SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

Tipo de artículo: Artículo original
Temática: Desarrollo de aplicaciones informáticas
Recibido: 25/08/2019 | Aceptado: 10/09/2019 | Publicado: 22/09/2019

Sistema nacional para el intercambio y gestión de información de ciberamenazas

National system for the exchange and management of information on cyber threats

Dennis Barrera Pérez[1*], Yailin Sánchez Borrell [2]

[1] Universidad de las Ciencias Informáticas, Cuba. dbperez@uci.cu
[2] Universidad de las Ciencias Informáticas, Cuba. ysanchezb@uci.cu

[*] Autor para correspondencia: dbperez@uci.cu

Resumen

En los últimos años se ha evidenciado un notable incremento de los ciberataques a nivel mundial. Los ciberdelincuentes emplean técnicas, que van desde el uso de Inteligencia Artificial (IA) para la creación de malware, hasta la introducción de códigos maliciosos en los sitios web para minar criptomonedas. Uno de los métodos novedosos para enfrentar la naturaleza hostil de los ciberataques constituye el intercambio de información de ciberamenazas. Su objetivo es establecer un procedimiento que permita la recopilación, almacenamiento y distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz, generando un conocimiento común y compartido. En el trabajo se presenta un sistema para el intercambio y gestión de información de ciberamenazas capaz de elevar los niveles de seguridad en las infraestructuras tecnológicas del país. El sistema permitirá que las entidades involucradas puedan compartir información sobre patrones de ataques y amenazas de una manera segura y automatizada mediante el empleo de estándares internacionales como Structured Threat Information Expression (STIX) y Trusted Automated Exchange of IndicatorInformation (TAXII). La información podrá ser importada y exportada en formatos como OpenIOC, CSV y STIX. Para la detección de ataques y reglas de correlación se emplea el sistema SIEM Open Source Security Information Management (OSSIM). Se considera que la solución propuesta contribuirá a mejorar la detección de ciberataques, mitigación de vulnerabilidades, así como un aumento en la detección y respuesta ante incidentes. Los experimentos realizados en la Universidad de las Ciencias Informáticas validan la implementación de esta propuesta a nivel nacional.

Palabras clave: ciberamenazas; ciberataques; intercambio de información

Abstract

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

In recent years, there has been a notable increase in cyber-attacks worldwide. Cybercriminals employ techniques, ranging from the use of Artificial Intelligence (AI) for the creation of malware, to the introduction of malicious codes in websitesto mine cryptocurrencies. One of the novel methods to confront the hostile nature of cyber-attacks is the exchange of cyberthreats information. Its objective is to establish a procedure that allows the collection, storage and distribution of the necessary information to act in a homogeneous, fast and efficient way, generating a common and shared knowledge. The paper presents a system for the exchange and management of information on cyberthreats capable of raising the levels of security in the technological infrastructures of the country. The system will allow entities involved to share information about attack patterns and threats in a secure and automated way by using international standards such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII). The information can be imported and exported in formats such as OpenIOC, CSV and STIX. The SIEM Open Source Security Information Management system (OSSIM) is used to detect attacks and correlation rules. It is considered that the proposed solution will contribute to improve the detection of cyber-attacks, vulnerability mitigation, as well as an increase in the detection and response to incidents. The experiments carried out at the University of Computer Sciences validate the implementation of this proposal at the national level.

Keywords: *cyber threats; cyber-attacks; information exchange.*

Introducción

Realizando un análisis del panorama actual de la ciberseguridad se pudo observar que en los últimos años se ha evidenciado un notable incremento de los ciberataques a nivel mundial (CISCO, 2019).Según un reporte de ISACA, en el 2018 los ciberataques se incrementaron considerablemente con respecto al año anterior siendo el Phishing el vector de ataque más común (44%), seguido por el malware (31%) y la ingeniería social (27%). Dentro de las principales amenazas se encontraron las campañas de ransomware como WannaCry y NotPetya causando daños a miles de equipos en todo el mundo. (ISACA, 2018)

Como nueva amenaza emergente se encuentra el malware de criptominado o el criptohacking que infecta las Pc de las víctimas para el minado de bitcoin. Según un reporte de McAfee' Labs el empleo de este tipo de malware ha crecido un 4.7% ysolo en el 3er trimestre del 2018 aumentó un 55%. (McAfee Labs, 2018)

Los reportes analizados afirman que algunas empresas han comenzado a implementar soluciones de inteligencia de amenazas para enfrentar la naturaleza hostil de los ciberataques, logrando un alto nivel de éxito. Por lo cual se evidencia una tendencia a la implementación de soluciones para el intercambio de información.

