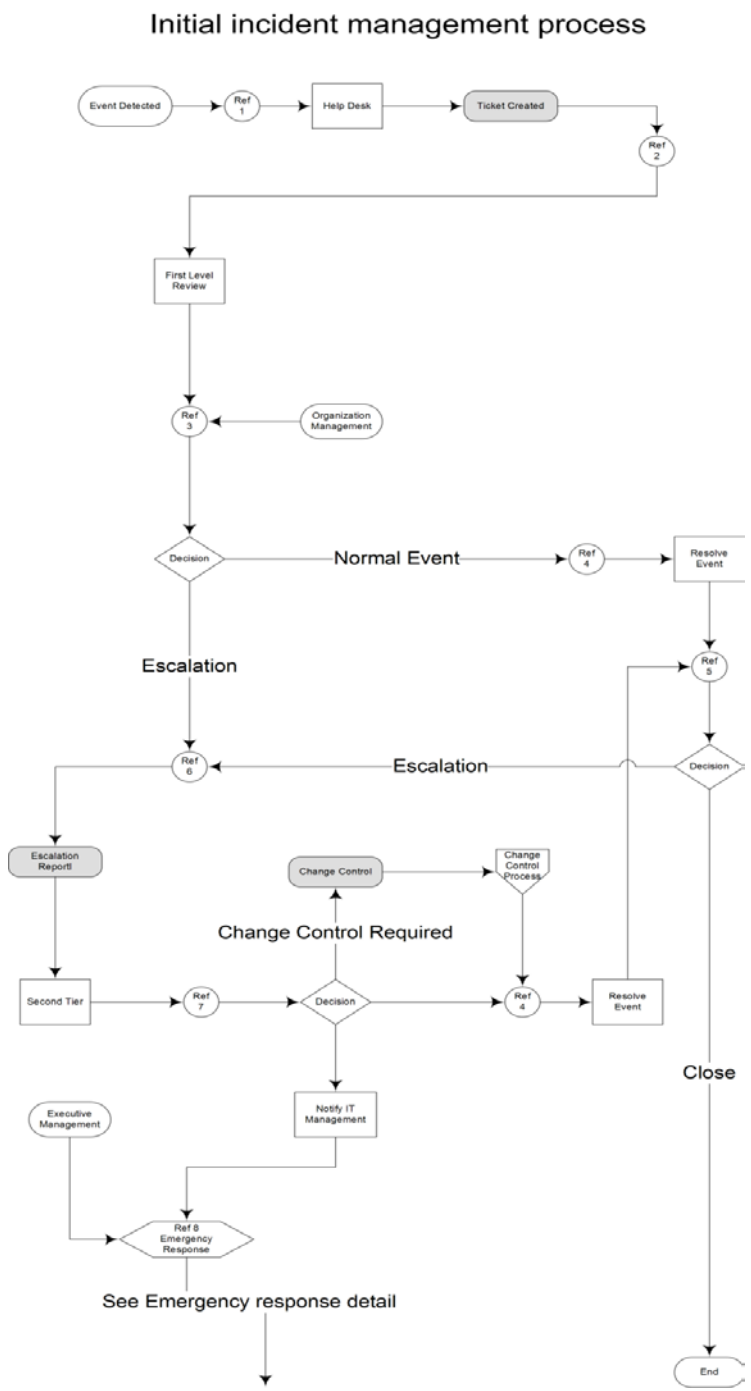
Analyzing a Security Alert

- Bromium edition

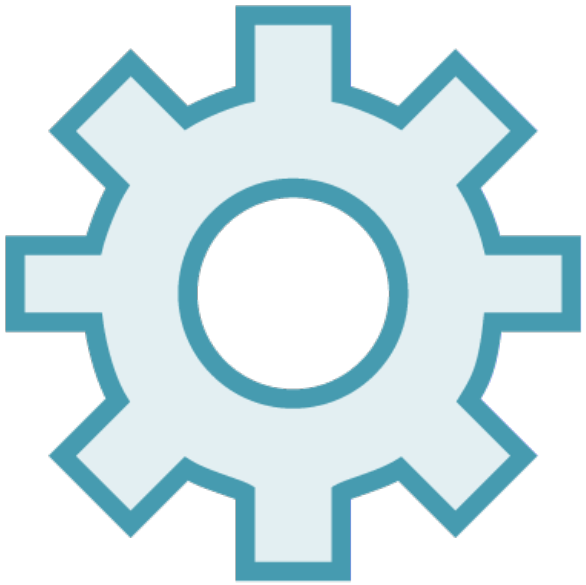
Malware Comes in Many Forms

Exploits found in the wild vary

