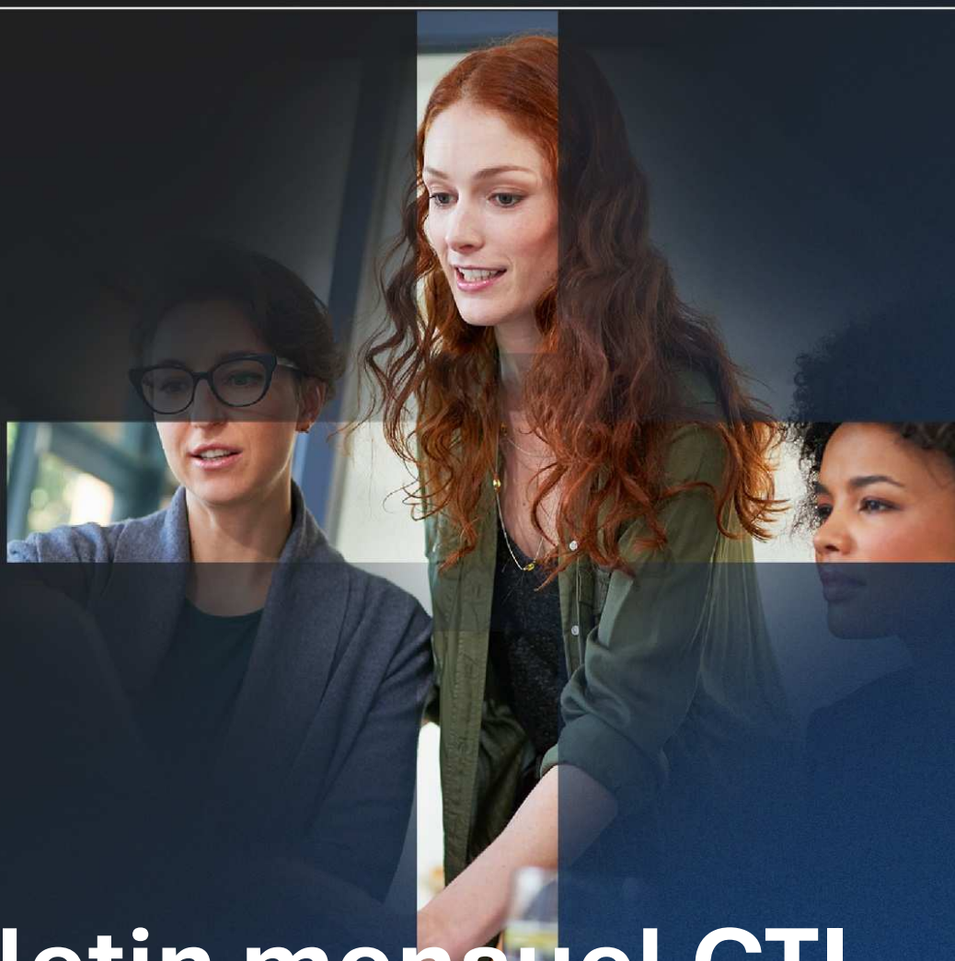
aDvens

For cyber, people & planet



Bulletin mensuel CTI

octobre 2025

CERT aDvens
CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

SOMMAIRE

1. SYNTHÈSE

Ce mois-ci, le CERT aDvens vous propose un panorama des menaces émergentes et des vulnérabilités récemment identifiées :

- Trois nouvelles failles de sécurité ont été détectées, dont une accompagnée d'une *preuve de concept* (PoC). Elles viennent compléter les failles précédemment recensées.
- Une présentation du groupe APT GHOSTWRITTER, lié aux services de renseignement biélorusses, avec une analyse de la chaîne d'attaque de son *malware* PicassoLoader, et de ses TTPs au travers de deux campagnes d'espionnage.

Ces sujets visent à anticiper les risques et à consolider votre posture de cybersécurité.

2. VULNÉRABILITÉS

Ce mois-ci, le CERT aDvens met en exergue **trois** vulnérabilités affectant des technologies fréquemment utilisées au sein des entreprises.
Elles sont présentées par ordre de gravité (preuves de concept disponibles, exploitation ...). L'application de leurs correctifs ou contournements est fortement recommandée.

2.1. Redis - CVE-2025-49844

Le 3 octobre 2025, Redis a publié un bulletin de sécurité concernant la vulnérabilité critique CVE-2025-49844, également nommée RediShell. Découverte par des chercheurs de Wiz, elle serait dans le code source depuis 13 ans.

Un défaut de libération de la mémoire dans Redis permet à un attaquant authentifié, en manipulant le mécanisme de *garbage collector* via un script Lua spécifiquement forgé, d'exécuter du code arbitraire.

2.1.1. Type de vulnérabilité

→ **CWE-416** : Use After Free

2.1.2. Risque

→ Exécution de code abitraire

2.1.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.1.4. Produits impactés

→ Redis OSS/CE/Stack :
- Versions antérieures à 6.2.20
- Versions antérieures à 7.2.11
- Versions antérieures à 7.4.6
- Versions antérieures à 8.0.4
- Versions antérieures à 8.2.2

→ Redis Software (Enterprise) :
- Versions antérieures à 6.4.2-131
- Versions antérieures à 7.2.4-138
- Versions antérieures à 7.4.6-272

- Versions antérieures à 7.8.6-207
- Versions antérieures à 7.22.2-12

2.1.5. Recommandations

- Mettre à jour Redis OSS/CE/Stack vers la version 6.2.20, 7.2.11, 7.4.6, 8.0.4, 8.2.2 ou ultérieure.
- Mettre à jour Redis Software (Enterprise) vers la version 6.4.2-131, 7.2.4-138, 7.4.6-272, 7.8.6-207, 7.22.2-12 ou ultérieure.
- Lorsque la mise à jour immédiate n'est pas possible, il est recommandé de restreindre temporairement l'utilisation des commandes EVAL et EVALSHA via les listes de contrôle d'accès (ACL).

Des informations complémentaires sont disponibles dans le bulletin de Redis.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Veeam Backup & Replication - CVE-2025-48983

Le 14 octobre 2025, Veeam a publié un bulletin de sécurité concernant la vulnérabilité critique CVE-2025-48983.