En (Fernández, 2017) se define como objetivo del intercambio de información: establecer un procedimiento que permita la recopilación, almacenamiento y distribución de la información necesaria para actuar de forma homogénea, rápida y eficaz, generando un conocimiento común y compartido.

Haciendo una revisión del estado de la seguridad informática a nivel nacional se pudo identificar como problema que se aprecia insuficiencia en los servicios de seguridad en el ciberespacio que ofrecen determinadas empresas, servicios que son aislados en su mayoría y sin una estrategia común. Los mecanismos empleados actualmente para el intercambio de información de amenazas, ataques y vulnerabilidades son insuficientes, el correo electrónico es la vía más utilizada para reportar y alertar sobre los mismos, sin embargo, se aprecia la necesidad de poder hacer fluir hacia todas las entidades información de ataques, vulnerabilidades, incidentes de una manera más rápida y ágil.

Por tales problemas en algunos casos, los ciberdelincuentes tienen efectividad en sus ataques durante un buen tiempo después de generado una alerta o conocida una determinada vulnerabilidad a nivel nacional. Para dar solución a la problemática planteada, se define como objetivo general de la investigación, la creación de un Sistema para el Intercambio y Gestión de Información de Ciberamenazas que contribuya a fortalecer y elevar los niveles de seguridad en nuestras instituciones.

Materiales y métodos o Metodología computacional

Como método de la investigación se empleó el Analítico-Sintético, para lo cual se realizó un análisis de los componentes de las plataformasde intercambio de ciberamenazas, lo cual contribuyó a la formalización de una solución para dar cumplimiento al objetivo propuesto.

Las fuentes de datos empleadas durante la investigación están constituidas por ciberamenazas analizadasen el año 2018 y 2019 por los Especialistas de Seguridad Informática de la Universidad de las Ciencias Informáticas.

Para el análisis de los referentes teóricos relacionados con la temática tratada, se realizó un estudio del estado del arte sobre los estándares y formatos para el intercambio de información, así como las plataformas de ciberinteligencia existentes. A continuación, se describen los principales estándares existentes:

- **OpenIOC**: Open Indicator of Compromise de Fireeye.
- **STIX™**: Structured Threat Information eXpression.
- **TAXII™**: Trusted Automated Exchange of Intelligence Information.
- **OTX:** Open ThreatExchange.

OpenIOC

Es una iniciativa liderada por la compañía MANDIANT perteneciente a la multinacional FireEye que ha estado presente de manera pionera en la definición y establecimiento del concepto IoC en la gestión de incidentes. Se distribuye abiertamente bajo licencia Apache2, se basa en un esquema XML para definir IoC y permite la extensión con información propia. Cuenta con un alto grado de madurez, simplicidad y reconocimiento. (OpenIOC, 2019)

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

STIX™

Es un lenguaje y formato de serialización usado para intercambiar CTI. STIX permite a las organizaciones compartir CTI entre sí de una manera coherente y legible, lo que permite a las comunidades de seguridad comprender mejor a qué ataques informáticos son más propensos y responder a esos ataques de forma más rápida y efectiva.(Barnum, 2012)

Actualmente se encuentra en su versión 2 e incluye el lenguaje CybOX desarrollado por Mitre.STIX está diseñado para mejorar muchas capacidades como el análisis colaborativo de amenazas, el intercambio automatizado de amenazas, la detección y respuesta automatizada. Serializa los datos en formato JSON y adopta un formato basado en grafos para ofrecer una representación muy intuitiva de los objetos y relaciones entre los mismos **(figura 1)**. Los objetos se agrupan en 12 dominios claves y dos relaciones entre ellos: patrones de ataques, campaña, acciones de respuesta, identidad, indicadores, comportamiento de intrusión, malware, observables, reportes, actores, herramientas y amenazas. (Oasis, 2019)

