Ciber IA de Darktrace

Un sistema inmune para el correo electrónico

> Hoy más que nunca, la seguridad actual del correo electrónico requiere innovación y un cambio de mentalidad para combatir el panorama de amenazas en evolución.
>
> **– Peter Firstbrook, VP Analyst de Gartner**

Introducción

Contenido

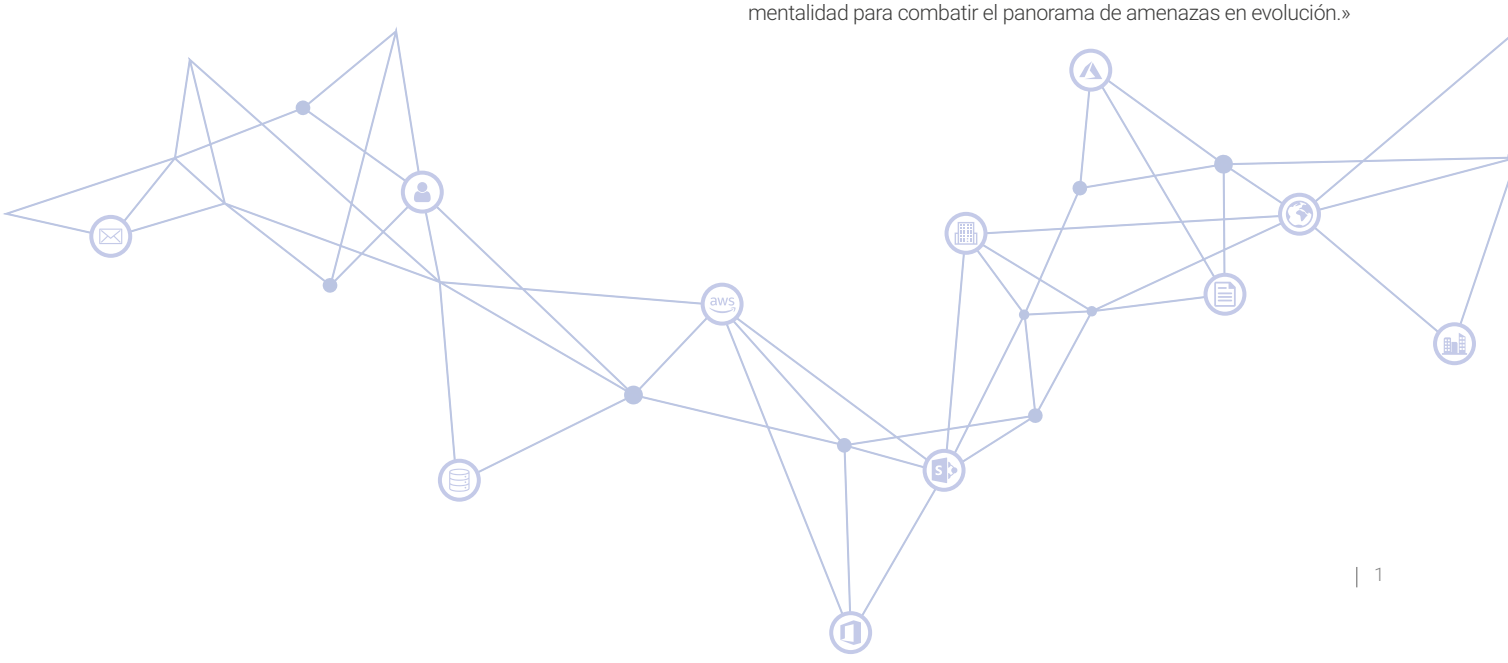
Las plataformas de colaboración y de correo electrónico representan el tejido que conecta cualquier negocio digital. Se comparte información, se idean planes y se forman alianzas en el ámbito digital de la correspondencia escrita. Aunque es un medio utilizado por el ser humano, el correo electrónico siempre será alimentado por una suposición generalizada de confianza, que sigue siendo el 'eslabón más débil' en la estrategia de seguridad de una organización.

Si bien esta suposición de confianza resulta esencial para la colaboración y el crecimiento; también significa que el correo electrónico, más que cualquier otra área del negocio, seguirá siendo estructuralmente resistente al espíritu actual de 'confianza cero' y, por lo tanto, no sorprende que el 94% de las ciberamenazas aún sigan procediendo del correo electrónico.

Para minimizar la influencia del error humano en esta área, la industria ha adoptado generalmente la idea de que se debe confiar en la tecnología para identificar los correos electrónicos maliciosos que incluso los empleados más perspicaces y cualificados no pueden detectar. No obstante, hasta hace poco tiempo, las defensas tradicionales han luchado para seguir el ritmo con innovaciones en el panorama de las ciberamenazas.

El phishing de objetivo definido, los ataques de suplantación de identidad y los robos de cuentas, en particular, siguen siendo vías de ataque fructíferas para los ciberdelincuentes que pretenden infiltrarse en una organización con facilidad. Los ataques por correo electrónico focalizados de este tipo, junto con las limitaciones de las defensas tradicionales, siguen siendo un gran desafío incluso para las organizaciones con las estrategias de seguridad más avanzadas y con más niveles.

Peter Firstbrook, VP Analyst de Gartner, resume bien la dinámica del mercado: «Los controles comunes, como los antivirus estándar, basados en la reputación, antispam y basados en firmas, están bien para las campañas de estafa y los ataques muy extendidos; pero no son lo suficientemente buenos como para protegerse contra ataques más focalizados, sofisticados y avanzados. Hoy más que nunca, la seguridad actual del correo electrónico requiere innovación y un cambio de mentalidad para combatir el panorama de amenazas en evolución.»



Inteligencia artificial de Darktrace: Una plataforma de sistema inmune

No obstante, gracias a la reciente aparición de la inteligencia artificial a escala empresarial, este 'cambio de mentalidad' finalmente se ha materializado en forma de un enfoque de 'sistema inmune' para la seguridad del correo electrónico.

Como sugiere Firstbrook, las defensas del correo electrónico tradicionales pueden ser adecuadas para amenazas sencillas e indiscriminadas, pero no están diseñadas para contraatacar ataques más avanzados que se han personalizado para destinatarios y empresas específicos.

Las puertas de enlace (gateways) de correo electrónico tradicionales y los controles nativos se basan en reglas codificadas de forma rígida y un conocimiento de los antiguos ataques para la detección. Por lo tanto, su alcance está limitado necesariamente a las amenazas que ya se han visto anteriormente, o que son al menos lo suficientemente básicas como para desencadenar una regla estática y binaria en el borde. Pero, como muchos líderes empresariales pueden afirmarle basándose en sus malas experiencias, este no es el desafío al que nos enfrentamos.

Afortunadamente, el cambio de estrategia que ha surgido en la seguridad del correo electrónico ha diferenciado en gran medida el 'enfoque común' de Firstbrook y una aplicación innovadora de la inteligencia artificial a escala empresarial. Esta distinción se ha comparado con la diferencia entre la 'piel protectora' de una organización y su 'sistema inmune' que aprende de las amenazas que consiguen pasar.

Mientras que su piel protectora conoce los antiguos ataques y puede detener amenazas muy conocidas, su 'sistema inmune' conoce los 'patrones de vida' individuales que caracterizan el flujo de trabajo digital de cada empleado. Y lo que es fundamental, estos 'patrones de vida' se manifiestan no solo en el tráfico de correo electrónico, sino también en el tráfico de red y de la Nube; y de una manera que se puede unificar en una imagen evolutiva y completa de la normalidad para cada usuario.

Esta comprensión única de toda la empresa está permitiendo a las organizaciones neutralizar más ataques focalizados que nunca, ya que sigue siendo el único enfoque que puede proporcionar las pruebas suficientes para determinar con precisión si las discretas desviaciones de un correo electrónico focalizado son realmente maliciosas.

Por primera vez, nuestras defensas del correo electrónico pueden preguntar eficazmente si sería extraño que un usuario recibiera un correo electrónico, teniendo en cuenta lo que el sistema sabe acerca de los 'patrones de vida' de dicho empleado, sus compañeros y toda la organización; no solo en el correo electrónico, sino también en la Nube y en la red corporativa.

También es el único enfoque que puede actualizar sus decisiones y acciones según las nuevas pruebas, incluso después de que se haya enviado un correo electrónico –tanto si dichas pruebas se manifiestan en el correo electrónico como si lo hacen mediante comportamientos maliciosos que surgen en la red.

Estas Notas del producto están concebidas para ilustrar la razón por la que una comprensión unificada y personalizada del tráfico de red, de la Nube y de correo electrónico representa un cambio de estrategia en el mercado de la seguridad del correo electrónico. Darktrace fue pionera en este enfoque con Antigena Email y su plataforma Enterprise Immune System. Los siguientes casos prácticos se incluirán en una de las cuatro categorías de ataques muy sofisticados que rutinariamente eluden su 'piel protectora', pero que la inteligencia artificial de Darktrace neutraliza fácilmente en cuestión de segundos:

- Phishing de objetivo definido y entrega de carga
- Robo de cuenta de una cadena de suministro
- Ingeniería social y solicitación
- Ataque a credenciales de empleado