Incident Response



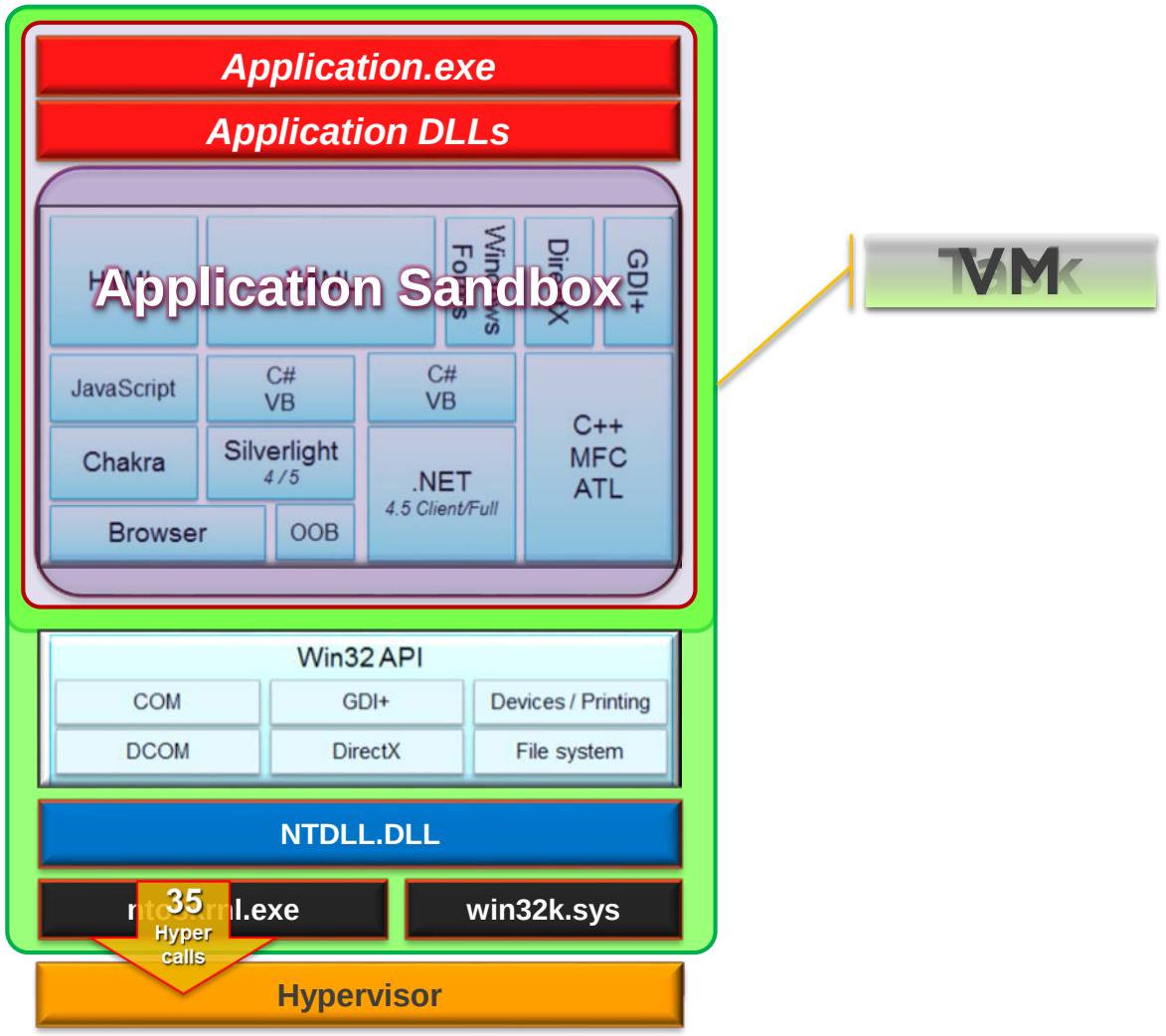
But what if we didn’t need
to do all of that?



Automation

But what if even much of that was handled?