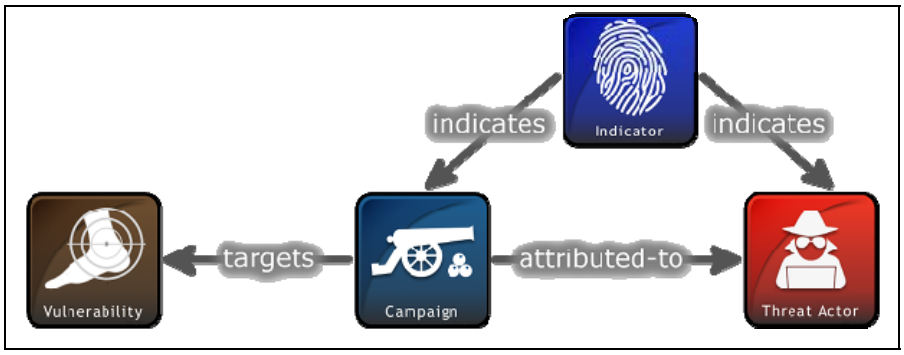

Figura 1. Ejemplo de relaciones de STIX. (Oasis, 2019)

TAXII™

Es un protocolo de capa de aplicación para la comunicación de información de ciberamenazas de una manera simple y escalable. TAXII es utilizado para intercambiar CTI a través de HTTPS, permite a las organizaciones compartir CTI mediante la definición de una API que se alinea con los modelos comunes de intercambio. (Oasis, 2019)

Está diseñado específicamente para soportar el intercambio de CTI representado en STIX y STIX 2.0. Define dos servicios principales para soportar modelos de compartición de la información, colecciones (un consumidor), canales (varios consumidores).

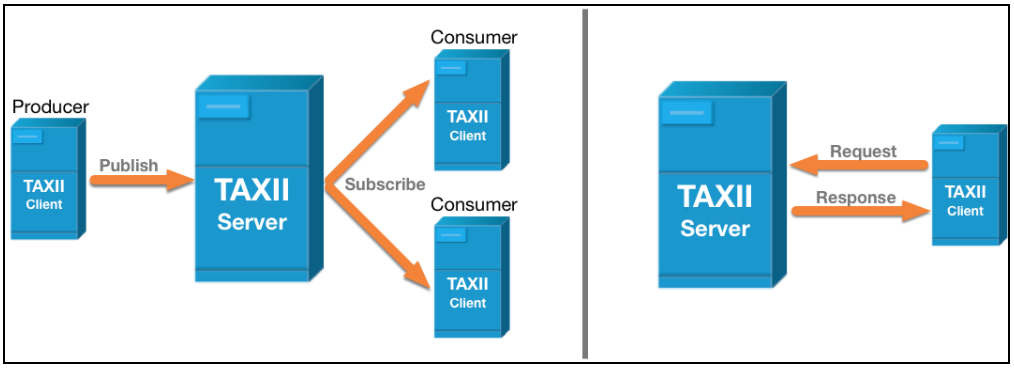

Figura 2. Modelos de compartición de la información. TAXII. (Oasis, 2019)

OTX

Empresas como AT&T Cybersecurity[2], creadora del sistema SIEM[3]de código abierto OSSIM[4]**,** posee la mayor comunidad de intercambio abierto de amenazas a nivel mundial conocida como OTX.Actualmente cuenta con más de 100,000 participantes en 140 países, que contribuyen con más de 19 millones de indicadores de amenazas diariamente. Ofrece datos de amenazas generados por la comunidad, permite la investigación colaborativa y automatiza el proceso de actualización de su infraestructura de seguridad con datos de amenazas de cualquier fuente. Funciona con su propio formato en combinación con OpenIOC y STIX. (OTX, 2019)

[2]AT&T Cybersecurity: anteriormente Alienvault. https://www.alienvault.com

[3]SIEM - Security Information and Event Management: Sistema de información y gestión de eventos de seguridad.

