Microsoft reveló el jueves que revocó más de 200 certificados utilizados por un actor de amenazas al que rastrea bajo el nombre *Vanilla Tempest*, quien los empleó para firmar de manera fraudulenta binarios maliciosos utilizados en ataques de ransomware.

Según el equipo de inteligencia de amenazas de Microsoft, estos certificados fueron *"empleados en archivos falsos de instalación de Teams para distribuir la puerta trasera Oyster y, finalmente, desplegar el ransomware Rhysida"*, como se explicó en una publicación compartida en X (anteriormente Twitter).

La compañía tecnológica afirmó que interrumpió esta actividad a principios de octubre, tras haberla detectado a finales de septiembre de 2025. Además de revocar los certificados comprometidos, actualizó sus soluciones de seguridad para detectar las firmas asociadas a los archivos falsos de instalación, la backdoor Oyster y el ransomware Rhysida.

Vanilla Tempest (anteriormente conocido como *Storm-0832*) es el nombre asignado a un actor de amenazas con fines económicos, también identificado como *Vice Society* o *Vice Spider*. Se estima que está activo al menos desde julio de 2022, y ha distribuido múltiples variantes de ransomware como *BlackCat*, *Quantum Locker*, *Zeppelin* y *Rhysida*.

Por su parte, *Oyster* (también conocido como *Broomstick* o *CleanUpLoader*) es una puerta trasera que suele propagarse a través de instaladores troyanizados de programas populares como Google Chrome o Microsoft Teams. Estos instaladores maliciosos se ofrecen en sitios web falsos, los cuales los usuarios encuentran al buscar los programas en Google o Bing.

"En esta campaña, Vanilla Tempest utilizó archivos falsos MSTeamsSetup.exe alojados en dominios maliciosos que imitaban a Microsoft Teams, como teams-download[.]buzz, teams-install[.]run o teams-download[.]top", indicó Microsoft. *"Es probable que los usuarios lleguen a estos sitios maliciosos mediante técnicas de envenenamiento SEO."*

Para firmar digitalmente estos instaladores y otras herramientas utilizadas después de la intrusión, se informó que el grupo hizo uso de servicios de firma de código legítimos como *Trusted Signing*, además de proveedores como *SSL[.]com*, *DigiCert* y *GlobalSign*.

Los primeros detalles de esta campaña fueron publicados el mes pasado por *Blackpoint Cyber*, quien explicó cómo los usuarios que buscaban Microsoft Teams en línea eran redirigidos a páginas de descarga falsas, donde se les ofrecía un archivo malicioso MSTeamsSetup.exe en lugar del cliente legítimo.

"Esta actividad evidencia el abuso continuo del envenenamiento SEO y de anuncios maliciosos para distribuir puertas traseras disfrazadas de software confiable," advirtió la compañía. *"Los actores de amenazas están explotando la confianza del usuario en los resultados de búsqueda y en marcas conocidas para obtener acceso inicial a los sistemas."*

Como medida de prevención, se recomienda descargar software únicamente desde fuentes verificadas y evitar hacer clic en enlaces sospechosos que aparezcan como anuncios en los resultados de motores de búsqueda.