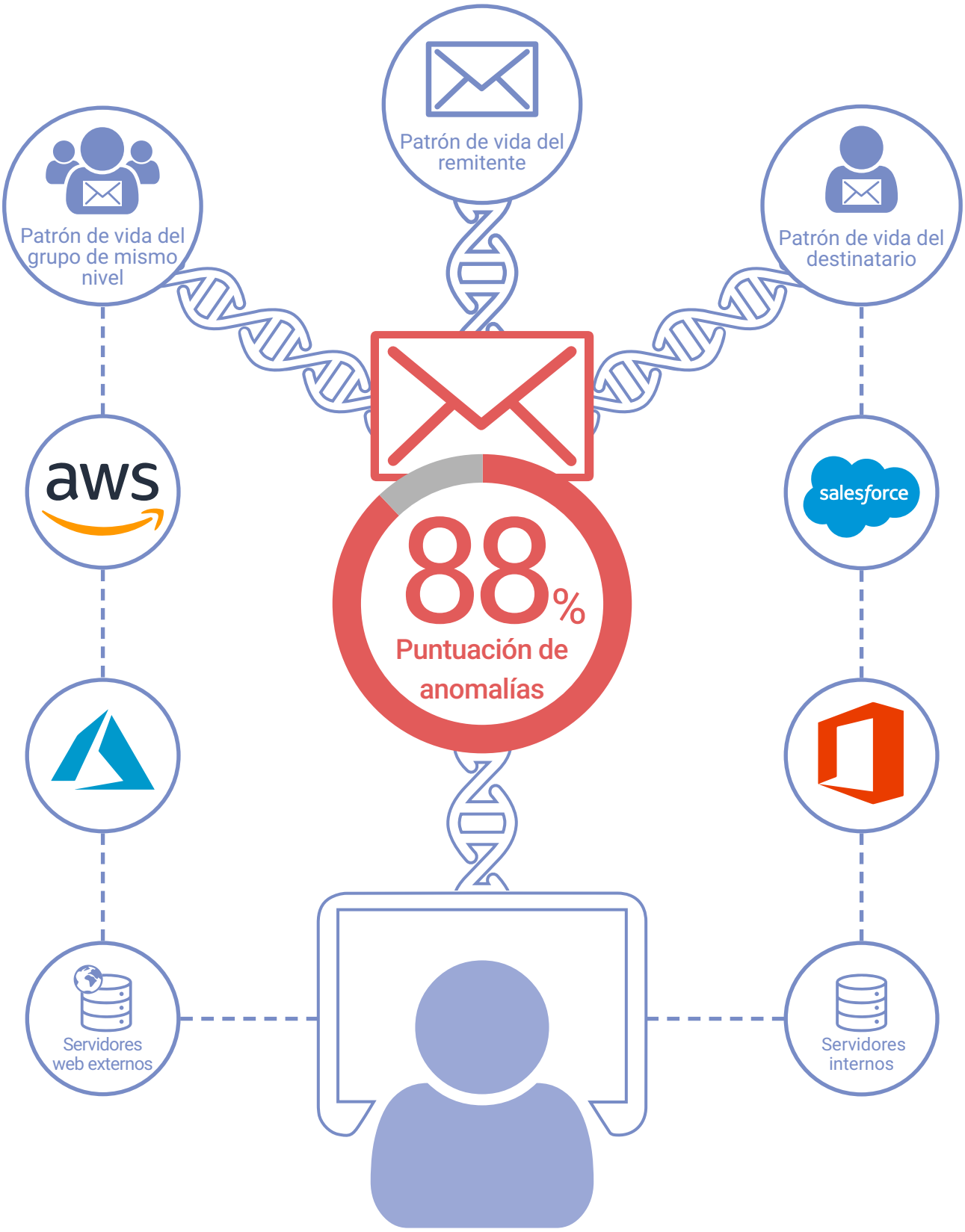
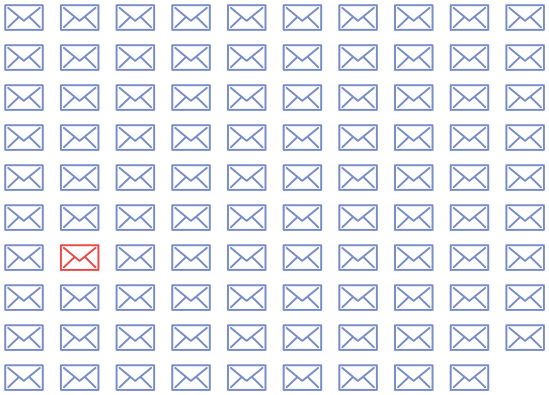


Figura 1: Antigena Email es la única solución que analiza los correos electrónicos en el contexto de toda la organización –no solo los datos del correo electrónico. Esta comprensión de toda la empresa le permite detectar los correos electrónicos maliciosos que eluden las defensas tradicionales en el borde.

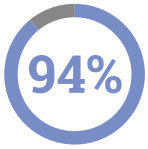
Phishing de objetivo definido y entrega de carga

> Antigena Email ha sido totalmente fundamental para la captura de amenazas con su comprensión de lo que es 'normal' tanto para el correo electrónico como para el tráfico de red.
>
> **– Head of IT, Entegrus**

1 de cada 99 correos electrónicos es un ataque de phishing



Source: Avanan



del malware actual procede de la bandeja de entrada

La mayoría de las campañas de phishing intentan engañar a los usuarios para que hagan clic en enlaces o archivos adjuntos maliciosos de un correo electrónico, con el objetivo final de obtener credenciales o implementar un malware destructivo en una organización. Estos ataques pueden enviarse como campañas 'drive-by' indiscriminadas contra miles de organizaciones, o como ataques de 'phishing de objetivo definido' elaborados que se personalizan para un destinatario o negocio específico.

Para defenderse contra las campañas de phishing, las defensas tradicionales generalmente analizan los correos electrónicos según la comprensión de los ataques antiguos, las listas negras y las firmas. Sin embargo, los ciberdelincuentes entienden este enfoque reactivo mejor que nadie, y tienen todos los incentivos para aprovechar nuevas tácticas y técnicas que eluden las defensas antiguas por diseño.

Sin embargo, aunque estos ataques nunca se han visto anteriormente y, por lo tanto, eludirán las defensas tradicionales en el borde, esto significa que en algún nivel de la descripción serán muy anómalos para el usuario o negocio a quien van dirigidos –al menos si se tienen en cuenta los 'patrones de vida' de todo el entorno digital. Esta realidad básica es precisamente la razón por la que es tan importante cerrar la brecha del conocimiento de seguridad tradicional entre el nivel del correo electrónico externo y toda la red, como lo ha hecho la Plataforma Immune System de Darktrace.

Con la inteligencia artificial de escala empresarial, Antigena Email es capaz de analizar enlaces, archivos adjuntos, dominios, contenidos y otros elementos de un correo electrónico junto con los 'patrones de vida' en la Nube y la red, correlacionando una enorme cantidad de puntos de datos que pueden demostrar que algunos correos electrónicos aparentemente fiables son claramente maliciosos.

A diferencia de cualquier otra solución, Antigena Email y el Immune System pueden correlacionar datos de la red, de la Nube y del correo electrónico para determinar si los dominios asociados con una carga y un remitente no son normales, si la ubicación de un enlace de un correo electrónico es extraña, si los temas de debate y el contenido son inusuales e, incluso, si los patrones de la ruta de la URL son sospechosos.

Este enfoque fundamentalmente único significa que la toma de decisiones de Darktrace es considerablemente más precisa que la de otras herramientas, de manera que puede realizar acciones muy proporcionadas y focalizadas para neutralizar los ataques de phishing a gran escala.

El Immune System también se encuentra en la posición única de ser capaz de detectar una infección en cualquier entorno y realizar automáticamente un análisis de la causa principal para ver si procede del correo electrónico. Si es así, protegerá inmediatamente al resto de empleados a los que va dirigido el mismo ataque. A esto lo denominamos 'respuesta autónoma estratégica' –en la que aprender del Paciente Cero permite la protección estratégica del resto del negocio sin la intervención humana. Desde la perspectiva de un equipo de seguridad, aún sigue siendo necesario que alguien limpie el portátil de la primera víctima, pero eso es mucho mejor que limpiar 200 o más portátiles.

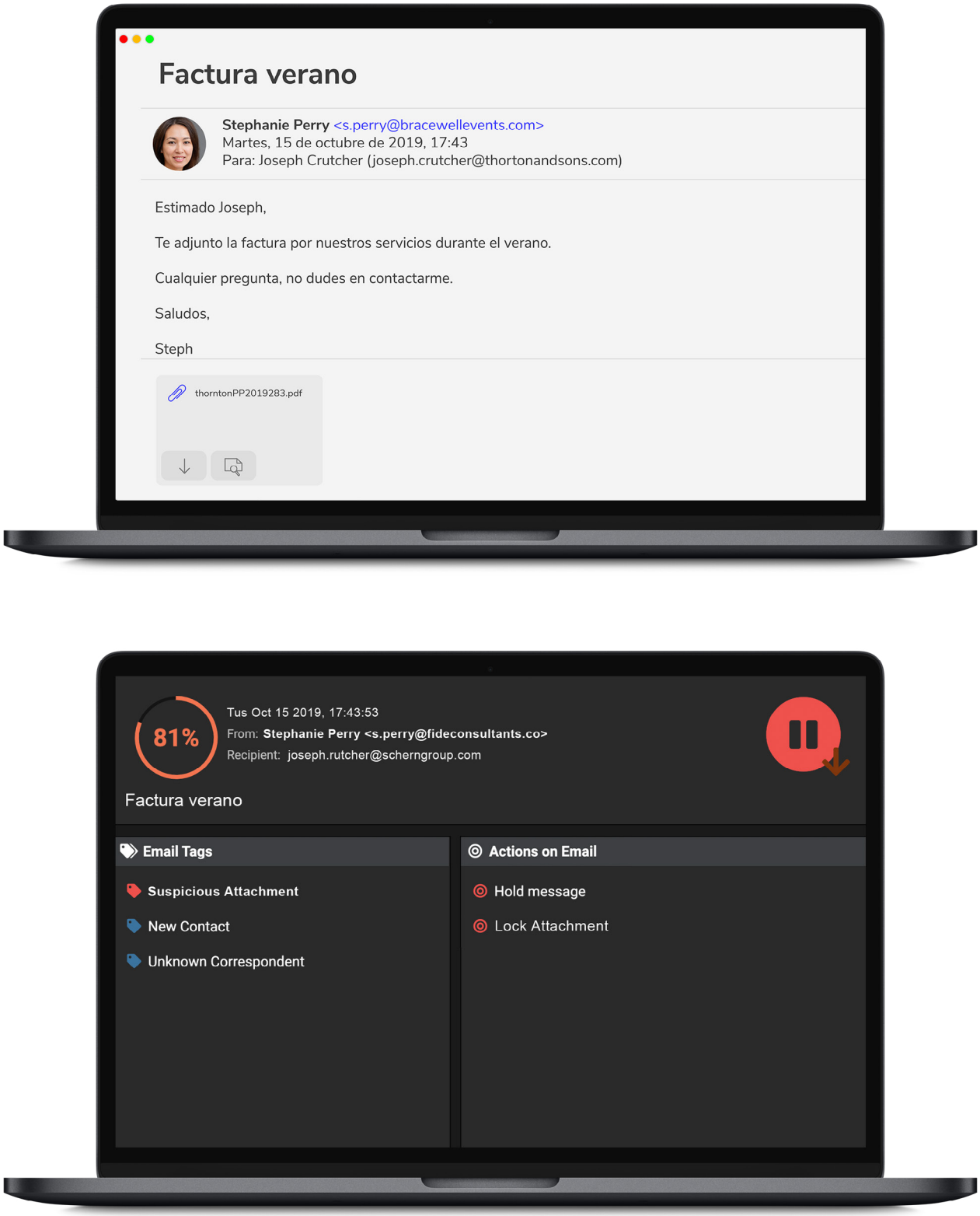


Figura 2: Un correo electrónico que incita a un empleado a hacer clic en un archivo adjunto que contiene una carga maliciosa, y la vista correspondiente en la interfaz de usuario de Darktrace, que muestra las etiquetas de anomalías y las acciones realizadas.