[4]OSSIM- Open Source Security Information Management.https://www.alienvault.com/products/ossim

Brinda además la posibilidad de suscribirse a los distintos PULSES (IoC de una fuente) así como la creación de nuevos, lo cual permite acceder a la información de ciberamenazas en tiempo real soportada por el laboratorio de AT&T Alienvault.

Con toda la información y eventos de seguridad que recolecta, ofrece un servicio de alerta y reporte de patrones de ataques, amenazas, vulnerabilidades, que puede ser adquirido de manera integrada en su producto comercial USM[5].

Es válido destacar que algunos de estos estándares constituyen el trabajo de varias organizaciones como MITRE, Department of Homeland Security, NationalCyber Security Communications, Integration Center y el US-CERT de Estados Unidos que han puesto grandes esfuerzos en la estandarización de esquemas de intercambio de información, que actualmente tienen gran aceptación a nivel internacional.

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

Por otra parte, se analizaron varias plataformas de intercambio de amenazas a nivel internacional como es el caso de MISP (Malware InformationSharingPlatform) y REYES (REpositorio común Y EStructurado de amenazas y código dañino)

MISIP fue creado por el ComputerIncident Response Center de Luxenbourg, es un proyecto de software libre y de código abierto que ayuda a compartir información de inteligencia de amenazas, incluidos los indicadores de ciberamenazas. Es considerada como una plataforma de inteligencia de amenazas para recopilar, compartir, almacenar y correlacionar IoC de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidades o incluso información de lucha contra el terrorismo. Almacena sus IoCde manera estructurada, realiza correlación y permite exportar la información en formatos para IDS o SIEM, en STIX o OpenIOC y sincronizarlos con otros MISP. (CIRCL, 2019)

Permite la creación de comunidades de confianza mediante las cuales se puede compartir características específicas de las amenazas dentro de una comunidad de confianza, sin tener que incluir información sobre el contexto del incidente.

[5]USM- Unified Security Management: https://www.alienvault.com/products/usm-anywhere

Figura 3. Arquitectura del proyecto MISP. (CIRCL, 2019)

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

Reyes

Es una solución desarrollada por el CCN-CERT[6]para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. Permite realizar cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes.Consiste en un metabuscador de información de diversas fuentes especializadas en ciberamenazas, que está integrado con herramientas de análisis del CCN-CERT. REYES está basada en la tecnología MISP, que es enriquecida con fuentes externas de información que permiten agilizar la prevención y la respuesta a incidentes. REYES se nutre de múltiples fuentes de información, especialmente analizadas y escogidas para englobarlas en una única solución. (REYES,2019)

Dentro de sus características principales se encuentran:

Priorización de la información

REYES procesa y analiza la información para mostrar a los analistas la información más relevante que permita agilizar las respuestas ante incidentes.

~~Información exclusiva~~

Al ser MISP su núcleo de información y estar federado con organismos internacionales, a través de REYES se puede tener acceso a gran información privilegiada.

Este sistema solo pude ser empleado por aquellas organizaciones que posean el certificado de SAT-INET[7].

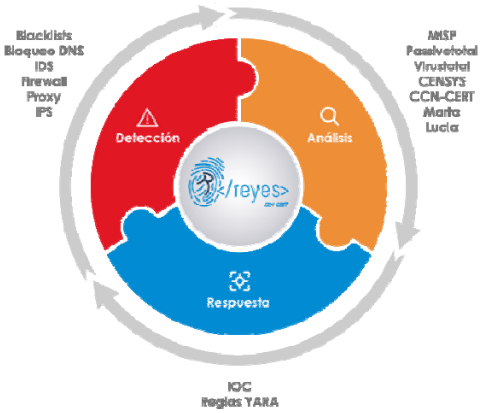

Figura 4. Funcionamiento del sistema REYES.

Resultados y discusión

En varias ocasiones muchas organizaciones en el país son víctimas de ciberataques con comportamientos similares. Por otra parte, es muy común que los especialistas de seguridad informática encargados de proteger las

infraestructuras, realicen trabajos en investigaciones sobre ciberamenazas que ya fueron realizados por otras entidades afectadas.

