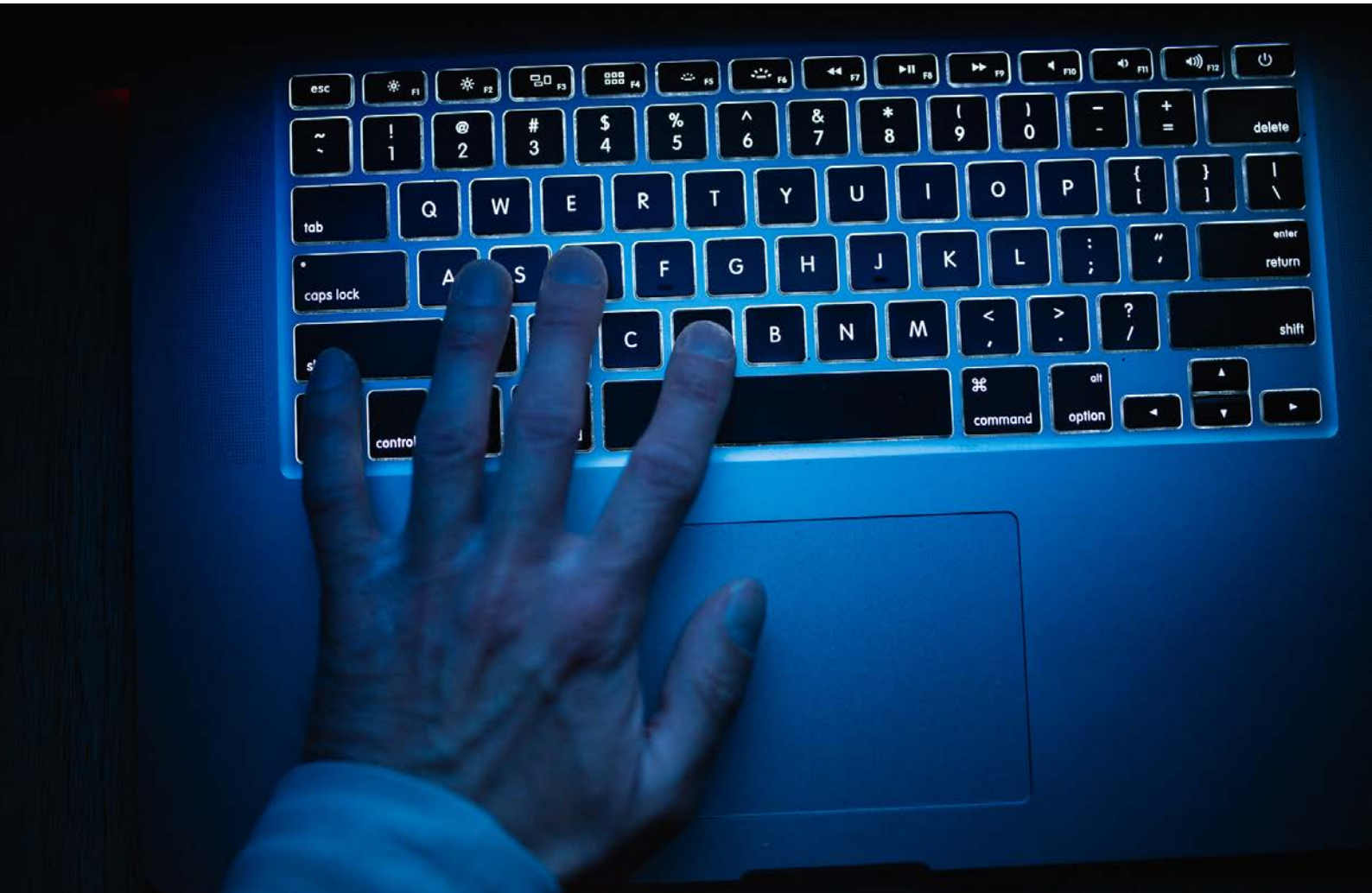
Texto
R. Contreras

ANALIZAMOS EL GRAN ESCÁNDALO DE CIBERSEGURIDAD DE 2020

SolarWinds, el enemigo invisible

El ataque silencioso sufrido por SolarWinds, empresa tejana que desarrolla software para administración de redes y sistemas corporativos, salió a la luz a mediados de diciembre, causando un gran revuelo en las redes y en los medios online, por su carga de profundidad, todavía difícil de calcular. Durante un tiempo que no se conoce con exactitud (los expertos apuntan mayo de 2020), el producto Orion IT de SolarWinds que utilizan unos 33.000 usuarios del sector público y privado, mayormente estadounidenses, fue hackeado, con todas las consecuencias nefastas que se puedan imaginar, algunas de las cuales tuvieron gran repercusión en los periódicos digitales.

Así, Kaspersky denunció al grupo Turla, sociedad asociada al servicio de inteligencia ruso FSB, aunque otras fuentes señalaron a Cozy Bear, vinculado al servicio de inteligencia extranjero moscovita (SVR), como brazo ejecutor del ataque. El secretario de Estado de Trump,



Mike Pompeo, apuntó directamente a Moscú. Como era de esperar, las autoridades del país eslavo calificaron las acusaciones de infundios.

Las alarmas se dispararon en EEUU, todo apuntaba a que un 'intruso' digital habría campado a sus anchas espiando y robando información a espuertas. Varios organismos estadounidenses se habrían visto comprometidos, entre ellos el Departamento de Tesorería y Comercio o el Departamento de Seguridad Nacional. El asunto es de tales dimensiones que Alan Woodward, un investigador de ciberseguridad de la Universidad de Surrey, calificó este ataque como el "el mayor truco desde hace años", la intrusión más grande desde la Guerra Fría.

Sunburst, el nuevo enemigo público

