Los perpetradores detrás del ransomware BianLian han sido detectados aprovechando vulnerabilidades de seguridad en el software JetBrains TeamCity para llevar a cabo sus ataques de extorsión.

Conforme a un informe reciente de GuidePoint Security, el incidente *«se inició mediante la explotación de un servidor TeamCity, dando como resultado la implementación de una variante en PowerShell del backdoor Go de BianLian».*

BianLian surgió en junio de 2022 y, desde entonces, ha centrado exclusivamente sus esfuerzos en extorsiones basadas en la exfiltración, tras la liberación de un descifrador en enero de 2023.

La secuencia de ataque observada por la firma de ciberseguridad involucra la explotación de una instancia vulnerable de TeamCity utilizando *CVE-2024-27198 o CVE-2023-42793* para obtener acceso inicial al entorno. Luego, se crean nuevos usuarios en el servidor de compilación y se ejecutan comandos maliciosos para llevar a cabo la postexplotación y el movimiento lateral.

En la actualidad, no está claro cuál de las dos vulnerabilidades fue empleada por los actores de amenazas para la infiltración.

Los actores de BianLian son conocidos por implantar un backdoor personalizado adaptado a cada víctima, escrito en Go, y también por dejar herramientas de escritorio remoto como AnyDesk, Atera, SplashTop y TeamViewer. Microsoft lo rastrea como BianDoor.

> *«Después de varios intentos fallidos de ejecutar su backdoor Go estándar, los perpetradores cambiaron a un enfoque 'vivir de la tierra' y aprovecharon una implementación en PowerShell de su backdoor, la cual proporciona funcionalidad casi idéntica a la que tendrían con su backdoor Go»,* indicaron los investigadores de seguridad Justin Timothy, Gabe Renfro y Keven Murphy.

El backdoor en PowerShell ofuscado («web.ps1») está diseñado para establecer un socket TCP para la comunicación de red adicional con un servidor controlado por los perpetradores, permitiéndoles realizar acciones arbitrarias en un host infectado.

> *«El backdoor, ahora confirmado, es capaz de comunicarse con el servidor de [control y comando] y ejecutarse de manera asincrónica según los objetivos de postexplotación del atacante remoto»,* señalaron los investigadores.

Esta divulgación se produce mientras VulnCheck detalla nuevos exploits de prueba de concepto (PoC) para una vulnerabilidad crítica que afecta a Atlassian Confluence Data Center y Confluence Server (CVE-2023-22527), la cual podría resultar en la ejecución remota de código de manera sin archivos y cargar directamente la web shell Godzilla en la memoria.

La vulnerabilidad ha sido aprovechada recientemente para desplegar el ransomware C3RB3R, mineros de criptomonedas y troyanos de acceso remoto durante los últimos dos meses, indicando una explotación extendida en entornos no monitoreados.

> *«Existen múltiples vías para llegar al mismo resultado. Aunque el uso de freemarker.template.utility.Execute parece ser el método preferido para explotar CVE-2023-22527, otras rutas más discretas generan distintos indicadores»,* observó Jacob Baines de VulnCheck.