McAfee Enterprise Security Manager

Operation SMN Content Pack

May 15, 2015

Important Note:

The information contained in this document is confidential and proprietary.
Please do not redistribute without permission.

Contents

1 Introduction

Axiom is a sophisticated, well-funded, state sponsored, advanced threat group. Operation SMN is a coordinated interdiction effort by leading private-industry security companies against Axiom. The coalition of vendors collaborated to release detection and removal signatures in several antivirus and other products. This content pack watches for antivirus events related to the Operation SMN identified malware.

2 Included Components

This section will detail the different components of the content pack.

2.1 Alarms

This content pack does not contain any alarms.

2.2 Correlation Rules

This content pack includes a correlation rule to detect specific IDS or IPS events related to Operation SMN and/or known malware files associated with Operation SMN.

- Attack – Operation SMN

2.3 Reports

This content pack does not contain any reports.

2.4 Variables

This content pack does not contain any variables.

2.5 Views

This content pack does not contain any views.

2.6 Watchlists

This content pack includes a watchlist containing a list of hashes of known Operation SMN file hashes.

- Operation SMN Malware

3 Prerequisites

The following re required in order to use the components in this content pack.

3.1 Add the appropriate IPS/IDS data sources

This content pack examines IPS or IDS events from a few specific devices. In order to monitor Operation SMN activity, the ESM must receive IDS/IPS events from a McAfee IPS, from a NitroGuard IPS, or from a Snort or Suricata based sensor using either the snort.org IDS rules or the EmergingThreats IDS rules.

3.2 Add appropriate antivirus data sources

This content pack examines antivirus events from a few specific devices. In order to monitor Operation SMN activity, the ESM must receive antivirus information from the McAfee Antivirus product or the TrendMicro Antivirus product.

4 Post-Installation Information and Configuration

Once the content pack is installed and the new policy has been deployed, and appropriate IDS/IPS and/or antivirus devices have been configured and are forwarding events to the ESM the correlation rule will commence processing events.

4.1 Correlation Rules

There are no parameters which can be adjusted in this content pack.

5 Use Case(s)

The Operation SMN Content Pack will detect events from Axiom Group's malware. Many systems infected with such malware have been detected and cleaned up. The malware was designed to exfiltrate core intellectual property (IP) and then maintain a long term presence in a victim's network.

While there should not be any ongoing infections of this malware, there may be a rare occasional recurrence.

This content pack may be most useful in historical correlation to see if previously unnoticed infections occurred within a network.

6 Appendix A – Rule Details

6.1 Attack – Operation SMN

An event indicates a computer has probably been exploited by Axiom.

These events are likely caused by an attacker from the cyber espionage group Axiom probing your network in search of valuable information.

This detection searches for Operation SMN events from a NitroGuard IPS, a Suricata sensor, or a snort sensor. It also looks for Operation SMN events from a McAfee or TrendMicro antivirus device. If one event is found from any of those, a correlated event is generated.