Pero vayamos a los hechos, FireEye, firma californiana fundada en 2004 y experta en análisis y prevención de vulnerabilidades, fue la que destapó el asunto, pues previamente había sido atacada. En unión con Microsoft y SolarWinds, anunciaron el descubrimiento de un sofisticado ataque a la cadena de suministro basado en el despliegue de Sunburst, un malware anteriormente desconocido, que fue utilizado contra los clientes de la plataforma Orion IT de la compañía SolarWinds. Los expertos de Kaspersky han encontrado varias similitudes de código entre Sunburst y las versiones conocidas de la puerta trasera Kazuar, un tipo de malware para acceder de forma remota a la máquina de una víctima.

Al estudiar la puerta trasera Sunburst, los expertos de Kaspersky descubrieron una serie de características superpuestas con Kazuar, una puerta trasera .NET previamente identificada, reportada por primera vez por Palo Alto en 2017, y utilizada en distintas campañas de ciberespionaje en todo el mundo. Múltiples similitudes en el código sugieren una conexión entre Kazuar y Sunburst, aunque de naturaleza indeterminada.

Microsoft niega la mayor

Alfonso Franco, director general de All4sec, explica que los cibercriminales fueron muy hábiles: metieron un fragmento de código trivial que no hacía nada siguiendo el mismo formato de "desarrollo de los desarrolladores del producto y al ver que pasaba desapercibido, insertaron un código malicioso que alcanzó el objetivo perseguido".

Microsoft se ha defendido públicamente de que, aunque los piratas informáticos fueron capaces de acceder a algunos de los códigos fuente suyos, no pudieron realizar ningún cambio. "La cuenta no tenía permisos para modificar ningún código o sistemas de ingeniería", garantizó Microsoft, y la investigación confirmó que no se realizaron cambios en el código.

Pese a la aureola que trae consigo SolarWinds, el fundador de All4sec no se siente sorprendido por un ataque que abre una nueva modalidad con un gran potencial devastador. "Hace un año advertimos de los riesgos que conllevan las herramientas gestionadas por terceros, como es el caso de los proveedores de servicios de seguridad (MSSP), que utilizan sistemas muy similares a SolarWinds".

