MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Revue de presse des cybermenaces

Centre d'analyse des cybermenaces

#12 – DÉCEMBRE 2025

A retenir

L'ampleur du phénomène des **vols de données** personnelles reste préoccupante. Plusieurs cas particulièrement sensibles tels que la **Fédération Français de Tir**, **France Travail**, **Weda** et l'**Urssaf** ont émaillé l'actualité de ce mois de novembre.

La dernière phase de l'opération **ENDGAME** a permis la saisie de **1 025 serveurs** utilisés pour diffuser des maliciels.

Les **LLM non-censurés** continuent de démontrer leur efficacité dans l'aide à la création d'outils malveillants.

Chiffre du mois

1 300 communes françaises auraient été touchées par une fuite de données. Elle aurait été causée par la compromission de la plateforme de gestion de prises de rendez-vous administratifs **Synbird** utilisée par les mairies concernées. Les données dérobées contiendraient les noms, prénoms, codes postaux, adresses de courriels et numéros de téléphone des administrés. Le Parisien

Principales cyberattaques

Fin octobre 2025, l'entreprise de services numériques toulousaine **Partitio**, filiale de **Konica Minolta**, a subi une cyberattaque revendiquée par le groupe de rançongiciel **INC Ransom**. Des preuves du vol de données ont été publiées, bien que l'impact opérationnel semble limité. La direction a confirmé l'incident, indiquant que les investigations techniques étaient en cours. LeMagIT

Les opérateurs du groupe de rançongiciel *(RaaS)* ***Stormous*** ont revendiqué une exfiltration de données de **30 000 comptes de France Travail**. Un communiqué de presse de la structure a confirmé le vol des données. Les premières investigations indiquent que les attaquants ont exploité des identifiants de connexion dérobés via des logiciels de type cleptogiciel. Solutions Numériques & Cybersécurité France Info

Le 14 novembre, l'**Urssaf** a confirmé un vol massif de données visant le service **Pajemploi.** Il est utilisé pour déclarer et rémunérer les assistants maternels et gardes d'enfants. Jusqu'à 1,2 million de professionnels pourraient être concernés. Les données dérobées comprennent des informations personnelles qui pourront être exploitées pour mener des fraudes ou des usurpations d'identité. Urssaf CNEWS

Mi-novembre, le logiciel médical **Weda** (groupe Vidal), utilisé par **23 000 praticiens**, a été mis hors-service après une cyberattaque, perturbant l'activité de nombreux établissements de santé. Dans le même temps, la plateforme de soins **Itélis** a subi une attaque similaire, provoquant des **difficultés d'accès aux dossiers médicaux**. Des données personnelles auraient été exposées. Acuité NEXT

Des **espions** supposément chinois ont exploité six **vulnérabilités** pour compromettre **50 000 routeurs ASUS** en fin de vie et qui ne bénéficient plus de mises à jour de sécurité. Cette campagne intitulée « **Operation WrtHug** » par les chercheurs qui l'ont détectée permet de prendre la main sur ces serveurs et de mener des opérations d'espionnage à grande échelle. 01Net

Le 26 novembre, la **Fédération Française de Football** a informé ses licenciés d'un **vol de données** consécutif au piratage d'un logiciel de gestion administrative utilisée par les clubs. Les données dérobées contiendraient le nom, prénom, genre, date et lieu de naissance, nationalité, adresse postale, adresse de courriel, numéro de téléphone et numéro de licencié. FFF La Dépêche

Pour aller plus loin…

[Trend Micro] Rapport de Trend Micro Research sur l'évolution des tactiques de **cyberespionnage** parmi les menaces persistantes avancées (**APT**) alignées avec la **Chine**.

[ENISA] L'agence de l'Union européenne pour la cybersécurité publie une **analyse sectorielle** relative aux menaces visant les **administrations** publiques.

[Trend Micro] Rapport sur les perspectives pour 2026 sur l'**usage** de l'**IA** par les **cybercriminels**.