Ataque de WeTransfer

Darktrace detectó un ataque de phishing dirigido a cinco usuarios de alto perfil de una organización académica de Singapur, cuidadosamente diseñado para engañarlos para que hicieran clic en un enlace malicioso.

Antigena Email asignó a estos correos electrónicos una puntuación de anomalías del 100% y realizó acciones para 'Detenerlos', evitando así que llegaran a sus destinatarios. También identificó los discretos indicadores de suplantación de servicios, a pesar de que la organización tenía una relación conocida con el remitente.

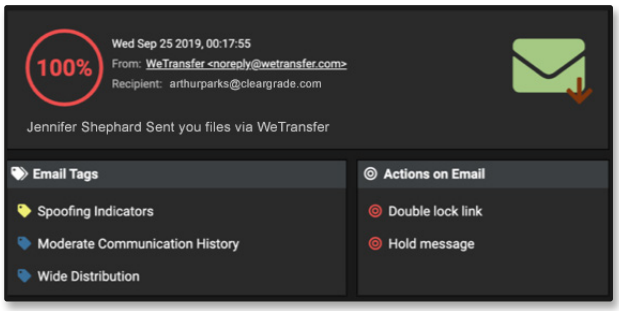


Figura 3: La interfaz de usuario que muestra los incumplimientos de modelos y las acciones

1. En los datos del encabezado, no había señales claras de que este correo electrónico tuviera otra fuente que no fuera WeTransfer, y le habría parecido perfectamente normal al destinatario. El 'Ancho' y la 'Profundidad' indican que esta dirección de correo electrónico se ha comunicado con numerosas personas de la organización, durante varios días.

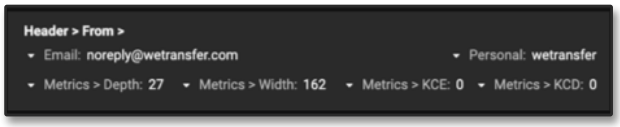


Figura 4: Los datos de conexión de los correos electrónicos correspondientes

2. Sin embargo, Antigena Email fue capaz de detectar una serie de discretas anomalías gracias a su comprensión de lo que es 'normal' para el usuario y la organización, junto con el contexto adicional obtenido del nivel de red.

a. En primer lugar, la 'puntuación de anomalías de la dirección IP' fue alto (63%). Esta medida indica lo inusual que es que esta dirección de correo electrónico envíe desde esta IP teniendo en cuenta los patrones de envío antiguos y, generalmente, es una indicación de una cuenta suplantada o secuestrada.

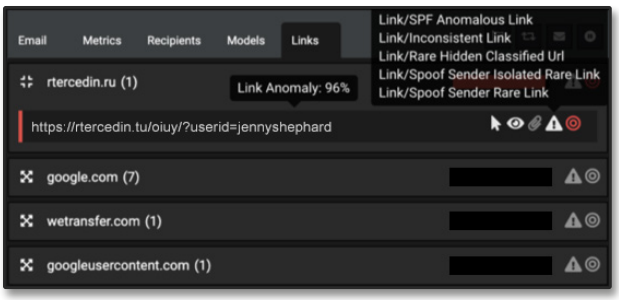


Figura 5: Un desglose de los enlaces mostrados en los correos electrónicos

b. Además, como Darktrace está constantemente modelando el comportamiento 'normal' de cada remitente externo, fue capaz de detectar una anomalía clave en el cuerpo del correo electrónico: un enlace que no coincidía en gran medida con lo que Darktrace había visto anteriormente de WeTransfer, lo que permitió a Antigena Email identificarlo como la carga maliciosa del correo electrónico.

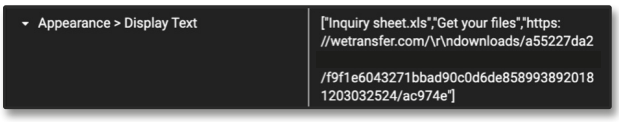


Figura 6: Antigena fue capaz de determinar dónde apareció el enlace en el correo electrónico

c. El enlace en cuestión recibió una puntuación de anomalías del 96%, y estaba oculto tras los botones de estilo 'haga clic aquí' en varias partes del correo electrónico, incluyendo un enlace falso: 'https://wetransfer.com/...' (en la imagen que aparece más abajo), y el texto 'Inquiry Sheet.xls' y 'Get Your Files'.

Este ataque era completamente nuevo y eludió el resto de herramientas basadas en firmas que la universidad tenía implementadas. De igual forma, debido a que el enlace utilizó un dominio completamente fiable y no redirigía a una carga obviamente maliciosa, es posible que incluso la detección heurística y el espacio seguro hubieran fallado.

Malware oculto en facturas falsas

Una importante firma de abogados se convirtió en uno de los objetivos principales de una campaña de phishing avanzada, que pretendía ocultar malware de robo de credenciales en archivos ISO, adjuntos a facturas falsas. Las defensas tradicionales del correo electrónico normalmente incluyen en su lista blanca los archivos ISO, mientras que los sistemas operativos montan automáticamente sus imágenes con un solo clic, lo que supone un evidente atractivo para los ciberdelincuentes.

Sin embargo, cuando una veintena de correos electrónicos maliciosos eludieron las defensas tradicionales del correo electrónico de la empresa, Darktrace detuvo la campaña al reconocer varios indicadores anómalos. Por ejemplo, uno de los modelos de inteligencia artificial que activaron los correos electrónicos fue "Archivo adjunto/MIME anómalo no solicitado", lo que significa que el tipo de MIME del archivo adjunto era muy inusual para el usuario y su grupo de mismo nivel, y que el destinatario nunca se había comunicado con el remitente para solicitar dicho archivo.

Al localizar la procedencia exacta de la amenaza, Darktrace realizó acciones quirúrgicas para desactivarla, en lugar de simplemente marcar todos los correos electrónicos potencialmente sospechosos con advertencias genéricas que probablemente serían ignoradas. Para contrarrestar los archivos ISO maliciosos, Darktrace convirtió los archivos adjuntos en archivos PDF inofensivos y movió los correos electrónicos a la carpeta de correo no deseado. Y lo que es fundamental, al detectar el primer correo electrónico de la campaña, la tecnología neutralizó automáticamente otros 20 correos electrónicos antes de que tuvieran la oportunidad de afectar al negocio.

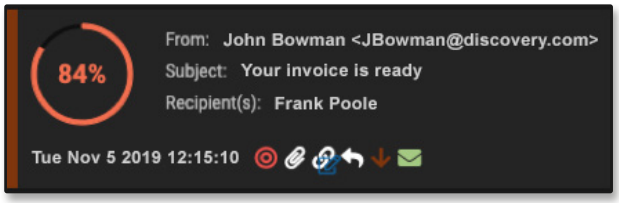


Figura 7: Encabezado de los correos electrónicos maliciosos, mostrando la acción sugerida

Ataque a libreta de direcciones de un municipio

Un ciberdelincuente logró obtener la libreta de direcciones de un municipio de los EE.UU., y envió un ataque a los destinatarios por orden alfabético, de la A a la Z. Cada correo electrónico estaba bien diseñado y personalizado para cada destinatario, y todos los mensajes contenían una carga maliciosa oculta tras un botón camuflado de distintas formas como un enlace de Netflix, Amazon y otros servicios de confianza.

Cuando llegó el primer correo electrónico, Darktrace reconoció inmediatamente que ni el destinatario ni nadie de su grupo de mismo nivel ni el resto de los empleados de la ciudad habían visitado antes ese dominio. El sistema también reconoció que la forma en la que se ocultaban los enlaces tras cada botón era muy sospechosa. Lanzó una alerta de alta confianza y sugirió bloquear de forma autónoma cada enlace según entrara en la red.

Lo que es muy interesante es que el hecho de que Antigena se hubiera implementado en 'Modo pasivo' proporcionó las pruebas claras y concretas de la capacidad del sistema para detener ataques discretos que otras herramientas pasan por alto: mientras que Antigena detectó y trató de neutralizar la campaña en la letra 'A', las herramientas de seguridad antiguas del equipo se dieron cuenta de la amenaza en la letra 'R'. En el 'Modo activo', Antigena habría neutralizado el ataque antes de que pudiera llegar a un solo usuario.

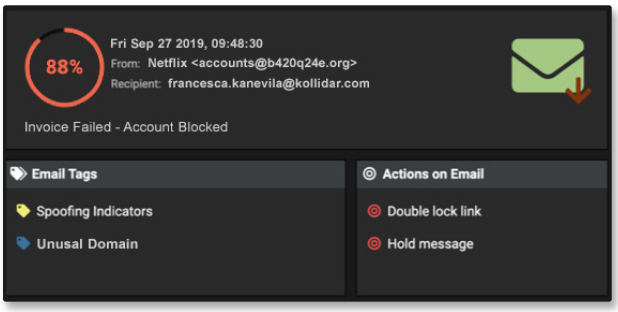
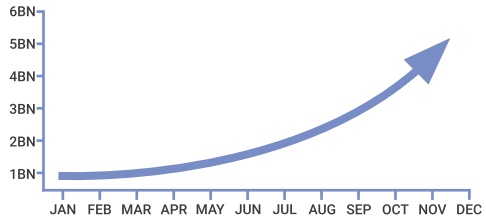


Figura 8: Antigena Email mostrando una puntuación de anomalías del 88%

Robo de cuenta de una cadena de suministro

Las pérdidas por robos de cuentas se han multiplicado más de tres veces en el último año hasta alcanzar los 5.100 millones de dólares estadounidenses.



Fuente: Javelin

Al secuestrar la información de la cuenta de un contacto de confianza de su cadena de suministro, los ciberdelincuentes pueden ganarse fácilmente la confianza de un destinatario de la red y convencerle para que haga clic en un enlace malicioso o transfiera millones fuera del negocio. Las defensas de correo electrónico antiguas presuponen la confianza, lo que permite que los robos de cuentas sofisticados pasen a menudo completamente desapercibidos.