Con el objetivo de minimizar los esfuerzos en el análisis de incidentes y aumentar la rapidez de las respuestas, se propone un **Sistema para el Intercambio y Gestión de Información de Ciberamenazas** denominado **UCI-CTI** quecontribuye a fortalecer y elevar los niveles de seguridad en nuestras infraestructuras tecnológicas.

El sistema está basado en la tecnología MISP y está especialmente ideado para ofrecer un mecanismo de intercambio para distintas organizaciones que internamente generan ciberinteligencia, por lo cual los usuarios tienen la oportunidad de facilitar y consumir información de ciberamenazas.

[7]SAT-INET: Sistema de Alerta Temprana (SAT) de Internet del CCN-CERT.

Características y funcionalidades del sistema

A continuación, se describen las características del sistema UCI-CTI y sus principales funcionalidades:

Intercambio de Información

El sistema está compuesto por varias instancias que pueden emplearse en cada una de las instituciones por separado. Su máxima utilidad se observa cuando varias organizaciones interactúan para formar una comunidad de intercambio de información. Los eventos de cada una pueden ser intercambiados entre varias instancias mediante un mecanismo de sincronización automático.

Grafo de asociación o de inteligencia

El sistema emplea un mecanismo de grafos de asociación o de inteligencia, permitiendo crear relaciones entre los nodos (IoC), los cuales son empleados por los analistas para obtener una visión más completa de las ciberamenazas.

Descarga de información

La información resultante de una investigación puede ser descargada en varios formatos (texto, json, xml y csv), estándar STIX y STIX v2 (xml y json), reglas de IDS (bro, snort y suricata), reglas YARA, RPZ Zone[8]para el filtrado a nivel de DNS y OpenIOC.

Representación de la información.

La información de ciberseguridad se representa en un formato compatible con STIX, por lo cual las instituciones que deseen intercambiar información pueden seleccionar mediante perfiles que tipo de información del estándar desean intercambiar y cómo.

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

El sistema permite la modelación de los eventos de seguridad como **entidades**, las cuales son descritas con uno o varios **atributos**, éstos a su vez pueden ser empleados por varios eventos, permitiendo así, la relación implícita entre entidades. Los atributos son agrupados por categorías.

[8]RPZ Zone- DomainNameService Response PolicyZones: Mecanismo para introducir políticas personalizadas en el DNS.

Otras características son:

- Base de datos de IoC que permite almacenar información técnica y no técnica sobre ciberamenazas.
- Sistema de correlación propio, que incluye la correlación entre eventos y entre atributos de cada evento, permitiendo realizar análisis de campañas, IoC y ataques.
- Interfaz de usuarios intuitiva con separación de funcionalidades por roles.
- API de integración con otras soluciones y módulos de expansión en lenguaje Python.

Arquitectura del Sistema

A continuación, se describe la arquitectura propuesta para el sistema UCI-CTI, así como la integración con otros modelos existentes para la ampliación de sus funcionalidades.

