DARKTRACE

Informe de amenazas para seguridad del correo electrónico

4 tendencias clave: del spear phishing al robo de credenciales

Introducción

Contents

Las plataformas de colaboración y de correo electrónico representan el tejido conectivo de cualquier empresa digital. La información se comparte, se conciben planes y se forman alianzas en la esfera digital de la correspondencia escrita. Sin embargo, como medio basado en el ser humano, el correo electrónico siempre se verá alimentado por una suposición generalizada de confianza que constituye 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, significa que el correo electrónico, más que cualquier otra área de la empresa, seguirá siendo estructuralmente resistente al espíritu moderno de 'confianza cero' y, por lo tanto, no sorprende que el 94% de las amenazas cibernéticas sigan originándose en el correo electrónico.

Para minimizar la influencia de la falibilidad humana en este área, la industria ha aceptado finalmente la idea de que hay que confiar en la tecnología para identificar mensajes maliciosos que pasan desapercibidos incluso para los empleados más exigentes y mejor formados. Sin embargo, hasta hace poco, las defensas tradicionales se han esforzado para mantenerse al ritmo de las innovaciones en el panorama de las ciberamenazas.

El spear phishing, los ataques de suplantación de identidad y el robo de cuentas en particular, siguen siendo vías útiles de ataque para los ciberdelincuentes que intentan infiltrarse en organizaciones con facilidad. Los ataques de correo electrónico dirigidos de este tipo, junto con las limitaciones de las defensas tradicionales, siguen siendo un desafío candente incluso para las organizaciones con las estrategias de seguridad por capas más completas y maduras.

Peter Firstbrook, vicepresidente analista de Gartner, ofrece un resumen certero de la dinámica del mercado: "Controles comunes, tales como la protección estándar contra correo no deseado basado en la reputación y los antivirus basados en firmas, son adecuados para ataques generalizados y campañas de estafas, pero no son una protección suficientemente buena contra ataques más dirigidos, sofisticados y avanzados. Ahora más que nunca, la seguridad del correo electrónico moderna exige innovación y un cambio de mentalidad para combatir el cambiante panorama de amenazas.

IA de Darktrace: Una plataforma de Immune System

Sin embargo, gracias a la reciente aparición de la IA a escala empresarial, este 'cambio de mentalidad' ha cristalizado finalmente en forma de un enfoque hacia la seguridad del correo electrónico basado en el 'sistema inmunológico'.

Como sugiere Firstbrook, las defensas tradicionales del correo electrónico pueden resultar adecuadas frente a amenazas sencillas e indiscriminadas, pero no se han diseñado para combatir ataques más avanzados y personalizados para destinatarios y empresas específicos.

Las bandejas de correo electrónico y controles nativos tradicionales basan la detección en reglas de codificación fija y en la comprensión de ataques históricos. Su alcance queda, por lo tanto, reducido necesariamente a amenazas ya vistas o que sean, al menos, lo suficientemente básicas como para activar una regla estática y binaria en la frontera. Pero –como muchos líderes empresariales podrán contarle señalando sus cicatrices– este no es el desafío al que nos enfrentamos.

Afortunadamente, el cambio de paradigma que se ha producido en la seguridad del correo electrónico queda fuera de una importante distinción entre el 'enfoque común' de Firstbrook y una nueva aplicación de IA de escala empresarial. Esta distinción ha sido comparada con la diferencia entre el 'tejido de protección' de una organización y su 'sistema inmunológico' de aprendizaje para las amenazas que lo atraviesan.

Mientras que su tejido de protección conoce los ataques históricos y puede detener amenazas ya conocidas, su 'sistema inmunológico' conoce 'patrones de vida' desarticulados característicos de cada empleado del flujo de trabajo digital. Crucialmente, estos 'patrones de vida' no solo se manifiestan en el tráfico de correo electrónico, sino también en el tráfico de la red y de la nube, y de un modo que puede unificarse en una imagen completa de normalidad en desarrollo para cada usuario.

Esta singular comprensión de toda la empresa permite a las organizaciones, ahora más que nunca, neutralizar ataques más dirigidos, ya que sigue siendo el único enfoque que puede proporcionar suficientes pruebas para determinar con precisión si las desviaciones sutiles en un mensaje de correo electrónico dirigido son realmente maliciosas.

Por primera vez, nuestras defensas de correo electrónico pueden preguntar si sería extraño para un usuario recibir un correo electrónico, dado que el sistema conoce los 'patrones de vida' de este empleado, de sus compañeros, y del resto de 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 a la luz de nuevas pruebas, incluso después de la entrega de un correo electrónico –independientemente de si dichas pruebas se hayan manifestado en el mensaje de correo electrónico o en conductas maliciosas que emergen en la red.

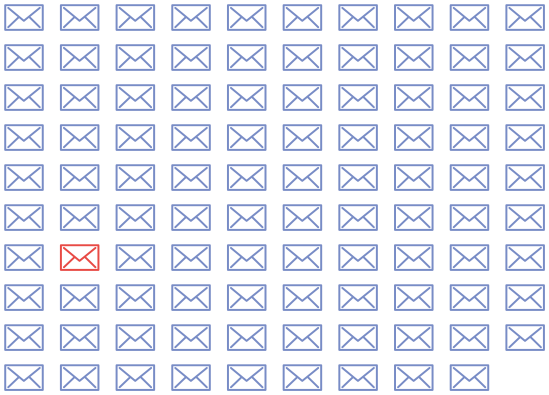
Este white paper técnico se ha diseñado para ilustrar por qué una comprensión unificada y personalizada del tráfico de la red, de la nube y del correo electrónico, representa un cambio de paradigma en el mercado de la seguridad del correo electrónico. Darktrace fue pionera en este enfoque con Antigena Email y su plataforma Enterprise Immune System. Los casos prácticos que se detallan a continuación, corresponden a unas de las cuatro categorías de ataques altamente sofisticados que suelen eludir su 'tejido de protección' pero que la IA de Darktrace neutraliza fácilmente en segundos:

- Spear phishing y entrega de cargas
- Robo de cuentas de la cadena de suministro
- Ingeniería social y solicitación
- Credenciales de empleados comprometidas

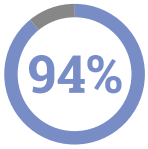
Spear phishing y entrega de cargas

> Antigena Email ha sido increíblemente valioso para atrapar amenazas gracias a su comprensión del tráfico 'normal' tanto de la red como del correo electrónico.
>
> **– Director de TI, Entegrus**

1 de cada 99 mensajes de correo electrónico es un ataque de phishing



Fuente: Avanan



del malware actual se origina en la bandeja de entrada

La mayoría de las campañas de phishing intentan engañar a los usuarios para que hagan clic en vínculos o archivos adjuntos maliciosos de un mensaje de correo electrónico con el objetivo de capturar credenciales o de implementar malware destructivo en una organización. Estos ataques puede ser lanzados bien en forma de campañas indiscriminadas contra miles de organizaciones o bien, como ataques de spear phishing diseñados a la medida de un destinatario o una empresa específica.

Para defenderse contra las campañas de phishing, las defensas tradicionales suelen analizar mensajes de correo electrónico sobre la base de su comprensión de ataques históricos, listas negras y firmas. Pero los ciberdelincuentes comprenden este enfoque reactivo mejor que nadie y aprovecharán cada incentivo para impulsar nuevas tácticas y técnicas que eludan las defensas heredadas por diseño.

Sin embargo, a pesar de que estos ataques no se han visto nunca antes y, por lo tanto, eluden las defensas tradicionales en la frontera, esto significa que en un cierto nivel de descripción serán altamente anómalos para el usuario o empresa blanco del ataque, al menos si se tienen en cuenta los 'patrones de vida' de todo el entorno digital. Esta verdad fundamental es precisamente la razón por la que resulta crítico cerrar la brecha de conocimientos de seguridad tradicionales entre la capa de correo electrónico externa y el resto de la red, tal y como ocurre en la plataforma de Immune System de Darktrace.

Con la IA de escala empresarial, Antigena Email puede analizar enlaces, archivos adjuntos, dominios, contenidos y otros elementos de un mensaje de correo electrónico junto con los 'patrones de vida' en la nube y en la red, correlacionando toda una constelación de puntos de datos que revelan que mensajes de correo electrónico aparentemente benignos son inequívocamente 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 identificar si los dominios asociados con una carga y un remitente son anormales, si la ubicación de un enlace en un mensaje de correo electrónico es extraña, si los temas de discusión y el contenido son inusuales e incluso si los patrones en la ruta del URL son sospechosos.

Este enfoque único y excepcional significa que la toma de decisiones de Darktrace es radicalmente más precisa que la de otras herramientas, de tal manera que puede emprender acciones muy proporcionadas y dirigidas para neutralizar ataques de phishing a escala.

El Immune System también está en una posición única, ya que es capaz de detectar una infección en cualquier entorno y realizar automáticamente un análisis de la raíz de problema para comprobar si se originó a través del correo electrónico. Si es así, protegerá instantáneamente al resto de empleados que son blanco del mismo ataque. Nosotros denominamos esto como 'respuestas autónoma', donde aprender del paciente cero permite la protección estratégica del resto de la empresa sin intervención humana. Desde la perspectiva de un equipo de seguridad, alguien aún necesita limpiar la computadora portátil de la primera víctima, algo mucho mejor que la limpieza de 200 o más.