Las cuentas que han sufrido ataques han sido responsables de varios ataques de alto perfil en grandes organizaciones en los últimos años. Los ciberdelincuentes cada vez aprovechan más las cadenas de suministro –compuestas por proveedores, socios y contratistas– en sus ataques para infiltrarse en una organización o establecer una comunicación sin conexión. A principios de este año, un informe acerca del denominado 'island hopping' –en el que los atacantes intentan expandirse a través de una fisura en las cadenas de suministro– descubrió que este método representa la mitad de los ataques actuales.

Los atacantes que tienen total acceso a la cuenta de correo electrónico de un proveedor pueden analizar las interacciones del correo electrónico anteriores y enviar una respuesta específica para el último mensaje. El lenguaje que utilizan a menudo parecerá fiable, por lo que las herramientas de seguridad de correo electrónico antiguas que buscan palabras o frases clave indicativas de phishing no podrán detectar estos ataques.

Antigena Email es capaz de formular una idea global de la normalidad de las palabras de cada usuario interno; por lo que, independientemente de lo fiable que pueda parecer la redacción para la mayoría de los observadores, humanos o máquinas; es capaz de identificar distribuciones irregulares de palabras y frases. Al analizar los patrones de comunicación con el contexto completo de todo el tráfico de red y de correo electrónico, Antigena Email utiliza varias medidas para identificar con seguridad los casos de robos de cuentas; algo que resulta imposible de detectar sin una comprensión detallada del comportamiento 'normal' de todo el entorno digital.

La tecnología identifica anomalías en el tema y el contenido de cada correo electrónico, y analiza todo ello según la coincidencia de la ubicación del inicio de sesión, los enlaces y los archivos adjuntos y los anteriores destinatarios comunes del remitente. Antigena Email utiliza esta comprensión multidimensional para determinar la probabilidad de que un correo electrónico de un proveedor de confianza sea legítimo. No presupone la confianza. Dependiendo de la gravedad de la amenaza, puede enviar una respuesta adecuada, bloqueando enlaces y archivos adjuntos o borrando completamente un correo electrónico de la bandeja de entrada de un empleado.

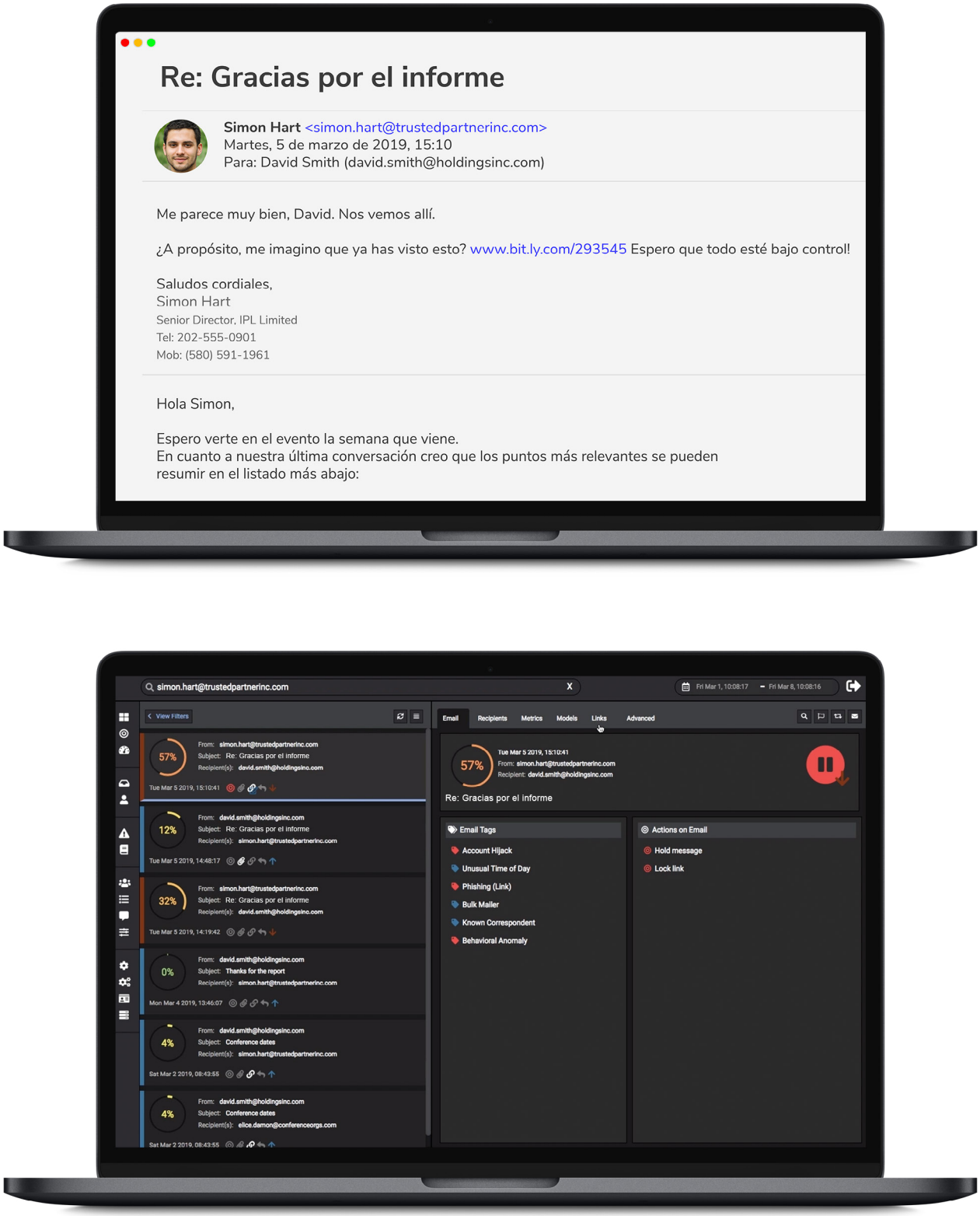


Figura 9: Una respuesta aparentemente fiable enviada desde la cuenta atacada de un proveedor de confianza siguiendo un hilo de comunicación por correo electrónico. El enlace contenía una carga maliciosa.

Ataques consecutivos a una cadena de suministro

Un cliente que estaba probando Antigena Email experimentó dos incidentes graves en días consecutivos, cuando las cuentas del correo electrónico de los proveedores de confianza se convirtieron en la fuente de una campaña maliciosa–muy probablemente después de que dichas cuentas fueran atacadas.

Antigena Email aún no se había configurado para realizar acciones autónomas, por lo que los usuarios estaban totalmente expuestos al contenido de los correos electrónicos. Sin embargo, en todos los casos, Antigena Email informó de que habría detenido los correos electrónicos y bloqueado dos veces las cargas de los enlaces, mientras que las herramientas de seguridad integradas de Microsoft no detectaron nada sospechoso y dejaron que pasara todo sin realizar ninguna acción.

Incidente 1 – Empresa de consultoría

En el primer caso, Antigena Email detectó que el remitente era muy conocido por la empresa, y que varios usuarios internos se habían comunicado directamente con él anteriormente. De hecho, ese mismo día, uno de estos usuarios intercambió correos electrónicos normales con la cuenta que pronto sería secuestrada. El proveedor en cuestión era una empresa de consultoría medioambiental con sede en el Reino Unido.

Menos de dos horas después de este intercambio rutinario, los correos electrónicos se enviaron rápidamente a 39 usuarios, cada uno de ellos con un enlace de phishing. Hubo una variación en las líneas del asunto y los enlaces que contenían los correos electrónicos, lo que significaba que eran correos electrónicos muy focalizados de un atacante muy preparado. El objetivo de los enlaces podría haber sido solicitar pagos, recopilar contraseñas o implementar malware.

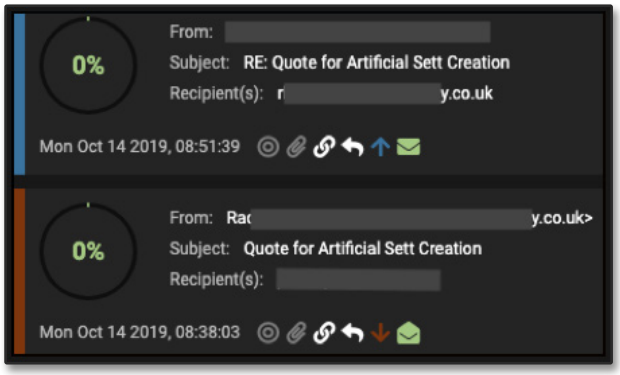


Figura 10: La comunicación anterior por correo electrónico 'normal' con el remitente–con una puntuación de anomalías del 0%

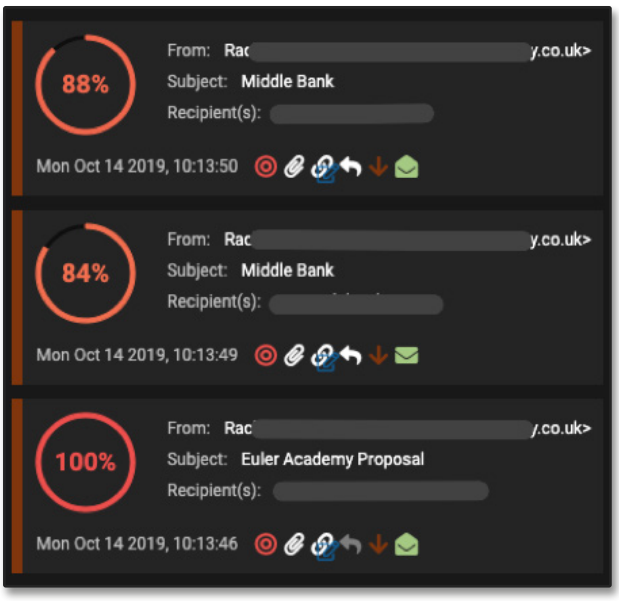


Figura 11: Los correos electrónicos enviados más tarde ese mismo día que contenían archivos adjuntos maliciosos

Antigena Email identificó todas las distintas señales de alarma que generalmente se asocian con robos de cuentas de cadenas de suministro:

1. Ubicación de inicio de sesión inusual: Antigena Email determinó que los correos electrónicos se habían enviado desde un servidor web de Outlook auténtico. Esto en sí mismo no era inusual para el proveedor, pero en estos datos de conexión también fue posible extraer la dirección IP geolocalizable, lo que reveló que el atacante inició su sesión desde una IP de los EE.UU., en lugar de desde su ubicación de inicio de sesión habitual del Reino Unido.

