Con la colaboración de:

CICLO DE EVENTOS DE PEQUEÑO FORMATO
FUNDACIÓN ASTIC

Ataques dirigidos y secuestro de información por *Ransomware* afectando a las AAPP

Estrategias para la prevención, defensa, detección y respuesta

POR MAOLE CEREZO

La actividad asociada a Ransomware durante 2014 se incrementó en términos generales respecto al año anterior en un 113% y en gran medida afectando a las Administraciones Públicas españolas. Ello ha ocasionado graves problemas por el secuestro de información, cifrando los equipos de los usuarios y la información que manejan. 2015 va en la misma línea, y hasta ahora el mecanismo de prevención ha sido el parcheo para evitar las vulnerabilidades y que éstas sean explotadas por la fauna de malware que espera a las puertas de nuestros sistemas. Sin embargo, en 2014 las "top 3" vulnerabilidades más explotadas tardaron 204, 23 y 54 días en disponer de parches por parte de los proveedores correspondientes.

Para debatir sobre las estrategias para la prevención, defensa, detección y respuesta avanzadas que mitigan estos y otros riesgos de ciberseguridad a los que están expuestas las Administraciones Públicas la Fundación ASTIC organizó un almuerzo de trabajo en colaboración con Symantec y Fujitsu. En él se conoció de mano de Joseba Garcia y Javier Ballesteros, Subdirector y Subdirector adjunto TIC del Ministerio de Empleo y Seguridad Social respetivamente la experiencia sobre las APTs que han sufrido y los elementos de detección que actualmente tienen desplegados y que han contribuido a minimizar el impacto de los mismos en su infraestructura.

Miguel Angel (ASTIC): agradece la presencia de Joseba García, Subdirector General TIC en el Ministerio de Empleo, y da paso a los expertos de SYMANTEC con el objeto de que expongan el caso del ataque sufrido en el Ministerio bajo la modalidad de ransomware, tipo de malware que se distribuye a equipos con la intención de cifrar el disco duro, secuestrando los datos e invitando a continuación al usuario a iniciar algún tipo de acción con el fin de recuperar dicha información.

Miguel Ángel Rodríguez, del Ministerio de Industria, abrió el evento confirmando que, si bien la seguridad es un aspecto crucial para preservar la información que se

Las amenazas más habituales "las constituyen el ciberespionaje, la ciberguerra, el cibercrimen o ciberterrorismo y el hacktivismo". Un informe elaborado por el Centro Criptológico Nacional indica "que los incidentes de seguridad sufridos en 2014 casi duplican a los experimentados durante 2013"-

maneja en la Administración, "a lo largo de los últimos años, como plasmación de los contenidos de la Estrategia de Ciberseguridad Nacional, cada vez se viene invirtiendo más del total del presupuesto de la AGE en seguridad".

Las amenazas más habituales "las constituyen el ciberespionaje, la ciberguerra, el cibercrimen o ciberterrorismo y el hacktivismo". Un informe elaborado por el Centro Criptológico Nacional indica "que los incidentes de seguridad sufridos en 2014 casi duplican a los experimentados durante 2013". Otro informe de SYMANTEC indica que en 2015 la ventana de parcheo de los equipos (tiempo comprendido entre la publicación de una vulnerabilidad y el desarrollo del parche que impide su explotación) está siendo en torno a los doscientos días.

El Ministerio de Empleo y Seguridad Social, como compartió García Celada "constituye un escenario especialmente crítico en materia de seguridad, registrando unos 40.000 usuarios internos y alrededor de tres millones de usuarios de transacciones electrónicas a través de los distintos sistemas". Tanto los servicios centrales como los organismos autónomos que de ellos dependen "cuentan con sistemas de defensa y barrera centralizados que en general han conseguido evitar daños importantes procedentes de ciberataques". Hace unos meses se produjo un ataque importante, que según el Centro Criptológico Nacional "mostraba indicios de haber sido auspiciado desde algún gobierno, y cuyas características le permitían superar los controles más habituales, mediante una auténtica ingeniería de búsqueda de información que partiendo de una simple navegación era capaz de localizar y descargar información que suponía relevante". Este ataque, reconoció el Subdirector General TIC, "supuso el punto de partida para la búsqueda de alternativas a los sistemas de protección hasta entonces habituales". Más recientemente "se produjeron invasiones de ransomware, capaces de expandirse por todo el sistema saltando todo tipo de barreras partiendo de la conexión de un usuario concreto. Este software fue capaz de establecer una cadena de alteración de privilegios de forma que, tras abrir una puerta, pudo llegar hasta las cabinas de almacenamiento". Este hecho "resultó especialmente preocupante al contar el Ministerio con un número de teletrabajadores cercano a los tres mil, y cuyos puestos móviles resultan mucho más difíciles de controlar y para el que no sirve el bastionado tradicional".

