El objetivo de esta actividad es defender la organización Castle&Sand de actores maliciosos. Esta empresa se encarga de la venta de artículos de alta calidad, caracterizada por tener empleados expertos y sede en múltiples ciudades. Para ellos es primordial la satisfacción del cliente y crear una experiencia en la que se sientan como en la playa.

Table Name	Description		
AuthenticationEvents	Records successful and failed logins to devices on the company network. This includes logins to the company's mail server.		
Email	Records emails sent and received by employees.		
Employees	Contains information about the company's employees.		
FileCreationEvents	Records files stored on employee's devices.		
InboundNetworkEvents	Records inbound network events including browsing activity from the Internet to devices within the company network.		
OutboundNetworkEvents	Records outbound network events including browsing activity from within the company network out to the Internet.		
PassiveDns (External)	Records IP-domain resolutions.		
ProcessEvents	Records processes created on employee's devices.		
SecurityAlerts	Records security alerts from an employee's device or the company's email security system.		

En el SOC hemos recibido una notificación que nos alerta de que Castle&Sand ha sido atacado mediante un ransomware y todos sus archivos han quedado completamente bloqueados. En el departamento hemos podido conseguir una copia. Encontrarás la nota de rescate llamada "PAY\_UP\_OR\_SWIM\_WITH\_THE\_FISHES.txt" en el siguiente enlace.

A través de la nota podemos obtener información que puede ser relevante para la investigación, entre ellas:

- El correo de contacto de la organización: sharknadorules\_gang@onionmail.org
- El ID único de descifrado: SUNNYDAY123329JA0

FileCreationEvents

Sabiendo el nombre del fichero, lo primero que haremos será encontrar la cantidad de ficheros que coincidan con este nombre y encontrar cuántos equipos tienen lo tienen.

```
| where filename == "PAY_UP_OR_SWIM_WITH_THE_FISHES.txt"
| count
>>> 774

FileCreationEvents
| where filename == "PAY_UP_OR_SWIM_WITH_THE_FISHES.txt"
| distinct hostname
| count
```

```
let ransom_hostnames = FileCreationEvents
| where filename == "PAY_UP_OR_SWIM_WITH_THE_FISHES.txt"
| distinct hostname;
Employees
| where hostname in (ransom_hostnames)
| distinct role
| count
```

>>> 18

Por lo que podemos hacer una aproximación del impacto que ha tenido el ransomware en la organización, afectando a 774 equipos diferentes que corresponden a empleados de hasta 18 roles distintos. Esto quiere decir que altos cargos de la organización con información altamente sensible y relevante pueden haber sido afectados, como por ejemplo ejecutivos, pero también parte del equipo de IT que disponen de roles administrativos altamente privilegiados.

```
let ransom_hostnames = FileCreationEvents
| where filename == "PAY_UP_OR_SWIM_WITH_THE_FISHES.txt"
| distinct hostname;
Employees
| where hostname in (ransom_hostnames) and role has "IT"
| distinct hostname
| count
```

>>> 18

De los equipos afectados, 18 de ellos pertenecen a empleados dentro del departamento de IT. Vamos a revisar en cuántos dispositivos se ha registrado una alerta relacionada con la nota de ransomware que dejaron los atacantes.

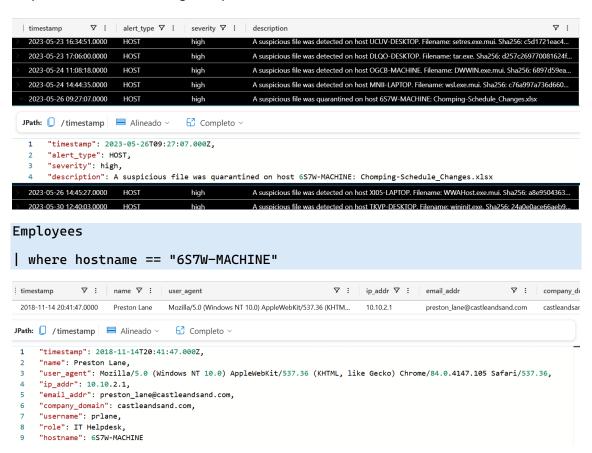
```
let impact_hosts = FileCreationEvents
| where filename == 'PAY_UP_OR_SWIM_WITH_THE_FISHES.txt'
| distinct hostname;
SecurityAlerts
| where description has_any (impact_hosts)
| count
>>> 652
```

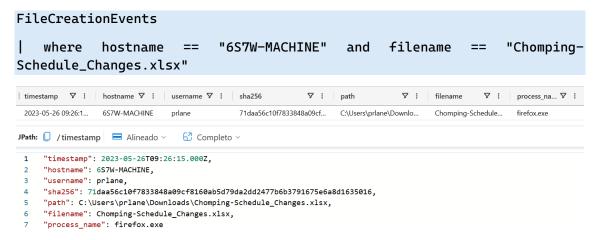
```
let impact_hosts = FileCreationEvents
| where filename == 'PAY_UP_OR_SWIM_WITH_THE_FISHES.txt'
```

```
| distinct hostname;
let helpdesk_hostnames = Employees
| where hostname in (impact_hosts)
| where role contains "IT Helpdesk"
| distinct hostname;
SecurityAlerts
| where description has_any (helpdesk_hostnames)
| count
```

