ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	Malware " Ranbyus"
Numéro de Référence	59800801/26
Date de Publication	08 Janvier 2026
Risque	Critique
Impact	Critique

« Ranbyus » est un cheval de Troie bancaire conçu pour voler des informations financières sensibles sur les systèmes Windows. Il se distingue par l'utilisation de techniques de type « Man-in-the-Browser », lui permettant de s'injecter dans les navigateurs web afin d'intercepter les identifiants bancaires, les données de formulaires et les cookies de session lors des connexions à des services bancaires en ligne. Diffusé principalement via des campagnes de phishing, des pièces jointes malveillantes ou des sites compromis, Ranbyus communique avec des serveurs de commande et contrôle pour exfiltrer les données volées et recevoir des instructions.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Hashs :

- 8cabd946e566724f51e4e0a9ad7782d4
- 26a0cca661d24799746eb5e926c41b0a0fa8d168
- a75a8644bc9758390ca2eceb6eb9d5267f6fc592642bc3e47862cadaaa2f2056
- 70ed202105feacd60ad60b43c12d71fe
- 0273f991246974931002c7596ae4f02ea5a5aa6d

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- 7483b4f3134a7d7effcd3afcee7babf848d961b58b417f49f772981cebcb6b66

Names :

- SmiaUFtnfDMOhp.exe
- GPG4Win
- Gpg4win
- WL-4c6ba412cc7976a65ee993c6f07f1331-0
- novie__pravila_dobavlenija obijavlenii_avito.com
- avito1.vir
- a75a8644bc9758390ca2eceb6eb9d5267f6fc592642bc3e47862cadaaa2f2056.exe
- smiauftnfdmohp.exe
- ChCzNepjrNzkIc.exe
- image.jpg

Domaines/IP C2:

- eagklqjctjaedi.com
- lknxcqqyjbpckr.com
- yfyrxxclvtslvd.net
- vflnaixoawoibw.cc
- rkdhdyyukmsukq.tw
- walnlekomhptcc.pw
- jtwabgkojurkvk.su
- ummqrccghuvurn.in
- ruqtlfflemojkx.me
- lakbinfqxtibnn.me
- 216.218.185.162

Fichiers créés:

- <startup folder>\calculator.lnk

- <startup folder>\command prompt.lnk
- <startup folder>\google chrome.lnk
- <system folder>\chcznepjrnzkic.exe
- <startup folder>\system check.lnk
- <system folder>\smiauftnfdmohp.exe

Sous clés du registre modifiées:

- HKLM\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list
- HKCU\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

Mutex:

- \Sessions\1{C20CD437-BA6D-4ebb-B190-70B43DE3B0F3}
- \Sessions\174EEDB5A000004F801D084A1AEVOsB_vefNWL
- \Sessions\1c:!users!<user>appdata!roaming!microsoft!windows!ietldcache!
- \Sessions\1InstalledMutex
- \Sessions\1MainConfigMutex
- \Sessions\1v&xEiR43#$
- WindowsUpdateTracingMutex
- 2D5C55C00000035401CFFA99LWRRQTZzVmQnU
- 87b3c64lkj48gd
- InstalledMutex
- v&xEiR43#$