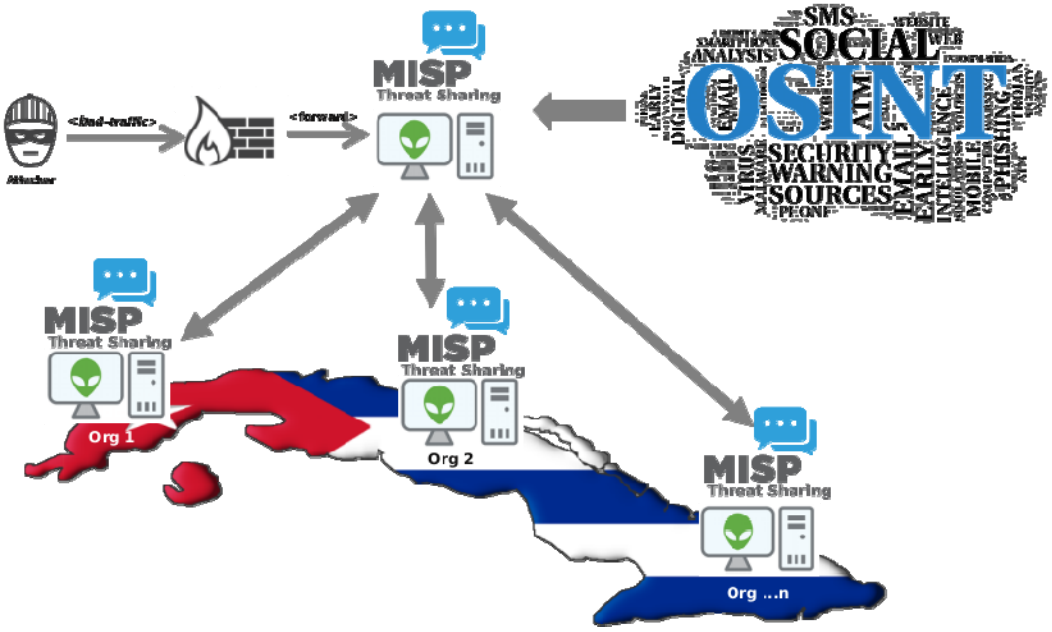

Figura 5. Arquitectura del sistema UCI-CTI. Elaboración propia.

Actualmente la solución se encuentra desplegada en la infraestructura tecnológica de la Universidad de las Ciencias Informáticas, sin embargo, su arquitectura está diseñada para ser flexible y adaptable para cada una de las instituciones donde se desee implementar. Como muestra la figura 5, la solución se encuentra integrada al sistema SIEM OSSIM mediante un conjunto de plugin o conectores. De manera tal que los IoC y eventos gestionados por OSSIM, son compartidos con el sistema UCI-CTI para el análisis e intercambio con la comunidad, estos datos se intercambian empleando estándares existentes como STIX por lo cual solo se comparte la información que cada institución considere necesaria. Otros de los componentes fundamentales sonlas fuentes de ciberinteligencia,aunque el sistema cuenta con algunas fuentes en su configuración predeterminada, permite incluir ademásinformaciónde fuentes públicas OSINT[9]empleadas para la correlación de los eventos y atributos dentro del sistema, e incluso se pueden importar pulsos de fuentes abiertas como es el caso de OTX.

Con el objetivo de ampliar las capacidades del sistema descrito y enfrentar la gran diversidad de ataques a que se enfrentan las instituciones, el mismo se integró con un modelo para la detección de ataques a las aplicaciones web a partir de patrones de ataques denominado AON descrito en (Pérez et al., 2019).

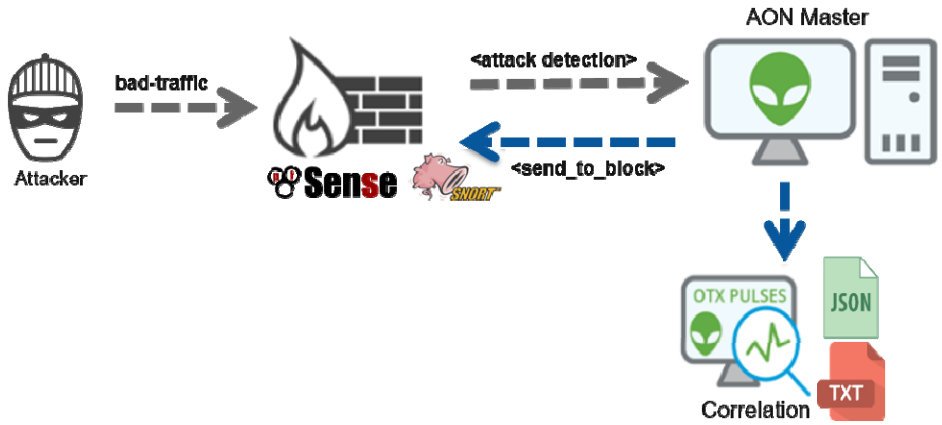

Figura 6. Arquitectura del sistema AON.(Pérez et al., 2019)

El modelo AON se encarga de detectar y bloquear peticiones a los sitios web a partir de patrones de ataques conocidos. Los resultados del análisis de cada ciberataque (IoC) pueden ser importados al sistema UCI-CTIpara que puedan ser compartidos con las demás organizaciones.

