Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°210	Fecha: 06-09-2023
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	La nueva variante del agente Tesla utiliza un exploit de Excel para infectar PC con Windows		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

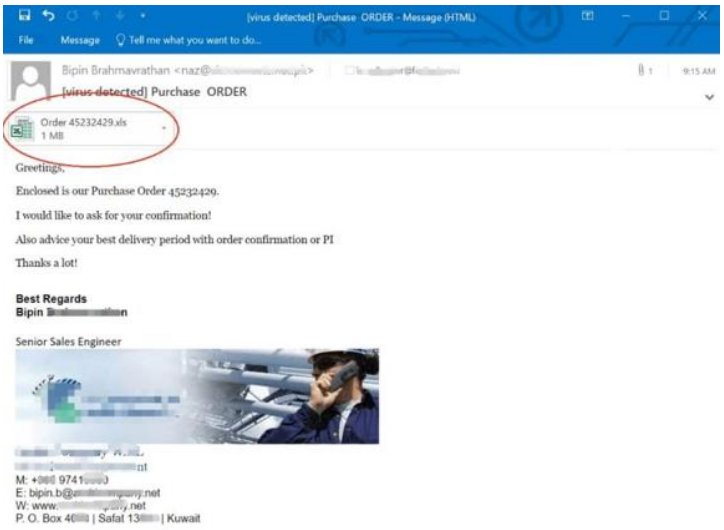
FortiGuard descubre una campaña de phishing que distribuye la nueva variante de la famosa familia de malware Agent Tesla a dispositivos Windows, la cual aprovecha la vulnerabilidad CVE-2017-11882/CVE-2018-0802 para ejecutar el malware.

El autor del informe, Xiaopeng Zhang, reveló que el malware puede robar "credenciales, datos de registro de teclas y capturas de pantalla activas" del dispositivo de la víctima. Los datos robados se transfieren al operador del malware a través de correo electrónico o protocolo SMTP. El malware infecta principalmente dispositivos Windows y garantiza su persistencia incluso cuando se reinicia el dispositivo o se finaliza el proceso de malware.

Para su información, el malware Agent Tesla también se ofrece como herramienta de malware como servicio. Las variantes de malware utilizan un ladrón de datos y un RAT (troyano de acceso remoto) basado en .NET para el acceso inicial.

2. DETALLES:

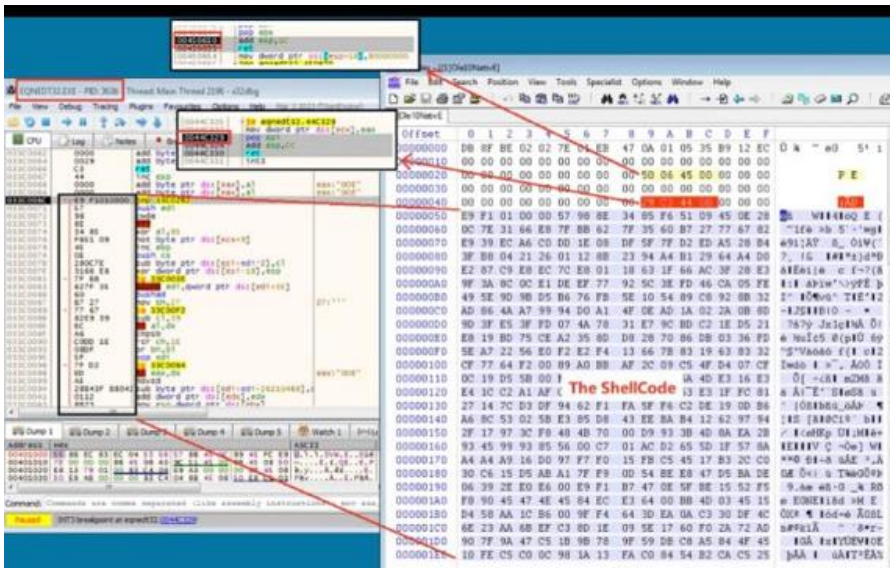
Se trata de una campaña de phishing, por lo que el acceso inicial se obtiene a través de un correo electrónico de phishing diseñado para engañar a los usuarios para que descarguen el malware. El correo electrónico es una notificación de orden de compra que solicita al destinatario que confirme su pedido a un proveedor de equipos industriales.



