Aquae Security: Un paso por delante de los ciberataques dirigidos

Las amenazas son cada vez más agresivas y ocurren con más frecuencia. Los ciberdelincuentes, con claros objetivos, preparan ataques con mucha información obtenida de fuentes públicas y combinando ingeniería social. Para ello, estos "chicos malos" estudian la superficie de ataque o de amenazas, para buscar el eslabón más débil y conocer a la víctima y sus activos tecnológicos potencialmente vulnerables. Con dicha premisa en mente, Aquae Security ha decidido contar con Blueliv para simular ciberataques en las diferentes cadenas de ataque o "kill chain", contra sus activos tecnológicos y empleados; de la misma forma que actuaría un ciberdelincuente o un *malware* tipo wannacry. De esta forma, Aquae Security, ha podido verificar la robustez de sus medidas de seguridad, de su SOC OT/IOT y los procesos vinculados a éste, así como el nivel de concienciación y de reacción de los usuarios y equipos implicados.

Eduardo Di Monte / Daniel Solís

Contextualizar es enfocar los esfuerzos

Para poder realizar un ataque dirigido con éxito, lo primero que hay que hacer es estudiar a los atacantes. Existen chicos malos de diferentes perfiles: bandas del fraude, los que atacan infraestructuras críticas, interfieren en elecciones, trafican con armas y/o, medicamentos, bandas que trabajan para mafias, gobiernos enemigos, terrorismo, etc. Pero ¿qué se ha convertido en estándar del cibercrimen en poco tiempo?:

– Se trafica con todo: credenciales, tarjetas de crédito, fotos, identidades, números de cuentas, pasaportes, etc.

– El *phishing* mediante *emails* sigue funcionando sorprendentemente bien (y de hecho es uno de los vectores de ataques que se ha usado como engaño para la posterior infección).

– Se crea *malware* a medida: para atacar a empresas y/o tecnologías en concreto. Un claro ejemplo es el caso del ataque contra IoT que provocó la *botnet* Mirai.

– El anonimato facilita la impunidad del atacante: gracias a redes como Tor (*dark web*), I2P, etc.

– Además, con muy poco tiempo de antigüedad, y en constante aumento, el *ransomware* está secuestrando equipos de empresas, sistemas SCADA, televisiones, etc. porque está siendo más fácil y efectivo extorsionar que realizar otros tipos de ataques.

Con estas premisas en mente, se decidió crear un escenario que contemplase varios de estos factores para poder ser más efectivos y así determinar el grado de exposición.

Contramedidas, como enfrentarse a los malos usando los valores diferenciales

El SOC IOT/OT de Aquae tiene unas ventajas respecto a los SOC tradicionales que ayudan a protegerse ante los ciberdelincuentes por varios factores que son determinantes:

– Se conocen los procesos de negocio de entornos industriales OT, así como el claro impacto en la operativa de negocio.

– Se dominan los vectores y puntos de ataque de las tecnologías internet tradicionales y de las tecnología industriales IOT/OT como sistemas SCADA, valores HVAC, etc. que tienen difícil acceso para otras industrias, así como para las empresas proveedoras de servicios de seguridad.

– Se tiene acceso a datos, indicadores y mediciones de comportamientos de dispositivos, en contraposición a los SOC tradicionales, que no acceden ni entienden los patrones de ataque modernos.

– Se entienden y contextualizan los aspectos y datos anteriores obteniendo información gracias a motores de Big Data que solo se pueden implementar dentro de in SOC/IOT. se pueden implementar.

Una vez mencionados estos factores diferenciales, desde Aquae se pretendía evaluar diferentes mecanismos de defensa, en busca de potenciales escollos para seguir la filosofía de mejora continua, entre los que cabe destacar:

A) Comprobar elementos de seguridad tradicionales y de IoT/OT.

B) Determinar el nivel de detección, correlación y entendimiento (qué capacidades del Big Data deben afinarse).

C) Chequear la reacción del equipo y los empleados: concienciación y capacidad forense.

D) Comprobar el nivel de entrenamiento del equipo ante incidentes de este tipo y su escalado de incidentes.