En este contexto, y con la colaboración de SYMANTEC, "se abordó una prueba consistente en incorporar una herramienta avanzada y, aprovechando los archivos descargados durante el ataque, estudiar el comportamiento de dicha herramienta ante esa acción concreta, creándose un entorno que permitiese analizar dicho comportamiento en

vivo". El objetivo final de esta prueba piloto fue "buscar la protección de los activos críticos ante una amenaza desconocida a priori, con el fin de definir controles avanzados de protección capaces de evitar la infección y producir un bloqueo temprano que evitase la expansión del ataque por los distintos sistemas". De esta forma se creó un entorno de laboratorio, dotado de las herramientas SYMANTEC Datacenter y Critical System Protection y con las librerías procedentes de la captura efectuada por el ransomware durante el ataque. La arquitectura en la que se estuvo trabajando "contaba tanto con Windows 7 como con XP, e incorporaba por un lado, las consolas de control de las herramientas de SYMANTEC y, por otro, una carpeta denominada "confidencial" y que debía ser protegida". Se procedió a "activar el ransomware, y a observar cómo se iba sucediendo una continua descarga de código binario y cómo se iban cifrando los elementos del sistema no protegidos, mientras los protegidos quedaban a salvo de dicha acción, sin poder accederse a ellos mediante aplicaciones distintas de las permitidas ni a través de aquéllas que pudieran intentar suplantarlas". De esta forma "se consigue contener el incidente, evitando el cifrado de la información relevante y manteniéndolo accesible para aplicaciones y usuarios autorizados". Este tipo de solución se basa en "conseguir un sistema proactivo, capaz en su configuración normal de ir desarrollando un aprendizaje sobre los tipos de acceso que sí deben ser permitidos, y que bloquee de forma eficaz los accesos no permitidos. Es importante determinar dónde se van a establecer los sistemas de protección avanzada necesarios, con el fin de evitar bloquear de forma preventiva todo el sistema y de permitir el desarrollo de su actividad normal por parte de los usuarios".

En definitiva, se trata de "disponer de cierta capacidad de parcheado virtual, de forma que se puedan aislar los entornos de ejecución y confinar las amenazas evitando su expansión por el sistema".

Desde la perspectiva de los integradores de servicios, se observa durante los últimos años un desplazamiento de la inteligencia a través de los distintos mercados. Según esto, el mercado financiero ha cedido su liderazgo al tecnológico, como fruto de la mayor regulación que viene experimentando a raíz de la crisis .

Un paso adelante en el estudio de este tipo de solución vendrá dado por "el análisis de su comportamiento en entornos reales, con el fin de determinar la capacidad real de aprendizaje de este tipo de herramienta y observar el rendimiento de la misma combinado con el de otros elementos de seguridad aportados por los dispositivos para permitir que los usuarios no vean afectada la gestión por la propia protección".

Carlos Fernández, CyberSecurity Specialist de SYMANTEC, reflexionó acerca de la importancia de determinar claramente qué es lo que ocurre realmente cuando se produce un incidente de seguridad. Comentó como mediante ejercicios de tabletop es posible simular estos incidentes de forma que "cuando tengamos que hacer frente a un ataque, nuestra respuesta no sea parte del problema. Para ello, las herramientas de la familia ATP de SYMANTEC actúan tanto sobre el perímetro del sistema como sobre el endpoint, permitiendo abordar acciones que normalmente exigen la instalación de otros agentes o requieren disponer de otro tipo de visibilidad. Mediante una consola principal que controla todo el tráfico de red, y a través del motor de análisis CYNIC, se detectan los archivos maliciosos y se obtiene una serie de detalles sobre los mismos: se les asigna una calificación, se identifican su URL e IP, su nombre, y se pasa a monitorizar la amenaza, marcando el origen de la misma y trazando su desplazamiento al tiempo que se obtienen distintos indicadores de compromiso"

En el propio transcurso de la descarga "se puede incorporar el enlace malicioso al black list, sin esperar a efectuar cambios en el firewall, de forma que siempre que se descargue ese fichero, entre de forma automática en cuarentena". En el caso de ficheros procedentes de dominios maliciosos pero no clasificados como malware a priori, éstos "son empaquetados y remitidos a SYMANTEC para su análisis ejecutando el archivo tanto en máquina virtual como física, y obteniendo como respuesta un reporte definitivo". Estas acciones "podrían llevarse a cabo de forma simultánea para varios ficheros que mostrasen los mismos indicadores de compromiso en todos los endpoints que tuviesen esos ficheros, aunque no hubiesen sido ejecutados". Del mismo modo "operaría para varios dominios conectados compartiendo el nodo común de la consola de gestión de antivirus, desplegándose a través de los distintos directorios".