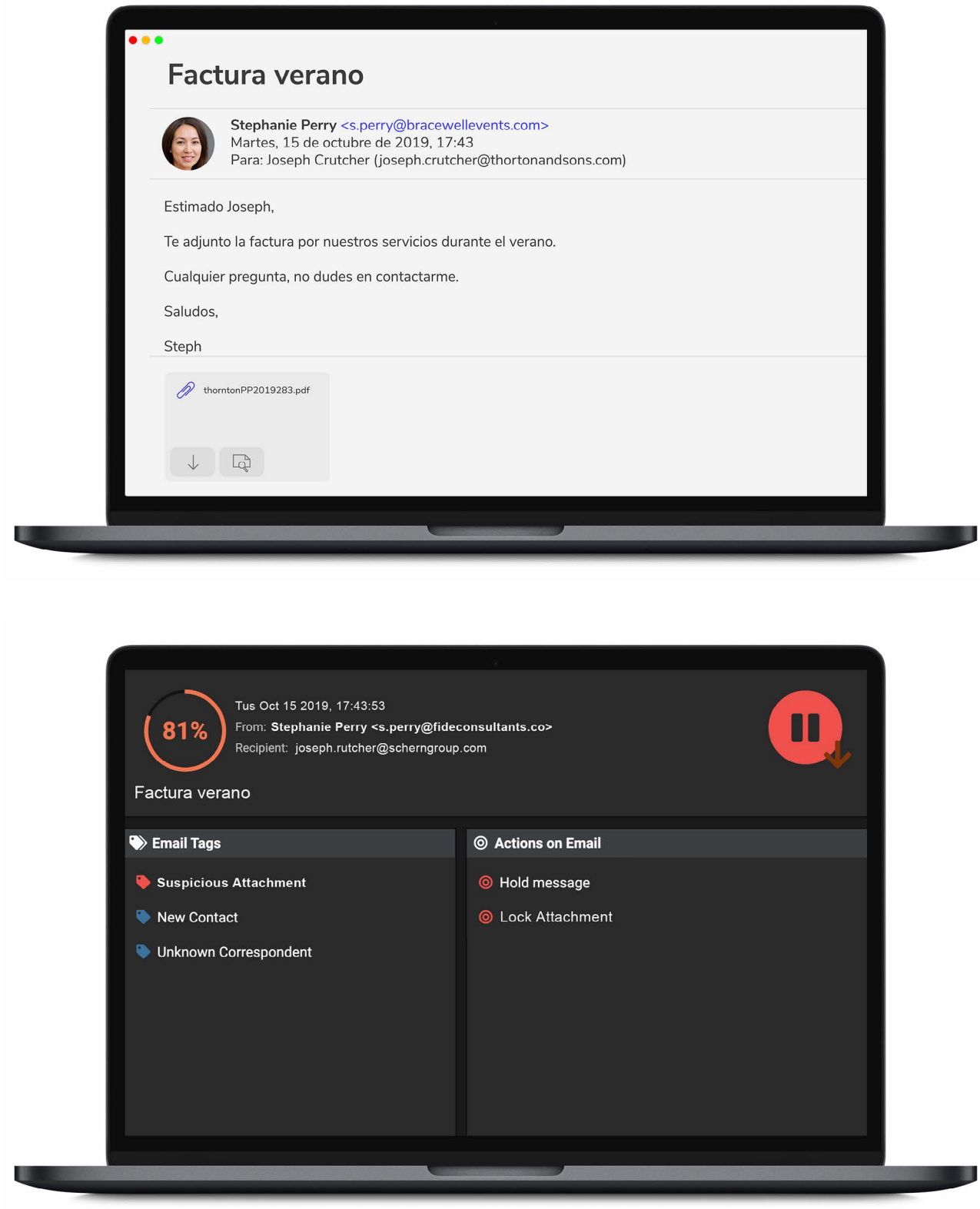


Figura 1: Un correo electrónico alentando a un empleado a hacer clic en un archivo adjunto que contiene una carga maliciosa y la vista correspondiente en la interfaz de usuario de Darktrace, mostrando las etiquetas de anomalías y las medidas adoptadas.

ESTUDIO DE CASO REAL

Ataque de WeTransfer

Darktrace detectó un ataque de phishing, dirigido a cinco destinatarios de alto perfil de una organización académica de Singapur, que se había creado con gran cuidado para convencerles de que hicieran clic en un enlace malicioso.

Antigena Email asignó a estos mensajes de correo electrónico una puntuación de anomalía del 100% y adoptó la medida de 'retenerlos', impidiendo la entrega. También identifico indicadores sutiles de un spoofing de servicios, a pesar de que la organización mantenía una relación conocida con el remitente.

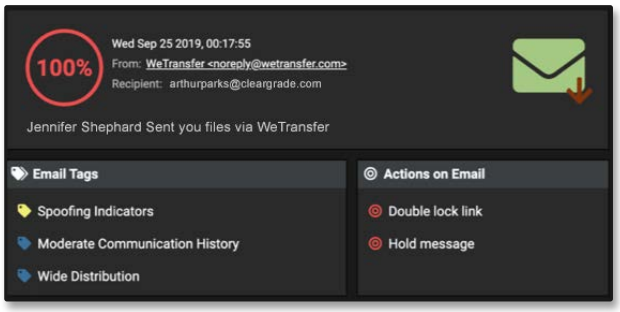


Figura 2: Interfaz de usuario donde se muestran las infracciones de modelos y las acciones

1. Los datos del encabezado no mostraban señales claras de que este mensaje de correo electrónico tuviera un origen distinto a WeTransfer, por lo que habría parecido perfectamente normal para el destinatario. Los parámetros 'Width' y 'Depth' indican que esta dirección de correo electrónico se había comunicado con muchas personas de la organización durante varios días.

Figura 3: Los datos de conexión de los mensajes de correo electrónico relevantes

2. Sin embargo, Antigena Email fue capaz de detectar una amplia gama de anomalías sutiles, dada su comprensión de lo 'normal' para el usuario y la organización, así como contexto adicional adquirido en la capa de la red.

a. En primer lugar, la 'puntuación de anomalía de la IP de la dirección' fue alta (63%). Este parámetro indica lo inusual que resulta para esta dirección de correo electrónico enviar desde esta IP teniendo en cuenta los patrones de envío históricos, algo que normalmente indica que se trata de spoofing o de una cuenta secuestrada.

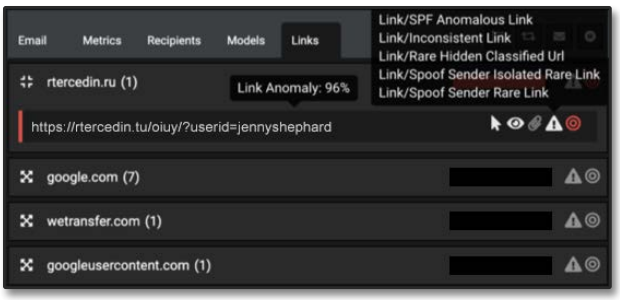


Figura 4: Desglose de los enlaces mostrados en los mensajes de correo electrónico

b. Por otra parte, como Darktrace crea constantemente modelos del comportamiento 'normal' de cada remitente externo, fue capaz de detectar una anomalía clave en el cuerpo del mensaje de correo electrónico, un vínculo que no era en absoluto coherente con lo que Darktrace había visto anteriormente en WeTransfer, lo que permitió a Antigena Email identificarlo como la carga maliciosa del mensaje de correo electrónico.

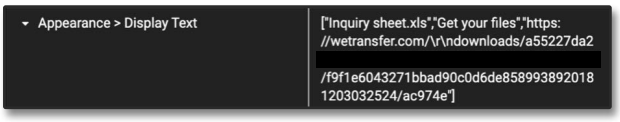


Figura 5: Antigena fue capaz de determinar dónde aparecía el enlace dentro del mensaje de correo electrónico

c. Al enlace en cuestión, se le dio una puntuación de anomalía del 96% y se ocultaba detrás de botones del estilo 'Haga clic aquí' en distintas partes del mensaje de correo electrónico, incluido un enlace falso 'https://wetransfer.com/...' (imagen de abajo) y los textos 'Inquiry Sheet.xls' y 'Get Your Files'.

Este ataque fue completamente novedoso y eludió el resto de herramientas basadas en firma que tenía la universidad. Del mismo modo, debido a que el vínculo utilizó un dominio totalmente benigno y no sugería de manera obvia una carga maliciosa, incluso la detección heurística y el sandboxing probablemente habrían fracasado.

ESTUDIO DE CASO REAL

Malware oculto en facturas falsas

Una importante firma de abogados se convirtió en uno de los principales objetivos de una campaña de phishing avanzado, que trataba de disfrazar un malware para el robo de credenciales dentro de archivos ISO adjuntos a facturas falsas. Las defensas de correo electrónico tradicionales normalmente incluyen los archivos ISO en listas blancas, mientras que los sistemas operativos montan automáticamente sus imágenes con un solo clic, aportándoles un claro atractivo a los responsables de la amenaza.

Sin embargo, cuando una veintena de mensajes de correo electrónico ilícitos atravesaron las defensas de correo electrónico tradicionales de la firma, Darktrace detectó la campaña reconociendo una amplia gama de indicadores de anomalías. Por ejemplo, uno de los modelos de IA que activaron los mensajes de correo electrónico fue 'Attachment/Unsolicited Anomalous MIME', que significa que el tipo MIME del archivo adjunto era muy inusual para el usuario y su grupo de compañeros, y que el destinatario jamás se había comunicado con el remitente para solicitar dicho archivo.

Mediante la localización exacta de la procedencia de la amenaza, Darktrace emprendió una acción quirúrgica para desarmarla, en lugar de limitarse a marcar todos los mensajes de correo electrónico potencialmente sospechosos con advertencias genéricas que probablemente serían ignoradas. Para combatir los dañinos archivos ISO, Darktrace convirtió los archivos adjuntos a PDF inofensivos y movió los mensajes de correo electrónico a la carpeta de correo no deseado. Y, lo que es más importante, tras detectar el primer mensaje de correo electrónico de la campaña, la tecnología neutralizó automáticamente otros 20 antes de que tuvieran la oportunidad de afectar a la empresa.

