Centro de
Investigación en
Computación

Indicadores

Detección de malware

Definición, ejemplos

Course

Análisis y Detección de Malware

Instructor

Acosta Bermejo Raúl

Lecture notes

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. IoC
3. IoA

Introduction

Introducción

Indicadores

- Cualquier recurso (archivo, paquete, URL, correo, etc.) o actividad que sea sospechosa de que un ataque esta en preparacion, en progreso o que ya se realizó, se pude utilizar para detectar un ataque.
- Por lo tanto un ataque puede prevenirse o mitigarse.
- Existen muchos sistemas que buscan identificar de manera única la presencia de estos recursos o actividades en tiempo real, sin embargo, en general,la identificación se hace en la etapa de análisis.

Indicator of Compromise

IoC

Definiciones

IoC

Introducción

- It is an object or activity that, observed on a network or on a device, indicates a high probability of unauthorized access to the system, in other words, that the system is compromised.
- Such indicators are used to detect malicious activity in its early stages as well as to prevent known threats:

- Threat

  It is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

  Examples: computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

IoC

Introducción

Types of threats

1. Malware
2. Emotet

   CISA describes emotet as “an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware.
3. Denial of Service (DoS)
4. Man in the Middle (MITM)
5. Phishing
6. SQL Injection
7. Password Attacks

Cualquier forma de ataque
Es una amenaza

IoC

Introducción

Examples of IoC

1. Unusual DNS lookups.
2. Suspicious files, applications, and processes.
3. IP addresses and domains belonging to botnets or malware C&C servers.
4. A significant number of accesses to one file.
5. Suspicious activity on administrator or privileged user accounts.
6. An unexpected software update.
7. Data transfer over rarely used ports.
8. Behavior on a website that is atypical for a human being.
9. An attack signature or a file hash of a known piece of malware.
10. Unusual size of HTML responses.
11. Unauthorized modification of configuration files, registers, or device settings.
12. A large number of unsuccessful login attempts.

IoC

Introducción

Examples of IoC (DarkReading, Ericka Chickowski)

1. Unusual Outbound Network Traffic
2. Anomalies in Privileged User Account Activity
3. Geographical Irregularities
4. Log-In Red Flags
5. Increases in Database Read Volume
6. HTML Response Sizes
7. Large Numbers of Requests for the Same File
8. Mismatched Port-Application Traffic
9. Suspicious Registry or System File Changes
10. Unusual DNS Requests
11. Unexpected Patching of Systems
12. Mobile Device Profile Changes
13. Bundles of Data in the Wrong Place
14. Web Traffic with Unhuman Behavior
15. Signs of DDoS Activity

IoC

Introducción

Referencias

- Estándares
  - https://csrc.nist.gov/glossary/term/indicator_of_compromise
- Empresas
  - https://encyclopedia.kaspersky.com/glossary/indicator-of-compromise-ioc/
  - https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise
  - https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/
  - https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise

Indicator of Attack

IoA

Definiciones

IoA

Introducción

Definition

They are similar to IoCs, but:

- Rather than focusing on forensic analysis of a compromise that has already taken place.
- IoA focus on identifying attacker activity while an attack is in process.

Data breach

- It is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- https://en.wikipedia.org/wiki/Data_breach

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652