[9]OSINT-Open SourceIntelligence: Datos recolectados de fuentes públicas de información.

SerieCientífica de la Universidad de las CienciasInformáticas
Vol. 12, No. 9, Mes Septiembre, 2019
ISSN: 2306-2495| RNPS: 2343
Pág. 20-32
http://seriecientifica.uci.cu

Funcionamiento del sistema

En las siguientes figuras se muestra la interfaz gráfica de la solución propuesta y su empleo en un caso de estudio relacionado con el análisis delransomwareWannacry que afectó a miles de computadoras en todo el mundo causando pérdidas de alrededor de $4 billones. (CBS News, 2017)

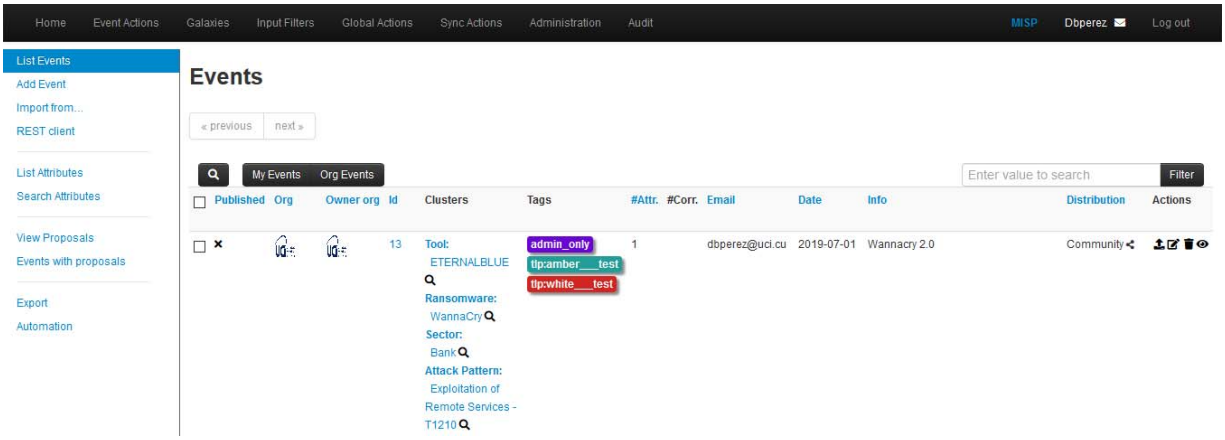

Figura 7. Análisis del ransomwareWannacry. Vista de Eventos.

