ALERTE n°BA18-02

Emotet, un malware avancé qui cible les établissements publics et privés

Date de publication : 31/07/2018

Un malware avancé, modulaire et destructif dénommé Emotet qui cible les établissements publics et privés prend du terrain.

En effet, Emotet est un cheval de Troie polymorphique qui possède plusieurs méthodes pour maintenir sa persistance et s'échapper de la détection typique des anti-virus et aussi des analyses via les environnements de sandbox.

Outre, l'infection par Emotet se fait en incitant les victimes à ouvrir des e-mails contenant des liens malveillants ou des pièces jointes PDF / document Microsoft Word malicieuses. Une fois installé, il tente de se propager via les réseaux locaux à l'aide des modules incorporés nommés : « NetPass.exe », « WebBrowserPassView », « Mail PassView », « Outlook scraper » et « credential enumerator ».

Dernièrement, les analyses de ce malware ont révélées qu'il est capable de collecter les données sensibles des établissements (Exemples : configuration des systèmes d'exploitation, données confidentielles, localisation géographiques des victimes, etc …) puis de communiquer avec des serveurs C&C afin d'envoyer les données collectées et recevoir les nouvelles commandes d'attaque.

Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

- Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau;
- Mettre à jour immédiatement vos systèmes d'exploitation ;

- S’assurer que les systèmes / firmwares de vos routeurs utilisés sont à jour et ceci depuis leurs sources officielles ;
- N’utilisez pas des mots de passe faibles pour administrer vos équipements réseaux et vos serveurs à distance ;
- Scanner périodiquement votre réseau afin de corriger les vulnérabilités détectées ;
- Appliquer des règles de filtrage rigoureuses pour éviter tout accès non autorisé à vos équipements réseaux via FTP, SSH, Telnet et HTTP/HTTPS et aussi aux partages des ressources via SMB ;
- Pour les e-mails reçus, vérifier l’authenticité et la fiabilité des expéditeurs, s’assurer qu’ils ne comportent pas des erreurs de frappe, des fautes d’orthographe ou des expressions inappropriées et en cas de doute n’y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu’il contient et supprimer le immédiatement.

Enfin, le Centre de Cyber-sécurité du Burkina (BF-CIRT) invite toutes les structures publiques et privées à lui signaler tout cas d’infection constatée sur leurs systèmes d’information en appelant au (+226) 25 37 53 60 – 63 ou en envoyant un courrier électronique à incidents@cirt.bf pour signaler un incident ou à cirt@cirt.bf pour des informations d’ordre général.

Pour plus d’informations techniques, visitez l’adresse https://www.us-cert.gov/ncas/alerts/TA18-201A.

Back to top

Computer Incidents Response Team (CIRT)
01 BP 6437 Ouagadougou 01
Tel : +226 50 37 53 60/61/62 Poste 262 – Fax : +226 50 37 53 64 – Email : cirt@cirt.bf – Web : http://www.cirt.bf