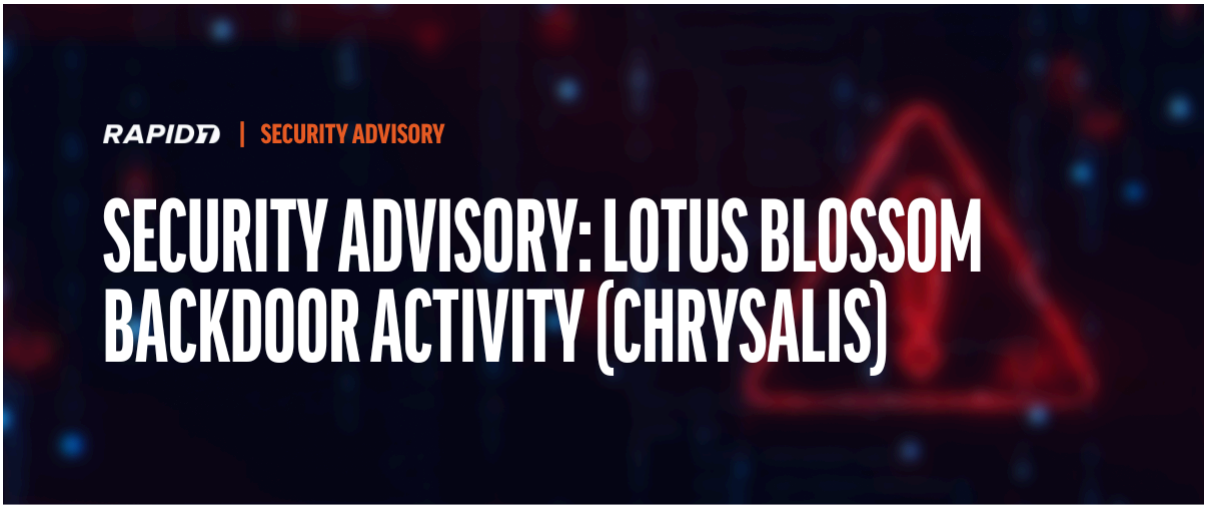

Activité dérobée de Lotus Blossom : Chrysalide

Rapid7 Labs, en collaboration avec l'équipe Rapid7 MDR, a mis au jour une attaque sophistiquée contre la chaîne d'approvisionnement, attribuée au groupe APT chinois Lotus Blossom. Actif depuis 2009, ce groupe est connu pour ses campagnes d'espionnage ciblées affectant les gouvernements, les télécommunications, l'aviation, les infrastructures critiques et les médias.

Notre enquête a révélé une compromission de l'infrastructure hébergeant Notepad++, utilisée pour diffuser une porte dérobée personnalisée, jusqu'alors non documentée, que nous avons nommée Chrysalis. Bien que cette vulnérabilité ne soit plus exploitée, Rapid7 recommande vivement une recherche de menaces rétrospective afin d'identifier toute exposition potentielle.

Ce que nous savons jusqu'à présent :

L'attribution à Lotus Blossom repose sur de fortes similitudes avec des outils et des techniques d'exécution déjà documentés, notamment des chargements latéraux et des artefacts cryptographiques communs observés dans plusieurs charges utiles. Ces indicateurs suggèrent avec un degré de certitude modéré une activité liée à Lotus Blossom.

Nous continuerons à mettre à jour notre analyse à mesure que de nouvelles informations seront disponibles.

Lire l'analyse complète

Rejoignez-nous demain : À l'intérieur de Chrysalis

Pour aider les équipes de sécurité à mieux comprendre cette activité et ses implications, Rapid7 organise un webinaire en direct demain : «

Au cœur de Chrysalis : Leçons tirées de la porte dérobée Notepad++ et de la nouvelle réalité des attaques contre la chaîne d'approvisionnement »,
le jeudi 5 février à 9 h 00 (heure de l'Est).
Animé par Christiaan Beek et Steve Edwards de Rapid7.

Cette session abordera les points suivants :

- Comment la porte dérobée Chrysalis a été livrée et utilisée
- Ce que cette campagne révèle sur les attaques modernes contre les chaînes d'approvisionnement
- Conseils pratiques pour la détection, la chasse et la défense

Inscrivez-vous maintenant

Transférer à un ami

Rapid7
Two Forbury Place
33 Forbury Road
Reading, RG1 3JH