Cette faille dans le service *Mount* de Veeam Backup & Replication permet à un attaquant authentifié d'exécuter du code arbitraire sur les hôtes de l'infrastructure de sauvegarde.

2.2.1. Type de vulnérabilité

Non identifiée

2.2.2. Risque

- Exécution de code arbitraire

2.2.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Produits impactés

- Veeam Backup & Replication versions comprises entre 12.x et 12.3.2.3617

2.2.5. Recommandations

Mettre à jour Veeam Backup & Replication vers la version 12.3.2.4165 Patch ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de Veeam.

2.2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.3. Apache Tomcat - CVE-2025-55754

Des chercheurs de MOBIA Technology Innovations ont découvert une vulnérabilité critique dans Apache Tomcat.

Un défaut de contrôle des séquences d'échappement ANSI existe dans les messages de journalisation. Un attaquant pourrait, via une URL spécifiquement forgée, injecter des séquences ANSI susceptibles de manipuler l'affichage de la console et le presse-papier, dans le but de tromper un administrateur pour qu'il exécute une commande contrôlée par l'attaquant.

2.3.1. Type de vulnérabilité

- **CWE-150** : Improper Neutralization of Escape, Meta, or Control Sequences

2.3.2. Risque

- Exécution de code arbitraire

2.3.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Requise	Impact sur la disponibilité	Élevé

2.3.4. Produits impactés

Apache Tomcat :

- Versions comprises entre 90.0.0.40 et 9.0.108
- Versions comprises entre 10.1.0-M1 et 10.1.44
- Versions comprises entre 11.0.0-M1 et 11.0.10

2.3.5. Recommandations

- Mettre à jour Apache Tomcat vers la version 9.0.109, 10.1.45, 11.0.11 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin d'Apache.

2.3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

3. BIÉLORUSSIE : LE GROUPE APT GHOSTWRITER

Auteur : Thibaut MADEC

3.1. Introduction

La Biélorussie présente un visage unique en Europe. République issue du démantèlement de l'Union soviétique en 1991, elle est dirigée par Alexandre Loukachenko depuis 1994. Si le communisme d'Etat total fut abandonné pour un nouveau modèle économique plus libéral, de larges secteurs du pays, comme l'agriculture et l'industrie, sont restés imperméables aux privatisations. Très proche ethniquement et culturellement de son voisin russe, le pays vit dans une forte dépendance de la Fédération de Russie, tout en tentant de minimiser les sanctions européennes qui lui sont appliquées. Si la Biélorussie a conscience de sa vassalisation à Moscou, qui se sert de son territoire comme d'une base arrière pour les opérations militaires en Ukraine, elle cherche également à s'imposer comme un espace de négociation entre les parties prenantes de la guerre en Ukraine.

Parfois surnommée « la dernière dictature d'Europe », elle souffre d'une opposition grandissante de sa société civile, une diaspora importante, qui ajoute à la polarisation de ce pays écarté entre deux mondes : passé et présent, Ouest et Est. Le Bélarus offre donc une géopolitique intéressante : à la fois exclu des autres pays du continent européen, et en même temps espace de conciliation entre l'Ouest et Moscou.

Malgré une économie exsangue, Minsk consacre des crédits importants à sa Défense. Cette puissance de troisième ordre semble disposer de deux à trois MOA APT étatiques documentés, ce qui est assez rare. La géopolitique et les enjeux biélorusses seront exposés, en même temps que les capacités cyber qui y sont dédiées. Le groupe APT GHOSTWRITER est ici analysé, avec sa stratégie, sa montée en compétence d'un réseau d'influence à un groupe APT crédible, son propre *malware* PicassoLoader, et ses TTPs dans deux campagnes, menées contre l'Ukraine et la Pologne.

3.2. Géopolitique de la Biélorussie

La parade militaire du Jour de l'Indépendance à Minsk, chaque 3 juillet, offre un spectacle saisissant, donnant à l'observateur l'impression d'être plongé en pleine Guerre Froide.

Figure 1. Défilé militaire de 2019 (Source : Ministère de la Défense de Fédération de Russie, Wikimedias).

Aujourd'hui encore, dans sa politique et son économie, la République de Biélorussie est foncièrement soviétique. Depuis l'extérieur, le pays peut se définir en 3 grands sujets et enjeux :

- Ses liens très étroits avec la Russie,
- Ses liens quasi inexistants avec le reste du continent européen, ou ses mauvaises relations avec ses voisins polonais, lituaniens et lettons,
- Une partie de sa population et de sa diaspora contestataire du régime de l'actuel dirigeant.

3.2.1. Liens avec la Russie

La Biélorussie est très proche culturellement de la Russie. Un projet d'union entre les deux pays fut même imaginé en 1997. La vassalisation du pays à la Russie s'est accélérée depuis 2020 et l'aide apportée par le Kremlin dans la réélection contestée d'A. Loukachenko de 2020. Il en résulte que le territoire biélorusse est utilisé comme base arrière de l'armée russe, et que les intérêts des deux pays sont directement convergents.

3.2.2. Liens avec l'Europe

Le Bélarus est conscient de sa position d'Etat satellite de la Russie, et son dirigeant tente un équilibrage avec le reste de l'Europe. A. Loukachenko n'avait cessé de proposer l'accueil pour une conférence de paix sur le séparatisme russe en Ukraine orientale, amenant aux accords de Minsk I et II. Malgré un isolement diplomatique croissant depuis 2020, Minsk continue à être utilisé comme lieu de rencontres et de négociations entre parties prenantes de la guerre en Ukraine, sous la surveillance du KBG biélorusse. De même, de nombreuses ambassades étrangères sont présentes à Minsk.

3.2.3. Surveillance domestique

Une opposition croissante de la population conteste le régime représenté par A. Loukachenko. Sa réélection de 2020, très fortement remise en cause, a gravement déstabilisé le pays. Une partie de la diaspora biélorusse réfugiée en Pologne, Lituanie et Lettonie voisines travaille à contester le régime biélorusse et appelle à son remplacement. Ce dernier se montre particulièrement autoritaire, réprime toute protestation et surveille sa population, domestique ou expatriée, de manière active.