De algunos detalles de los seis ataques de ransomware sufridos en el Ministerio Economía y Competitividad desde el pasado mes de octubre habló Ignacio Cudeiro. El Ministerio dispone de "una solución de análisis basada en un entorno de laboratorio sandbox, y en un software que desde un endpoint permite inhabilitar el acceso a recursos o trasladar el CPD a una VLAN de cuarentena". Cuando "el motor de análisis no es capaz de calificar la amenaza y el vector de entrada viene generado por una navegación por una URL que todavía no se ha reportado como maliciosa, se plantea un problema grave de seguridad". ¿Existe alguna solución para este tipo de caso? Preguntó. Y, ¿En qué se basa el patrón de detección del malware? ¿Existe, aparte del reconocimiento de firmas, algún análisis que permita verificar el comportamiento anómalo de un fichero? Planteó ¿?Javier Merino, socio adherido de ASTIC.

El *CyberSecurity Specialist* de SYMANTEC recordó que, fundamentalmente, existen tres tipos de entrada para el malware: el correo, la navegación web y los propios endpoints. Explicó que el motor de análisis de SYMANTEC "cubre estos tres vectores de entrada, investigando la reputación de ficheros y dominios mediante la inteligencia de seguridad más completa del mercado, acometiendo a continuación un análisis de comportamiento y aplicando la tecnología SONAR, que reconoce los patrones primarios de comportamiento de los ficheros, identificando su posible troyanización". Si estos tres análisis concluyen sin una calificación clara del fichero, "se invoca CYNIC, con cinco motores distintos de detección, análisis estático y dinámico, y la posibilidad de, en última instancia, recurrir al bare metal". Todo esto trata de "analizar en definitiva el comportamiento de los ficheros identificando los patrones comunes al malware: establecer persistencias, escalar privilegios, eludir el borrado, detener servicios, etc." Cuando un software a priori "limpio" intenta efectuar un tipo de acciones que en principio, no debería abordar, se califica como malware. 1033

Desde la perspectiva de los integradores de servicios, se observa durante los últimos años un desplazamiento de la inteligencia a través de los distintos mercados. Según esto, el mercado financiero ha cedido su liderazgo al tecnológico, como fruto de la mayor regulación que viene experimentando a raíz de la crisis. En opinión de María Gutiérrez, Security Manager de FUJITSU, "la tendencia imperante hoy en día en las organizaciones no pasa sólo por dotarse de mecanismos avanzados de protección, sino también por estrategias de vigilancia y monitorización, dado que las amenazas son múltiples y cambiantes. La seguridad no sólo implica a la tecnología implantada sino también a la gestión y a la organización de los recursos que permitan maximizar el rendimiento de la infraestructura disponible".

Carlos Abad, del Centro Criptológico Nacional, comentó como en su organismo se viene registrando, desde 2014, una media situada entre 1.300 y 1.400 incidentes de seguridad mensuales, con una tendencia creciente, que no sólo procede de un incremento de los ataques, sino también de la implantación de un mayor número de sondas y de un mayor porcentaje de notificaciones. En el caso concreto del ransomware, "se han detectado durante 2015 doscientos quince casos, incluyendo tanto los ataques que culminaron con el cifrado de discos como aquéllos limitados a contactos con DNS bloqueados gracias a la implementación de políticas de blacklisting de dominios". También "se ha venido observando durante los últimos meses una constante evolución tecnológica del malware, con capacidad para generar daños irreparables".

Por su parte, el Teniente Coronel de Infantería del Mando Conjunto de Ciberdefensa, José Luis Quintero, recordó que la Estrategia Nacional de Ciberseguridad "no sólo descarga responsabilidades en el Ministerio de Defensa, sino que incorpora otros actores como el Ministerio de Industria, el de Presidencia, el C.N.I., INCIBE..." En estos momentos, el Ministerio de Defensa "está sufriendo ataques en consonancia con los experimentados por otros organismos públicos y privados, incluyendo numerosos casos de ransomware".

