Se han revelado más detalles acerca de un conjunto de vulnerabilidades de cross-site scripting (XSS) en el servicio de análisis de código abierto de Microsoft Azure HDInsight, las cuales han sido corregidas y que podrían ser utilizadas por un actor de amenazas para llevar a cabo actividades maliciosas.

> *«Esto sugiere que los actores de amenazas están simplificando sus operaciones al hacer que sus técnicas sean versátiles»,* señalaron los investigadores de Trend Micro en un nuevo análisis publicado esta semana.

En el incidente investigado por la empresa de ciberseguridad, se dice que una víctima no identificada primero recibió un malware de robo de información con certificados de firma de código de Validación Extendida (EV), seguido de ransomware utilizando la misma técnica de entrega.

En el pasado, las infecciones de QakBot han utilizado muestras firmadas con certificados de firma de código válidos para eludir las protecciones de seguridad.

Los ataques comienzan con correos electrónicos de phishing que emplean señuelos conocidos para engañar a las víctimas y hacer que ejecuten archivos adjuntos maliciosos que se hacen pasar por archivos PDF o JPG, pero que en realidad son ejecutables que inician la compromiso al ejecutarse.

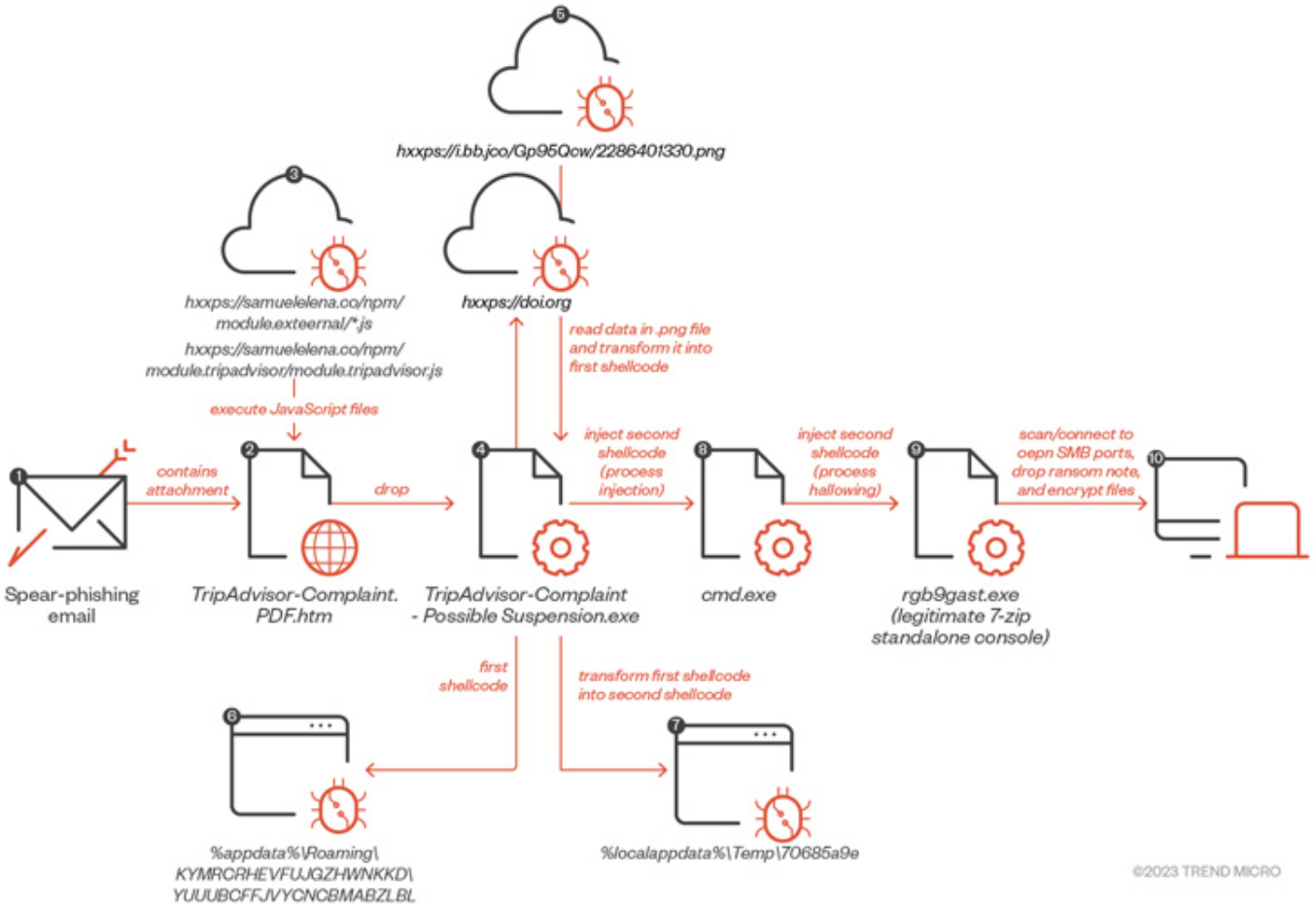
Mientras que la campaña dirigida a la víctima entregó malware de robo de información en julio, una carga de ransomware llegó a principios de agosto después de recibir un mensaje de correo electrónico que contenía un falso archivo adjunto de queja de TripAdvisor («TripAdvisor-Complaint.pdf.htm»), desencadenando una secuencia de pasos que culminaron en la implementación de ransomware.

