ManageEngine
Log360

Ciberseguridad en los tiempos de **COVID**

Como proteger su empresa de las ciberamenazas basadas en COVID-19

Introducción

A medida que el mundo se está enfrentando a los desafíos de COVID-19, hay otro tipo de amenaza para las empresas: el riesgo de crímenes cibernéticos en el tema de COVID-19. Los atacantes se han aprovechado de esta sensación de temor que está rodeando el virus desde el inicio de la pandemia. En una atmósfera de incertidumbre, cualquier información aparente sobre una crisis en curso se convierte en un poderoso anzuelo. Esto es algo que los hackers conocen y han estado explotando.

Los investigadores de seguridad han descubierto múltiples casos de ataques de ransomware, ataques de phishing y malware payloads en la tema de COVID-19 desde el año pasado. Según una investigación de Barracuda Networks, los ataques de pishing temáticos de COVID-19 han aumentado un 26% en comparación con el año pasado. Esta es la situación en la que nos encontramos en este momento.

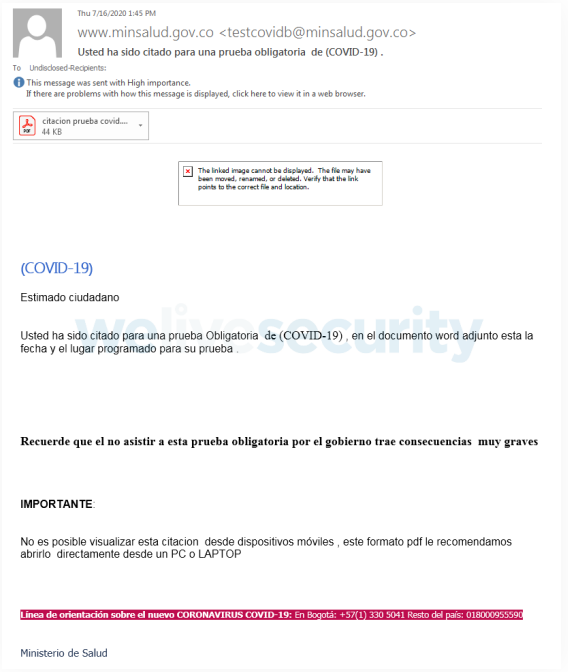
Este e-book le dará una descripción general de estos ciberataques y consejos de expertos sobre cómo aumentar sus defensas de seguridad para combatirlos. El mejor curso de acción para evitar ataques como estos es, por supuesto, no morder el anzuelo. Pero primero necesita aprender cómo identificar el anzuelo de un hacker, para que pueda evitarlo de manera efectiva.

Ladrones de contraseñas en mapas de coronavirus en vivo

En uno de los primeros casos reportados de ataques basados en COVID-19, un malware se fue codificado con un mapa en vivo que rastrea la pandemia. Cuando una víctima desprevenida hace clic en el enlace al mapa, el malware se descargará en la computadora de la víctima. Este tipo de malware roba información de la cuenta que ya está almacenada en la computadora, como nombres de usuario y contraseñas guardadas en el navegador, cookies y otros archivos que se encuentran en el disco duro del dispositivo infectado.

Fuente: kerbsonsecurity.com

Pruebas obligatorias de COVID-19



Se supone que la orden para "la prueba obligatoria de COVID" está en el adjunto de este correo electronico. Una vez que el usuario hace clic en el adjunto, se instala un Remote Access Trojan (RAT) en la computadora de la víctima. Una vez instalado, el malware puede capturar keystrokes, robar datos sensibles de la computadora, activar el micrófono y ademas extraer información copiada en el portapapeles. Este correo electrónico es parte de una sofisticada serie de ataques denominada Operación Spalax que se dirigen principalmente a industrias del sector de la energía y la metalúrgica en Colombia.