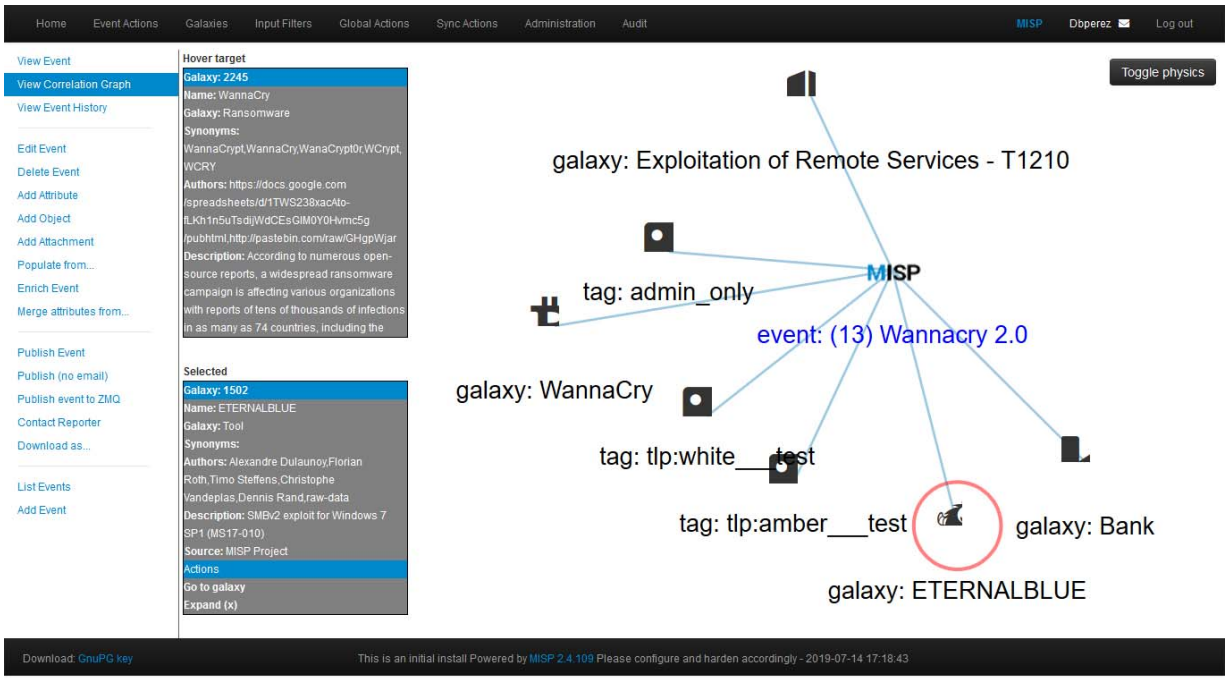

Figura 8. Análisis del ransomwareWannacry. Vista de Grafos de Correlación.

Conclusiones

Después de finalizada la investigación se pudo arribar a las siguientes conclusiones:

- Las pruebas realizadas en la infraestructura tecnológica de la Universidad de las Ciencias Informáticas, han demostrado que es posible implementar este sistema a nivel nacional y su aporte es novedoso, por lo cual se propone extender la solución en un principio al resto de las universidades del país con el apoyo del MES.

Se considera que la implementación del sistema a nivel nacional permitiría que los Equipos de Respuesta a Incidentes (IRT) participen de forma activa compartiendo información de valor y mejorando la seguridad de las instituciones.

Referencias

1. Barnum, S. (2012). Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corporation, 11, 1-22.
2. CBS News, «WannaCry» ransomware attack losses could reach $4 billion. (2017). Consultado 14 de junio de 2019, de https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
3. CIRCL » Malware Information Sharing Platform MISP - A Threat Sharing Platform. (2019). Consultado10 de mayo de 2019, de https://www.circl.lu/services/misp-malware-information-sharing-platform/
4. CISCO 2018. Reporte anual de Ciberseguridad. (2018). Consultado de https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf
5. Cisco Cybersecurity Report Series - Download PDFs - Cisco. (2019). Consultado5 de junio de 2019, de https://www.cisco.com/c/en/us/products/security/security-reports.html#~archives
6. Fernández, M. A. R., & García, P. P. (2017). El intercambio de información de ciberamenazas. Cuadernos de estrategia, (185), 139-170.
7. ISACA. (2019). State of Cybersecurity 2019 - ISACA. Consultado6 de junio de 2019, de https://www.isaca.org/info/state-of-cybersecurity-2019/index.html
8. McAfee Labs Threats Reports – Threat Research | McAfee. (2018). Consultado8 de junio de 2019, de https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html
9. Oasis, Cyber Threat Intelligence Technical Committee. (2019). Consultado 10 de mayo de 2019, de https://oasis-open.github.io/cti-documentation

10. Open Threat Exchange (OTX) | AlienVault. (2019). Consultado 11 de junio de 2019, de https://www.alienvault.com/open-threat-exchange
11. OpenIOC: Back to the Basics(2019). Consultado12 de junio de 2019, de FireEyewebsite: https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html
12. Pérez, D. B., Brito, H. R. G., & Borrell, Y. S. (2019). Modelo para la detección de ataques a las aplicaciones WEB e intercambio de ciberamenazas. RevistaTelemática, 17(2), 71-80.
13. REYES-REpositorio común Y EStructurado de amenazas y código dañino. (2019). Consultado 14 de junio de 2019, de https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html