2. Los enlaces no coincidían: Todos los enlaces de phishing que contenían los correos electrónicos estaban hospedados en la plataforma para desarrolladores Microsoft Azure –probablemente para evitar las verificaciones de reputación en el dominio de host. A pesar de que generalmente se confía en la legitimidad de azurewebsites.net en Internet, Antigena Email fue capaz de detectar que este dominio no coincidía en gran medida con el remitente, basándose en el historial de la comunicación por correo electrónico anterior. El subdominio inusual también indicaba que el nombre de host tenía una puntuación de rareza máxima en el contexto del tráfico de red de la organización. Debido a que los otros productos de seguridad de correo electrónico no se beneficiaban de esta inteligencia contextual, les habría sido imposible llegar a esta conclusión.

3. Destinatarios inusuales: Se asignó una puntuación de 'anomalía de asociación' del destinatario para determinar la probabilidad de que este grupo específico de destinatarios recibiera un correo electrónico de la misma fuente. Al añadir contexto a su investigación a lo largo del tiempo, Antigena Email dedujo que este grupo de destinatarios era 100% anómalo con solo el tercer correo electrónico.

Usage > Darktrace Host Rarity	100
Usage > Domain External User Hostnames	0
Usage > Domain Inconsistency Score	88

Figura 12: Métricas alertadas por la rareza e inconsistencia del hipervínculo

4. Anomalía de tema: Las líneas del asunto de dichos correos electrónicos hacían pensar que intentaban parecer discretos y profesionales y, por lo tanto, cualquier intento basado en firmas de buscar palabras clave asociadas con phishing habría fallado. Sin embargo, Antigena Email reconoció que estos destinatarios generalmente no recibían correos electrónicos sobre propuestas comerciales que utilizaban ese estilo de redacción.

Property	Value
Recipient > Metrics > Association Anomaly	100

Figura 13: Antingea Email rápidamente detectó que este grupo de receptores no estaba íntimamente relacionado

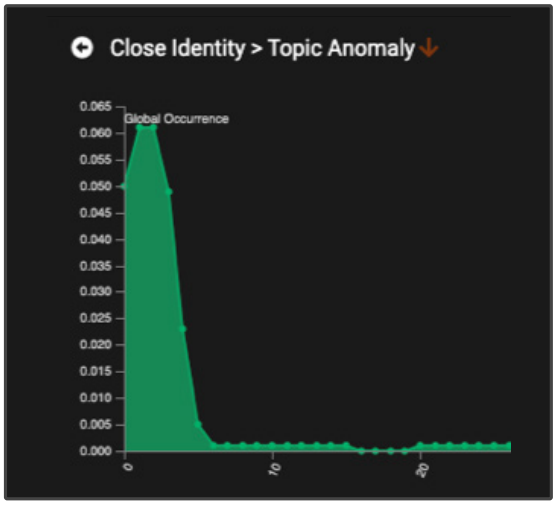


Figura 14: La vista del resumen de la medida de Anomalía de tema.

Incidente 2 – Ataque a proveedor de SaaS

Un segundo ataque al día siguiente provocó el envío de correos electrónicos a 55 usuarios internos de un proveedor de SaaS que conocía la empresa. Debido a la inacción por parte de Microsoft, los destinatarios leyeron más del 50% de estos correos electrónicos. Antigena Email alertó de que dichos correos electrónicos debían detenerse, evitando así que llegaran a la bandeja de entrada.

1. Como había ocurrido anteriormente, todos los correos electrónicos enviados desde la cuenta que había sido atacada contenían un enlace de phishing malicioso. Sin embargo, en este caso, el enlace permaneció activo durante un periodo de tiempo más largo, lo que permitió realizar una reconstrucción precisa de lo que los usuarios finales se habrían encontrado.

2. Afortunadamente, aquellos que habían interactuado con los correos electrónicos fueron encontrados fácilmente y las cuentas se recuperaron, gracias a la inteligencia compartida por Antigena Email y la Plataforma Immune System de Darktrace en la red. El Immune System también pudo ver que los dispositivos de la red física se conectaron al host del phishing. Trabajando en sincronía con Antigena Email, el Immune System marcó dichas interacciones con dominios sospechosos de phishing en la red.

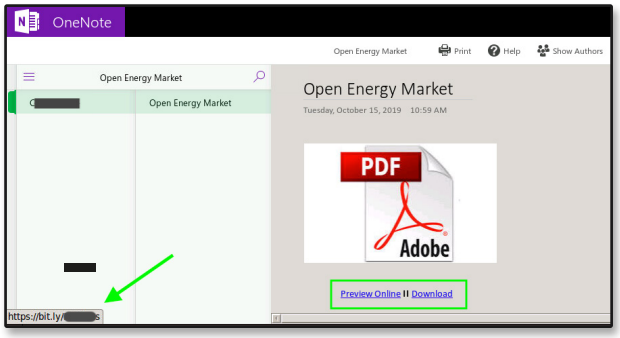


Figura 15: Captura de pantalla que muestra un enlace oculto

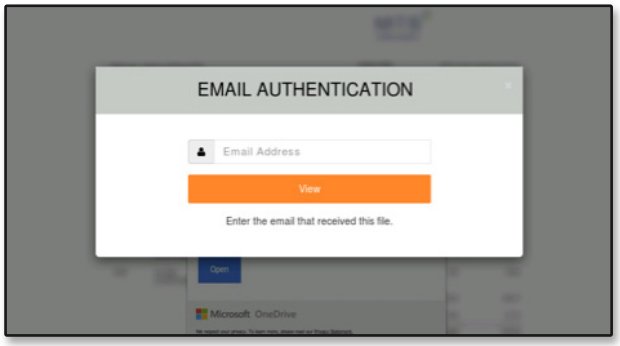


Figura 16: Este cuadro redirigía a un formulario que recopilaría las credenciales del usuario.

3. Aunque los enlaces estaban integrados en los 'enlaces seguros' de Microsoft ATP (lo que significaba que Microsoft habría realizado una verificación en tiempo real de los enlaces cuando el usuario hiciera clic en ellos), las conexiones a los puntos de conexión reales del tráfico de red confirmaron que la información disponible de Microsoft en ese momento hacía pensar que los enlaces eran seguros, exponiendo a los usuarios al punto de conexión malicioso.

4. El propio enlace estaba hospedado en la conocida plataforma de uso compartido de archivos SharePoint. Al visitar el enlace, se redirigía al usuario a un documento que se presentaba como un informe sobre el mercado energético. Sin embargo, un botón que solicitaba al usuario que descargara el archivo redirigía a otra página web aparentemente fiable que estaba configurada para pedir el correo electrónico y la contraseña del usuario –y los enviaba directamente al atacante.

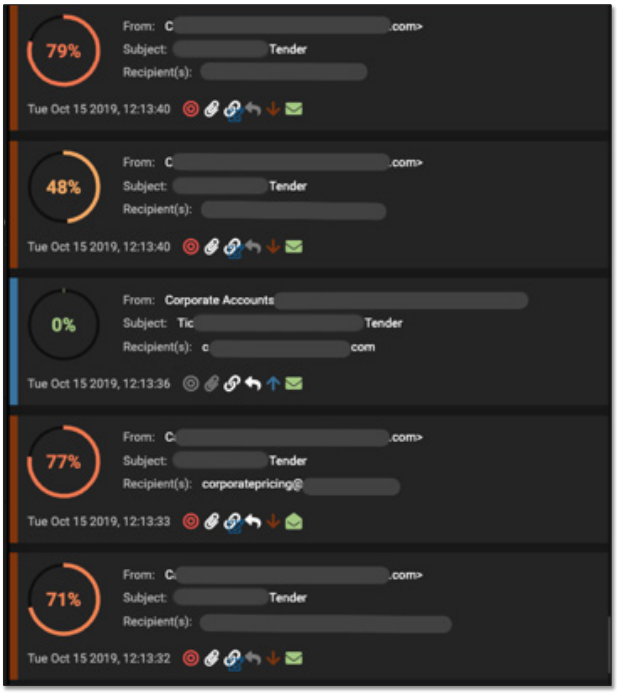


Figura 17: Los correos electrónicos del Incidente 2 tal y como aparecían en Antigena Email Console, incluyendo los correos salientes que se enviaron como respuesta. Esto revela que el usuario de las 'cuentas corporativas' reconoció el correo electrónico al abrir un ticket.

Archivo malicioso oculto en una página de OneDrive

Un ciberdelincuente avanzado secuestró la cuenta de correo electrónico de un proveedor de un gran grupo de hoteles, utilizando la cuenta de confianza para enviar una carga maliciosa a la organización. Aunque el ataque consiguió eludir las defensas tradicionales de la empresa, Antigena Email neutralizó la amenaza en cuestión de segundos.

1.El análisis de un correo electrónico anterior reveló que Antigena Email comprendió que había una relación entre los dos remitentes.

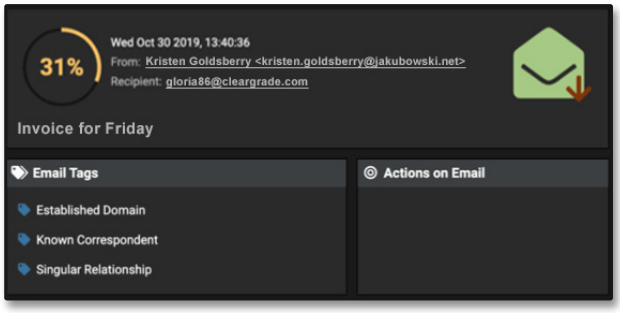


Figura 18: Un ejemplo de una comunicación anterior

2. Un correo electrónico posterior se marcó como muy anómalo al compararlo con los patrones de comunicación anteriores del remitente.

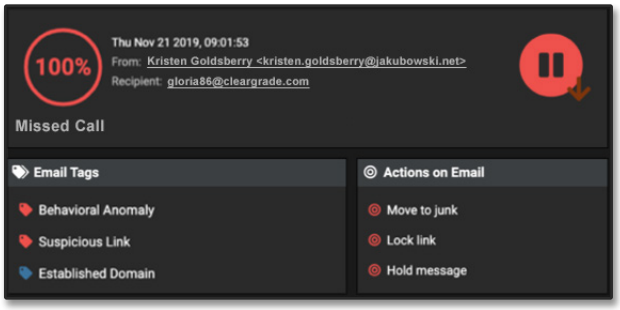


Figura 19: Un correo electrónico posterior etiquetado y tres incumplimientos del modelo asociado

3.Como podemos ver, todos estos correos electrónicos fueron etiquetados con el modelo de 'Anomalía de comportamiento', y Antigena Email decidió que la mejor acción que se podía realizar era detener estos mensajes para que no llegaran a los destinatarios a los que iban dirigidos.