El problema, como apunta Alfonso Franco, es que hay muchos servicios y sistemas que pueden verse envueltos. Ya no es cuestión de que te manden un ransomware y secuestren tus datos, sino que estás en el core de la red. Hay tantas empresas que tienen estas herramientas, que tener un éxito en este ataque puede causar daños sin precedentes.

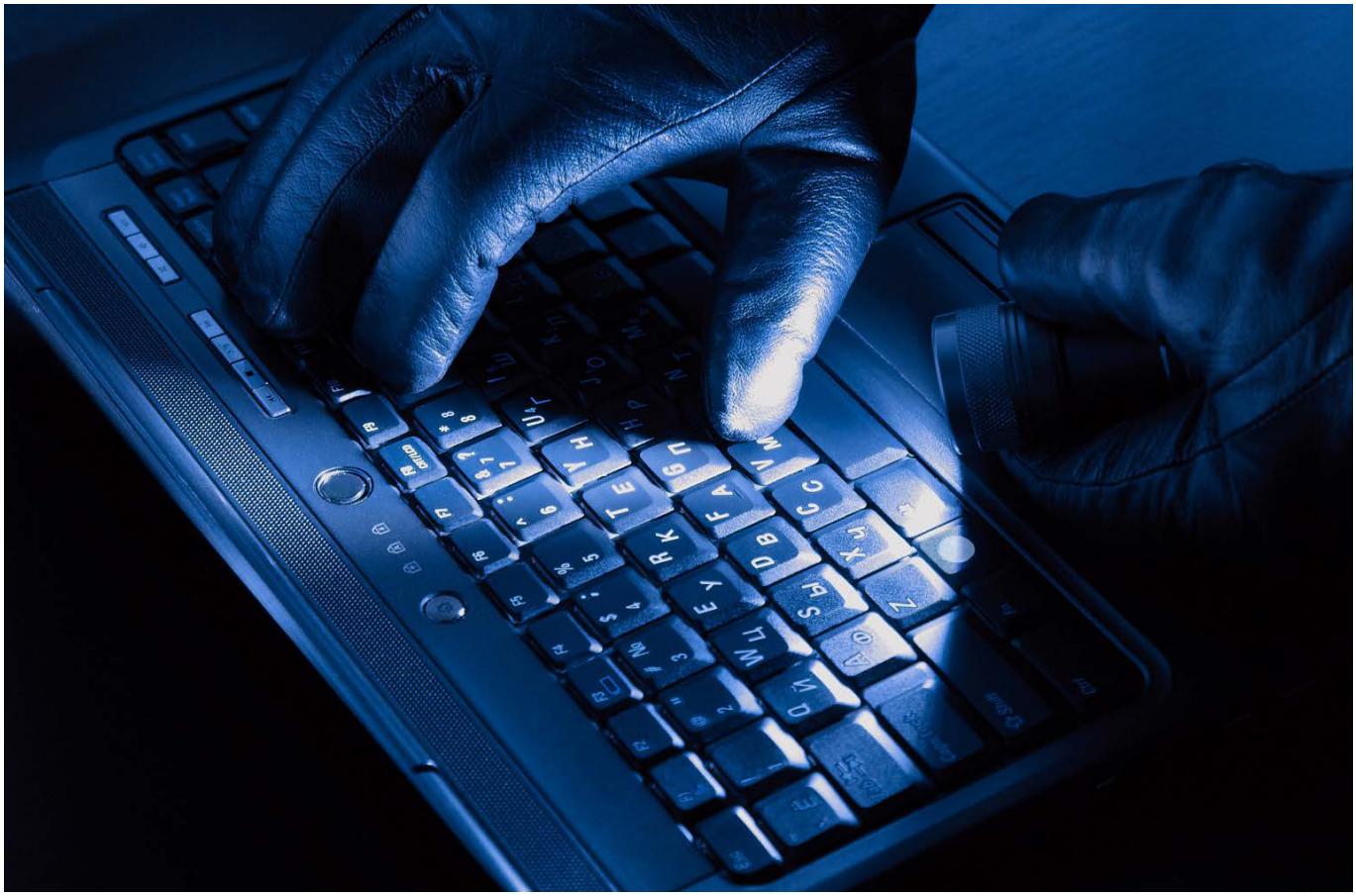
¿Un código inofensivo?

