THREAT HUNTING WORKSHEET

Name: Jonathan Cancho
Date: 04/02/18

Kill Chain Analysis

Reconnaissance (Targeted System)

Patient Zero: System and User Information

Computer Name: Demo_AMP_Intel

Operating System: Windows 7, SP 1.0

Vulnerable Applications: Internet Explorer 11, Office 2016

Logged-in Username: johndoe

MAC Address: 17:a3:d6:ce:86:ea

Host IP Address(es): 11.8.170.55, 67.124.30.176

Delivery

Attacker Infrastructure and Dropper File

Malicious Domains:

Dropper File Name:

IP Addresses:

Dropper File Type:

Exploitation

Infection Vector

- ☐ Email: Attachment
- ☐ Email: Phishing Link
- ☐ Web: Phishing Link
- ☐ Web: Exploit Kit
- ☐ Active Exploitation
- ☐ Other:

Installation

Malware Binary

File Name: OLD.EXE

Malware Family Name: Olympic Destroyer

File Type: PE Executable

Command and Control

Command and Control (C2) Communications

Domains Contacted:

URLs Contacted:

IPs 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: destructive

Executive Summary

Date/Time of Patient Zero initial infection: Mar 8 20:49

Total number of systems affected: 1

Timeline:

Security recommendations: Patch vulnerabilities in IE11 and Office2016

Sponsored by the Cisco Advanced Threat Solutions team and Cisco Incident Response Services. For assistance with an ongoing breach, contact IncidentResponse@cisco.com or call 1-844-831-7715.