#### >>> 27

De las 652 alertas recibidas relacionadas con la nota de rescate de ransomware, 27 de ellas están relacionadas con equipos que pertenecen al equipo de IT Helpdesk. Debido a que se maneja un número menor de datos y estos equipos pertenecen a uno de los departamentos más sensibles de la organización, vamos a comenzar a investigar por este lado. El objetivo es encontrar anomalías en las alertas que nos den una pista de qué ha ocurrido exactamente. Al navegar sobre las alertas que se disparan en las detecciones de ficheros sospechosos, vemos una anomalía en el equipo 6S7W-MACHINE donde el archivo Chomping-Schedule\_Changes.xlsx fue puesto en cuarentena el día 26 de mayo de 2023 a las 09:27:07. Este equipo pertenece a Preston Lane, por lo que se orientará la investigación por esta vía.





El fichero apareció por primera vez en el equipo el 26 de mayo de 2023 a las 9:26 AM, está asociado al hash Sha256 71daa56c10f7833848a09cf8160ab5d79da2dd2477b6b3791675e6a8d1635016 y fue creado desde Firefox.

```
FileCreationEvents
| where filename == "Chomping-Schedule_Changes.xlsx"
| distinct hostname
| count
```

### >>>11

Se han detectado 11 equipos distintos en los que este fichero fue creado. Si nos basamos en la aplicación relacionada con la creación del fichero y la ubicación del mismo (carpeta de descargas), muy posiblemente se haya realizado una descarga desde internet, por lo que debemos comprobar qué dominios se han utilizado para dicha descarga.

# OutboundNetworkEvents | where url has "Chomping-Schedule\_Changes.xlsx"

timestamp	meth ∇ :	src_ip ∇ ∶	url ∇ :	user_agent
> 2023-05-25 16:43:06.0000	GET	10.10.2.80	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT €
> 2023-05-25 16:47:48.0000	GET	10.10.3.216	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:50.0)
> 2023-05-25 16:47:49.0000	GET	10.10.5.68	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident
> 2023-05-25 16:48:26.0000	GET	10.10.3.136	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT $\epsilon$
> 2023-05-26 09:25:26.0000	GET	10.10.2.1	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.:
> 2023-05-26 10:21:36.0000	GET	10.10.4.127	https://jawfin.com/published/images/files/Chomping-Schedule	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWeb
> 2023-05-27 09:13:17.0000	GET	10.10.3.124	http://shark fin.com/modules/public/published/Chomping-Sche	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWe
> 2023-05-27 09:16:36.0000	GET	10.10.2.108	http://shark fin.com/modules/public/published/Chomping-Sche	Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWeb
> 2023-05-27 09:16:36.0000	GET	10.10.3.44	http://shark fin.com/modules/public/published/Chomping-Sche	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6
> 2023-05-27 10:44:42.0000	GET	10.10.4.231	http://shark fin.com/modules/public/published/Chomping-Sche	Mozilla/5.0 (Windows NT 6.2; rv:47.0) Gecko/2010
> 2023-05-27 11:49:07.0000	GET	10.10.2.67	http://shark fin.com/modules/public/published/Chomping-Sche	Mozilla/5.0 (Windows NT 5.1; WOW64; rv:48.0) Ge

Los dos dominios relacionados con la descarga de estos ficheros son jawfin[.]com y sharkfin[.]com. Concretamente, el empleado del departamento de IT donde se encontró el fichero en cuarentena descargó el fichero desde una página con dominio jawfin[.]com, ya que en la tabla anterior podemos ver que la IP de origen 10.10.2.1 es la que corresponde a Preston Lane.

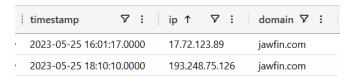
## PassiveDns

# 

Este listado de IPs son las que resuelven en el dominio implicado en la descarga de un archivo potencialmente malicioso y, por tanto, posiblemente relacionado con el ataque. Teniendo en cuenta el momento de la descarga del archivo en el equipo de Preston, la IP en la que resuelve el dominio más cercana a este periodo es 193.248.75.126.

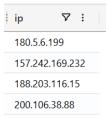
## **PassiveDns**

| where domain has "jawfin.com" and timestamp between (datetime(2023-05-23T07:00:15.000Z) .. datetime(2023-05-27T23:26:15.000Z))



En cuanto al dominio sharkfin[.]com, las siguientes 4 IP resuelven en dicho dominio:

```
PassiveDns
| where domain has "sharkfin.com"
| distinct ip
```



Si recogemos las IP relacionadas con ambos dominios sospechoso y revisamos las peticiones entrantes en los eventos de red de la página de Castle&Sand, veremos que en total se encuentran 39 registros de eventos, siendo el primero de ellos el 20 de marzo de 2023 a las 3:11:57 AM.

```
let ip_addr_ransom = PassiveDns
| where domain has_any ("sharkfin.com", "jawfin.com")
| distinct ip;
```

## InboundNetworkEvents

| where src\_ip in (ip\_addr\_ransom)

count

## >>> 39

