Universidad Nacional de San Agustín de Arequipa
Facultad de Ingeniería, Producción y Servicios
Escuela Profesional de Ciencia de la Computación

Trabajo de Investigación Formativa 2

Fundamentos de Seguridad de la Información

Alumna: Chullunquía Rosas, Sharon Rossely Alisson
Docente: Mg. Lucy Delgado Barra
Fecha: 19 de septiembre de 2021

Arequipa, Perú

Índice de Contenidos

Índice de Figuras

1. Ejercicio

De manera individual debe reportar al menos tres Sites donde se monitorea la seguridad y las amenazas que aparecen en tiempo real, identifique tres ataques e indique que servicio de seguridad ha sido vulnerado

2. Kaspersky

2.1. Amenazas detectadas en la última semana

1. DangerousObject.Multi.Generic
2. Trojan.WinLNK.Agent.gen
3. Worm.Win32.Autoit.aku

2.2. Servicios de seguridad vulnerados

- Integridad
- Confiabilidad
- Confidencialidad

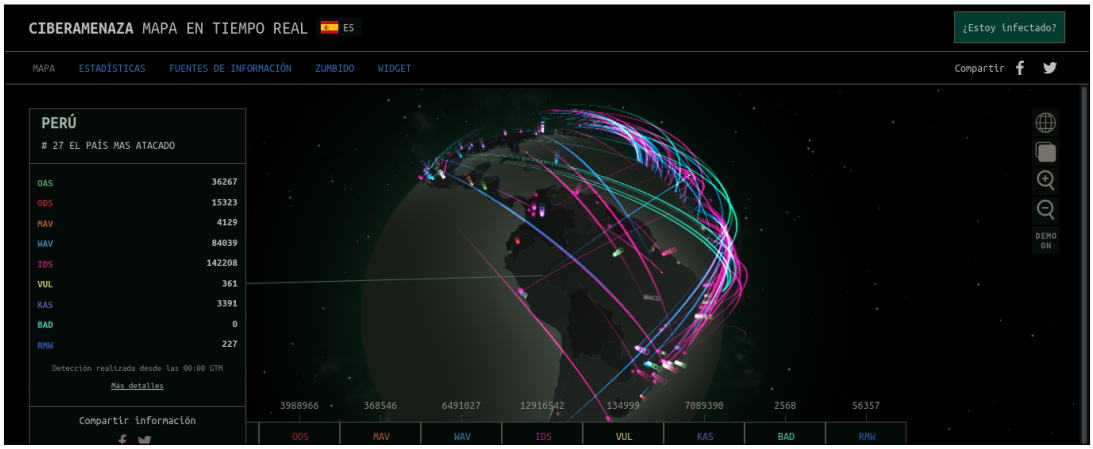

Figura 1: Kaspersky[1]

3. Fortinet

3.1. Amenazas detectadas en la última semana

1. Trojan.Win32.Miner.bbb
2. Virus.Win32.Renamer.j

3. DangerousObject.Multi.Generic

3.2. Servicios de seguridad vulnerados

- Confiabilidad
- Integridad
- Confidencialidad

Figura 2: Fortinet[2]

4. FireEye

4.1. Amenazas detectadas en la última semana

1. Trojan.MSIL.Witch.gen
2. Worm.Win32.Autoit
3. Trojan.WinLNK.Agent.rd

4.2. Servicios de seguridad vulnerados

- Confidencialidad
- Integridad
- Confiabilidad

Figura 3: FireEye[3]

5. Descripción de las amenazas Destectadas

- **DangerousObject.Multi.Generic:** Software malicioso es detectado por KL Cloud Technologies.
- **Trojan.WinLNK.Agent.gen:** Software malicioso de esta familia contiene enlaces para descargar archivos maliciosos, o la ruta para ejecutar un archivo ejecutable malicioso diferente, diseñado para destruir, bloquear, modificar o copiar datos.
- **Worm.Win32.Autoit.aku:**El malware de esta familia consiste en un script AutoIt que ejecuta varias tareas destructivas. El malware se propaga a través de recursos de red o medios extraíbles al copiarse en carpetas abiertas para lectura/escritura (si se encuentran).
- **Virus.Win32.Renamer.j:** Los virus se replican en los recursos de la máquina local. A diferencia de los gusanos, los virus no usan los servicios de red para propagarse o penetrar en otras computadoras. Una copia de un virus llegará a las computadoras remotas solo si el objeto infectado, por alguna razón no relacionada con la función del virus, está activado en otra computadora.
- **Trojan.Win32.Miner.bbb:** El malware en esta familia usa secretamente la capacidad del procesador de una computadora infectada para generar criptomonedas (bitcoins).
- **Trojan.WinLNK.Agent.rd:** El software malicioso de esta familia contiene enlaces para descargar archivos maliciosos, o la ruta para ejecutar un archivo ejecutable malicioso diferente, diseñado para destruir, bloquear, modificar o copiar datos.

Referencias

[1] "Cyberthreat real-time map." https://cybermap.kaspersky.com/. Accessed: 2021-09-18.

[2] "Fortinet." https://threatmap.fortiguard.com/. Accessed: 2021-09-18.

[3] "Fireeye." https://www.fireeye.com/cyber-map/threat-map.html. Accessed: 2021-09-18.