3.3. Politique cybernétique de la Biélorussie

Pays de 9 millions d'âmes, puissance tertiaire et économie soviétique, la Biélorussie peut pour autant appuyer ses intérêts sur 3 MOA :

- **MOUSTACHEDBOUNCER** : Ce groupe a été documenté en 2023, mais est vraisemblablement actif depuis 2014. Il cible de manière quasi exclusive les ambassades étrangères en Biélorussie et leurs personnels diplomatiques. Il opère son interception au niveau des fournisseurs d'accès Internet dans des attaques de type *Man-in-the-Middle*. Ce groupe a également développé la porte dérobée modulaire NightClub et le *malware* Disco.
- **WINTER WIVERN** (*alias* TA473, UAC-0114 ou Group G1035) : Ce groupe n'a pas d'affiliation formelle mais sert les intérêts russes et biélorusses, et opère depuis 2020. Il se caractérise par des TTPs créatifs pour des moyens limités, notamment en exploitant la CVE-2023-5631 qui affecte les portails *webmail* Roundcube. Il cible des entités publiques européennes et parfois asiatiques, ou certaines entreprises, à des fins d'espionnage dans le contexte de la guerre en Ukraine. **La CTI Advens avait publié un article sur ce groupe APT dans le bulletin mensuel de mars 2024**.
- **GHOSTWRITER** (*alias* UNC1151, UAC-0057, Storm-0257, FrostyNeighbor, Blue Dev 4, Moonscape ou TA445) : Actif depuis 2016, le groupe a été documenté pour la première fois en 2020, et est formellement affilié aux services de renseignement de Minsk. Il cible à la fois les pays d'Europe de l'Est pro-OTAN et des citoyens biélorusses. A ses débuts, GHOSTWRITER s'était spécialisé dans des campagnes de désinformation avec la rédaction de faux articles, d'où son nom. Le groupe a fait évoluer ses compétences après 2020 et opère des campagnes d'espionnage. Il a également développé son propre *malware* : PicassoLoader.

Dans l'actuel état de la recherche, l'implication du Kremlin est aujourd'hui suspectée dans cette récente montée en compétence, bien qu'aucun élément concret ne puisse venir le confirmer formellement. La

> collaboration entre les agences de renseignement, notamment le FSB russe et le KGB biélorusse, est déjà effective et entérinée officiellement par A. Loukachenko. La Biélorussie avait montré de sérieuses lacunes techniques dans sa gestion des troubles internes de 2020, notamment contre le groupe Cyber Partisans, composé de dissidents et d'anciens officiers. Ces défaillances semblent incompatibles avec le niveau affiché aujourd'hui par GHOSTWRITER.

3.4. GHOSTWRITER

Le groupe tire son nom de ses premières campagnes de désinformation à partir de 2016 : il dérobait des identifiants réels de journalistes, éditorialistes et blogueurs afin de publier des articles en leurs noms dans un narratif anti-OTAN en Europe centrale et orientale. Les supports étaient variés ; journaux en ligne, blogs, réseaux sociaux, dans un objectif d'influence et de désinformation. Ces articles sont relayés dans un second temps par courriel et sur des réseaux sociaux. Le nom GHOSTWRITER renvoie indistinctement au groupe et à la campagne d'influence, continue depuis 2016. Cette campagne s'articulait autour d'un narratif anti-OTAN avant 2020. À partir de mi-2020, ce narratif évolue ensuite spécifiquement contre les voisins directs de la Biélorussie.

Depuis 2016, des noms de domaine usurpant des ressources légitimes sont enregistrés afin d'exfiltrer des identifiants de médias, de fournisseurs de messagerie web régionaux, des administrations nationales et locales, ainsi que des entreprises privées. Les pays ciblés sont l'Ukraine, la Pologne, la Lituanie, la Lettonie, l'Allemagne, mais également la France, l'Espagne et l'Irlande (et notons l'exception notable de l'Estonie). Des médias biélorusses et personnalités publiques d'opposition ont également été ciblées en Biélorussie.

Le groupe affine ses TTPs après 2020 : Il utilise GoPhish pour les envois de courriels d'hameçonnage avec le service SMTP2GO pour se légitimer. CloudFlare est désormais utilisé pour l'hébergement à la place de Freenom, ce qui peut indiquer une augmentation de ses crédits.

Deux petits *malwares* sont développés en .NET avec des fonctionnalités de commandes basiques :

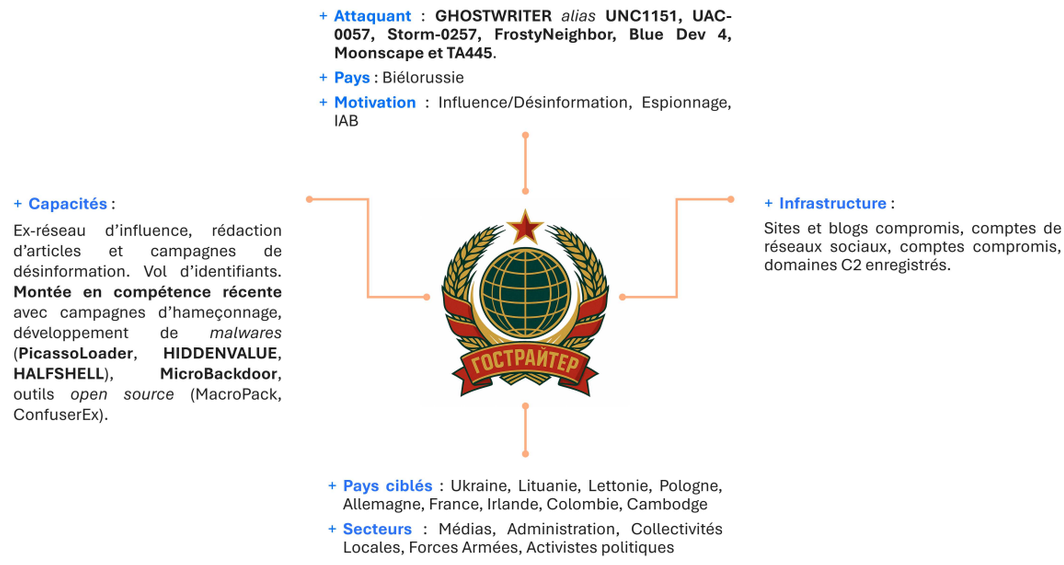
- HIDDENVALUE : Porte dérobée distribuée par courriel d'hameçonnage. Elle permet l'exécution de commandes à distance et la collecte d'information sur la machine compromise.
- HALFSHELL : Variante, qui offre de nouvelles commandes des techniques d'évasion.

