

Les protections de Windows complètement inefficaces à la technique AtomBombing !



Les protections de Windows complètement inefficaces à la technique AtomBombing !

Des chercheurs en sécurité ont découvert un mécanisme qui exploite une propriété propre à Windows pour en contourner tous les mécanismes de protection.

Une véritable bombe atomique pour l'intégrité de Windows. Une équipe de chercheurs de la société de sécurité israélienne Ensilo déclare avoir trouvé un moyen qui permet à un code malveillant de contourner toutes les barrières de sécurité possibles et inimaginables de l'OS de Microsoft. Et quelle que soit sa version. En l'occurrence, les experts ont effectué leurs travaux sur Windows 10.

La technique, qu'ils ont dénommée « AtomBombing » exploite les « Atom Tables ». Inhérentes au système d'exploitation, ces tables permettent aux applications de stocker les données et y accéder. Elles peuvent aussi être utilisées pour organiser le partage des informations entre les applications. « *Nous avons découvert qu'un attaquant pouvait écrire du code malveillant dans une table atom et forcer un programme légitime à récupérer ce code depuis la table*, explique le responsable de l'équipe de recherche Tal Liberman. *Nous avons également constaté que le programme légitime, maintenant infecté du code malveillant, peut être manipulé pour exécuter ce code.* » De plus amples détails sur la technique d'intrusion sont présentés sur cette page.

Pas de correctif possible

Ce n'est évidemment pas le premier cas connu de technique d'injection de code pour pénétrer le système et affaiblir son intégrité. Mais ces techniques s'appuient généralement sur des vulnérabilités de l'OS et la manipulation de son utilisateur amené, sans en avoir conscience, à déclencher l'exécution d'un code malveillant à travers un programme, comme un navigateur par exemple, pour contourner les barrières de sécurité.

Mais rien de tout cela dans le cas présent. « *AtomBombing est exécuté simplement en utilisant les mécanismes sous-jacents à Windows. Il n'est pas nécessaire d'exploiter les bugs ou les vulnérabilités du système d'exploitation*, assure le chercheur. *Comme la question ne peut être résolue, il n'y a pas de notion de correctif. Ainsi, la réponse pour atténuer [le risque] serait de plonger dans les appels des API et de surveiller les activités malveillantes.* » Autrement dit, pas de correctif possible mais du monitoring système en temps réel en quelque sorte (comme en propose au passage Ensilo). L'autre solution serait que Microsoft modifie l'architecture de Windows. Ce qui n'est pas prévu dans l'immédiat.

Ensilo reste discret – et c'est bien normal – sur la méthode pour injecter le code. A notre sens, l'exécution d'un tel script nécessite soit la complicité involontaire de son utilisateur (ce qui n'est pas nécessairement le plus compliqué), soit l'accès direct à une machine non protégée. En cas de succès, l'AtomBombing fait alors tomber toutes les barrières de protection selon les niveaux de restriction, peut accéder à des données spécifiques, y compris les mots de passe chiffrés, ou encore s'installer dans le navigateur pour en suivre toutes les opérations. Explosif !

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Original de l'article mis en page : AtomBombing, le code insensible aux systèmes de protection de Windows