Fuente: welivesecurity.com

Sitios de registro de vacunas falsos

Cuando comenzó la vacunación contra COVID-19, se detectaron numerosos sitios de registro de vacunas falsos. El objetivo de estos sitios era recopilar las credenciales de los usuarios y también engañar a los usuarios para que paguen por una vacuna. Esta estafa en ocasiones también circulaba por Whatsapp. Está tan extendido que varios departamentos de policía de todo el mundo emitieron avisos para advertir a las personas que eviten hacer clic en dichos enlaces. Aquí hay un aviso emitido por la guardia civil de España.

Entonces, ¿qué debe hacer para proteger a sus usuarios de estas amenazas y, por extensión, de la red empresarial?

1. La mejor defensa contra ataques de phishing es la prevención. Evite abrir correos electrónicos sospechosos, especialmente relacionados al tema de COVID-19, vacunas etc.

2. Por favor, no crea en noticias falsas. Cuando tenga dudas acerca de la credibilidad de una fuente, búsquela en internet.

3. Es mejor evitar compartir enlaces o mensajes de redes sociales. Podrían contener malware.

4. Si hay algunos errores en el dominio, podría ser malicioso. Por ejemplo, cdc.gov es el dominio de una organización del gobierno de los Estados Unidos, el Centro para el Control y la Prevención de Enfermedades. cdc-gov.org es un dominio malicioso que contiene malware. Se han encontrado a menudo correos electrónicos enviados desde estos dominios maliciosos. Recurso: Kaspersky

5. Los correos electrónicos de phishing con dominios que imitan a los CDC y la Organización Mundial de la Salud han sido visto con frecuencia, por lo que debe indicar a sus empleados que tengan cuidado al abrir correos electrónicos no comerciales.

6. Por ejemplo, las siguientes URLs se han marcado como maliciosas:
   - http://bodica.com.ru/office/coronavirus/-act-today-or-people-will-die-f4d3d9cd99ca
   - http://uk-covid-19-relieve.com
   - https://chase-covid19s.com

Estos son solo tres ejemplos de los cientos de dominios maliciosos con temática de COVID-19 que existen. Algunos dominios maliciosos incluso tienen **https://**, pero eso no garantiza que sean seguros.

Los usuarios suelen caer en nuevas estafas de phishing. Entonces, ¿cuál es el plan para cuando lo hagan?

1. Supervise las instalaciones de software en los dispositivos.

2. No todas las instalaciones de archivos son maliciosas, entonces, ¿cómo diferenciar un software legítimo? Cualquier instalación de software seguida de un cambio en el Windows Registry es muy probable que sea un ataque. Es importante observar esta métrica de cerca después de una nueva instalacion de software. La mayoría de las soluciones SIEM capturan esto mediante reglas de correlación.

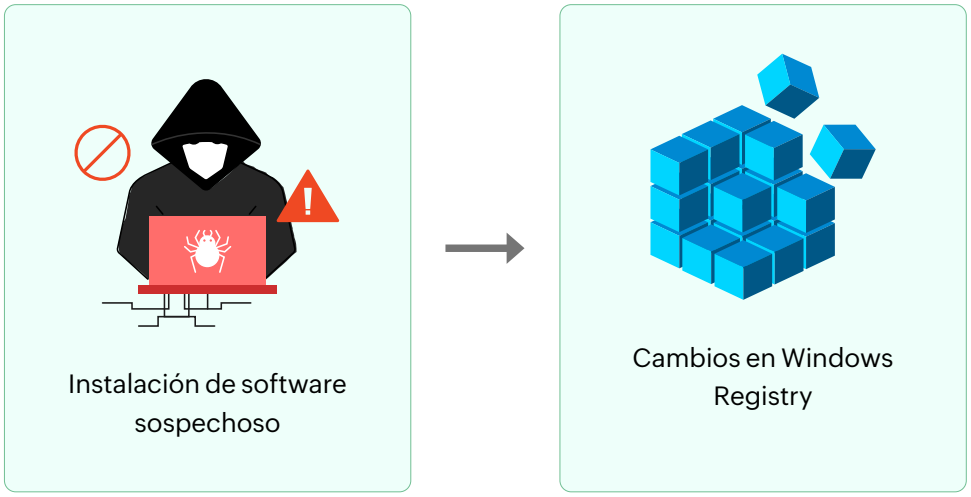
3. Configure workflows automatizados para eliminar los procesos maliciosos identificados por las reglas de correlación.