Modus operandi de los "chicos malos"

El cibercrimen tiene modelos de negocio más que probados, por eso era necesario enfocar la simulación de un ataque contra Aquae y sus activos. Se debía entender qué es la cadena de destrucción o "kill chain". Esto es, ¿cómo actúan los chicos malos?. Básicamente como se ilustra en la **Figura 1**:

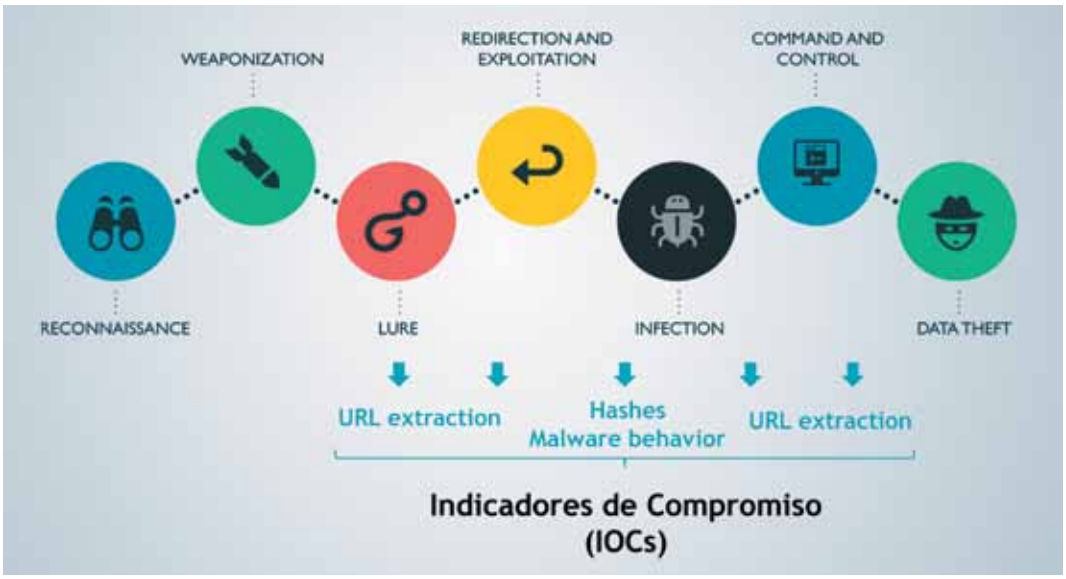

Figura 1.- Modus operandi – Kill Chain.

– Buscan información de lo que hay expuesto.

– Crean su arsenal y se arman con lo que consideran mas efectivo.

– Lanzan una campaña para engañar y conseguir el acceso; normalmente con un *exploit kit* que puede bajarse un *malware* para realizar la infección.

– Empiezan a producir la comunicación con

un servidor malicioso, una vez se ha infectado a un sistema o usuario.

– En este momento se produce la exfiltración, el secuestro del equipo, etc.

Simulación de un ataque tipo *ransomware* o similar

Para poder alcanzar con un ataque efectivo a los usuarios/empleados del grupo Aquae, fue necesario evadir las protecciones perimetrales. Pero previamente a ello, se planteó el ataque de la siguiente forma:

1. Determinar la superficie de ataque (*attack surface*): Las empresas y las personas no son conscientes de la cantidad de información que hay expuesta de ellos. Es fácil para los chicos malos obtener *emails*, perfiles profesionales y particulares, infraestructura, tecnologías de protección pata afilar el ataque, etc.

2. Preparar la Ingeniería social: forzar a víctimas a abrir correos maliciosos, visitar enlaces con *exploit kits*, usar dispositivos infectados (USBs), etc. Existen múltiples técnicas, pero el *phishing* sigue siendo muy efectivo. Por ejemplo, enviar una factura o un documento con *malware* suele surgir efecto, como así hacen los *cryptolockers* o los *credential grabbers*.

3. Realizar la intrusión: era prioritario conseguir acceso directo a la red interna. El pragmatismo en un ataque es lo que marca la diferencia; hay demasiada literatura barata con las famosas APTs. Lo que suele ser relevante para las compañías es saber entender el análisis de comportamiento o *behavioural analysis*, no únicamente patrones de ataque.