4. Antigena Email identificó varias desviaciones del 'patrón de vida' normal del remitente externo, incluyendo el 'País de origen anómalo' y la 'Dirección IP de origen anómala'.

5. El enlace malicioso del correo electrónico tampoco coincidía en gran medida con los 'patrones de vida' de la empresa en el correo electrónico y el tráfico de red y, por estas razones, Antigena Email lo bloqueó.

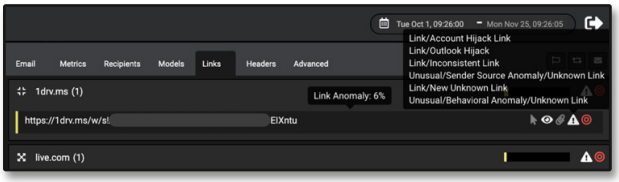


Figura 20: El enlace malicioso identificado

6. El propio enlace estaba oculto tras el texto de la pantalla 'Recuperar mensaje' y redirigía a una página de OneDrive. El uso de dominios de almacenamiento de archivos para hospedar contenido malicioso es difícil de detectar utilizando un enfoque tradicional, ya que es imposible incluir en la lista negra servicios como SharePoint; y decidir si un enlace como este es malicioso o fiable requiere una comprensión del correo electrónico en el contexto de toda la organización.

Ingeniería social y solicitación

> Tenemos implementado Antigena Email, así como herramientas de seguridad antiguas. Nos quedamos impactados por las cosas que las herramientas tradicionales no pudieron detectar y que Antigena Email sí que detectó.
>
> **– CTO, Bunim Murray Productions**

de los ataques en las bandejas de entrada del usuario no contenían malware

Los ataques de solicitación y de ingeniería social generalmente implican un intento sofisticado de suplantación de identidad, en el que los atacantes camuflados piden urgentemente a un destinatario que responda, que establezca comunicaciones sin conexión o que realice una transacción sin conexión. Sus objetivos van desde el fraude electrónico hasta el espionaje corporativo e, incluso, el robo de propiedad intelectual. Si bien las organizaciones deberían invertir, sin duda, en formación de seguridad y formar a sus empleados para que presten atención a las señales de advertencia; por mucho que les orienten, no podrán garantizar una inmunidad total frente a estos ataques cada vez más sofisticados.

Aunque las campañas de phishing tradicionales generalmente incluyen una carga maliciosa oculta tras un enlace o archivo adjunto, los intentos de ingeniería social a menudo implican el envío de 'correos electrónicos limpios' que solo contienen texto. Estos ataques eluden fácilmente las herramientas de seguridad tradicionales que se basan en correlacionar enlaces y archivos adjuntos con listas negras y firmas. Además, este vector de ataque generalmente implica el registro de nuevos dominios 'similares', que no solo engañan al destinatario sino que también eluden las defensas tradicionales.

Antigena Email cuenta con una comprensión unificada de lo que es 'normal' en todo el tráfico de red y de correo electrónico que evoluciona con el negocio, lo que le permite detectar casos discretos de solicitación. Los correos electrónicos limpios que eluden las defensas tradicionales se pueden identificar en cuestión de segundos gracias a la gran variedad de medidas; que incluyen las similitudes sospechosas con usuarios conocidos, las asociaciones anormales entre destinatarios internos e, incluso, las anomalías en el contenido y el tema del asunto de los correos electrónicos.

La mayoría de los casos, los ataques de ingeniería social intentan establecer inmediatamente una conversación sin conexión, lo que significa que las medidas de seguridad lentas y reactivas suelen intervenir únicamente después de que se hayan producido los daños. Su gran comprensión de cada usuario, dispositivo y relación con la organización permite a Antigena Email responder proactivamente y con gran confianza la primera vez, por lo que pudo intervenir en esta fase inicial tan importante.

Antigena también es único en su capacidad de adaptar de forma inteligente las respuestas a los tipos de amenazas específicas. Entiende que el elemento 'peligroso' en un ataque de solicitación a menudo será el propio contenido del correo electrónico y, por lo tanto, el sistema evitará que se entregue antes, incluso, de que el destinatario tenga la oportunidad de realizar la solicitud urgente que le pide el atacante.

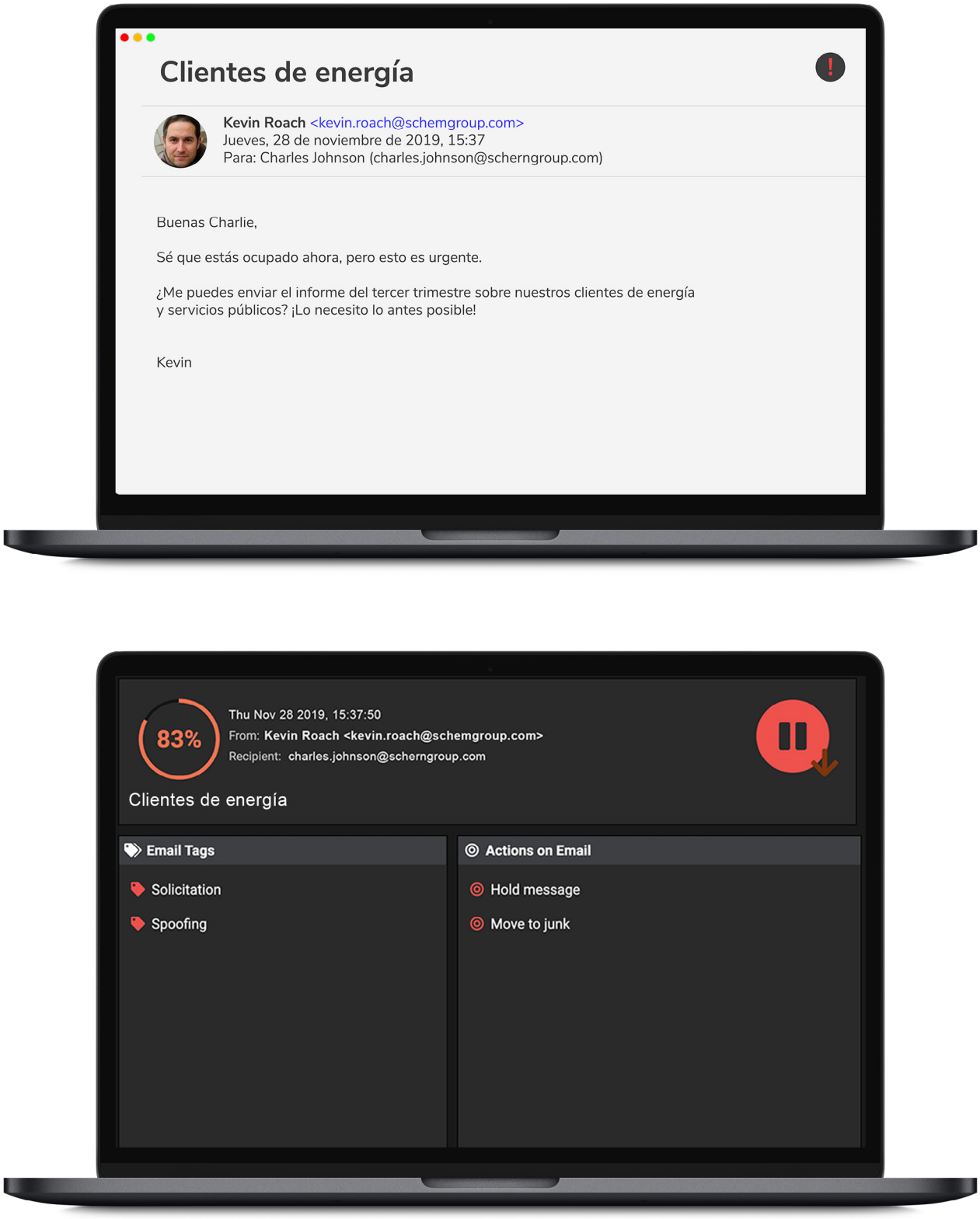


Figura 21: Un atacante que se hace pasar por un ejecutivo para aprovecharse de documentos confidenciales. Fíjese en la dirección de correo electrónico suplantada.

Ataque de suplantación de identidad

Antigena Email detectó un ataque dirigido a 30 empleados de una empresa multinacional de tecnología. Estaba claro que se había realizado una investigación exhaustiva, ya que para cada usuario al que estaba dirigido, el atacante se hizo pasar por el ejecutivo de nivel C con el que tenían más probabilidades de comunicarse. Antigena Email identificó el ataque de ingeniería social y, como resultado, detuvo todos los correos electrónicos para que no llegaran a los destinatarios a los que iban dirigidos.

1. La línea del asunto de cada correo electrónico incluía el nombre del empleado al que iba dirigido, y procedía de una dirección de Gmail aparentemente no relacionada. A pesar de la ausencia de una carga maliciosa (como enlaces o archivos adjuntos), Antigena Email fue capaz de identificar los correos electrónicos como maliciosos.

2. Darktrace no solo identificó los intentos de suplantación de identidad al reconocer el nombre similar del dominio, sino que además los correos electrónicos habían incumplido el modelo de 'No asociación', lo que indicaba que en toda su comprensión del correo electrónico y el entorno de red de la empresa, no había visto ninguna prueba de que hubiera una relación entre dicho remitente y la organización.

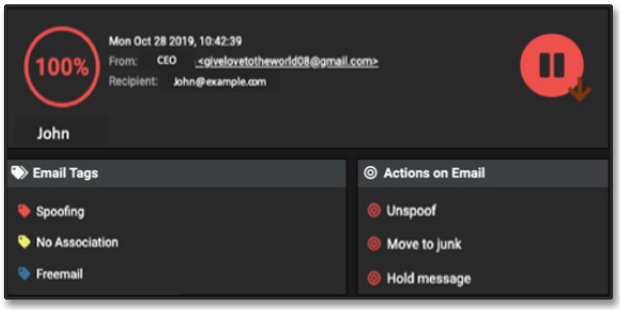


Figura 22: Uno de los 30 correos electrónicos, con una puntuación de anomalías del 100%

3. Al correlacionar varios indicadores leves, Antigena reconoció estos correos electrónicos como componentes de un ataque coordinado, por lo que los mantuvo en un búfer para que el equipo de seguridad de la organización los revisara.

4. Antigena Email no solo identificó a los tres ejecutivos de nivel C cuya identidad había sido suplantada, sino que además reconoció que el atacante también había suplantado la dirección personal externa legítima de su CEO.