Faits marquants

La **Fédération française de tir** (FFTir) a confirmé un **vol de données**, survenu à la mi-octobre, relatif à plus de 274 000 licenciés, incluant état-civil, coordonnées et numéros de licence. L'échantillon diffusé sur les forums cybercriminels alimente des craintes quant à une **possible exploitation par des individus malveillants** cherchant à identifier des tireurs sportifs pour leur dérober leur arme. En novembre, **plusieurs faits** ont été signalés à **Paris**, **Nice** et **Limoges**. Ces événements renforcent l'attention portée à l'usage potentiel des données compromises. Une enquête est en cours, menée par la **BL2C** sous l'autorité du **Parquet de Paris**. Cybermalveillance La Dépêche France 3 Régions

Du 10 au 13 novembre, la dernière phase de l'opération **ENDGAME** a permis de démanteler **1 025 serveurs** utilisés pour diffuser des maliciels tels que **Rhadamanthys**, **VenomRAT** et **Elysium**. L'opération, coordonnée par **Europol** et **Eurojust**, a entraîné plusieurs perquisitions, la saisie de noms de domaines et l'interpellation d'un suspect lié à VenomRAT. Europol

Les investigations menées par **Le Monde**, **Bayerische Rundfunk** (Allemagne), l'**Echo** (Belgique), et la **BNR** (Pays Bas) révèlent les conséquences de la **mise en vente de millions de données de localisation collectées *via* des applications mobiles**. L'analyse d'un échantillon de 278 millions d'enregistrements en Belgique, montre que certains trajets de hauts responsables de la Commission européenne et du Parlement peuvent être reconstitués. Ces informations, vendues par des courtiers en données, permettent d'identifier les **lieux de résidence**, les **déplacements** et les **accès à des sites sensibles**. Le Monde

Informations sur la menace

L'agence centrale américaine de cybersécurité (**CISA**) a publié une mise à jour de son analyse consacrée à la famille de rançongiciel **Akira**. Le document signale pour la première fois le chiffrement d'une machine virtuelle **Nutanix AHV** en juin 2025. Cette évolution étend les capacités du groupe à d'autres environnements de virtualisation, *via* l'exploitation d'une vulnérabilité **SonicWall**. La solution Nutanix AHV étant utilisée par près de **25 000 entreprises dans le monde**, dont plusieurs acteurs français majeurs, cette adaptation technique marque une étape notable dans l'activité du rançongiciel. CISA

Les chercheurs d'**Unit42** ont testé les dernières versions de LLM non-censurés **WormGPT 4** et **KawaiiGPT**. Les essais menés sur WormGPT 4 ont démontré la capacité de cette IA à **créer un rançongiciel** permettant de chiffrer des fichiers PDF, rédiger une ransomnote et suggérant des techniques d'exfiltration *via* le réseau TOR. L'autre LLM concerné, KawaiiGPT, a permis de **créer un courriel d'hameçonnage ciblé** accompagné d'un **nom de domaine usurpé** crédible et des liens de **collecte d'identifiants** notamment. Bleeping Computer

Des chercheurs ont signalé une **vulnérabilité** critique dans **7-Zip** (CVE-2025-11001), permettant l'exécution de code à distance et de parcourir les répertoires. Toutes **les versions antérieures à 25.00 sont vulnérables**, exposant les systèmes à une compromission complète. GB Hackers

Le collectif cybercriminel ***ShinyHunters***, connu pour de vastes **vols de données et extorsions**, lance **ShinySp1d3r**, une nouvelle plateforme de **rançongiciel-en-tant-que-service**. L'outil mis à la disposition d'autres groupes permet d'effectuer facilement des attaques et de publier les données volées en cas de refus de payer. Le projet réunit plusieurs acteurs liés à ***ShinyHunters*** et ***Scattered Spider*** sous une bannière commune, ***SLSH***. Bleeping Computer

Le 7 novembre, **Microsoft** a publié une étude sur « **Whisper Leak** », une attaque par canal auxiliaire visant les **modèles de langage à distance**. En observant uniquement le trafic réseau, un attaquant peut **inférer les sujets d'échanges** d'un utilisateur, même chiffrés. Plus l'adversaire collecte d'échantillons, plus la fuite d'information devient précise. Pour un attaquant placé au niveau du fournisseur d'accès à Internet ou du routeur, cette technique pourrait servir à surveiller des **discussions sensibles**. Microsoft

Dans un registre similaire, les chercheurs de **Threat Fabric** ont identifié un **nouveau maliciel** permettant d'espionner les conversations de n'importe quelle messagerie, chiffrée ou non. Ce maliciel nommé **Sturnus** exploite les fonctions d'accessibilité des **smartphones** sous système d'exploitation **Android** lui permettant de capter tout ce qui apparaît à l'écran. Numérama

Anticipation / Réglementation

La **Commission européenne** a validé la création du consortium **DC-EDIC** pour soutenir les biens communs numériques et l'infrastructure souveraine. Basée à Paris et regroupant initialement la France, l'Allemagne, les Pays-Bas et l'Italie, l'entité mutualisera les ressources pour développer des technologies ouvertes et réduire la dépendance extérieure. Son lancement officiel est attendu en décembre 2025. Commission européenne