

# NerisBot Lab

Se ha detectado actividad de red inusual en un entorno universitario, lo que indica posibles intenciones maliciosas. Estas anomalías, observadas hace seis horas, sugieren la presencia de comunicaciones de comando y control (C2) y otros comportamientos dañinos dentro de la red.

Su equipo ha recibido la tarea de analizar los registros recientes de tráfico de red para investigar el alcance y el impacto de estas actividades. La investigación busca identificar servidores de comando y control y descubrir interacciones maliciosas.

***P1-Durante la investigación del tráfico de red, se observaron patrones inusuales de actividad en los registros de Suricata, lo que sugiere un posible acceso no autorizado. Una dirección IP externa inició intentos de acceso y posteriormente se detectó la descarga de un archivo ejecutable sospechoso. Esta actividad indica claramente el origen del ataque. ¿Cuál es la dirección IP desde la que se originó el acceso no autorizado inicial?***

Vamos a realizar la siguiente búsqueda:

```
index=* sourcetype="suricata" eventtype=suricata_eve_ids_attack | stats values(dest_ip) values(http.http_user_agent) values(http.http_content_type) values(http.http_protocol) values(http.status) values(http.hostname) values(http.url) by src_ip
```

Con esta búsqueda vamos a poder observar toda la trazabilidad de la actividad maliciosa:

| src_ip         | values(dest_ip) | values(http.http_user_agent)   | values(http.http_content_type)         | values(http.http_protocol) | values(http.status) | values(http.hostname)          | values(http.url)   |
|----------------|-----------------|--|--|----------------------------|---------------------|--------------------------------|--|
| 195.113.232.97 | 147.32.84.165   | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)  |  |                            |                     | cdn.ad4game.com                | /afa4c2125ff0443d57a0d92e767d2164.swf<br>/ba4678a2414fd12965ad29e79c1e9610.swf   |
| 195.113.232.98 | 147.32.84.165   | jupdate  |  |                            |                     | javadi-esd.sun.com             | /update/1.6.0/map-1.6.0.xml  |
| 195.113.232.99 | 147.32.84.165   | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)<br>Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.14) Gecko/2009090217 Ubuntu/9.04 (jaunty) Firefox/3.0.14 |  |                            |                     | bannerfarm.ace.advertising.com | /CDN/155095/HK_160x600_v1_5.25.11.jpg<br>/CDN/178743/160x600_1.14.11.jpg<br>/CDN/178757/dailyfinance_160_600_0410                      |
| 195.88.191.59  | 147.32.84.165   | Download<br>Mozilla/4.0 (compatible; MSIE 6.0.2900.2180; Windows NT 5.1.2600)  | application/octet-stream<br>text/plain |                            | 200                 | nocomcom.com                   | /bl/choose.exe?t=0.8925135<br>/bl/client.exe?t=0.9562799<br>/xx4.txt<br>/sv/fjuivgfhurew.exe?t=0.3069879<br>/temp/3425.exe?t=0.3419458 |

Veamos como en la ultima columna tenemos la IP origen que es la IP atacante.

**P2-Investigar el dominio del atacante ayuda a identificar la infraestructura utilizada para el ataque, evaluar su conexión con otras amenazas y tomar medidas para mitigar futuros ataques. ¿Cuál es el nombre de dominio del servidor del atacante?**

El dominio se puede observar en la columna de hostname de la misma captura de pantalla:

**P3-Conocer la dirección IP del sistema atacado ayuda a enfocar los esfuerzos de remediación y a evaluar el alcance de la vulneración. ¿Cuál es la dirección IP del sistema atacado en esta brecha?**

En la columna values(dest\_ip) podemos observar la IP destino que hace referencia a la IP que fue atacada

**P4-Identifique todos los archivos únicos descargados al host comprometido. ¿Cuántos de estos archivos podrían ser potencialmente maliciosos?**

En la ultima columna podemos ver todas las descargas que se realizaron en total son 5 los archivos potencialmente maliciosos.

**P5-¿Cuál es el hash SHA256 del archivo malicioso disfrazado de .txtarchivo?**

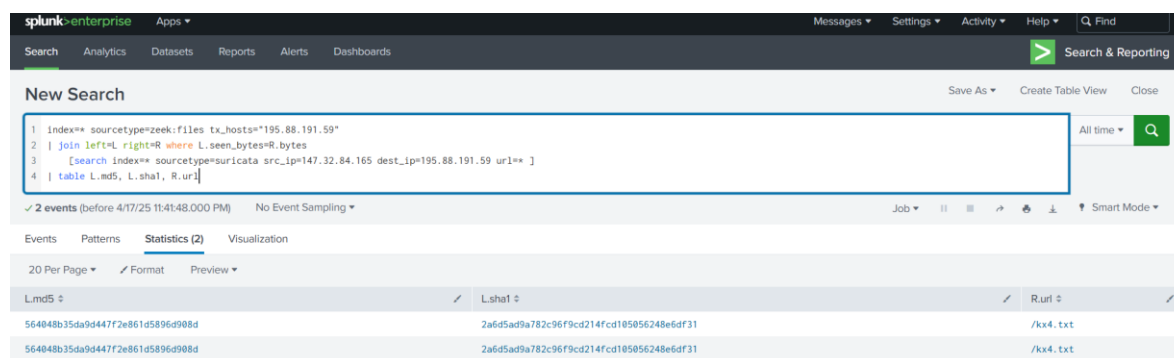
Para la ultima búsqueda la sentencia cambia:

```
index=* sourcetype=zeek:files tx_hosts="195.88.191.59"
```

```
| join left=L right=R where L.seen_bytes=R.bytes
```

```
[search index=* sourcetype=suricata src_ip=147.32.84.165 dest_ip=195.88.191.59 url=*]
```

```
| table L.md5, L.sha1, R.url
```



The screenshot shows the Splunk Enterprise interface. The search bar contains the following query:

```
1 index=* sourcetype=zeek:files tx_hosts="195.88.191.59"
2 | join left=L right=R where L.seen_bytes=R.bytes
3 [search index=* sourcetype=suricata src_ip=147.32.84.165 dest_ip=195.88.191.59 url=*]
4 | table L.md5, L.sha1, R.url
```

The results table shows 2 events. The columns are L.md5, L.sha1, and R.url.

| L.md5                            | L.sha1                                   | R.url    |
|----------------------------------|--|----------|
| 564848b35da9d447f2e861d5896d908d | 2a6d5ad9a782c96f9cd214fcd105056248e6df31 | /xx4.txt |
| 564848b35da9d447f2e861d5896d908d | 2a6d5ad9a782c96f9cd214fcd105056248e6df31 | /xx4.txt |

Veremos la lista del hash para el archivo .txt