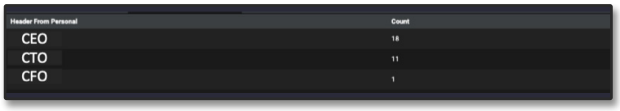


Figura 23: Los tres ejecutivos de nivel C identificados

5. Además, la puntuación de exposición de los usuarios cuya identidad había sido suplantada era alta, lo que indicaba que eran objetivos de alto perfil y, por lo tanto, se incumplía el modelo de 'Pesca de pez gordo'. Entender que los usuarios internos principales habían sido atacados permitió a la inteligencia artificial de Darktrace priorizar este ataque, e inició una respuesta proporcional en tiempo real.

Solicitud de nómina de CEO

En un distribuidor de electricidad, la inteligencia artificial de Darktrace detectó un convincente intento de suplantación de identidad descubierto en una cuenta de correo electrónico de Office 365. El correo electrónico, supuestamente del CEO de la empresa, se envío a un miembro del departamento de nóminas solicitándole a dicho empleado que actualizara la información de depósito directo del CEO.

Debido a que el correo electrónico imitaba correctamente el estilo de redacción típico del CEO, podría haber tenido éxito fácilmente si la inteligencia artificial de Darktrace no hubiera estado analizando el flujo del correo electrónico de la empresa en relación con el resto del negocio.

1. Al aprender el 'patrón de vida' normal del empleado, del CEO y de toda la organización en el tráfico de red y en la Nube, Darktrace fue capaz de identificar inmediatamente una serie de discretas anomalías en el correo electrónico, incluyendo la dirección del remitente falsificada.

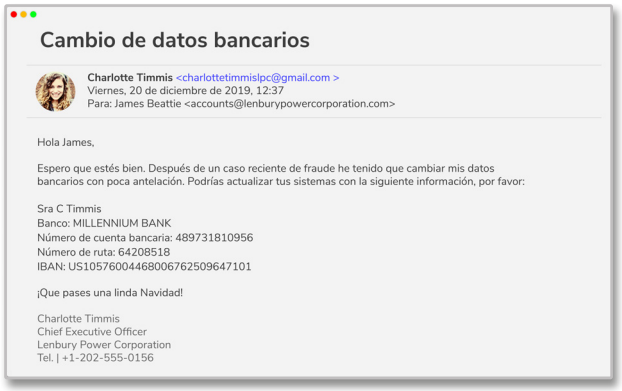


Figura 24: Captura de pantalla del correo electrónico que suplantó la identidad del CEO

2. Entre otros indicadores leves, la inteligencia artificial de Darktrace calculó automáticamente la proximidad anómala del dominio a la de los empleados internos y los contactos de confianza.

3. La inteligencia artificial respondió inmediatamente, bloqueando los enlaces del correo electrónico y lo marcó claramente como una suplantación de identidad antes de que pudiera llegar al departamento de nóminas. La gran comprensión de Darktrace del tráfico de red y de la Nube le permitió neutralizar una amenaza muy grave que las herramientas basadas en firmas habrían pasado por alto.

Ataque de suplantación de identidad de un 'Vicepresidente Financiero'

Este incidente implicó la suplantación de identidad de un Vicepresidente Financiero de una conocida institución financiera. Los ciberdelincuentes enviaron 11 correos electrónicos similares a la organización, pero Antigena Email realizó acciones para detener todos los correos, gracias a su comprensión multidimensional de lo que es 'normal' en todo el tráfico de red, de la Nube y de correo electrónico. Al analizar la dirección de correo electrónico no relacionada y claramente anómala en relación con el contenido de los correos electrónicos, Darktrace reconoció este intento de suplantación de identidad; mientras que la puerta de enlace heredada de la empresa dejó pasar a los 11 correos electrónicos.

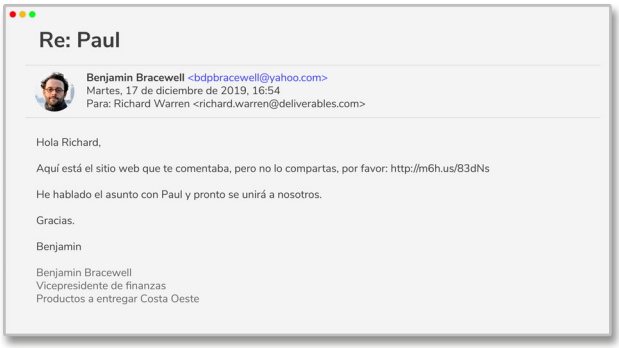


Figura 25: Captura de pantalla del correo electrónico que compartía un enlace sospechoso

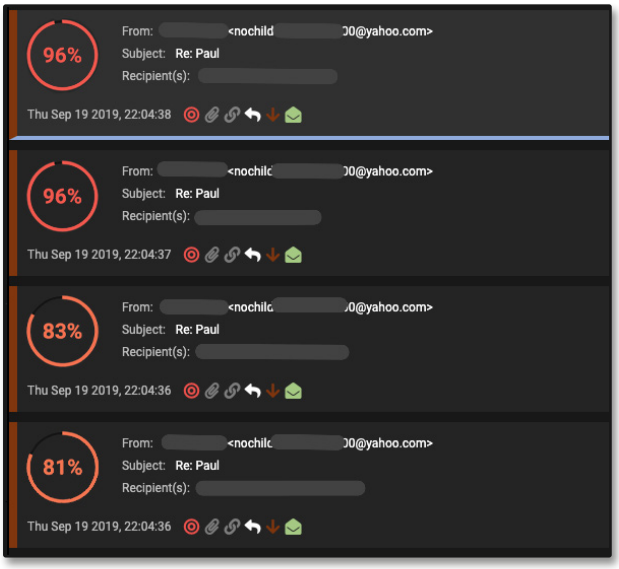
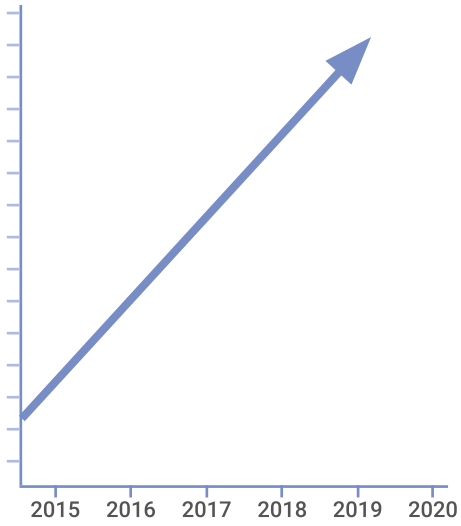


Figura 26: Cuatro de los 11 correos electrónicos, en los que se muestra la alta puntuación de anomalías y la acción asociada de Antigena Email

Ataque a credenciales de empleado

Los ataques a credenciales han aumentado un 280% entre 2016 y 2019



Los líderes empresariales raramente tienen en cuenta lo valiosa que puede ser una bandeja de entrada corporativa hasta que cae en las manos equivocadas. Sin embargo, una vez que entran en la bandeja de entrada, los ciberdelincuentes disfrutan de una gran variedad de opciones de ataque y puntos de pivote para elegir. La facilidad con la que los atacantes pueden obtener acceso –ya sea a través de campañas de phishing, intentos de ataque por fuerza bruta o intercambios en la Internet oscura– debería ser motivo de alarma.

En muchos casos, los atacantes saquearán su bandeja de entrada para hacerse con los valiosos datos que contiene. La información personal, desde los chats privados hasta los datos de facturación, puede aprovecharse para cometer fraudes o chantajes; al mismo tiempo que los antiguos hilos de correo electrónico pueden contener información altamente confidencial de la empresa. Las listas de clientes, los documentos de precios e, incluso, los planes de desarrollo y la información de las IP a menudo pueden ser descubiertos con solo unas palabras de búsqueda.

En otros casos, los delincuentes utilizarán la cuenta como punto de partida para las siguientes fases de un ataque. Pueden permanecer en silencio en segundo plano para recopilar información sobre socios o ejecutivos de gran valor, revisar documentos, leer conversaciones y aprender a mezclarse cuando inevitablemente ataquen. Igual que con los robos de cuentas de cadenas de suministro, la capacidad de leer un hilo de correo electrónico en curso y continuar con una respuesta aparentemente fiable es a menudo la forma más eficaz de realizar con éxito una misión de ataque sin levantar sospechas.

Aunque las posibilidades para los atacantes son casi infinitas, las opciones para los defensores son limitadas. Los robos de cuentas corporativas generalmente se controlan mediante defensas simples y estáticas; incluyendo las reglas de 'viaje imposible' que raramente detectan a los atacantes que saben cómo esconderse. Sin embargo, gracias a su visión de toda la empresa, la Plataforma Immune System de Darktrace complementa estos enfoques basados en reglas detectando las amenazas que consiguen pasar.

Al aprender el 'patrón de vida' normal de cada usuario, el Immune System detecta las discretas desviaciones que desenmascaran incluso a los delincuentes más cuidadosos–tanto si dichas desviaciones se manifiestan en comportamientos de inicio de sesión sospechosos como en creaciones de reglas de bandeja de entrada o modificaciones en los permisos de usuario. A medida que las ciberamenazas se desarrollen y sean cada vez más avanzadas, aprovechar la inteligencia artificial de autoaprendizaje en todo el negocio digital será la única forma viable de mantener a los delincuentes fuera de su bandeja de entrada.