L'activité se poursuit en 2022 avec l'offensive russe en Ukraine, et le ciblage d'utilisateurs ukrainiens Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki (Ok.ru, réseau social russophone) et VK, toujours dans un but de désinformation. Cependant, le MOA suivi comme UNC1151/GHOSTWRITER semble se consacrer de plus en plus à l'espionnage, plutôt qu'aux opérations d'influence, et change d'envergure. Le 07 mars 2022, le CERT-UA publie une alerte sur le ciblage d'entités publiques ukrainiennes pour distribuer MicroBackdoor *via* des courriels d'hameçonnage et attribué à UNC1151. MicroBackdoor est une porte dérobée *open source* utilisée pour la communication C2.

À partir de 2022, le CERT-UA émet plusieurs alertes sur la distribution d'un nouveau *malware* PicassoLoader. Les Ukrainiens attribuent officiellement le développement de ce produit malveillant à UNC1151/GHOSTWRITER.

Les ressources ou infrastructures n'indiquent aucun chevauchement avec les groupes APT de la Fédération de Russie, cependant certaines activités de ces derniers sont fortement convergentes avec celles de GHOSTWRITER à des périodes similaires.

La matrice diamant suivante illustre les activités de GHOSTWRITER à un échelon stratégique :



3.5. PicassoLoader

Le *malware* tire son nom de l'utilisation de fichiers JPEG utilisés pour dissimuler la charge utile dans une superposition de fichiers.

Dans un premier incident, le CERT-UA identifie le 16 mars 2023 une campagne de courriels d'hameçonnage avec un document PPT en pièce jointe, comportant une miniature de l'Université de Défense Ivan Chernyakhivsky, l'Académie Militaire ukrainienne, et une macro. Son ouverture génère le fichier APPDATA%\Signal_update_6.0.3.4\glkgh90kjykjkl650kj0.dll avec un raccourci pour l'exécuter. glkgh90kjykjkl650kj0.dll est identifié comme PicassoLoader, doit télécharger une image et la déchiffrer pour lancer Cobalt Strike Beacon.

Dans un deuxième incident signalé le 23 juillet 2023, le CERT-UA identifie le ciblage d'organismes publics ukrainiens par des courriels d'hameçonnage comportant cette fois des documents XLS. PerekazF173_04072023.xls et Rahunok_05072023.xls contiennent une macro légitime, et une autre permettant de lancer PicassoLoader et d'en assurer la persistance. Le *malware* comporte une nouvelle fonctionnalité : il ne s'exécute pas s'il détecte Avast, FireEye ou Fortinet sur l'ordinateur de la victime (en recherchant les processus AvastUI.exe, AvastSvc.exe, xagt.exe, fcappdb.exe, FortiWF.exe). PicassoLoader télécharge ensuite, déchiffre et lance le cheval de Troie njRAT.

L'analyse d'un incident indique comment les victimes sont incitées à déclencher les macros :

- Un fichier Excel comportant des macros (XLSM) envoyé dans un courriel se fait passer pour un tableau de calcul de salaire de personnels ukrainiens.
- La macro est nommée « sumpropua », abréviation de « Suma Propisom UA », une translittération latine de l'ukrainien « сума прописом UA ». Ce terme désigne des documents financiers où le montant total versé doit être indiqué en toutes lettres.
- Ce procédé de conversion monétaire en lettre est fastidieux et l'utilisation de macros y est courante pour remplir automatiquement les cellules.