En muchos foros se habla de dónde puede venir la brecha, ya que hay muchos equipos de desarrollo externalizados, en India o Polonia, "porque al final cuando externalizas hay que ver quién gestiona ese código, donde está guardado y en qué condiciones, qué se hace con ese código realmente…".

La receta, y no es cuestión de inventar la rueda como incide Franco, es que "hay que revisar el desarrollo, verificarlo, que no haya componentes de código sin desarrollar… pero claro, en productos complejos como SolarWinds es muy difícil que alguien pueda revisar todo ese código".

Y lo peor de todo es que el software malicioso ya inserto en la empresa puede hacer de su capa un sayo, y saquear a su antojo. SolarWinds tiene acceso a sistemas de red, a estadísticas de tráfico, a movilización de sistemas y es capaz de ejecutar comandos desde fuera, cualquier función del producto queda en sus manos. Al tomar el control de SolarWinds pueden extraer información de los sistemas que está modificando, planos y mapas de red de la arquitectura que hay instalada en cada cliente, cuántos dispositivos es-

<< El hackeo de la herramienta Orion IT de SolarWinds inaugura una gama de ataques en la que son los proveedores de servicios y desarrollo de software los que propician, sin ser conscientes de ello, la introducción de malware en sus entornos de clientes, con todos los riesgos que ello supone.



"Varios organismos estadounidenses se habrían visto comprometidos, entre ellos el Departamento de Tesorería y Comercio o el Departamento de Seguridad Nacional"

tán funcionando, qué tipo de sistemas tienen dentro de la red… un vergel de información.

Certificados de actualización

"Con SolarWinds, los sistemas de protección tradicional no han servido porque han confiado en las actualizaciones habituales en la nube, un sistema de actualización similar al de muchos entornos (Microsoft, NetApp, Office 365). Si tenemos un certificado válido de un sistema del que usamos sus servicios, no tenemos por qué pensar mal si nos piden una actualización. El problema es que los hackers atacaron directamente a los sistemas de actualización de SolarWinds, y no a las empresas", explica un hacker experto que prefiere mantener su anonimato.

La misma fuente revela cómo se descubrió el pastel: "El sistema de certificación de drivers que se utiliza para actualizar software, no mostraba el mismo certificado de seguridad que el que se usa con la infraestructura de seguridad de SolarWinds. Es como el certificado para la declaración de la renta, no depende del ciudadano sino de una entidad certificadora como es la Fábrica de Moneda y Timbre, y no se puede falsear". También se dieron cuenta de que las cuentas de servicio estaban teniendo un comportamiento extraño. Al enviar los clientes información a Internet, también percibieron que se producía una gran cantidad de tráfico hacia unos dominios concretos que descargaban información. Todos esos comportamientos son aparentemente 'normales' (es decir pueden ser autorizados), pero resultan atípicos, porque si una cuenta de servicio (que es una autorización para ejecutar SolarWinds en un servidor concreto) de pronto se loga en un equipo con todas las credenciales y empieza a descargarse información, seguro que hay gato encerrado.

Nuestro confidente teme que esto solo sea la punta del iceberg, "hay muchas empresas que de manera reservada han empezado a anunciar que también han detectado comportamientos extraños en sus cuentas. A lo mejor se han comprometido otros sistemas de actualización de software". Suspicacia que de confirmarse podría tener unas consecuencias muy negativas para las organizaciones privadas y públicas de todo el mundo. ■