Security Through Isolation



Fast Micro-Virtualization

Easy Seamless Integration

Powerful Policy and Management

vSentry Task Isolation

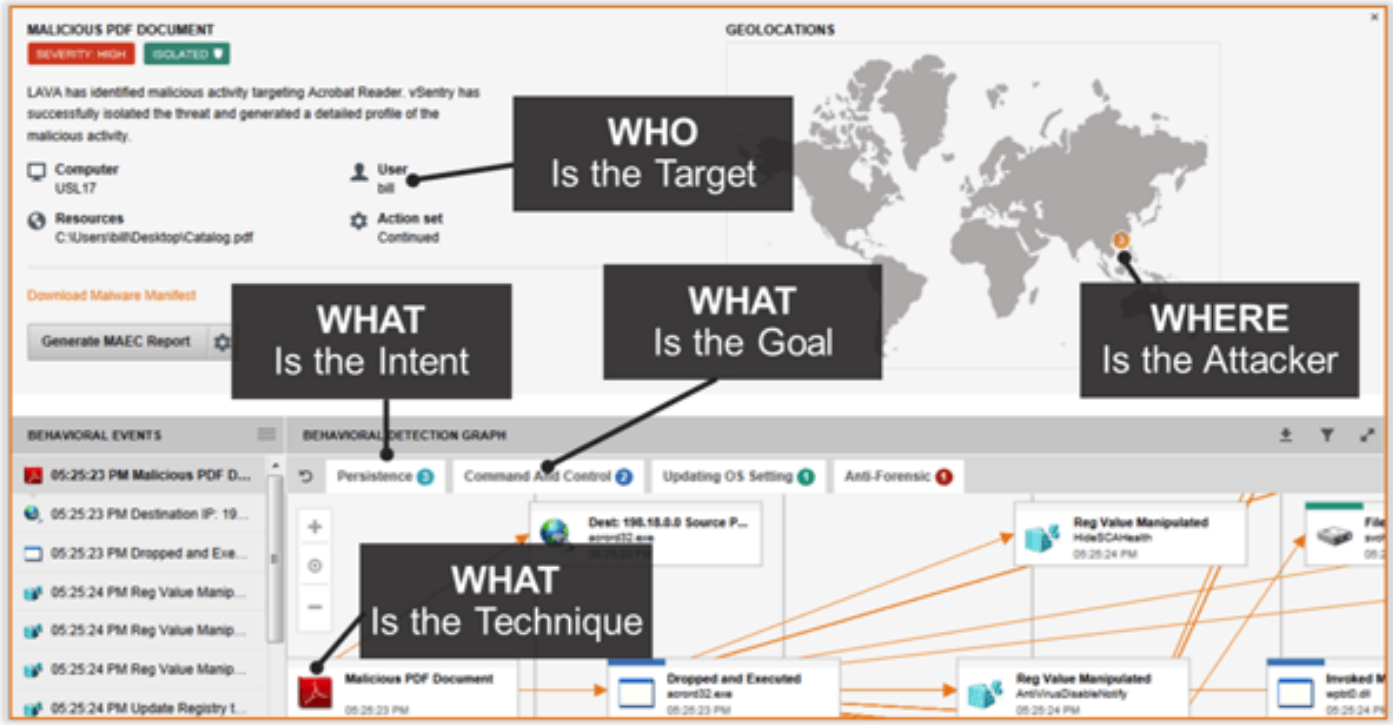
Physical-to-virtual

Bromium Alert

BEP

Lava

BEM



Lab

Setup Windows Server

Run BEC MSI

Setup Windows VM

Run Bromium Installer

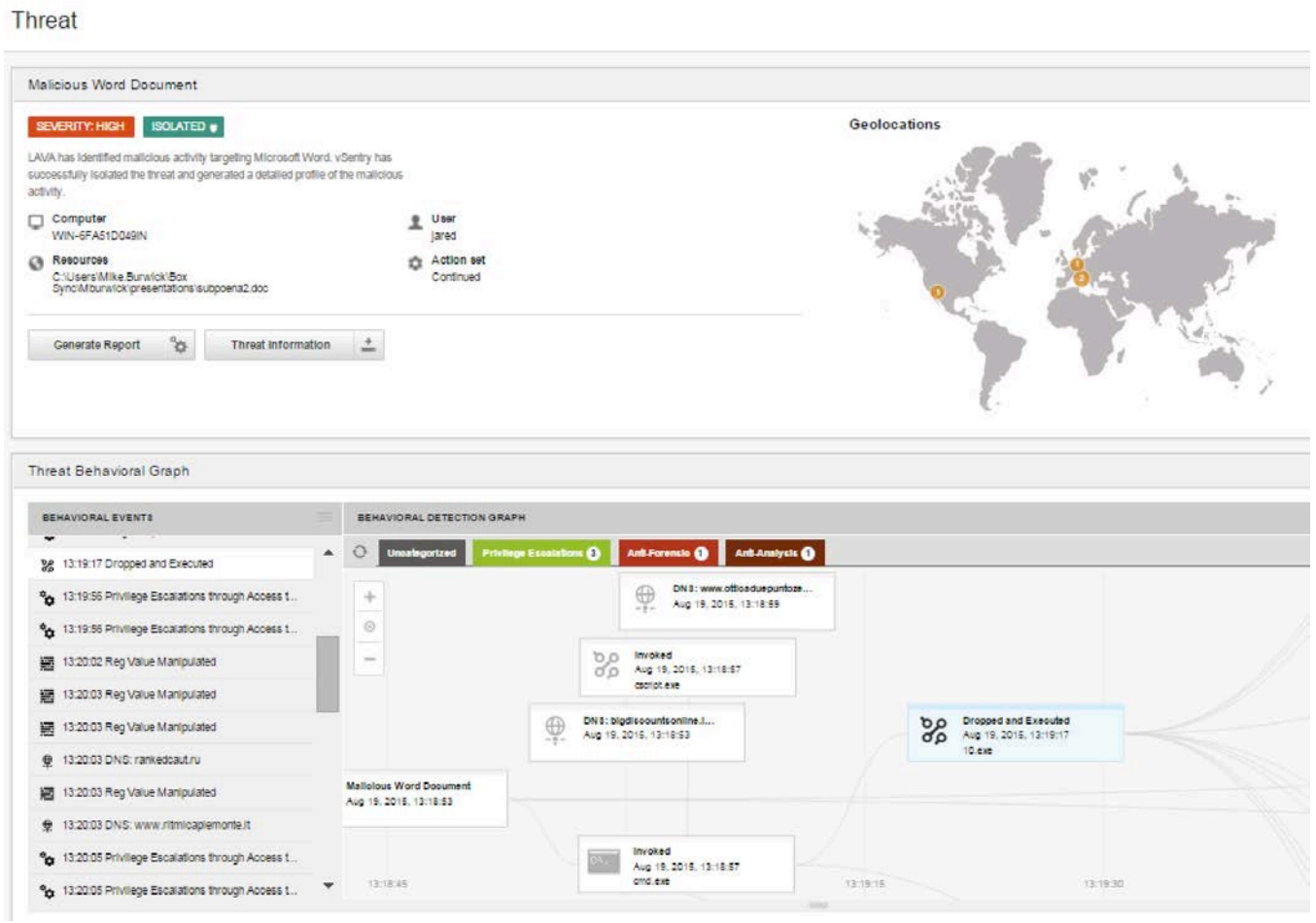
Install KEY

Download the Office Malware

Open the document

Close the document

Lava Event


Threat
Malicious Word Document
SEVERITY: HIGH
ISOLATED
LAVA has identified malicious activity targeting Microsoft Word. vSentry has successfully isolated the threat and generated a detailed profile of the malicious activity.
Computer
WIN-6FA51D049IN
User
jared
Resources
C:\Users\Mike.Burwick\Box Sync\Mburwick\presentations\subpoena2.doc
Action set
Continued
Generate Report
Threat Information
Geolocations
Threat Behavioral Graph
BEHAVIORAL EVENTS
BEHAVIORAL DETECTION GRAPH
Uncategorized
Privilege Escalations
Anti-Forensic
Anti-Analysis
13:19:17 Dropped and Executed
13:19:56 Privilege Escalations through Access t...
13:19:56 Privilege Escalations through Access t...
13:20:02 Reg Value Manipulated
13:20:03 Reg Value Manipulated
13:20:03 Reg Value Manipulated
13:20:03 DNS: rankedcaut.ru
13:20:03 Reg Value Manipulated
13:20:03 DNS: www.ritmicapiemonte.it
13:20:05 Privilege Escalations through Access t...
13:20:05 Privilege Escalations through Access t...
Invoked
Aug 19, 2015, 13:18:57
cscript.exe
Dropped and Executed
Aug 19, 2015, 13:19:17
10.exe
Malicious Word Document
Aug 19, 2015, 13:18:53
Invoked
Aug 19, 2015, 13:18:57
cmd.exe

IOCs

Five W's

Attack Categories

- Process/event graphing

Indicators of Compromise

- Reputation
  - File hash
    - Known malware?
  - IP addresses

Details

Run scripts against trace file

Files

Extract

Examine

- Requires most experience

Summary

Roadmap

Malware Analysis with Bromium

Lab