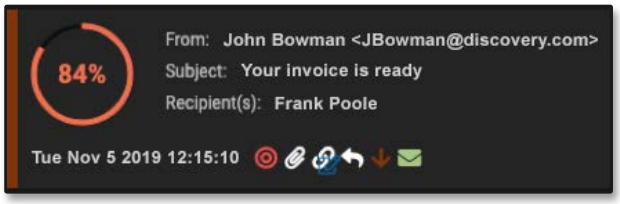


Figura 6: Encabezado de mensajes de correo electrónico maliciosos, mostrando la acción sugerida

Agenda de direcciones municipal comprometida

Un agente responsable de una amenaza consiguió hacerse con la libreta de direcciones municipal de un ayuntamiento de Estados Unidos y lanzó un ataque a los destinatarios por orden alfabético, de la A a la Z. Cada mensaje de correo electrónico había sido bien diseñado y personalizado para el destinatario, y todos los mensajes contenían una carga maliciosa oculta en un botón camuflado en forma de enlace a 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 o del resto del personal de la ciudad, había visitado ese dominio con anterioridad. El sistema también reconoció que el modo en que se habían ocultado los enlaces detrás de cada botón era muy sospechoso. Esto activó inmediatamente una alerta de confianza alta y sugirió bloquear cada enlace de manera autónoma conforme accedía a la red.

Curiosamente, el hecho de haber implementado Antigena en 'modo pasivo' pudo demostrar con evidencias claras y concretas la capacidad del sistema para frustrar ataques sutiles que habrían pasado desapercibidos para otras herramientas: mientras que Antigena detectó e intentó neutralizar la campaña en la letra 'A', las herramientas heredadas del equipo de seguridad reaccionaron a la amenaza en la letra 'R'. En el 'modo activo', Antigena habría neutralizado el ataque antes de que hubiera podido llegar a un solo usuario.

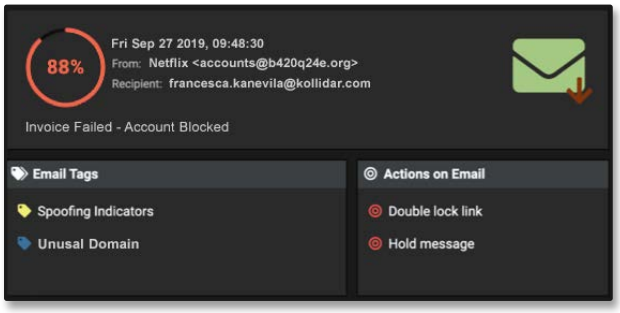
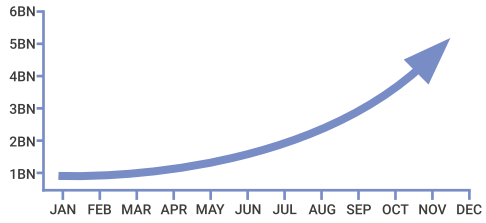


Figura 7: Antigena Email mostrando una puntuación de anomalía del 88%

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

Mediante el secuestro de la información de una cuenta de un contacto de confianza de su cadena de suministro, los responsables de cualquier amenaza pueden ganarse fácilmente la confianza de un destinatario de la red, persuadiéndole para hacer clic en un enlace malicioso o para realizar una transferencia de millones fuera de la empresa. Las defensas de correo electrónico heredadas asumen la confianza, lo que significa que los robos sofisticados de cuentas a menudo pasan completamente desapercibidos.

En los últimos años, las cuentas comprometidas han sido responsables de varios ataques de alto perfil en grandes organizaciones. Los ciberdelincuentes se aprovechan cada vez más de las cadenas de suministro –compuestas por proveedores, socios y contratistas– en sus ataques para infiltrarse en organizaciones o para establecer comunicaciones fuera de línea. A principios de este año, un informe sobre ataques conocidos como 'island hopping' –en el que los atacantes intenta expandirse a través de una brecha en cadenas de suministro– reveló que este método representa la mitad de los ataques actuales.

Los atacantes que tienen acceso total a la cuenta de correo electrónico del proveedor, pueden estudiar interacciones de correo electrónico anteriores para generar una respuesta dirigida al mensaje más reciente. El idioma que utilizan a menudo parecerá benigno, por lo que las herramientas de seguridad de correo electrónico heredadas, que buscan palabras o frases clave que indiquen un phishing, no lograrán detectar estos ataques.

Antigena Email es capaz de formular una noción completa de las palabras/frases 'normales' para cada usuario interno, por lo que, independientemente del grado de verosimilitud que pudiera tener el mensaje para la mayoría de observadores –humanos o máquinas–, puede identificar distribuciones irregulares de palabras y frases. Para el análisis de los patrones de comunicación con el contexto completo de todo el tráfico de correo electrónico y de la red, Antigena Email utiliza una serie de parámetros para identificar con seguridad casos de secuestros de cuentas, algo imposible de detectar sin poseer una comprensión detallada del comportamiento 'normal' de todo el entorno digital.

La tecnología identifica anomalías en el tema y el contenido de cada mensaje de correo electrónico y analiza esto en relación con la coherencia de la ubicación del inicio de sesión, los enlaces y archivos adjuntos, y destinatarios anteriores comunes para el remitente. Antigena Email utiliza esta comprensión multidimensional para estimar la probabilidad de que un mensaje de correo electrónico de un proveedor de confianza sea de hecho legítimo. No asume la confianza. Dependiendo de la gravedad de la amenaza, puede responder de la manera adecuada, bloqueando los enlaces y archivos adjuntos o retirando el mensaje de correo electrónico completo de la bandeja de entrada de un empleado.

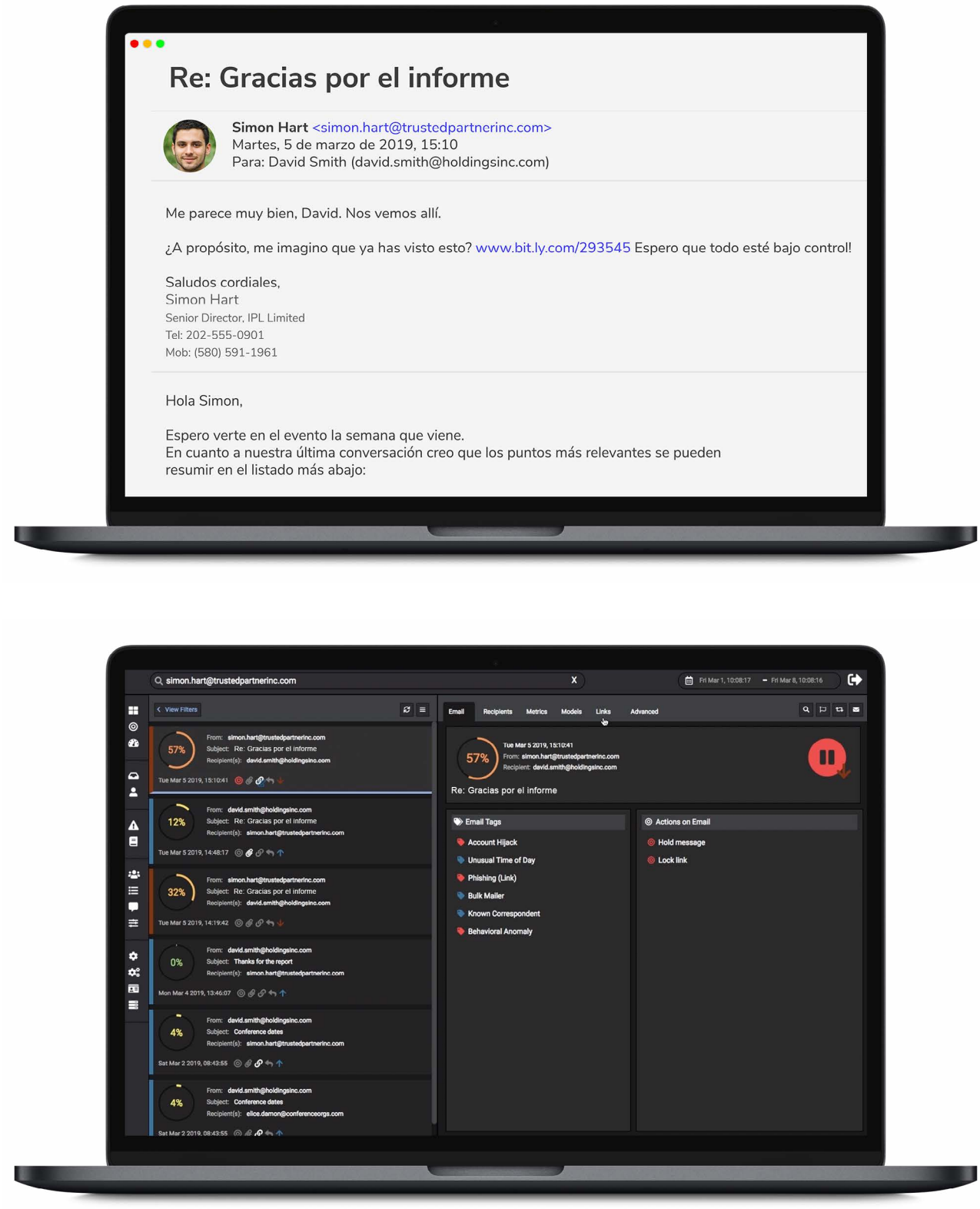


Figura 8: Una respuesta convincente enviada desde una cuenta comprometida de un proveedor de confianza siguiendo un hilo de correspondencia por correo electrónico. El enlace contenía una carga maliciosa.

ESTUDIO DE CASO REAL

Ataques consecutivos a la cadena de suministro

Un cliente que estaba probando Antigena Email experimentó dos incidentes graves en días sucesivos, en los que las cuentas de correo electrónico de proveedores de confianza se convirtieron en la fuente de una campaña maliciosa–muy probablemente después de que estas cuentas se vieran comprometidas.