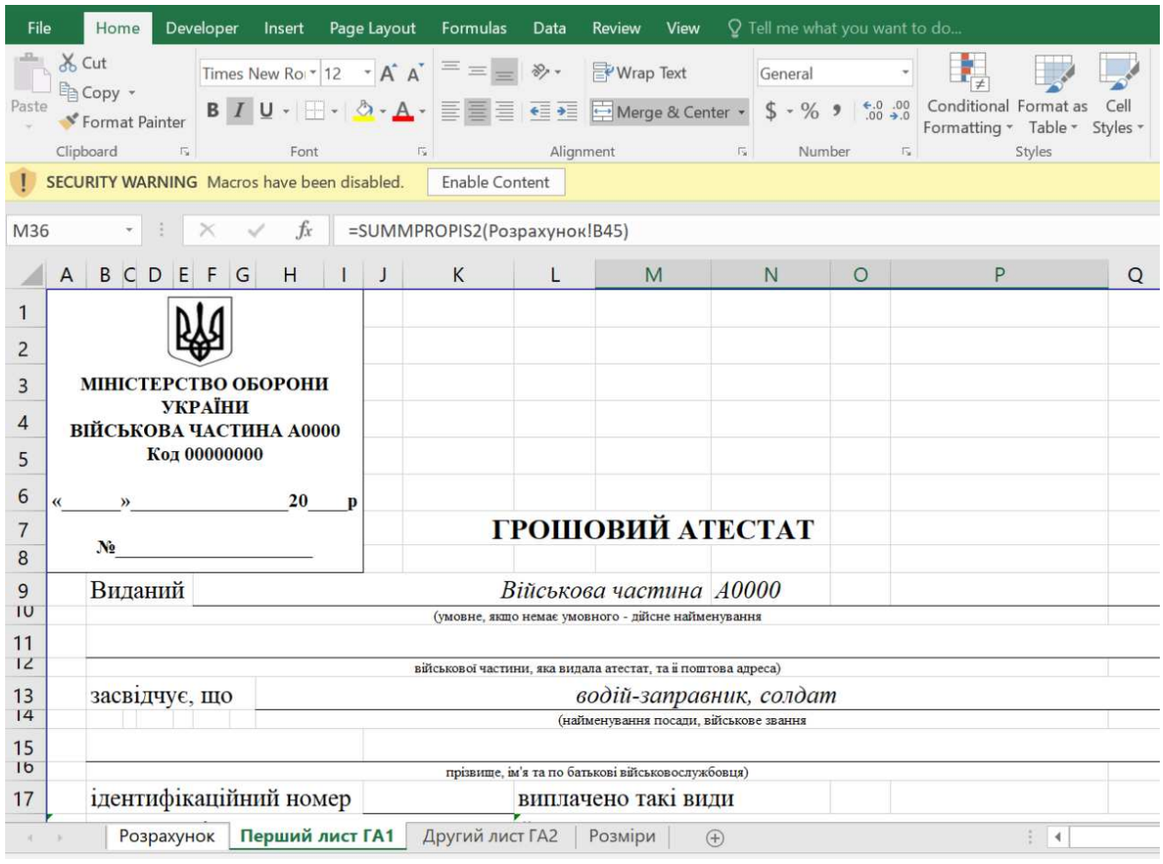


Figure 2. Document XLSM malveillant distribué en PJ (Source : Fortinet).

La fonction malveillante *SUMMPROPIS2* s'exécute quant à elle dès l'ouverture du fichier *via* la fonction *Workbook_Open()*. Cette fonction malveillante est présente dans plusieurs cellules, ce qui permet au *malware* de s'exécuter plusieurs fois après l'ouverture du fichier. Le code VBA utilise des obfuscations simples pour éviter la détection, le fichier binaire malveillant intégré est encodé sous forme de chaîne hexadécimale.

Parallèlement, la fonction malveillante principale *OpenModule* décode un fichier binaire à partir de cette chaîne et l'enregistre dans le répertoire *%AppData%\Microsoft\fhasbqwn.dll*.

3.5.1. Premier chargement

Le chargeur de la première étape est exécuté avec la commande suivante :

```
C:\Windows\System32\regsvr32.exe /u /s « %AppData%\Microsoft\fhasbqwn.dll
```

L'option /s permet une exécution silencieuse sans aucune ouverture de boite de dialogue Windows. L'option /u entraîne l'exécution de la fonction exportée *DllUnregisterServer*. Cette DLL est protégée par ConfuserEx, un outil *open source* de protection des applications .NET, afin d'empêcher toute analyse.

Une seconde fonction exportée *DllCanUnloadNow* est exécutée avec la commande suivante :

```
C:\Windows\System32\rundll32.exe %Temp%\kbdlisus.dll,DllCanUnloadNow
```

Un fichier JPEG apparemment inoffensif est téléchargé depuis un nom de domaine enregistré par les attaquants (ici hxxps://ellechina[.]online/01_logo_HLW-300x168[.]jpg)

Figure 3. Exemple d'image téléchargée (Source : Fortinet).

Des données binaires supplémentaires dans le JPEG contiennent le chargeur de seconde étape, chiffré et compressé dans une superposition de fichiers. Cette superposition est déchiffrée avec l'algorithme AES, avec une clé codée en dur. Un autre fichier .NET sdafsfdpieowrfb.exe est ainsi extrait, lui aussi protégé par ConfuserEx.

Voici d'autres exemples d'images téléchargées par PicassoLoader (Source : Cisco Talos) :

3.5.2. Second chargement

Ce chargeur de deuxième niveau recherche des processus d'analyse anti-virus précis comme Avast, ou des outils comme Process Explorer et Process Hacker. Si ces processus sont détectés, l'opération est interrompue. Une DLL de troisième palier est extraite et placée dans %AppData%, nommée aléatoirement d'après un sous-répertoire, comme *Adobe.dll* ou *Microsoft.dll* par exemple.

sdafsfdpieowrfb.exe crée ensuite une tâche planifiée nommée « Scheduled », décrite comme « NTFS Volume Health Scan ». Microsoft Corporation est renseigné comme auteur de la tâche afin de passer pour une tâche légitime du système. Au lieu d'utiliser schtasks.exe pour créer la tâche planifiée, le *malware* utilise la fonction COM *ITaskFolder::RegisterTaskDefinition*. Il peut s'agir d'un mécanisme de dissimulation aux EDR, capables de détecter une utilisation suspecte de schtasks.exe. Cette

tâche exécute ensuite la DLL précédemment déposée, afin d'assurer la persistance quand la victime se connecte à Windows.

Cette dernière DLL, développée en C/C++ est un chargeur pour distribuer Cobalt Strike Beacon afin de s'implanter sur l'ordinateur de la victime, avec une adresse URL de serveur C2 identifiée.

Une autre activité de PicassoLoader est rapportée par le CERT-UA entre le 12 et le 18 juillet 2024, ciblant des collectivités territoriales ukrainiennes. L'utilisation de ce *malware* porte la signature exclusive de la menace GHOSTWRITER. Des documents XLS contenant des macros malveillantes sont envoyés par mail au sujet de la réforme des collectivités locales (projets USAID/DAI et HOVERLA). Les agents visés et le thème utilisé dénote d'un ciblage précis de la part de l'attaquant.

3.6. Campagnes de GHOSTWRITER

On observe ainsi que les capacités, les motivations et l'envergure de GHOSTWRITER évoluent fortement à partir de l'offensive de 2022. On suspecte que ces évolutions ont été initiées avant l'offensive, à partir de 2020. L'état actuel du renseignement suspecte également que cette montée en compétence d'un réseau d'influence rédigeant de faux articles, vers un acteur de la menace crédible porté sur l'espionnage et potentiel IAB, s'est faite à l'initiative du Kremlin et avec son aide. Ces hypothèses sont probables compte tenu du rôle de proxy de Moscou joué par le Bélarus, et que son territoire sert de base arrière aux troupes russes sur le théâtre ukrainien.

3.6.1. Campagne de novembre-décembre 2024

Cibles biélorusses

On observe que les TTPs mobilisés contre des cibles ukrainiennes sont également utilisés contre des citoyens biélorusses.