El correo electrónico contiene un archivo adjunto malicioso de MS Excel titulado Orden 45232429.xls. Este documento está en formato OLE y contiene datos de ecuaciones diseñadas que explotan una antigua vulnerabilidad de seguridad RCE rastreada como CVE-2017-11882/CVE-2018-0802 en lugar de utilizar una macro VBS.

Esta vulnerabilidad causa daños en la memoria en el proceso EQNEDT32.EXE y permite la ejecución de código arbitrario a través del método ProcessHollowing, en el que un pirata informático reemplaza el código del archivo ejecutable con código malicioso.

Un código shell descarga/ejecuta el archivo Agent Tesla (dasHost.exe) desde este enlace "hxxp://2395.128.195/3355/chromium.exe" en el dispositivo de destino. Es un programa .NET protegido por IntelliLock y .NET Reactor. Los módulos relevantes están cifrados/codificados en la sección Recursos para evitar que su módulo principal sea detectado y analizado.



Sobre las capacidades del malware, éste establece un enlace de teclado a través de la API SetWindowsHookEx() para monitorear las entradas de teclado de bajo nivel y llama al procedimiento de enlace de devolución de llamada "this.EiqpViCm9()" cada vez que la víctima escribe algo en el dispositivo. El malware roba el título del programa, la hora y el contenido de entrada a intervalos regulares. Un temporizador llama a un método para verificar el archivo log.tmp cada 20 segundos y envía la información al atacante a través de STMP. Además, el malware utiliza otro temporizador con un intervalo de 20 minutos para comprobar las actividades del dispositivo y determinar cuándo realizar capturas de pantalla.

El malware Agent Tesla también garantiza la persistencia incluso cuando se reinicia el dispositivo o se finaliza el proceso de malware, mediante dos métodos. Ejecuta un comando para crear una tarea en el sistema TaskScheuler en el módulo de carga útil o agrega un elemento de ejecución automática en el registro del sistema. Estos métodos permiten que la duplicación de dasHost.exe se inicie automáticamente cuando se reinicia el sistema.

Vale la pena señalar que Microsoft publicó correcciones para esta vulnerabilidad en noviembre de 2017 y enero de 2018. Sin embargo, todavía está siendo explotada por actores de amenazas que indican la presencia de dispositivos sin parches. Según la investigación de FortiGuard, observan alrededor de 1300 dispositivos vulnerables diariamente y mitigan 3000 ataques a nivel IPS por día. Según los datos compartidos por la empresa de ciberseguridad Qualys, CVE-2017-11882 sigue siendo una de las fallas más favorecidas, explotada por "467 malware, 53 actores de amenazas y 14 ransomware", hasta la fecha 31 de agosto de 2023.

3. RECOMENDACIONES:

- Nunca hacer clic en enlaces ni abrir archivos adjuntos en correos electrónicos de remitentes que no conoce o en los que no confía, y menos si solicita información personal o financiera
- Mantener el software actualizado lo antes posible, según los parches de seguridad que los proveedores oficiales liberan en sus publicaciones o notificaciones automáticas.
- Utilizar un programa antivirus y antimalware licenciado y actualizado.
- Verificar la URL cuidadosamente, que esté contenida en cualquier correo que reciba, antes de visitar el sitio web.
- Utilizar un filtro de spam para reducir la cantidad de correos de phishing que pueda recibir.
- Informarse sobre el phishing. Cuanto más sepa sobre el phishing, mejor podrá detectarlo.

Fuente de Información:	• hxxps://www.hackread.com/agent-tesla-variant-excel-exploit-windows-pc/ • hxxps://thehackernews.com/2023/09/alert-phishing-campaigns-deliver-new.html