Antigena Email aún no había sido configurado para emprender acciones de manera autónoma, por lo que los usuarios quedaron totalmente expuestos al contenido de los mensajes de correo electrónico. No obstante, Antigena Email advirtió en todos los casos que habría retenido los mensajes de correo electrónico y bloqueado doblemente las cargas de los enlaces, mientras que las herramientas de seguridad integradas de Microsoft no detectaron nada sospechoso y dejaron pasar todo sin emprender acciones de ningún tipo.

Incidente 1 - Consultoría

En el primer caso, Antigena Email reconoció que el remitente era bien conocido para la empresa y que distintos usuarios internos habían mantenido anteriormente correspondencia directa con ellos. De hecho, ese mismo día, más temprano, uno de estos usuarios estaba escribiéndose normalmente con la cuenta que pronto iban a secuestrar. El proveedor en cuestión era una firma de consultoría ambiental con sede en el Reino Unido.

Menos de dos horas después de este cambio de rutina, se enviaron rápidamente mensajes de correo electrónico a 39 usuarios, cada uno conteniendo un enlace de phishing. En las líneas del asunto y en los enlaces que contenían los mensaje de correo electrónico, se introdujeron variaciones que sugerían que se trataba de mensajes de correo electrónico muy dirigidos creados por un delincuente bien preparado. El objetivo de los enlaces podría haber sido solicitar pagos, contraseñas o distribuir malware.

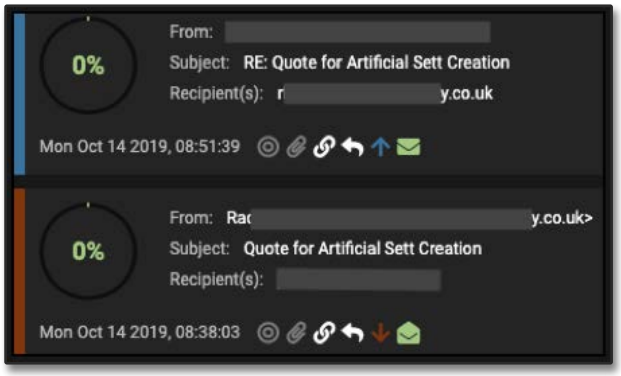


Figura 9: Correspondencia 'normal' más temprana con el remitente–con una puntuación de anomalía del 0%

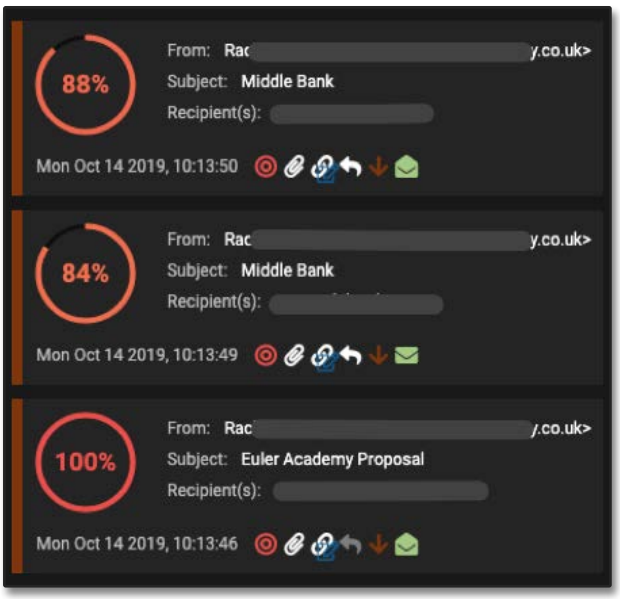


Figura 10: Mensajes de correo electrónico enviados posteriormente ese mismo que contenían archivos adjuntos maliciosos

Antigena Email identificó toda la gama de banderas rojas se asocian con el robo de cuentas de la cadena de suministro:

1. Ubicación de inicio de sesión inusual: Antigena Email determinó que los mensajes de correo electrónico habían sido enviados desde un auténtico servidor web de Outlook. Esto en sí no era inusual para el proveedor, pero a partir de los datos de esta conexión también fue posible extraer la dirección IP geolocalizable, revelando que el delincuente realizó el inicio de sesión desde una IP en Estados Unidos, en vez de hacerlo desde la ubicación usual de inicio de sesión en el Reino Unido.

2. Incoherencia de enlaces: Los enlaces de phishing contenidos en los mensajes de correo electrónico estaban todos alojados en la plataforma de desarrolladores Microsoft Azure, probablemente para eludir las comprobaciones de reputación del dominio de host. A pesar de la legitimidad ampliamente asumida de azurewebsites.net en la Web, Antigena Email fue capaz de detectar que este dominio era muy incoherente para el remitente sobre la base del historial de correspondencia anterior. El subdominio poco usual también indicaba que el nombre de host tenía una puntuación máxima de rareza en el contexto del tráfico de la red de la organización. Debido a que otros productos de seguridad para correo electrónico no aprovechan las ventajas que ofrece esta inteligencia contextual, no les habría sido posible llegar a esta conclusión.

3. Destinatarios inusuales: La puntuación de 'anomalía de asociación' del destinatario se asigna para estimar la probabilidad de que este grupo específico de destinatarios recibiera un mensaje de correo electrónico de la misma fuente. Al agregar contexto a su investigación con el paso del tiempo, Antigena Email dedujo, tan solo en el tercer mensaje de correo electrónico, que este grupo de destinatarios era 100% anómalo.

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

Figura 11: Metrics triggered by the rarity and inconsistency of the link

4. Anomalía del tema: Las líneas de asunto de estos mensajes de correo electrónico sugieren un intento de parecer profesional y mostrar un bajo perfil, por lo que habría fallado cualquier intento basado en firmas para buscar palabras clave asociadas con el phishing. Sin embargo, Antigena Email reconoció que estos destinatarios no suelen recibir mensajes de correo electrónico sobre propuestas de negocio utilizando este estilo de redacción.

Property	Value
Recipient > Metrics > Association Anomaly	100

Figura 12: Antigena Email detectó rápidamente que este grupo de destinatarios no estaba estrechamente relacionado

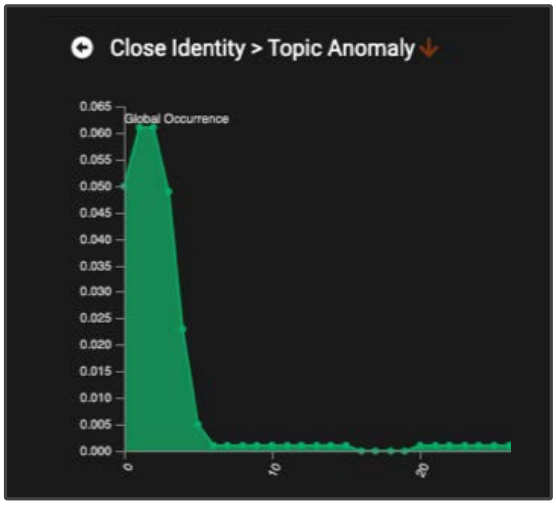


Figura 13: La vista de resumen del parámetro 'Topic Anomaly'

Incidente 2 - Proveedor de SaaS comprometido

En un segundo ataque, al día siguiente, se enviaron mensajes de correo electrónico a 55 usuarios internos a través de un proveedor de SaaS conocido por la empresa. Debido a la ausencia de acciones por parte de Microsoft, más del 50% de esos mensajes de correo electrónico fueron leídos por los destinatarios. Antigena Email advirtió de que había que retener estos mensajes de correo electrónico para impedir que llegaran a la bandeja de entrada.

1. Al igual que antes, los mensajes de correo electrónico enviados desde la cuenta comprometida contenían un enlace de phishing malicioso. En este caso, sin embargo, el enlace se mantuvo activo durante un largo periodo de tiempo, permitiendo reconstruir con precisión lo que se habrían encontrado los usuarios finales.

2. Afortunadamente, resultó sencillo encontrar a quienes interactuaron con los mensajes de correo electrónico y se recuperaron las cuentas, todo gracias a la inteligencia compartida de la plataforma de Immune System y Antigena Email de Darktrace. El Immune System también pudo detectar que los dispositivos de la red física se estaban conectando al host de phishing. Trabajando en sincronía con Antigena Email, el Immune System marcó estas interacciones con dominios de phishing sospechosos en la red.

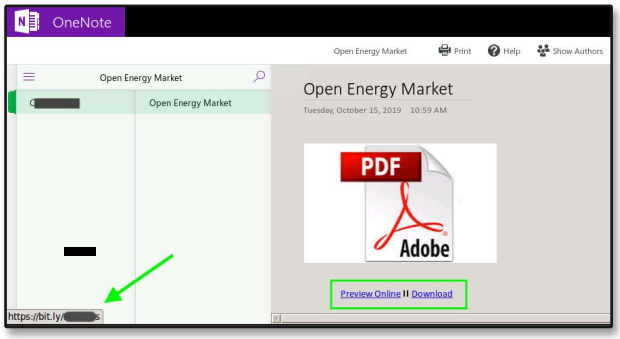


Figura 14: Captura de pantalla exponiendo un enlace oculto

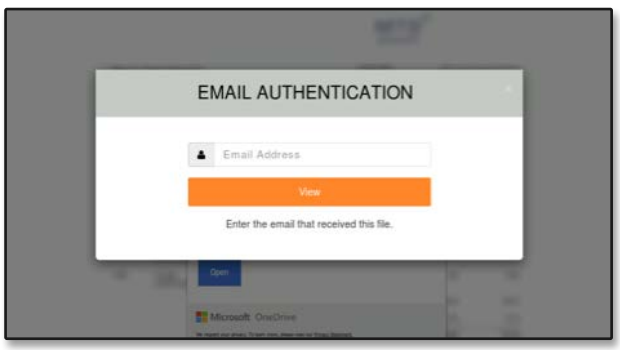


Figura 15: Esto dirigía hasta un formulario que habría capturado las credenciales del usuario

3. Aunque los enlaces estaban integrados en 'enlaces seguros' de Microsoft ATP (lo que significa que Microsoft habría realizado una comprobación en tiempo real de los enlaces cuando el usuario hubiera hecho clic en ellos), las conexiones a los puntos de conexión actuales en el tráfico de la red confirmaron que la información disponible para Microsoft en aquel momento, llevó a la conclusión de que los enlaces eran seguros, exponiendo a los usuarios al punto de conexión malicioso.