Des courriels d'hameçonnage sont envoyés joignant une archive RAR, contenant un tableur Excel nommé политзаключенные(по судам минска).xls (« Prisonniers politiques (tribunaux de Minsk).xls »). L'archive a été créée le 14 janvier 2025, la temporalité correspondant vraisemblablement à l'élection présidentielle du 26 janvier 2025. À date, c'est la première fois que l'activité GHOSTWRITER est dirigée contre des Biélorusses et non plus contre des personnels étrangers.

Le document XLS contient là encore une macro VBA qui s'active à l'ouverture du document dès que les macros sont autorisées par la victime. Celle-ci crée un fichier DLL dans le répertoire *%Temp%\Realtek(r)Audio.dll*, et lancé par la commande suivante :

```
C:\Windows\System32\regsvr32.exe /u /s "C:\Temp\Realtek(r)Audio.dll”
```

Il lance regsvr32.exe qui active la fonction *DllUnregisterServer* implantée dans la première DLL, qui charge et exécute Dwnldr.dll. Celui-ci est protégé par ConfuserEx, selon un mode opératoire déjà rencontré chez UNC1151. Cette dernière DLL héberge une version simplifiée de PicassoLoader. Ce variant semble avoir été modifié pour en faire un outil moins coûteux et plus facilement remplaçable.

Dwnldr.dll crée un tableau Excel leurre dans *%AppData%\Roaming\Microsoft\temp.xlsx*, tout en téléchargeant d'autres fichiers depuis Internet. Le fichier temp.xlsx est immédiatement ouvert dans Excel afin de faire croire à la victime qu'il consulte la pièce jointe политзаключенные(по судам минска).xls :

	A	B	C	D	E	F	
1	Имя и фамилия	Предъявленые обвинения	Решение суда	Вид наказания	Судья	Прокурор	Место з
2	Троцкий Василий	ст. 369 Уголовного кодекса — Оскорбление представителя власти	1 год и 2 месяца	лишение свободы в колонии в условиях общего режима	Андрушенко Андрей	Ярошникова	освобож
3		ст. 391 Уголовного кодекса — Оскорбление судьи					
4							
5	Синяк Евгений	ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок, либо активное участие в них	2 года	ограничение свободы с направлением в исправительное учреждение открытого типа ("химия")	Маручек Сергей	Ярошик, Плышевский	
6							
		ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок,		ограничение свободы без направления в			

Sheet1

Figure 4. Fichier contenant une liste de personnes inculpées avec des noms de procureurs et de juges (Source : SentinelOne).

L'origine des données pour tromper la victime fait preuve d'une ingénierie sociale redoutable. Si les données affichées peuvent faire croire à une fuite gouvernementale, ces données sont en réalité issues du site Spring96, un site d'opposition politique interdit en Biélorussie.

Pendant ce temps, Dwnldr.dll récupère un fichier JPG depuis un nom de domaine appartenant aux attaquants :

Figure 5. Fichier récupéré depuis hxxps://everythingandthedog[.]shop/petsblog/2020/2/25/tips-for-taking-difficult-dogs-on-a-walk[.]jpg (Source : SentinelOne)..

La requête HTTP est émise avec une chaîne User-Agent codée en dur :

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/555.36 (KHTML, like Gecko) Chrome/97.0.4692.71
Safari/537.36
```

Le fichier JPG est ici bénin et provient d'une banque d'image en sources ouvertes. La même image existe sur le site légitime hxxps://www.everythingandthedog[.]com, copié par les attaquants. Le fichier est ensuite renommé et enregistré dans *%APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll*. Il est ainsi enregistré pour être chargé au démarrage de la machine.

L'analyse révèle que ce fichier JPG est réellement inoffensif. La distribution de la charge utile est gérée par les attaquants seulement après vérification de plusieurs informations : *UserAgent*, adresses IP etc... De précédents incidents sur des cibles

ukrainiennes montrent que la charge utile n'est distribuée que sur des machines comportant une IP ukrainienne.

Cibles ukrainiennes

La même activité a ciblé des personnels ukrainiens à la même période, avec de légères variations. Les courriels d'hameçonnage sont envoyés avec le thème d'une initiative anti-corruption au sein des agences gouvernementales ukrainiennes. Les attaquants ont utilisé Macropack, un outil d'obfuscation *open source* aujourd'hui abandonné, pour écrire les macros d'autres documents XLS malveillants.

Du reste le *pattern* est le même qu'observé précédemment. Une fois la macro exécutée, une DLL .NET obfusquée lance une fonction exportée *via* rundll32.exe. Un document leurre s'affiche pendant qu'un fichier image est téléchargé depuis le domaine hxxps://sciencealert[.]shop. Encore une fois, la même image est disponible depuis un domaine légitime hxxps://www.sciencealert[.]com copié par les attaquants. Une fois téléchargé, le *malware* décompresse le fichier à l'emplacement suivant *%APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll*.

Un fichier texte de configuration est créé dans *%APPDATA%\Roaming\Microsoft\SystemCertificates\config*.

Ce dernier est utilisé pour exécuter MSBuild.exe qui compile une nouvelle application : *C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe %AppData%\Roaming\Microsoft\SystemCertificates\config*

Si la commande réussit, un fichier est créé à cet emplacement, qui contient la charge utile finale : *%AppData%\Roaming\Microsoft\SystemCertificates\Bin\Certificate.exe*

D'autres campagnes d'hameçonnage ont ciblé des entités ukrainiennes aux mêmes dates avec pour thème le ravitaillement des forces armées. Des documents XLS joints contiennent des macros malveillantes, la chaîne d'infection suit ensuite le même *pattern*.

3.6.2. Campagne d'avril 2025

En juillet 2025, une campagne est observée active depuis avril 2025 et attribuée à GHOSTWRITER, qui cible l'Ukraine et la Pologne. Cette fois, les fichiers XLS malveillants sont compressés dans des archives, probablement distribuées par courriels malveillants. Les fichiers XLS exécutent des macros VBA, qui créent des fichiers DLL chargés par regsvr32.exe. Cette première DLL est obfusquée avec ConfuserEx, collecte des informations et les envoie à un serveur C2 auprès de qui elle récupère les instructions de la deuxième étape.

Cibles ukrainiennes

Le fichier leurre покрокова інструкція.pdf (« instruction étape par étape ») contenu dans l'archive a été créé le 30 mai 2025. Un document légitime similaire a été publié le 17 avril 2025 par le Ministère de la Transformation Numérique d'Ukraine. L'archive contient également des fichiers XLS dont la chaîne d'infection menant à la DLL évolue entre juin et juillet 2025. En voici trois exemples :

- Une macro VBA enregistre une DLL dans *%TEMP%\DefenderProtectionScope.log* et utilise la méthode Shell.ShellExecute pour la charger avec la commande *regsvr32 /u /s %TEMP%\DefenderProtectionScope.log*.
- Une macro VBA déchiffre la DLL et l'enregistre dans *%LOCALAPPDATA%\Serv\0x00bac729fe.log*. Elle crée ensuite un fichier LNK (*%APPDATA%\Microsoft\Windows\Protection overview.lnk*) configuré pour exécuter la commande *C:\Windows\System32\regsvr32.exe /u /s "%LOCALAPPDATA%\Serv\0x00bac729fe.log"*.
- Un autre exemple ne dépose pas directement de DLL, mais écrit d'abord un fichier Microsoft Cabinet (CAB) dans *%TEMP%\sdw9gobh0n*. Un fichier LNK est créé qui utilise expand.exe pour extraire la DLL du fichier CAB vers *%LOCALAPPDATA%\Logs\sdw9gobh0n.log*.

Cette DLL sert à télécharger un chargeur de second temps pour collecter des informations sur les machines compromises :

- Identifiant et version de la plateforme du système d'exploitation,
- Nom d'hôte,
- Nom du processeur (*via* une requête WMI),

- Nom d'utilisateur actuel,
- Date d'installation du système d'exploitation (*via* une requête WMI),
- Date de démarrage du système,
- Nom et date d'installation du produit antivirus installé (*via* une requête WMI),
- Informations sur l'adresse IP utilisée pour la navigation Internet (obtenues par une requête HTTP GET à l'adresse hxxps://ip-info.ff.avast[.]com/v1/info).

Ces informations sont ensuite envoyées au C2 via une requête HTTP POST, ici par exemple hxxps://punandjokes[.]icu/cannabis-jokes.jpg. Des informations sont envoyées toutes les 10 minutes, une tentative pour télécharger la prochaine séquence est initiée toutes les 30 minutes. Une fois celle-ci récupérée, elle est enregistrée dans *%APPDATA%\Microsoft\System\ProtectedCertSystem.dll*. Elle est exécutée avec la commande suivante :

```
rundll32 %APPDATA%\Microsoft\System\ProtectedCertSystem.dll,#1
```

Cibles polonaises

La même activité a ciblé la Pologne avec des documents 1_39ZO ZGWRP_zaproszenie.pdf en polonais. Cette invitation à l'assemblée générale de la Związek Gmin Wiejskich Rzeczypospolitej Polskiej (Union des Communes Rurales de Pologne) confirme encore la tendance de GHOSTWRITER à cibler des collectivités locales. Là encore, le document PDF est copié sur un PDF légitime créé le 21 avril 2025 par les autorités polonaises. Les autres documents XLS malveillants contiennent des macros développées avec MacroPack qui suivent des processus identiques de ceux déjà observés.

La DLL développée en C++ génère une deuxième DLL enregistrée dans l'emplacement *%APPDATA%\DiagnosticComponents\DiagnosticComponents.dll*.

Elle utilise là encore l'interface COM du planificateur de tâches Windows pour enregistrer la tâche planifiée \ExpDiagnosticDataSettings qui doit exécuter DiagnosticComponents.dll. Cette dernière sert de chargeur pour Cobalt Strike Beacon qui communique avec un serveur C2 distant (ici hxxps://medpagetoday[.]icu).

Les infrastructures C2 identifiées sont les mêmes dans les activités qui ont ciblé l'Ukraine et la Pologne. Pour chacun des domaines enregistrés, les attaquants utilisent les serveurs proxies Cloudflare. Les noms de domaine usurpent là encore des sites légitimes (par exemple medpagetoday[.]icu copie medpagetoday[.]com).

On note que le nom de domaine sweetgeorgiayarns[.]online, utilisé comme C2 par les attaquants, redirige automatiquement vers le site légitime curseforge[.]com qui traite de jeux vidéos. Un site curseforge[.]icu, enregistré de la même manière, opère la même redirection vers curseforge[.]com. Il n'est pas confirmé si cette redirection est volontaire ou non. Cette configuration pourrait permettre de contourner les services de filtrage web.

3.7. Matrice MITRE ATT&CK

INITIAL ACCESS

T1566.001 : Phishing: Spearphishing Attachment T1190 : Exploit Public Facing Application

EXECUTION

T1053.005 : Scheduled Tak/Job : Scheduled Task T1059.005 : Command and Scripting Interpreter : Visual Basic T1059.006 : Command and Scripting Interpreter : Python T1203 : Exploitation for Client Execution

PERSISTANCE

T1547.001 : Boot or Logon Autostart Execution : Registry Run Keys / Startup Folder

DEFENSE EVASION

T1218.005 : System Binary Proxy Execution: Mshta T1112 : Modify Registry T11140 : Deobfuscate/decode files or information T1027 : Obfuscated Files or Information T1208.011 : System Binary Proxy Execution: Rundll32 T1218.010 : System Binary Proxy Execution: Regsvr32

PRIVILEGE ESCALATION

T1574.002 : Hijack Execution Flow: DLL Side-Loading

DISCOVERY

T1057 : Process Discovery T1518.001 : Security Software Discovery

IMPACT

T1491 : Defacement T1486 : Data Encrypted for Impact T1498 : Network denial of service

COMMAND AND CONTROL

T1071 : Application Layer Protocol T1105 : Ingress Tool Transfer

3.8. Conclusion

GHOSTWRITER présente un profil inédit et unique dans l'environnement des unités APT étatiques. À la base réseau d'influence, spécialisé dans la rédaction de faux articles, sorte de ferme à trolls améliorée, le groupe a capitalisé sur ses capacités de vol d'identifiants pour se renouveler totalement. Ce renouvellement ne s'est à priori pas fait sur la base des seules compétences des membres ou du KGB biélorusse, et pose l'hypothèse de programmes d'échanges entre services et officiers russes et biélorusses. Peu importe, car GHOSTWRITER, avec de nouvelles tactiques, et de nouveaux outils, se positionne aujourd'hui comme acteur de la menace crédible.

Outre son historique unique, GHOSTWRITER conserve encore à ce stade une identité particulière, avec des noms de domaine copiant des sites légitimes, ou des charges utiles camouflées dans des images.

Ceci étant dit, avec son changement d'envergure, GHOSTWRITER peut être amené à prendre un rôle plus actif et moins confidentiel en Europe. Si l'acteur s'est pour l'instant concentré sur l'Ukraine et ses voisins immédiats, les intérêts biélorusses peuvent l'amener à cibler d'autres pays d'Europe occidentale. D'après Mandiant, le groupe a déjà enregistré un nom de domaine imitant un site de l'armée française en 2021. Cette montée en puissance attendue peut se faire à l'iniative du Bélarus, ou pour mener des attaques par proxy pour le compte de Moscou.

