Actores de amenazas patrocinados por el estado que supuestamente trabajan para Rusia, se han dirigido al Tesoro de Estados Unidos, la Administración Nacional de Telecomunicaciones e Información (NTIA) del Departamento de Comercio y otras agencias gubernamentales, con el fin de monitorear el tráfico interno de correo electrónico como parte de una campaña de ciberespionaje generalizada.

The Washington Post, citando fuentes no identificadas, informó que los últimos ataques fueron obra de APT29 o Cozy Bear, el mismo grupo de hackers que cree haber orquestado una violación de datos de la firma de seguridad cibernética estadounidense FireEye hace algunos días, que lleva al robo de su Red de Herramientas de Prueba de Penetración de Equipos.

El motivo y alcance total de qué inteligencia se vio comprometida sigue sin estar claro, pero existen indicios de que los adversarios manipularon una actualización de software lanzada por el proveedor de infraestructura de TI con sede en Texas, SolarWinds, a inicios de este año, para infiltrarse en los sistemas de las agencias gubernamentales, así como en FireEye y montar un ataque de cadena de suministro altamente sofisticado.

«El compromiso de los productos de gestión de red Orion de SolarWinds plantea riesgos inaceptables para la seguridad de las redes federales», dijo Brandon Wales, director interino de la Agencia de Seguridad e Infraestructura y Ciberseguridad de Estados Unidos (CISA), que publicó una directiva de emergencia, en la que insta a las agencias civiles federales para revisar sus redes en busca de actividad sospechosa y desconectar o apagar los productos SolarWinds Orion inmediatamente.

Los productos de seguridad y redes de SolarWinds son utilizados por más de 300 mil clientes en todo el mundo, incluidas empresas Fortune 500, agencias gubernamentales e instituciones educativas.

También sirve a varias de las principales empresas de telecomunicaciones de Estados Unidos, las cinco ramas del ejército del mismo país y otras organizaciones gubernamentales prominentes como el Pentágono, el Departamento de Estado, la NASA, la Agencia de

Seguridad Nacional (NSA), el Servicio Postal, la NOAA, el Departamento de Justicia y la oficina del presidente de Estados Unidos.

Campaña evasiva para distribuir la backdoor de SUNBURST

FireEye, que está rastreando la campaña de intrusión en curso bajo el nombre de «UNC2452«, dijo que el ataque a la cadena de suministro aprovecha las actualizaciones del software empresarial SolarWinds Orion troyanizado para distribuir la puerta trasera llamada SUNBURST.

> *«Esta campaña puede haber comenzado ya en la primavera de 2020 y actualmente está en curso. La actividad posterior al compromiso de la cadena de suministro ha incluido el movimiento lateral y el robo de datos. La campaña es el trabajo de un actor altamente calificado y la operación se llevó a cabo con una seguridad operativa significativa»*, dijo FireEye en un análisis este domingo.

Según los informes, la versión falsa del complemento SolarWinds Orion, además de disfrazar su tráfico de red como el protocolo del Programa de Mejora de Orion (OIP), se comunica a través de HTTP a servidores remotos para recuperar y ejecutar comandos maliciosos que cubren la gama de software espía, incluidos los que se utilizan para transferir archivos, ejecutar archivos, perfilar y reiniciar el sistema de destino y deshabilitar los servicios del sistema.

El Programa de Mejora de Orion se utiliza principalmente para recopilar datos de estadísticas de uso y rendimiento de los usuarios de SolarWinds con fines de mejora del producto.

Además, las direcciones IP utilizadas para la campaña fueron ofuscadas por servidores VPN ubicados en el mismo país que la víctima para evadir la detección.

Microsoft también corroboró los hallazgos en un análisis separado, indicando que el actor del ataque, al que llama Solorigate, aprovechó la confianza asociada con el software SolarWinds para insertar código malicioso como parte de una campaña más grande.

> *«Se incluyó una clase de software malicioso entre muchas otras clases legítimas y luego se firmó con un certificado legítimo. El binario resultante incluyó una puerta trasera y luego se distribuyó discretamente en organizaciones específicas»*, dijo Microsoft.

Aviso de seguridad de SolarWinds

En un aviso de seguridad publicado por SolarWinds, la compañía informó que el ataque apunta a las versiones 2019.4 a 2020.2.1 del software SolarWinds Orion Platform, que se lanzó entre marzo y junio de 2020, y recomendó a los usuarios actualizar a la versión Orion Platform 2020.2.1 HF 1 de inmediato.

Se espera que la compañía, que se encuentra investigando el ataque en coordinación con FireEye y la Oficina Federal de Investigaciones de Estados Unidos, publique una revisión adicional, 2020.2.1 HF 2, el 15 de diciembre, que reemplaza el componente comprometido y proporciona varias medidas de seguridad adicionales.

FireEye reveló la semana pasada que fue víctima de un ataque de un gobierno extranjero altamente sofisticado, que comprometió sus herramientas de software utilizadas para probar las defensas de sus clientes.

Con un total de 60, las herramientas del Red Team robadas, son una combinación de herramientas disponibles públicamente (43%), versiones modificadas disponibles públicamente (17%) y las que se desarrollan internamente (40%).

Además, el robo también incluye cargas útiles de explotación que aprovechan

vulnerabilidades críticas en Pulse Secure SSL VPN (CVE-2019-11510), Microsoft Active Directory (CVE-2020-1472), Zoho ManageEngine Desktop Central (CVE-2020-10189) y Servicios de Escritorio Remoto de Windows (CVE-2019-0708).

La campaña parece ser un ataque a la cadena de suministro a escala global, ya que FireEye dijo que detectó esta actividad en distintas entidades en todo el mundo, que abarcan empresas gubernamentales, de consultoría, tecnología, telecomunicaciones y extractivas en América del Norte, Europa, Asia y Medio Oriente.

Los indicadores de compromiso (IoC) y otras firmas de ataques relevantes diseñadas para contrarrestar SUNBURST se pueden ver aquí.