4. El propio enlace estaba alojado en la bien conocida plataforma de intercambio de archivos SharePoint. Al hacer clic en el enlace, el usuario era dirigido hasta un documento que se presentaba como un informe sobre el mercado de la energía. Sin embargo, un botón que solicitaba al usuario la descarga del archivo, le redirigía a otra página web convincente que estaba configurada para solicitar al usuario la dirección y contraseña de correo electrónico para enviarlas directamente al delincuente.

Figura 16: Los mensajes de correo electrónico del Incidente 2 tal y como aparecen en la consola de Antigena Email, incluidos los que fueron enviados como respuesta. Revela que el usuario de 'cuentas corporativas' confirmó el mensaje de correo electrónico abriendo una incidencia de soporte técnico.

ESTUDIO DE CASO REAL

Archivo malicioso oculto en una página de OneDrive

Un agente responsable de una amenaza avanzada secuestró la cuenta de correo electrónico de un proveedor de un gran grupo hotelero, usando la cuenta de confianza para enviar una carga maliciosa a la organización. Aunque el ataque logró eludir las defensas heredadas de la empresa, Antigena Email neutralizó la amenaza en cuestión de segundos.

1. El análisis de un mensaje de correo electrónico anterior revela que Antigena Email comprendió que existía una relación entre los dos remitentes.

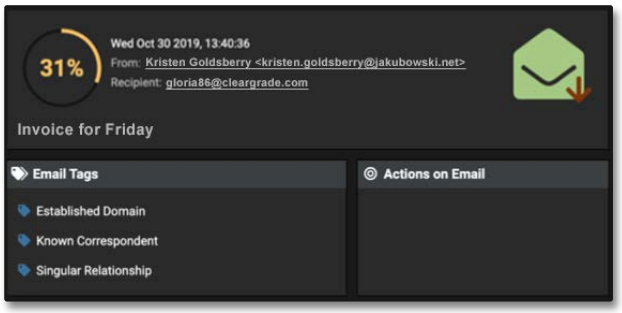


Figura 17: Un ejemplo de una comunicación anterior

2. Posteriormente, se marcó un correo electrónico como muy anómalo en comparación con los patrones de comunicación anteriores del remitente.

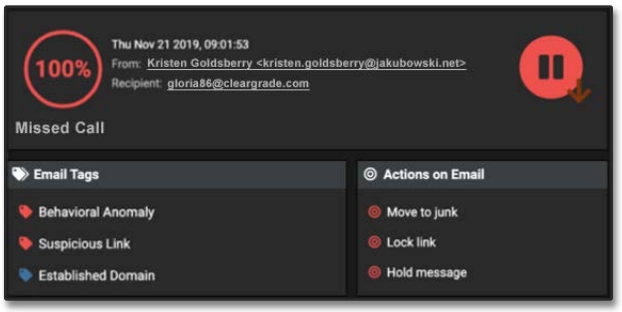


Figura 18: Un mensaje de correo electrónico posterior marcado y tres violaciones de modelos asociadas

3. Como podemos ver, estos mensajes de correo electrónico se marcaban con el modelo 'Behavioral Anomaly', por lo que Antigena Email decidió que la mejor acción a emprender era retener estos mensajes e impedir que llegaran a los destinatarios a los que iban destinados.

4. Antigena Email identificó múltiples desviaciones del 'patrón de vida' normal del remitente externo, incluidos 'país de la fuente anómalo' y 'dirección IP de la fuente anómala'.

5. El enlace malicioso del correo electrónico también era muy incoherente con los 'patrones de vida' de la empresa en el tráfico de correo electrónico y de la red, por lo que fue bloqueado por Antigena Email.

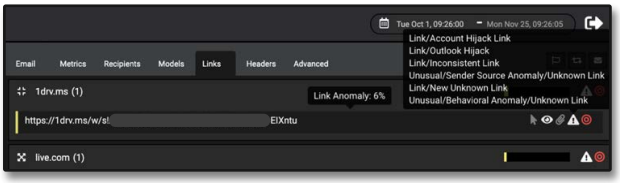


Figura 19: El enlace malicioso identificado

6. El propio enlace estaba oculto detrás del texto de pantalla 'Retrieve Message' y dirigía hacia una página de OneDrive. El uso de dominios de almacenamiento de archivos para alojar contenido malicioso es difícil de detectar aplicando un enfoque tradicional, ya que resulta imposible incluir servicios como SharePoint en listas negras, por lo que decidir si un enlace como este es malicioso o benigno, requiere comprender el correo electrónico en el contexto más amplio de la organización.

Ingeniería social y solicitación

> Tenemos Antigena Email así como de otras herramientas de seguridad heredadas. Estábamos asombrados por las cosas que las herramientas tradicionales no detectaban y que Antigena Email sí lo hacía.
>
> **– CTO, Bunim Murray Productions**

de los ataques en las bandejas de entrada de los usuarios no contenían malware

Los ataques de ingeniería social y solicitación generalmente implican un intento de suplantación de identidad sofisticado, en los que los delincuentes encubiertos solicitan con urgencia una respuesta, la desconexión de las comunicaciones o la realización de una transacción fuera de línea. Sus objetivos van desde el fraude electrónico al espionaje corporativo e incluso el robo de IP. Mientras que las organizaciones deberían invertir, sin duda, en la capacitación y educación en seguridad de sus empleados para buscar señales de advertencia, esto no garantiza per se una inmunidad total contra estos ataques cada vez más sofisticados.

Mientras que las campañas de phishing tradicionales generalmente incluyen una carga maliciosa oculta detrás de un enlace o archivo adjunto, los intentos de ingeniería social a menudo implican el envío de 'mensajes de correo electrónico limpios' que solo contienen texto. Estos ataques eluden fácilmente las herramientas de seguridad heredadas que se basan en la correlación de enlaces y archivos adjuntos con listas negras y firmas. Además, este vector de ataque generalmente implica registrar nuevos dominios 'semejantes' que no solo engañan al destinatario, sino que además eluden las defensas tradicionales.

Antigena Email posee una comprensión unificada de los 'normal' a través del todo el tráfico de correo electrónico y de la red, que evoluciona con la empresa, lo que le permite detectar casos sutiles de solicitación. Los mensajes de correo electrónico limpios que eluden las defensas tradicionales pueden identificarse en segundos sobre la base de una enorme gama de parámetros, incluidas similitudes sospechosas para usuarios conocidos, asociaciones anormales entre destinatarios internos e incluso anomalías en el contenido y el asunto.

En la mayoría de los casos, los ataques de ingeniería social tienen por objetivo llevar inmediatamente la conversación fuera de línea, lo que significa que unas medidas de seguridad lentas y reactivas tienden a intervenir solo cuando el daño está hecho. La poderosa comprensión de cada usuario, dispositivo y relación en la organización que posee Antigena Email, le permite responder de manera proactiva y con un alto grado de confianza la primera vez, interviniendo en esta etapa crucial y temprana.

Antigena también es único en su capacidad para adaptar respuestas de forma inteligente a tipos de amenazas específicas. Comprende que el elemento 'peligroso' del ataque de solicitación a menudo será el propio contenido del mensaje de correo electrónico y, por lo tanto, el sistema impedirá la entrega antes de que el destinatario tenga incluso la oportunidad de cumplir la petición urgente del delincuente.