Para hacer frente las estafas de phishing:

Los feeds de inteligencia de amenazas capturan el tráfico de sitios sospechosos. Detenga la comunicación con estas entidades maliciosas al bloquear el dominio, la URL o la dirección IP.

Responder al software malicioso descargado:

Regla de correlación:



Workflow asociado:

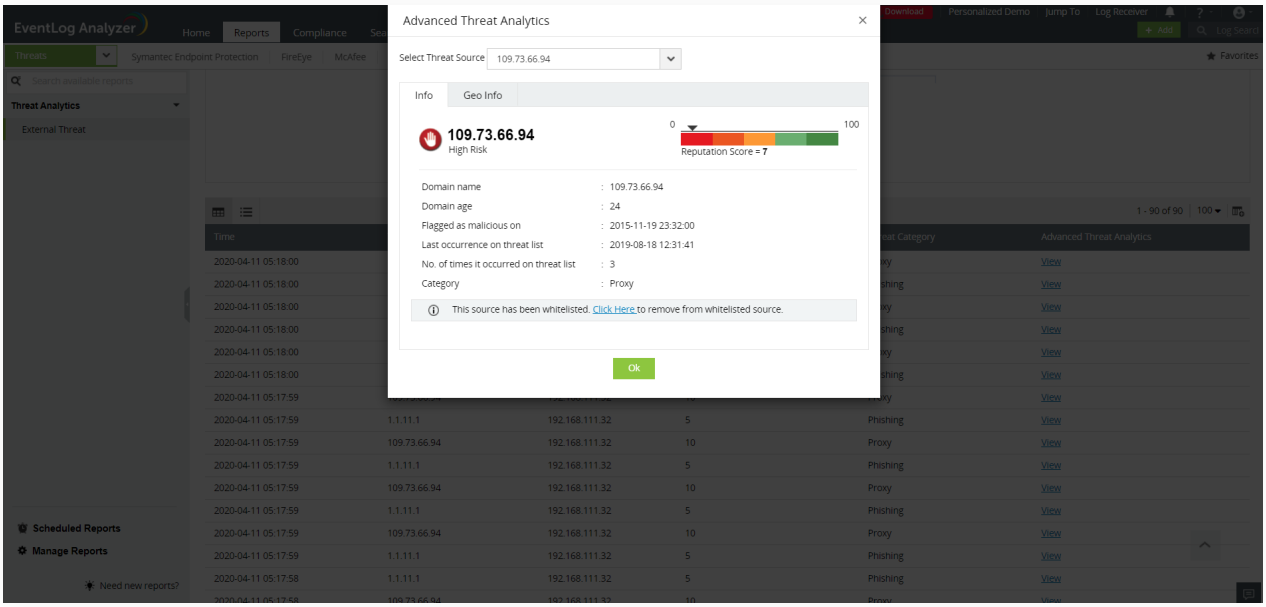
Mata el proceso malicioso

Cómo ManageEngine Log360 puede ayudarte en combatir estas amenazas cibernéticas

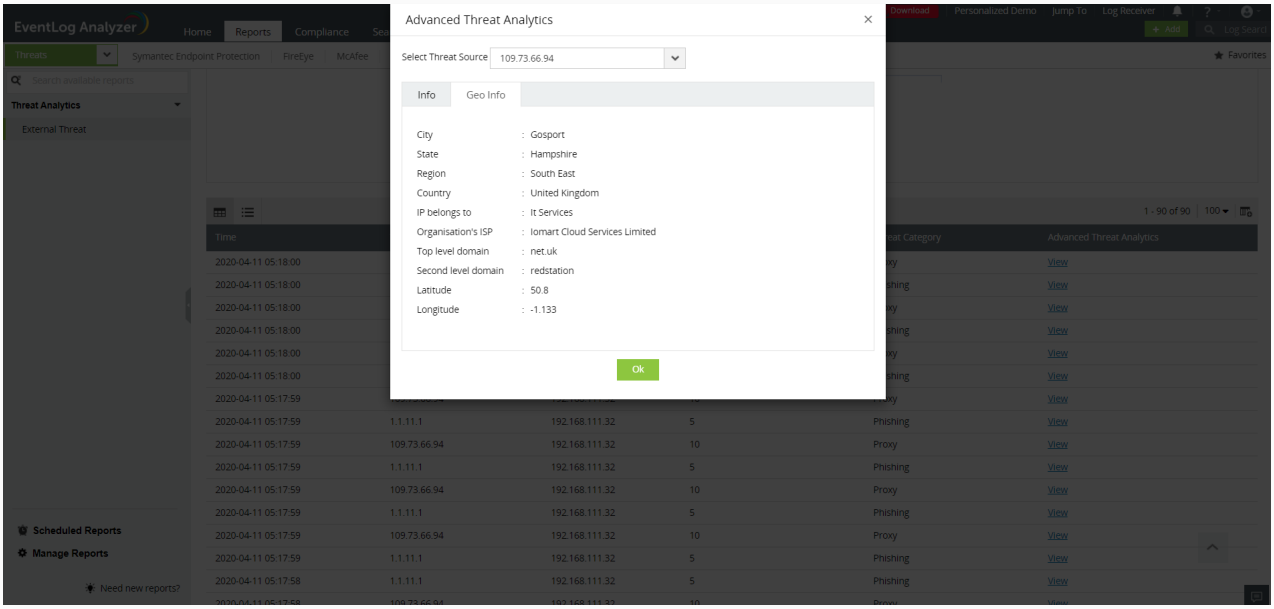
Log360, una solución integral de gestión de eventos e información de seguridad (SIEM), tiene una plataforma de inteligencia de amenazas incorporada que se actualiza dinámicamente con la información más reciente sobre dominios y URL maliciosos, incluidos los recientes con el tema de COVID-19. Con esta solución, puede recibir alertas en tiempo real cuando un usuario intenta contactar o descargar algo de estos sitios.

Evaluar el nivel de riesgo que representan tales amenazas:

El módulo Advanced Threat Analytics de Log360 utiliza una puntuación basada en la reputación para evaluar la gravedad de las amenazas. Cada dominio que interactúe con su red se evaluará en función de su reputación. Si un dominio no tiene un historial registrado de actividad maliciosa o asociación con dominios maliciosos, la puntuación de reputación será alta. Por el contrario, si el dominio ha sido marcado por comportamiento malicioso o está asociado con dominios sospechosos, la puntuación de reputación para ese dominio será baja.



Además, puede obtener información sobre la ubicación del dominio, el ISP de la organización propietaria del dominio y más. En una situación en la que está siendo atacado, toda la información sobre el atacante ayudará.



Conclusión:

Las estafas temáticas de COVID-19 discutidas en este e-book son solo algunos ejemplos de la multitud de posibles ataques que han surgido en los últimos días. Estar atento a ataques como estos y realizar los cambios necesarios en su arquitectura de seguridad será crucial en los próximos días. Si cree que una solución de gestión de eventos e información de seguridad (SIEM) le ayudará, puede probar Log360. Además, puede programar una demostración gratuita en la que nuestros expertos en productos responderán a sus preguntas sobre la solución y demostrarán las ventajas de utilizar Log360 en su organización.

¡Manténgase a salvo! Superemos esta crisis juntos.