> *«En este punto, es importante señalar que, a diferencia de las muestras del malware de robo de información que investigamos, los archivos utilizados para*

> *dejar la carga de ransomware no tenían certificados EV»*, indicaron los investigadores.

> *«Sin embargo, ambos provienen del mismo actor de amenazas y se distribuyen utilizando el mismo método de entrega. Por lo tanto, podemos asumir una división de tareas entre el proveedor de la carga y los operadores».*

Este desarrollo se produce mientras que IBM X-Force descubrió nuevas campañas de phishing que distribuyen una versión mejorada de un cargador de malware llamado DBatLoader, que se utilizó como conducto para distribuir FormBook y Remcos RAR a principios de este año.



Las nuevas capacidades de DBatLoader facilitan la elusión del Control de Cuentas de Usuario (UAC), la persistencia y la inyección de procesos, lo que indica que se está manteniendo activamente para dejar programas maliciosos que pueden recopilar información sensible y permitir el control remoto de sistemas.

Los recientes ataques, detectados desde finales de junio, también están diseñados para distribuir malware común como Agent Tesla y Warzone RAT. La mayoría de los mensajes de correo electrónico se han dirigido a hablantes de inglés, aunque también se han visto correos electrónicos en español y turco.

> *«En varias campañas observadas, los actores de amenazas tenían un control suficiente sobre la infraestructura de correo electrónico para permitir que los correos electrónicos maliciosos pasaran las autenticaciones de correo electrónico SPF, DKIM y DMARC»*, afirmó la compañía.

> *«La mayoría de las campañas utilizaron OneDrive para preparar y recuperar cargas útiles adicionales, mientras que una pequeña fracción utilizó transfer[.]sh o dominios nuevos/comprometidos».*

En noticias relacionadas, Malwarebytes reveló que una nueva campaña de publicidad maliciosa está apuntando a usuarios que buscan el software de videoconferencia Cisco Webex en motores de búsqueda como Google para redirigirlos a un sitio web falso que distribuye el malware BATLOADER.

BATLOADER, por su parte, establece contacto con un servidor remoto para descargar una carga cifrada de segunda etapa, que es otro malware de robo de información y keylogger conocido como DanaBot.

Una técnica novedosa adoptada por el actor de amenazas es el uso de URL de plantillas de seguimiento como mecanismo de filtrado y redirección para identificar y determinar a posibles víctimas de interés. Los visitantes que no cumplen con los criterios (por ejemplo, solicitudes que provienen de un entorno aislado) son redirigidos al sitio legítimo de Webex.

> *«Dado que los anuncios parecen tan legítimos, no hay duda de que las personas harán clic en ellos y visitarán sitios inseguros»*, dijo Jérôme Segura, director de inteligencia de amenazas en Malwarebytes.

> *«El tipo de software utilizado en esos anuncios indica que los actores de amenazas*

> *están interesados en víctimas corporativas que les proporcionarán credenciales útiles para futuras 'pruebas de penetración' en redes y, en algunos casos, implementación de ransomware».*