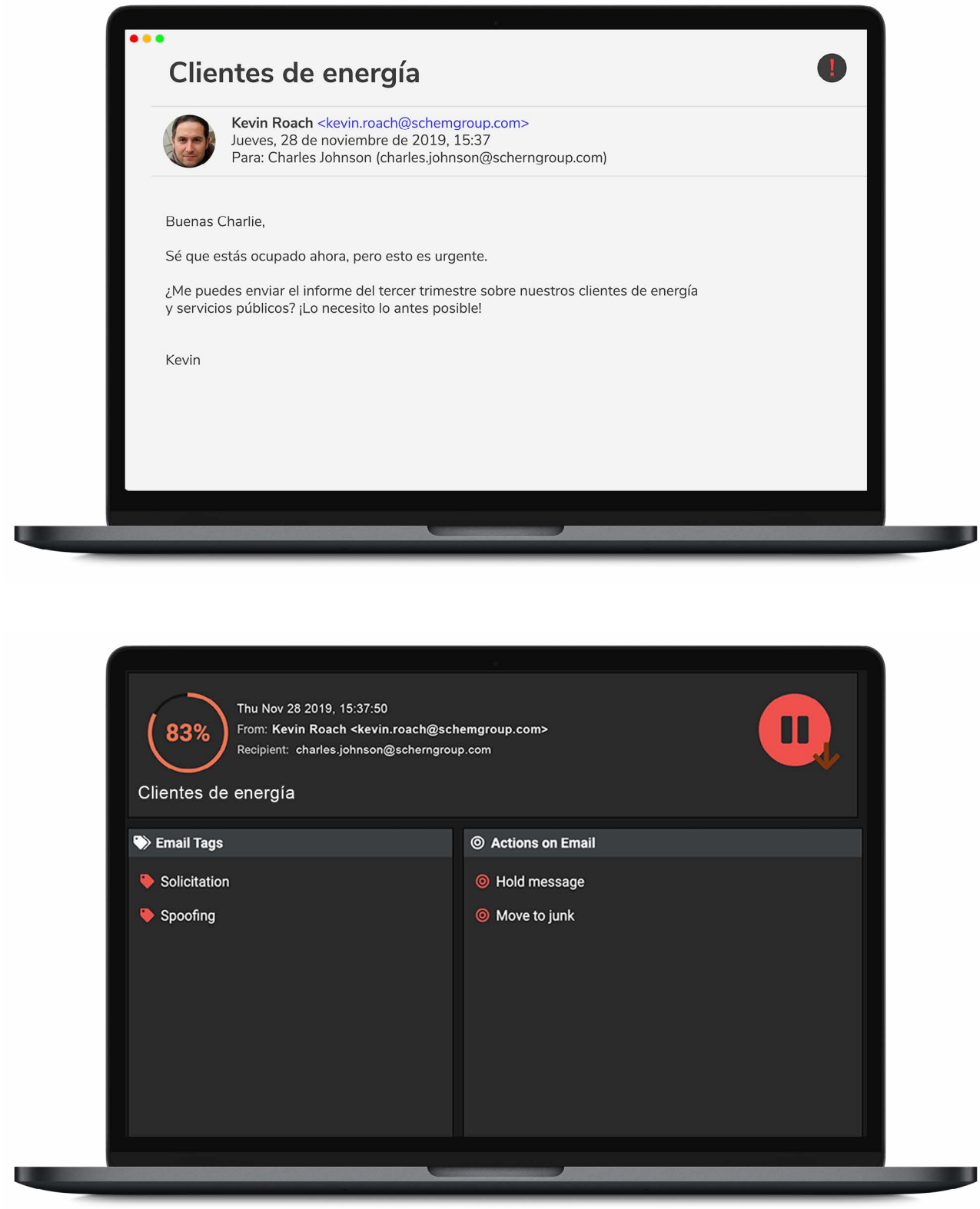


Figura 20: Un delincuente haciéndose pasar por un ejecutivo, tratando de hacerse con documentos confidenciales. Observar la dirección de correo electrónico falsa.

ESTUDIO DE CASO REAL

Ataque de suplantación de identidad

Antigena Email detectó un ataque dirigido contra 30 empleados de una empresa tecnológica multinacional. Estaba claro que se había realizado una extensa investigación de cada usuario blanco del ataque, ya que el delincuente había suplantado cuidadosamente la identidad de un ejecutivo de nivel C con el que tenían más probabilidades de comunicarse. Antigena Email identificó el ataque de ingeniería social y, como resultado, retuvo los mensajes de correo electrónico impidiendo que llegaran a sus destinatarios.

1. La línea de asunto de cada mensaje de correo electrónico incluía el nombre del empleado objeto del ataque y provenía de una dirección de Gmail que aparentemente no estaba relacionada. Aún así, a pesar de la falta de una carga maliciosa (como enlaces o archivos adjuntos), Antigena Email fue capaz de identificar los mensajes de correo electrónico como maliciosos.

2. Darktrace no solo identificó los intentos de suplantación de identidad, mediante el reconocimiento del nombre de dominio que era similar, sino que además detectó que los mensajes de correo electrónico habían infringido el modelo 'No Association', indicando que en toda su comprensión del entorno de correo electrónico y de la red de la empresa, no había visto ningún indicio de relación entre este remitente y la organización.

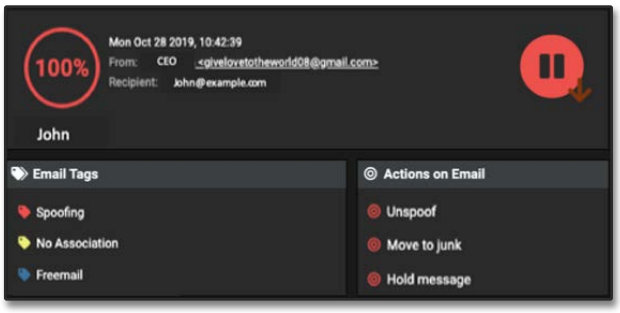


Figura 21: Uno de los 30 mensajes de correo electrónico con una puntuación de anomalía del 100%

3. Mediante la correlación de múltiples indicadores débiles, Antigena reconoció estos mensajes de correo electrónico como componentes de un ataque coordinado y los retuvo en un búfer para que los revisara el equipo de seguridad de la organización.

4. Antigena Email no solo identificó a los tres ejecutivos de nivel C cuya identidad estaba siendo suplantada, sino que también detectó que el delincuente estaba utilizando una falsificación de la dirección personal externa legítima de su CEO.

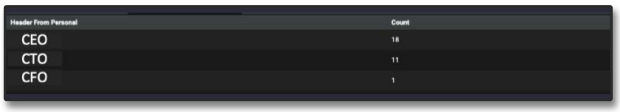


Figura 22: Tres ejecutivos de nivel C identificados

5. Además, la puntuación de exposición de los usuarios cuya identidad fue suplantada era alta, indicando que eran objetivos de alto perfil y, por lo tanto, incumplían el modelo 'Whale Spoof'. Comprender que usuarios clave internos había sido objeto de un ataque, permitió a la IA de Darktrace priorizar este ataque, iniciando una respuesta proporcionada en tiempo real.

ESTUDIO DE CASO REAL

Solicitud de la nómina del CEO

En un distribuidor de electricidad, la IA de Darktrace detectó un intento de spoofing convincente en una cuenta de correo electrónico de Microsoft 365. El mensaje de correo electrónico, supuestamente del CEO de la empresa, fue enviado a un miembro del departamento de nóminas solicitando que el empleado actualizara la información del depósito directo del CEO.

Como el mensaje de correo electrónico imitaba correctamente el estilo típico de escritura del CEO, podría haber cumplido su función correctamente y con facilidad si la IA de Darktrace no hubiera analizado el flujo de correos electrónicos de la firma en relación con el resto de la empresa.

1. Al aprender el 'patrón de vida' normal del empleado, el CEO y el resto de la organización a través de la nube y del tráfico de la red, Darktrace fue capaz de detectar inmediatamente varias anomalías sutiles en el mensaje de correo electrónico, incluida la dirección falsificada del remitente.

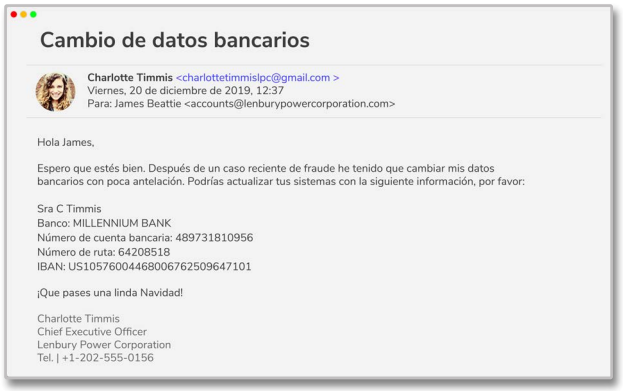


Figura 23: Captura de pantalla de un mensaje de correo electrónico suplantando la identidad del CEO

2. Entre otros indicadores débiles, la IA de Darktrace determinó automáticamente la proximidad anómala del dominio en relación con la de los empleados internos y contactos de confianza.

3. La IA respondió inmediatamente, bloqueando los enlaces del mensaje de correo electrónico y marcándolo claramente como falso, antes de que pudiera llegar al departamento de nóminas. La profunda comprensión de Darktrace del tráfico de la nube y de la red, le permitió neutralizar una amenaza muy grave que habría pasado desapercibida para herramientas basadas en firmas.

ESTUDIO DE CASO REAL

Ataque de spoofing al vicepresidente financiero

Este incidente supuso la suplantación de la identidad de un vicepresidente financiero de una entidad financiera muy conocida. Los agentes responsables de la amenaza enviaron 11 mensajes de correo electrónico similares a la empresa, pero Antigena Email reaccionó, reteniéndolos todos sobre la base de su comprensión de lo que es 'normal' en el tráfico de la red, la nube y el correo electrónico. Analizando la dirección de correo electrónico inconexa y claramente anómala en relación con el contenido de los mensajes de correo electrónico, Darktrace reconoció este intento de spoofing, mientras que la pasarela heredada de la empresa permitió el paso de los 11 mensajes de correo electrónico.

Figura 24: Captura de pantalla de un mensaje de correo electrónico compartiendo un enlace sospechoso

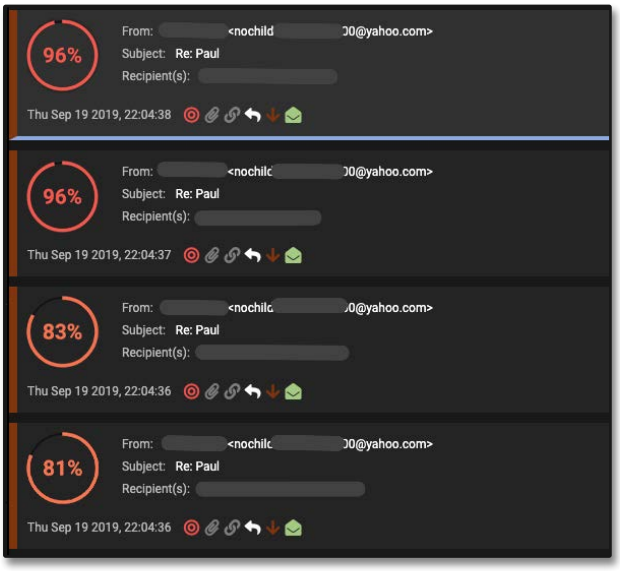
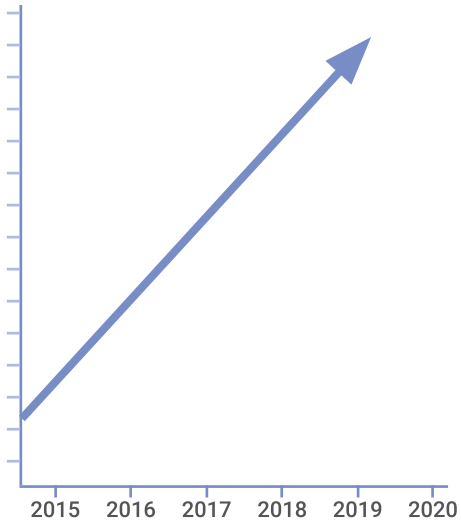


Figura 25: Cuatro de los 11 mensajes de correo electrónico mostrando la alta puntuación de anomalía y la acción asociada de Antigena Email

Credenciales de empleados comprometidas

El problema de las credenciales comprometidas ha aumentado un 280% entre 2016 y 2019



Los líderes empresariales raramente consideran el gran valor que posee la bandeja de entrada corporativa hasta que cae en las manos equivocadas. Pero una vez dentro, los agentes responsables de la amenaza disfrutan de una amplia gama de opciones de ataque y puntos de apoyo entre los que elegir. La facilidad con la que los atacantes pueden obtener acceso –ya sea a través de campañas de phishing, intentos de fuerza bruta o intercambios en la Dark Web– debería ser causa de alarma.

En muchos casos, los delincuentes saquearán los valiosos datos que contiene su bandeja de entrada. La información personal de chats privados o los detalles de facturación, pueden ser aprovechados para cometer fraude o chantaje, mientras 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 guías e información de la IP están a menudo a sólo algunos términos de búsqueda de ser descubiertos.

En otros casos, los delincuentes utilizan la cuenta como un punto de partida para las siguientes etapas de un ataque. Es posible que se encuentren trabajando silenciosamente en segundo plano reuniendo información sobre ejecutivos o socios de alto valor, revisando documentos, leyendo conversaciones y aprendiendo cómo integrarse cuando inevitablemente lancen su ataque. Al igual que ocurre con el robo de cuentas de la cadena de suministro, la posibilidad de leer un hilo de mensajes de correo electrónico activo y realizar un seguimiento con una respuesta creíble, constituye a menudo el modo más eficaz para llevar a cabo una misión de ataque sin despertar sospechas.

Aunque las posibilidades para los delincuentes son prácticamente infinitas, las opciones para los defensores son limitadas. Los robos de cuentas corporativas suelen monitorizarse mediante sencillas defensas estáticas, incluidas reglas de 'viaje imposible' que rara vez atrapan a los delincuentes que saben cómo ocultarse. Sin embargo, gracias a la vista que posee de toda la empresa, la plataforma de Immune System de Darktrace complementa estos enfoques basados en reglas detectando las amenazas que eluden estas defensas.

Mediante el aprendizaje del 'patrón de vida' normal de cada usuario, el Immune System detecta desviaciones sutiles que desenmascaran incluso a los delincuentes más cuidadosos

–independientemente de si estas desviaciones se manifiestan en comportamientos de inicio de sesión sospechosos, creaciones de reglas para la bandeja de entrada o ediciones de los permisos de usuario. Conforme se desarrollan las ciberamenazas y se vuelven más avanzadas, aprovechar la IA con capacidad de autoaprendizaje en toda la empresa digital, será la única solución viable para mantener a los delincuentes fuera de su bandeja de entrada.

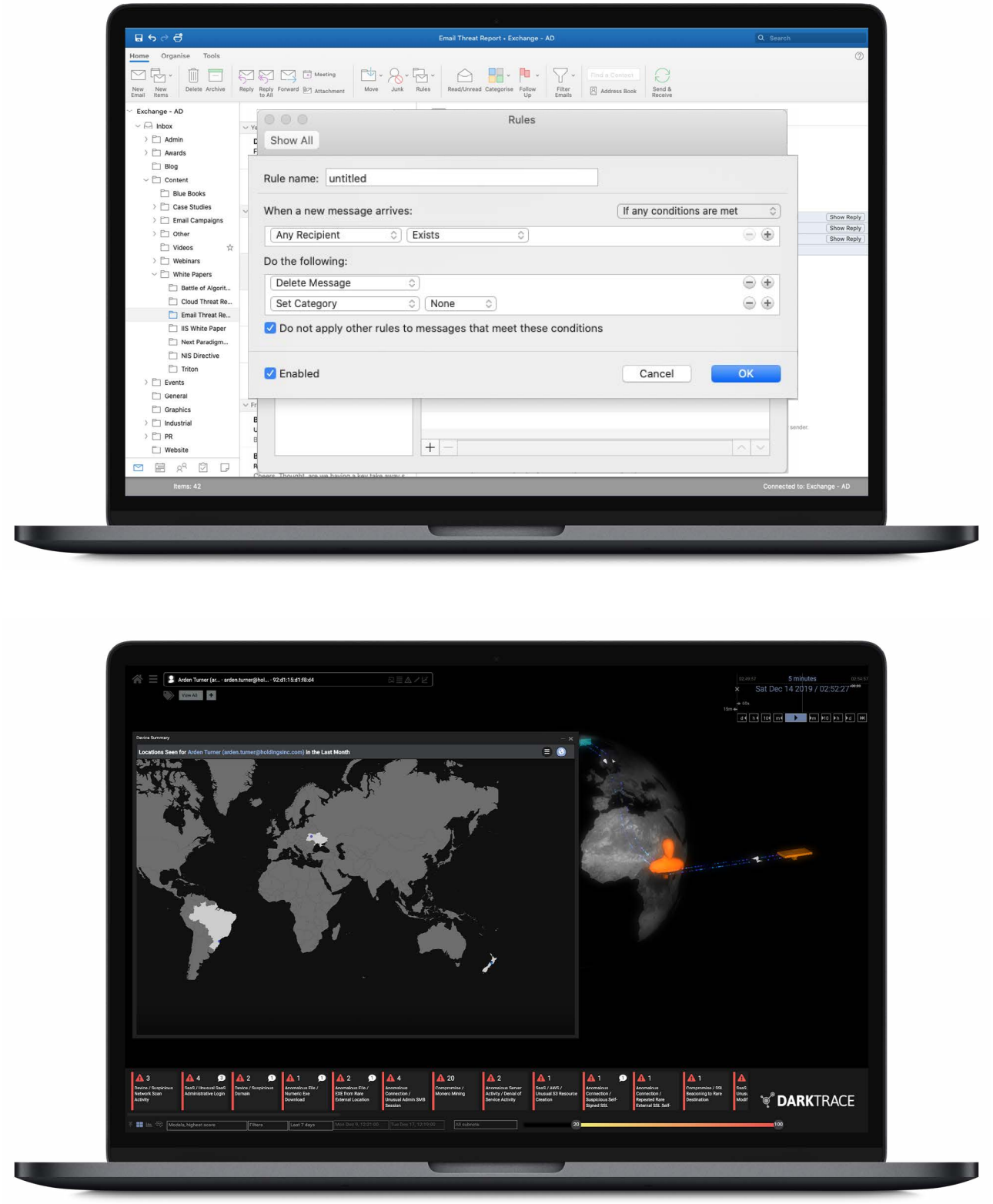


Figura 26: Configuración de una regla de procesamiento de correo electrónico en una cuenta comprometida y Threat Visualizer mostrando las ubicaciones geográficas de inicio de sesión.

ESTUDIO DE CASO REAL

Compromiso de Microsoft 365 y Microsoft Teams

Recientemente, una cuenta de Microsoft 365 se vio comprometida en una empresa de contabilidad pública con sede en Estados Unidos. Darktrace detectó inicialmente varias anomalías, incluido un repentino aumento del tráfico de correo electrónico saliente, así como la inusual ubicación de inicio de sesión —mientras que la empresa y casi todos sus usuarios estaban ubicados en Wisconsin, se utilizó una dirección IP ubicada en Kansas para iniciar sesión en la cuenta de Microsoft 365. Además del inicio de sesión inusual, se detectó un inicio de sesión en Microsoft Teams desde la misma dirección IP de Kansas.

Figura 27: Justo después de crearse la nueva regla de correo electrónico, se produjo un inicio de sesión en Microsoft Teams desde una IP que era 100% rara

Las reglas de 'viaje imposible' por sí solas habrían pasado por alto estas anomalías, pero la comprensión de la actividad y el comportamiento de las diferentes aplicaciones de SaaS permitió que la IA de Darktrace reconociera estos eventos como un caso sistemático de robo de credenciales. Cuando posteriormente el agente responsable de la amenaza creó una nueva regla de correo electrónico, Darktrace pudo relacionar este evento con los otros comportamientos anómalos y comprender su naturaleza potencialmente maliciosa.

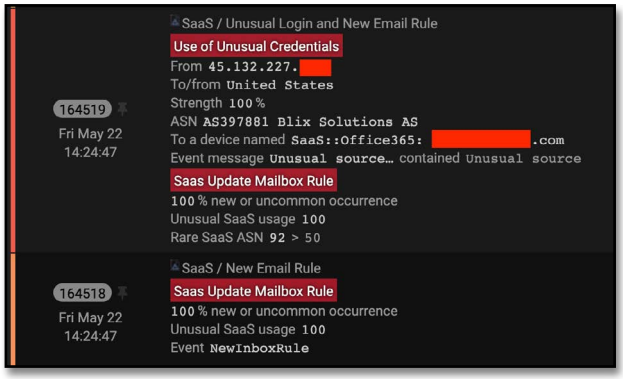


Figura 28: El módulo de SaaS de Darktrace detectó un inicio de sesión en la cuenta de Microsoft 365 del usuario desde una IP que era 100% rara y la creación de nuevas reglas para el buzón de correo electrónico. Todos los factores indicaban una actividad de SaaS 100% inusual

Cinco minutos después, Antigena Email alertó sobre un gran número de mensajes de correo electrónico salientes que contenían una línea de asunto genérica y un archivo PDF adjunto. La tecnología también detectó un pico claro en el número de mensajes de correo electrónico salientes de este usuario y marcó cada uno ellos con la etiqueta 'Out of Character' que, en este caso, indicaba un cambio en el comportamiento normal con el aumento de destinatarios, así como un probable compromiso interno.

