

# Apostar por la IA:

neutralizar las amenazas antes de que los ciberatacantes se hagan de oro

José Badia, Country Manager España



# Próximamente

**DARKTRACE**

- Retos de seguridad a los que se enfrentan los servicios financieros
- IA de autoaprendizaje y respuesta autónoma
- Hallazgos de amenazas de Darktrace:
  - Ciberataques inspirados en Hafnium
  - Frustrado el ransomware GandCrab
  - Ataque Shodan contra la vulnerabilidad de la nube

- Aumento del número de troyanos bancarios y ataques a la cadena de suministro
- Los trabajadores a distancia manejan datos sensibles de los clientes
- Urgencia de actualizar la infraestructura bancaria digital
- Presión para cumplir la normativa

# Las amenazas en cifras

**DARKTRACE**

**74%**

de los bancos y aseguradoras  
experimentaron un aumento de la  
ciberdelincuencia, 2020-21

**\$5.9 million**

coste medio de una brecha  
de datos en el sector  
financiero

**436**

campañas de phishing  
únicas al mes

- Depende de las normas, las firmas y los libros de juego
- Retrospectiva
- Falta de visibilidad y contexto
- Respuestas demasiado tímidas o demasiado agresivas



Un "sistema inmunológico" digital que:

- Aprende su negocio desde la base
- Se adapta a los cambios del entorno
- Es independiente de los datos
- Identifica signos sutiles de ataques nunca vistos

*"Darktrace AI hace el trabajo pesado para nuestro equipo de seguridad. Somos más eficientes al centrarnos en la gestión de los ciberriesgos, en lugar de en el triaje y la documentación."*  
**CISO, NKGSB Bank**

# Respuesta autónoma

**DARKTRACE**

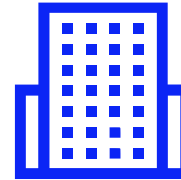
Un cerebro con capacidad de decisión que:

- **Toma** medidas específicas para neutralizar los ataques en curso
- **Realiza** miles de cálculos a velocidad de máquina a partir de datos en tiempo real
- **Permite** que el negocio continúe sin interrupción, actuando de forma proporcional
- **Protege** todo el patrimonio digital

*"Cualquiera que sea el problema, dondequiera que esté en nuestra infraestructura, Darktrace detendrá su propagación, ganando un tiempo precioso para que podamos mitigar la amenaza".*

**Head of IT Operations, PPS  
Insurance**

- Se han detectado varios intentos de ataque a servidores Exchange orientados a Internet a través de la vulnerabilidad ProxyLogon
- Los servidores comprometidos descargaron archivos ejecutables ocultos en carpetas ZIP desde un dominio inusual
- Ataque neutralizado antes de que la vulnerabilidad se hiciera pública

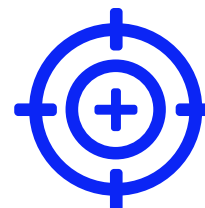


**Sector:** Servicios financieros



**Actividad anómala:**

- Actividad de minería de divisas
- SSL sospechoso y caducado
- Transferencia de archivos enmascarados
- Archivo anómalo / Descarga de archivos del sistema frente a Internet
- Dispositivo / Nuevo agente de usuario PowerShell
- Archivo anómalo / Múltiples EXE desde ubicaciones externas raras
- Conexión anómala / Powershell a un externo raro



**Acción antigena:**

Bloqueo de conexiones específicas a través de los puertos 443 y 8080



# Resumen del incidente y acción antigena

**Incident Log**

Beginning on Sunday 7<sup>th</sup> March 12:28 UTC, the device [REDACTED].local exhibited the following events worth of investigation

- Possible HTTP Command...
- Unusual Repeated Conne...
- Possible SSL Command an...
- Multiple Suspicious File D...

Sun 7<sup>th</sup> 12:00 Mon 8<sup>th</sup> 00:00 Mon 8<sup>th</sup> 12:00 Tue 9<sup>th</sup> 00:00 Tue 9<sup>th</sup> 12:00 Wed 10<sup>th</sup> 00:00 Wed 10<sup>th</sup> 12:00 Thu 11<sup>th</sup> 00:00 Thu 11<sup>th</sup> 12:00 Fri 12<sup>th</sup> 00:00 Fri 12<sup>th</sup> 12:00 Sat 13<sup>th</sup> 00:00 Sat 13<sup>th</sup> 12:00

1. Possible HTTP Command and C...    2. Unusual Repeated Connections    3. Possible SSL Command and...    4. Multiple Suspicious File Downl...

### Summary

The device [EXAMPLE].local was observed making multiple SSL connection to the rare external endpoint telepra.ph, with the same SSL fingerprint (JA3 hash).

Moreover, this device only used this fingerprint for connections to a limited set of endpoints – suggesting that the activity was initiated by a standalone process as opposed to a web browser.

If such behavior is unexpected, further investigation may be required to determine if this activity represents malicious command and control as opposed to legitimate telemetry.

### Suspicious Application

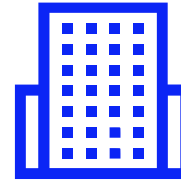
JA3 client hash    94d4b9644db7c35313308bc0c2a71a35

### Suspicious Endpoint Contacted by Application

|                            |  |
|----------------------------|--|
| Time                       | 11 <sup>th</sup> Mar 2021 08:52:34 – 12 <sup>th</sup> Mar 19:19:46 |
| Endpoint                   | telegra.ph   |
| Hostname rarity            | 100%   |
| Hostname first observed    | 11 <sup>th</sup> Mar 2021 08:52:34 UTC                             |
| Most recent destination IP | 149.154.164.13   |
| Most recent ASN            | AS62041 Telegraph Messenger Inc                                    |

Fri Mar 12 15:18:48    **Antigena Response –**  
Block connections to 198.98.61.152 port 8080, 38.108.185.64 port 443, 38.108.185.79 port 443, microsoftsoftwaredownload.com port 8080 and od.lk port 443 for 2 hours

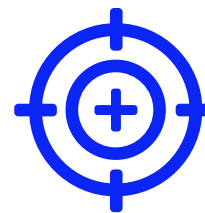
- Archivo malicioso descargado por error a través del correo electrónico
- Dispositivo infectado conectado a la infraestructura del ransomware GandCrab
- Antigena identificó y detuvo el ataque de forma autónoma



**Sector:**  
Servicios financieros

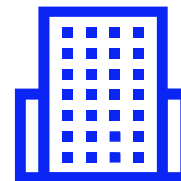


**Actividad anómala:**  
Cifrado de casi 5.000 documentos internos y adición de una nota de rescate



**Acción antigena:**  
Identificó el ataque y detuvo todas las comunicaciones salientes del dispositivo infectado, evitando la posterior pérdida de datos

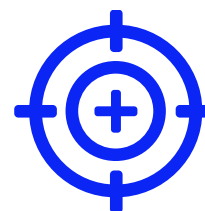
- Error en la configuración de los controles nativos de la nube
- Se dejó un importante servidor expuesto a Internet cuando debía estar aislado tras un cortafuegos
- El servidor expuesto fue finalmente descubierto y el objetivo de los ciberdelincuentes que escaneaban Internet a través de Shodan.



**Sector:** Servicios financieros



**Actividad anómala:** Escaneo de Internet a través de Shodan



**Acción antigena:** Alertó inmediatamente al equipo de seguridad de la amenaza en cuestión de segundos

# Preguntas

