

THREAT HUNTING WORKSHEET



Name:
Date:

Kill Chain Analysis

Reconnaissance (Targeted System)

Patient Zero: System and User Information

Computer Name:	Logged-in Username:
Operating System:	MAC Address:
Vulnerable Applications:	Host IP Address(es):

Delivery

Attacker Infrastructure and Dropper File

Malicious Domains:	IP Addresses:
Dropper File Name:	Dropper File Type:

Exploitation

Infection Vector

- | | | |
|---|---|--|
| <input type="checkbox"/> Email: Attachment | <input type="checkbox"/> Web: Phishing Link | <input type="checkbox"/> Active Exploitation |
| <input type="checkbox"/> Email: Phishing Link | <input type="checkbox"/> Web: Exploit Kit | <input type="checkbox"/> Other: |

Installation

Malware Binary

File Name:	File Type:
Malware Family Name:	

Command and Control

Command and Control (C2) Communications

Domains Contacted:	IPs Contacted:
URLs Contacted:	

Actions on Objective

Threat Behavior

- ☐ Process injection detected? (if so, which process)
- ☐ Escalation of privileges detected? (if so, which method)
- ☐ PowerShell / scripting commands detected? (if so, list)

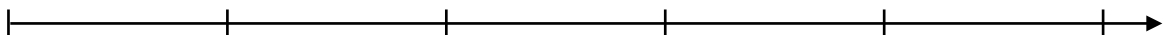
Known Malware Capabilities:

Executive Summary

Date/Time of Patient Zero initial infection:

Total number of systems affected:

Timeline:



Security recommendations:

