NOTICE DE SECURITE

TLP: CLEAR = **Diffusion sans restriction.**

Les documents avec ce marquage peuvent être diffusés sans restriction, sous réserve du respect des règles de copyright. Les bénéficiaires peuvent partager les documents et informations sans restriction.

URLZone : Un malware bancaire actif ciblant les systèmes Windows			
Référence	CICERT-NTS-2026-025	**Date de 1ère publication**	22/07/2026
Plateforme	Microsoft Windows	**Dernière mise à jour**	22/07/2026
Catégorie	Alertes en cours	**Sévérité**	**Critique**

RISQUES

- Vol d'informations sensibles et d'identifiants
- Compromission des comptes bancaires en ligne
- Exécution de commandes à distance
- Téléchargement et installation d'autres malwares
- Perte de confidentialité des données
- Utilisation du poste compromis comme point d'entrée dans le réseau interne

DESCRIPTION

Le CI-CERT attire l'attention sur la détection d'activités réseau associées au malware URLZone, également connu sous les noms Bebloh ou Shiotob. URLZone est un cheval de Troie bancaire ciblant principalement les systèmes Microsoft Windows. Il est capable de communiquer avec des serveurs de commande et de contrôle (C2) afin de recevoir des instructions, exfiltrer des données et télécharger d'autres charges malveillantes.

MODE DE FONCTIONNEMENT

- Infection du secteur de démarrage (VBR) afin d'assurer sa persistance.
- Exécution avant le chargement du système d'exploitation Windows.
- Dissimulation de sa présence pour échapper à la détection.
- Établissement d'une communication avec un serveur de commande et de contrôle (C2).
- Téléchargement et exécution d'autres logiciels malveillants.
- Réception et exécution de commandes envoyées par l'attaquant

NOTICE DE SECURITE

SYSTEME AFFECTES

- Microsoft Windows

MODE D'INFECTION

URLZone est généralement distribué via :

- Infection initiale du système, généralement via des courriels malveillants, des téléchargements frauduleux ou des sites compromis.
- Installation du malware sur le système Windows ciblé.
- Établissement d'une communication avec un serveur de commande et de contrôle (C2).
- Réception d'instructions à distance depuis l'infrastructure des attaquants.
- Collecte et transmission des informations ciblées.
- Téléchargement et exécution de charges malveillantes supplémentaires.
- Maintien de la persistance sur le système compromis.

ANALYSE TECHNIQUE

IoC :SHA256

538c2aef8837dad9784e306915b50d22a46476df40fe85c4fc11fe453268207f
28ca81fb398691d2103dbacf6b7962cbdc7835c25d7d75bcbca952540d297c20
62a19def1dbca132c4e1d53848356be78df6a1f80947ecb0ed7f76f85a94514f
93db052f216d86750abd09077924f4c05f553d3eba140b3940e7d45107f002f1
a04955e7f68e46ff3d068a945a60285b3ffce607c00bd2f389719b5d45fddaa9
0e7a9a2df9a4db4c537f248ce239aba17bfa3618afcfc30de5d2a460b80b2b55
15896a44319d18f8486561b078146c30a0ce1cd7e6038f6d614324a39dfc6c28
1ede3e09794eb4fbb5a9a67702aeca7495d7b9d12b47dc4493d5f645fa04279d
8c6477d2457a28f715a34e9501d2bf06a17518adefb65910fd644543d91f472f
fcb208a9d8ad4c6ade0798410c3620bb3d57613efd1c01d35bd5b3b42c90db9b
b0752f8ae7d2a4922f018c8f02fd0e20d7674eadf94374734b75e64084af1d84
3e325fe43a78054dad21049abc7ea56510959eb2da5a1e21dae3fe168106cade
d761e6d23070cde26710566a09c847e6c9d112cc973e10a1422d94ae481056f7
79051cfe2b37ddc439c18bc0c1856958dd026a7a6dd0a24de4222d91dbfda22c
03fe36e396a2730fa9a51c455d39f2ba8168e5e7b1111102c1e349b6eac93778
6badf0748ca6cbd4a1f1175dbb8a6dbbee1656c7086378418e1397bce025aa60
a81763026ec8170cffede178386fe07912ae458cf530561770ba969d677a06a6

RECOMMANDATIONS

NOTICE DE SECURITE

Pour les utilisateurs

- Ne cliquez pas sur les liens ou pièces jointes suspects
- Téléchargez vos logiciels uniquement depuis des sources officielles
- Maintenez votre système et vos applications à jour
- Utilisez un antivirus/EDR et garde-le à jour
- Activez l'authentification multifacteur (MFA)
- Utilisez des mots de passe forts et uniques
- Vérifiez régulièrement vos comptes bancaires
- Évitez les connexions sensibles sur les Wi-Fi publics
- Sauvegardez régulièrement vos données importantes

Pour les entreprises

- Maintenir les systèmes Windows à jour
- Déployer une solution EDR sur les postes de travail
- Mettre en œuvre un filtrage DNS
- Sensibiliser les utilisateurs aux courriels suspects
- Activer l'authentification multifacteur (MFA)
- Mettre en place des règles IDS/IPS pour détecter les communications C2
- Signalez tout incident à cert.incidents@anssi.gouv.ci