Una de las experiencias del Ministerio de Fomento que ha resultado positiva relativa a incidentes basados en phishing fue expuesta por Rafael Santos. Comentó que "en la mayoría de estos ataques se utilizan traducciones automáticas de las páginas web o de los correos originales, lo que da lugar a una presencia fácilmente reconocible de errores y faltas de ortografía". La difusión de ésta característica típica del phishing entre los usuarios "ha contri-

buido a bloquear en gran medida este tipo de ataques".

Y en el caso concreto del Ministerio de Empleo ¿cuál resultó ser el vector de entrada del ataque?, ¿cuánto tiempo se tardó en eliminar la amenaza?, ¿existe una estimación del coste asociado a la existencia de esa brecha en la seguridad?, preguntó Miguel Ángel Rodríguez.

García Celada contó que la entrada se produjo al acceder a un correo privado desde un dispositivo del Ministerio. Curiosamente, "la contaminación se extendió hacia recursos no accesibles desde el puesto de entrada, y este comportamiento anómalo fue lo que detrajo mayor tiempo para el análisis de la infección, dando lugar a que los primeros intentos de contención resultasen ineficaces". El impacto en el funcionamiento de la organización resultó importante, al bloquear un puesto que ocupaba una posición estratégica y generar quince días de trabajos extraordinarios hasta conseguir restablecer la normalidad. La existencia de copias de seguridad aisladas permitió recuperar, a su vez, la totalidad de la información.

Para la Security Manager de Fujitsu "algunos organismos de la administración, por su tamaño, tienen muy difícil establecer un control absoluto sobre sus conexiones a Internet, y las auditorías suelen descubrir con frecuencia deficiencias en este aspecto de la seguridad, a menudo relacionada con las tareas de mantenimiento de los sistemas".

¿Existe alguna posibilidad de controlar este tipo de brechas? Se planteó.

Según José Carlos Cerezo, Especialista en Seguridad de SYMANTEC, la mayor parte de las medidas que se adoptan tradicionalmente "son de naturaleza reactiva, lo que supone en la práctica ir por detrás de las amenazas". En el caso comentado del Ministerio de Empleo, "la filosofía es distinta, se aborda la seguridad de forma proactiva, bien protegiendo la información para impedir su robo o su cifrado, bien protegiendo sistemas para evitar que se vean comprometidos con independencia del tipo de amenaza o de la variante del malware empleados en el ataque. La proactividad pasa por reducir el riesgo al máximo, monitorizando el riesgo residual y obteniendo así el máximo control posible".

En opinión de Ignacio Cudeiro, "una mayor proactividad basada en una mayor defensa de la información, a menudo impacta de forma muy negativa en el servicio". ¿Cómo se puede dotar de proactividad a la seguridad sin afectar al servicio?, planteó.

Para Celia Andrés, del Ministerio de Educación, Cultura y Deporte, en nuestro país "los ciudadanos en general no prestan gran atención a la seguridad, lo cual constituye un problema cultural importante. Debería hacerse un esfuerzo por impartir formación a los empleados públicos con el fin de mentalizar a los usuarios de los sistemas de información de la Administración acerca de la importancia de la seguridad y contribuir así a minimizar por esta vía el impacto de las amenazas".

En este sentido, Jorge Navas, Coordinador del Equipo de Auditoría Informática de la Intervención General de la Administración del Estado, informó de que las auditorías de sistemas en organismos públicos "recogen la dificultad de evaluar la mentalidad que impera en los usuarios en materia de seguridad". Existe una técnica cada vez más difundida consistente "en enviar un falso phishing a todos los usuarios de una organización, de forma que todos ellos lo reciban de forma simultánea, evaluándose a continuación las respuestas y poniendo al corriente de su error a los usuarios que corresponda". Este tipo de acción "resulta inocua, no cuesta nada, permite evaluar el riesgo latente, da lugar a que se hable sobre seguridad en la organización y sirve para refrescar las buenas prácticas en la memoria de los usuarios".

Los problemas citados a lo largo del debate, tal y como concluyó David Fernández de SYMANTEC, "no se resuelven sólo mediante la aplicación de controles técnicos. Las personas, así como los procesos y las organizaciones, tienen tanta o más importancia que la inteligencia y la tecnología". La solución tecnológica planteada por SYMANTEC "no elimina el riesgo de raíz, pero lo reduce de forma considerable tanto para las amenazas conocidas como para las desconocidas, y puede ser de especial aplicación a las infraestructuras críticas de la Administración Pública". Se trata de una capa de defensa que "es a la vez una capa de detección al orientarse a reducir la ventana de exposición integrando el SYMANTEC endpoint, un elemento de red y un elemento de correo, agilizando la respuesta". ✱