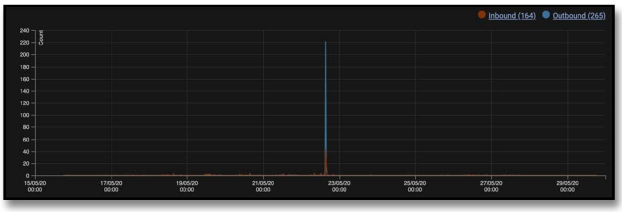


Figura 29: Antigena Email detectó un aumento en los destinatarios que indicaba una violación grave en el comportamiento normal de este usuario

El inusual comportamiento de inicio de sesión detectado por el módulo de SaaS de Darktrace podría estar relacionado con el comportamiento anómalo de los mensajes de correo electrónico salientes marcados por Antigena Email, lo que permitió al equipo de seguridad conocer el alcance del ataque y neutralizarlo a medida que se desarrollaba. Quedaba claro que la cuenta se estaba utilizando para llevar a cabo actividades maliciosas, ya que cada uno de los 220 mensajes de correo electrónico salientes utilizaba una línea de asunto genérica y contenía un archivo adjunto sospechoso. Por lo tanto, el equipo de seguridad inhabilitó inmediatamente la cuenta comprometida.

Figura 30: Una recreación del mensaje de correo electrónico enviado por el atacante con el archivo adjunto malicioso

ESTUDIO DE CASO REAL

‘Cambio de datos bancarios’ enviado desde el departamento de contabilidad

Cuando la cuenta de Microsoft 365 de un departamento de contabilidad se vio comprometida y se utilizó para enviar mensajes de correo electrónico de phishing dirigidos, Darktrace pudo realizar un seguimiento del movimiento del atacante dentro de la bandeja de entrada, relacionando la información del módulo de SaaS de Darktrace con las alertas de Antigena Email para tener una imagen completa de la amenaza y detener el ataque.

Parece que la cuenta de SaaS se había visto comprometida a través de un ataque de spear phishing entrante o bien, había sufrido alguna otra forma de ataque antes de que Darktrace comenzara a supervisar la organización. A pesar de que la ciber IA de Darktrace no había supervisado el problema inicial, pudo distinguir el comportamiento posterior del atacante como malicioso basándose en su comprensión activa en constante evolución de la organización y de su fuerza de trabajo.

Cuando el usuario de la cuenta inició sesión desde una dirección IP francesa 100% rara, el módulo de SaaS de Darktrace detectó inmediatamente la anomalía así como una serie de actividades llevadas a cabo después del inicio de sesión inusual. Al mismo tiempo, Antigena Email detectó el envío de un mensaje de correo electrónico.

Figura 31: Se detectó un inicio de sesión desde una IP 100% rara para este usuario y cuenta de SaaS

Además, Darktrace identificó más actividad adicional desde una segunda ubicación de inicio de sesión rara, una dirección IP suiza. Cuando se inició sesión en la cuenta desde esta IP, se produjo muy poca actividad de correo electrónico. En su lugar, la ciber IA detectó que el agente responsable de la amenaza usaba su acceso de SaaS ilegítimo para acceder a información sobre el usuario legítimo de la cuenta y a archivos relacionados con bancos, facturas y pagos.

A continuación, Antigena Email identificó una serie de comunicaciones por correo electrónico que, al verlos en el contexto de la cuenta de SaaS comprometida, señalaban una clara amenaza. Los mensajes de correo electrónico no contenían archivos adjuntos ni enlaces maliciosos evidentes. Sin embargo, el asunto de la respuesta final del destinatario era ‘Cambio de detalles bancarios’, lo que sugería sin duda alguna que el agente malicioso había enviado correos electrónicos indicando al destinatario que cambiara la información de pago para enviar dinero al atacante en lugar de a la empresa.

Parece que los atacantes revisaron archivos bancarios y de facturación para encontrar un cliente con una gran factura a pagar, y después utilizaron la cuenta de correo electrónico comprometida para lanzar un ataque de phishing saliente, cambiando los detalles de facturación. Gracias a que la IA de Darktrace correlacionó información dentro de la plataforma de SaaS, sumado a la información proporcionada por Antigena Email, este ataque de phishing dirigido pudo ser detenida impidiendo que causara daños y comprometiera otras cuentas.

En la siguiente captura de pantalla también se indica una serie de reglas de procesamiento de la bandeja de entrada configuradas en la cuenta comprometida, mostrando acciones típicas del robo cuentas.

Figura 32: Registros de Darktrace de las nuevas reglas de la bandeja de entrada configuradas en la cuenta de SaaS comprometida

ESTUDIO DE CASO REAL

Inicio de sesión inusual en un banco panameño

En un ataque de fuerza bruta contra un conocido banco de Panamá, se utilizó una cuenta de Microsoft 365 con inicios de sesión que se originaban en un país que se apartaba de los 'patrones de vida' normales de las operaciones de la empresa.

Darktrace identificó 885 inicios de sesión en un periodo de 7 días. Mientras que la mayoría de las autenticaciones tenían su origen en direcciones IP de Panamá, el 15% de las autenticaciones se originaban en una dirección IP que era 100% rara y se encontraba en la India. Un análisis más detallado reveló que este punto de conexión externo estaba incluido en varias listas negras de spam y que recientemente se había asociado con un comportamiento abusivo en línea –posiblemente análisis no autorizados de Internet o piratería.

Figura 33: La interfaz de usuario mostrando las ubicaciones de inicio de sesión

Darktrace también detectó lo que parecía ser un abuso de la función de restablecimiento de contraseña, ya que se observó que el usuario de la India cambiaba los privilegios de la cuenta de una manera muy inusual. Lo que señaló esta actividad como especialmente sospechosa fue que tras el restablecimiento de la contraseña, se observaron inicios de sesión fallidos desde una IP asociada normalmente con la organización, lo que sugería que el usuario legítimo estaba 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 34: La actividad asociada con la cuenta de SaaS, destacando las credenciales modificadas

ESTUDIO DE CASO REAL

Intento de acceso desde una zona rural de Japón

En una corporación de servicios financieros con sede en Europa, se observó que se utilizaban credenciales para el inicio de sesión en Microsoft 365 desde una dirección IP inusual vinculada con una localidad de una zona rural de Japón.

Aunque es posible acceder desde ubicaciones remotas cuando un usuario viaja o utiliza un servicio proxy, también podría ser un claro indicador de credenciales comprometidas y acceso malicioso por parte de un usuario no autorizado. Dado que el punto de acceso era sustancialmente diferente al de las IP que solían acceder, Darktrace marcó esto como una anomalía y sugirió realizar inmediatamente una investigación detallada.

El equipo de seguridad fue capaz de bloquear de forma remota la cuenta de Microsoft 365 y restablecer las credenciales, impidiendo así más actividad por parte del agente malicioso. Si esta actividad hubiera pasado desapercibida, el agente responsable de la amenaza podría haber usado sus privilegios de acceso para distribuir malware en la organización o solicitar un pago fraudulento.

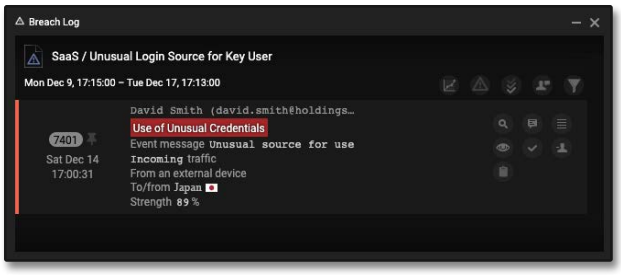


Figura 35: El inicio de sesión desde Japón violó varios modelos

ESTUDIO DE CASO REAL

Cuenta de Microsoft 365 comprometida y saboteada

En una organización internacional sin fines de lucro, Darktrace detectó un robo de cuenta en Microsoft 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.

ESTUDIO DE CASO REAL

Ataque de fuerza bruta automatizado

Darktrace detectó varios eventos de inicio de sesión fallidos en una cuenta de Microsoft 365 utilizando la misma credencial todos los días durante toda una semana. Cada lote de intentos de inicio de sesión se realizó exactamente a las 6.04 p.m. durante seis días. La coherencia tanto en la hora del día como en el número de intentos de inicio de sesión, indicaba un ataque de fuerza bruta automatizado, que se programa para dejar de hacerse después de un número determinado de intentos fallidos con el fin de evitar bloqueos.

Darktrace consideró muy anómalo este patrón de intentos fallidos y alertó al equipo de seguridad. Si Darktrace no hubiera correlacionado los múltiples indicadores débiles y no hubiera concretado las señales sutiles de una amenaza emergente, este ataque automatizado podría haber continuado durante semanas o meses, realizando conjeturas sistemáticas de la contraseña del usuario sobre la base de otra información que ya había reunido.

Figura 36: Un gráfico que ilustra los repetidos intentos de inicio de sesión

Descubra Antigena Email en su propio entorno.

[Haga clic aquí para solicitar una prueba gratuita.]

Acerca de Darktrace

Darktrace es la empresa líder mundial en Cyber AI 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 3.500 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 1.200 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.

Contacto

América Latina: +55 11 97242 2011
Norteamérica: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Asia-Pacífico: +65 6804 5010
info@darktrace.com | darktrace.com
@darktrace