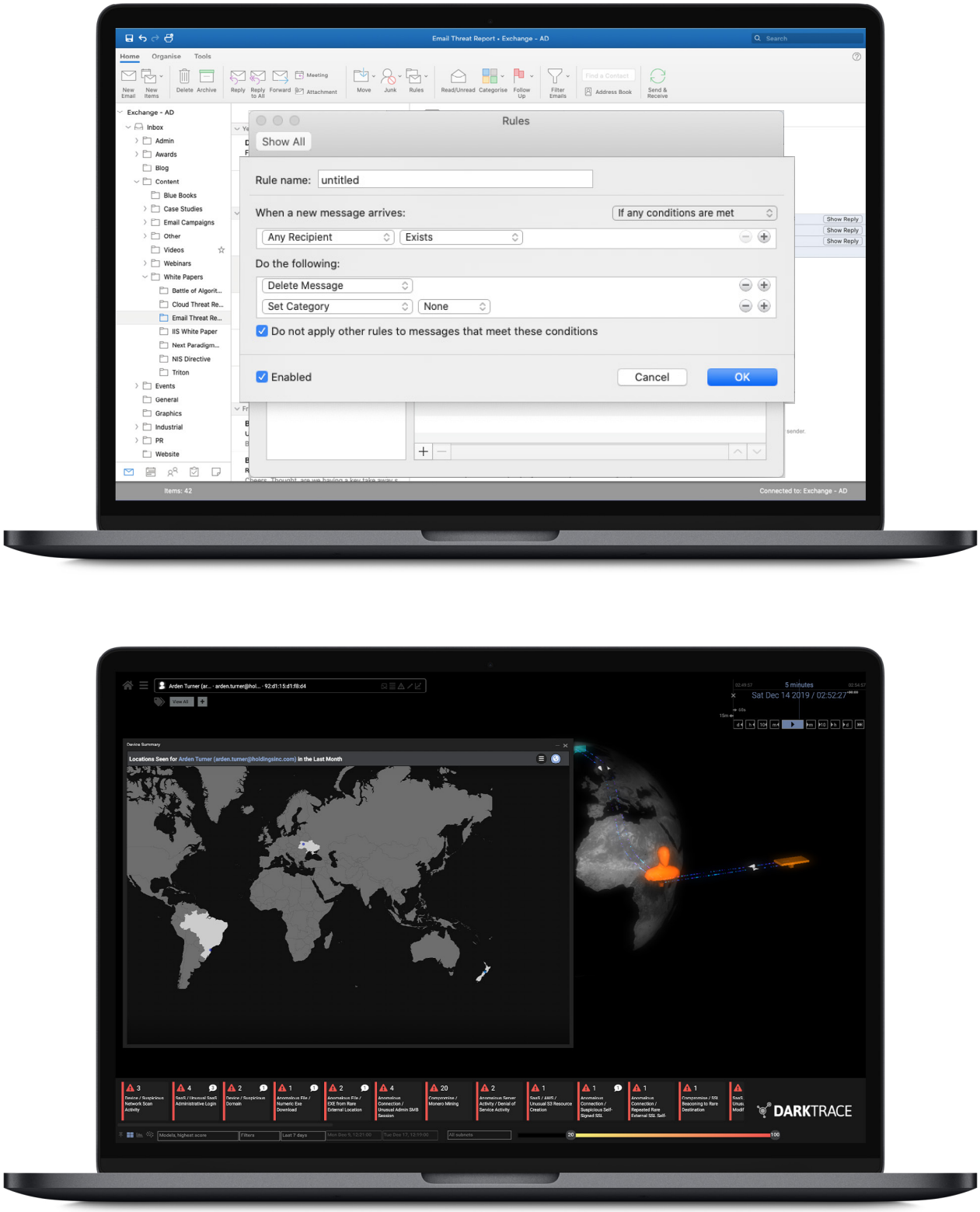


Figura 27: Una regla de procesamiento de correo electrónico que está siendo configurada en una cuenta que ha sido atacada, y el Threat Visualizer mostrando las ubicaciones geográficas de inicio de sesión.

Inicio de sesión inusual en un banco de Panamá

Se utilizó una cuenta de Office 365 en un ataque por fuerza bruta contra un conocido banco de Panamá, con inicios de sesión que procedían de un país que no coincidía con los 'patrones de vida' normales de las operaciones de la compañía.

Darktrace identificó 885 inicios de sesión durante un periodo de 7 días. Aunque la mayoría de las autenticaciones procedían de direcciones IP de Panamá, el 15% de las autenticaciones procedían de una dirección IP que era 100% extraña y estaba ubicada en la India. Un análisis más exhaustivo reveló que este punto de conexión externo estaba incluido en varias listas negras de correo no deseado y recientemente se había asociado con un comportamiento abusivo en Internet –posiblemente por piratería o detección en Internet no autorizada.

Figura 28: La interfaz de usuario que muestra las ubicaciones de inicio de sesión

Entonces, Darktrace fue testigo de lo que parecía ser un abuso de la función de restablecimiento de la contraseña, ya que se observó que el usuario de la India había cambiado los privilegios de la cuenta de una manera muy inusual. Lo que marcó la actividad como especialmente sospechosa fue el hecho de que después del restablecimiento de la contraseña, se observaron intentos de inicio de sesión fallidos desde una IP normalmente asociada con la organización, lo que sugirió que el usuario legítimo había sido bloqueado.

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Figura 29: La actividad asociada con la cuenta de SaaS, destacando las credenciales modificadas

Intento de acceso desde una zona rural de Japón

En una corporación de servicios financieros con sede en Europa, se observó que una credencial de Office 365 había iniciado sesión desde una dirección IP inusual vinculada a una zona rural de Japón.

Aunque el acceso desde ubicaciones remotas es posible en el que caso de que un usuario viaje o utilice un servicio proxy, este hecho también podría ser un claro indicador de un ataque a credenciales y acceso malicioso por parte de un usuario no autorizado. Dado que el punto de acceso era muy distinto al de las IP de acceso habituales, Darktrace lo marcó como anómalo e inmediatamente sugirió una investigación más exhaustiva.

El equipo de seguridad pudo bloquear de forma remota la cuenta de Office 365 y restablecer las credenciales, evitando así que el delincuente realizara más actividades. Si esta actividad hubiera pasado desapercibida, el ciberdelincuente podría haber utilizado sus privilegios de acceso para implementar un malware en la organización o solicitar un pago fraudulento.

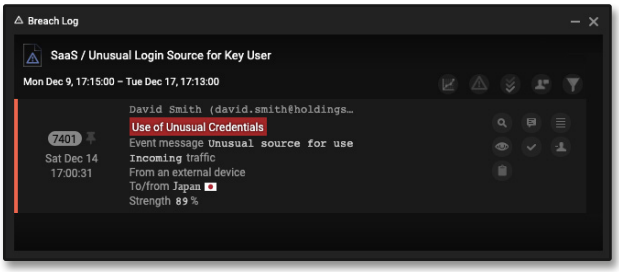


Figura 30: El inicio de sesión desde Japón incumplió varios modelos

Ataque y sabotaje a una cuenta de Office 365

En una organización internacional sin fines de lucro, Darktrace detectó un robo de cuenta en Office 365 que eludió la regla de 'viaje imposible' estático de Azure AD. Aunque la organización tenía oficinas en todos los rincones del mundo, la inteligencia artificial de autoaprendizaje de Darktrace identificó un inicio de sesión desde una dirección IP que era históricamente inusual para ese usuario y su grupo de mismo nivel e inmediatamente alertó al equipo de seguridad.

A continuación, Darktrace alertó sobre el hecho de que una nueva regla de procesamiento de correo electrónico, que eliminaba los correos electrónicos entrantes y salientes, se había configurado en la cuenta. Esto indicaba una clara señal de que se estaba produciendo un ataque y el equipo de seguridad pudo bloquear la cuenta antes de que el atacante pudiera provocar daños.

Con esta nueva regla de procesamiento de correo electrónico implementada, el atacante podría haber iniciado numerosos intercambios con otros empleados del negocio, sin que el usuario legítimo lo hubiera sabido nunca. Esta es una estrategia común utilizada por los ciberdelincuentes que buscan obtener acceso continuo y aprovechar varios puntos de apoyo en una organización, posiblemente para preparar un ataque a gran escala.

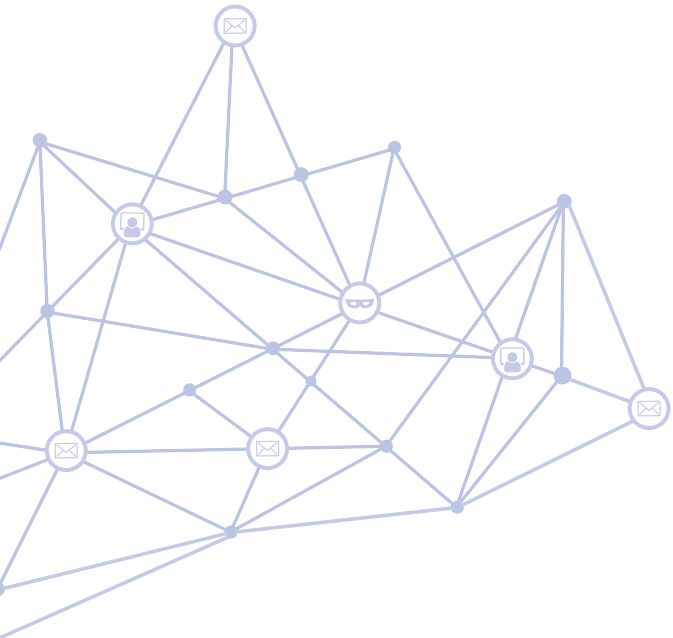
Al analizar la extraña dirección IP junto con el comportamiento distinto a la 'forma de ser' del presunto usuario, Darktrace identificó con seguridad este hecho como un caso de robo de cuenta, evitando así graves daños al negocio.

Ataque por fuerza bruta automatizado

Darktrace detectó varios eventos de inicio de sesión fallidos en una cuenta de Office 365 utilizando la misma credencial, todos los días durante una semana. Cada serie de intentos de inicio de sesión se realizó exactamente a las 18:04 h durante seis días. La coincidencia tanto de la hora del día como del número de intentos de inicio de sesión era indicativa de un ataque por fuerza bruta automatizado, que estaba programado para interrumpirse después de un cierto número de intentos fallidos para evitar bloqueos.

Darktrace consideró que este patrón de intentos fallidos era muy anómalo y alertó al equipo de seguridad. Si no fuera por Darktrace, que correlacionó varios indicadores leves y detectó las señales discretas de que se estaba produciendo una amenaza, este ataque automatizado podría haber continuado durante semanas o meses, lo que permitiría hacer averiguaciones informadas sobre las contraseñas de los usuarios basándose en la información que ya había recopilado.

Figura 31: Un gráfico que muestra los intentos repetidos de inicio de sesión



Acerca de Darktrace

Darktrace es la empresa líder mundial en ciber IA y creadora de la tecnología de Autonomous Response (Respuesta Autónoma). La IA de auto-aprendizaje se ha modelado en el sistema humano y es utilizado por más de 3.000 organizaciones para proteger contra las amenazas dirigidas hacia la nube, correo electrónico, IoT (Internet de las cosas), redes y sistemas industriales.

La empresa tiene más de 1.000 empleados y cuenta con sede en San Francisco y Cambridge, Reino Unido. Cada 3 segundos, la IA de Darktrace defiende contra una amenaza cibernética, evitando que causen daños.

Contacte con nosotros

Norteamérica: +1 (415) 229 9100

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

Latinoamérica: +55 11 97242 2011

info@darktrace.com | darktrace.com

@darktrace