Pero, ¿por qué sigue funcionando algo tan aparentemente sencillo? Las tecnologías de protección no son infalibles y los usuarios siguen siendo muy vulnerables al engaño. Además, los usuarios son el punto ideal para la propagación de ataques o el puente perfecto para una expansión de un ataque o metástasis intrusiva y en masa.

Cabe desatacar que para ser 100% efectivos, en coordinación con Aquae, se hizo un *profiling* de las tecnologías perimetrales, ejecutando un banco de pruebas y viendo qué potenciales ataques podrían tener éxito. Por estos motivos se decidió realizar un ataque mediante correos que serían recibidos por los empleados, de los que se había obtenido datos a través de internet.

Ejecución del ataque

Tal y como se observa en la **Figura 2**, se realizó un ataque de *phishing* con técnicas de ofuscación para intentar evadir las medidas tradicionales de seguridad, tales como antivirus y filtros anti-*spam*, y así llegar a los usuarios.

En el envío de correos falsos se usó un correo con un dominio de origen falso que solicitaba una serie de acciones y que redireccionaba a un portal malicioso, con el objetivo de robar credenciales y conseguir infectar al usuario posteriormente.

Dicho en otros términos, el ataque se realizó en dos grandea fases o dos ataques de forma segmentada:

1. *Phishing* simple: para la recolección de información, conocimiento de su tecnología, cuentas de usuario, portales, etc, y arrojar un poco de conocimiento de la organización; necesario para ser más contundente posteriormente.

2. Posteriormente, ejecutar un ataque de *spear phishing*: adjuntando un archivo ofimático, el cual no era detectado por los sistemas antivuirus ni anti-*spam*, de la misma forma que los "chicos malos" proceden para evitar las medidas de protección.

Figura 2.- Simulación de ciberataque.

De esta forma, solo cabía esperar que un usuario cayese bajo el engaño y permitiese a nuestro "malware" darle acceso a su equipo y proceder a realizar una serie de acciones, tal y como las haría un atacante.

Cabe mencionar que todo este proceso se hizo en coordinación con Aquae, acotando las pruebas según perfiles de usuarios o *targets*. Además, se aprovechó para evaluar los tiempos y procedimientos de respuesta del centro de gestión de incidencias del SOC OT/IOT, tal y como se ha mencionado con anterioridad.

Finalmente, se evaluó la capacidad de investigación de los ataques realizados por parte del equipo de seguridad, así como la calidad y el tiempo de respuesta. Quedó demostrado el buen uso de recursos y orden en la contención para defenderse de ataques de esta índole. Dicho entrenamiento fue crucial para mitigar, de forma efectiva, otros ataques que han ocurrido posteriormente.

Conclusiones

Después de este ejercicio de entrenamiento al equipo de seguridad de Aquae, cabe destacar que:

– Los datos sin capacidades para analizarlos no son información sino ruido. Es necesario tener capacidades reales de *big data*, no solo en cuanto a almacenamiento, sino también en cuanto a contextualización y entendimiento.

– La ciberinteligencia o *threat intelligence* es cada vez más importante y vital para seguir estudiando a los "chicos malos" y probar sus técnicas de ataque contra las compañías; estudiar y entender al enemigo es cada vez más necesario.

– La formación continua y entrenamiento en acciones y pruebas de este tipo, debe ocurrir de forma recurrente, para estar preparados de cara a futuros contratiempos.

– La unión hace la fuerza y la colaboración con terceros para intercambiar información, sobre ataques y técnicas, así como información de los *threat actors* es una obligación independientemente del sector en el que se trabaje.

– La innovación en la implementación de nuevas medidas, como señuelos o engaños, dentro de un SOC OT/IOT solo puede realizarse con quien tiene las competencias, los datos y el conocimiento de la tecnología y queda fuera del alcance de los SOC tradicionales o empresas que no estén vinculados a dichos negocios industriales. ■

Eduardo Di Monte
CISO
Aquae Security – Grupo AGBAR

Daniel Solís
CEO
BLUELIV