3.9. Indicateurs de compromission

TLP	TYPE	VALEUR	DESCRIPTION
TLP:CLEAR	SHA-256	5df1e1d67b92e2bba8641561af9967e3a54ec73600283c66b09c8165ddcb7de9	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	699c50014cdbe919855c25eb35b15dfc8e64f73945187da41d985a9d7be31a71	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	26ea842c4259c90349a1f4db92efa89ac4429a5ff380e7f72574426cfd647f1a	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	6e562afa3193c2ca5d2982e04de78cf83faa203534a6098ab5f08df94bbeb944	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	3fff6c8a8ef3f153ebbe6d469a0d970953358a25bb9b4955a2592626f011cbd6	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	730c1a02bb31d548d91ba23fce870b1dc53c4802ea4fcb0d293f96de670d74af	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	57e0280dc5b769186588cc3a27a8a9be6f6e169551bbef39f95127e9326627f2	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	f6fec3722a8c98c29c5de10969b8f70962dbb47ba53dcbcd4a3bbc63996d258d	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	deaa3f807de097c3bfff37a41e97af5091b2df0e3a6d01a11a206732f9c6e49c	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	aac430127c438224ec61a6c02ea59eb3308eb54297daac985a7b26a75485e55f	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	06380c593d122fc4987e9d4559a9573a74803455809e89dd04d476870a427cbe	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	082877e6f8b28f6cf96d3498067b0c404351847444ebc9b886054f96d85d55d4	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	082903a8bec2b0ef7c7df3e75871e70c996edcca70802d100c7f68414811c804	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	69636ddc0b263c93f10b00000c230434febbd49ecdddf5af6448449ea3a85175	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	a2a2f0281eed6ec758130d2f2b2b5d4f578ac90605f7e16a07428316c9f6424e	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	8a057d88a391a89489697634580e43dbb14ef8ab1720cb9971acc418b1a43564	Campagne contre l'Ukraine de juillet 2025

TLP	TYPE	VALEUR	DESCRIPTION
TLP:CLEAR	SHA-256	707a24070bd99ba545a4b8bab6a056500763a1ce7289305654eaa3132c7cbd36	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	5fa19aa32776b6ab45a99a851746fbe189f7a668daf82f3965225c1a2f8b9d36	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	c7e44bba26c9a57d8d0fa64a140d58f89d42fd95638b8e09bc0d2020424b640e	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	7c77d1ba7046a4b47aec8ec0f2a5f55c73073a026793ca986af22bbf38dc948c	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	SHA-256	559ee2fad8d16ecaa7be398022aa7aa1adbd8f8f882a34d934be9f90f6dcb90b	Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	MD5	e34d6387d3ab063b0d926ac1fca8c4c4	довідка.zip
TLP:CLEAR	MD5	2556a9e1d5e9874171f51620e5c5e09a	dovidka.chm
TLP:CLEAR	MD5	bc6932a0479045b2e60896567a37a36c	file.htm
TLP:CLEAR	MD5	bd65d0d59f6127b28f0af8a7f2619588	ignit.vbs
TLP:CLEAR	MD5	fb418bb5bd3e592651d0a4f9ae668962	Windows Prefetch.lNk
TLP:CLEAR	MD5	a9dcaf1c709f96bc125c8d1262bac4b6	desktop.ini
TLP:CLEAR	MD5	d2a795af12e937eb8a89d470a96f15a5	core.dll (.NET-лоадер)ukr
TLP:CLEAR	MD5	65237e705e842da0a891c222e57fe095	microbackdoor.dll (MicroBackdoor)
TLP:CLEAR	SHA-256	4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b	Document XLSM
TLP:CLEAR	SHA-256	c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8	fhasbqwn.dll - Chargeur de premier niveau
TLP:CLEAR	SHA-256	2927794d7c550c07303199752b8226f197d7ef497d04cf038859f95b60edc9ce	JPEG hébergeant la charge utile
TLP:CLEAR	SHA-256	b03c9f7823810e3eeef3c0b1d6c00da4f16fdc2ced92f97f78e5676d0989d9b3	sdafsfdpieowrfb.exe - chargeur de second niveau
TLP:CLEAR	SHA-256	de8c789ef2e1da81182a7529e7b42adf2984cd6e70b02e60fd770ebe658086ae	Chargeur Cobalt Strike

TLP	TYPE	VALEUR	DESCRIPTION
TLP:CLEAR	SHA-256	815c1571356cf328a18e0b1f3779d52e5ba11e5e4aac2d216b79bb387963c2be	Document Excel malveillant
TLP:CLEAR	SHA-256	6f4642a203541426d504608eed7927718207f29be2922a4c9aa7e022f22e0deb	Document Excel malveillant
TLP:CLEAR	SHA-256	88c97af92688d03601e4687b290d4d7f9f29492612e29f714f26a9278c6eda5b	Document Excel malveillant
TLP:CLEAR	SHA-256	9649d58a220ed2b4474a37d6eac5f055e696769f87baf58b1d3d0b5da69cbce5	Document Excel malveillant
TLP:CLEAR	SHA-256	af8104e567c6d614547acb36322ad2ed6469537cd1d78ae1be65fbde1d578abc	Document Excel malveillant
TLP:CLEAR	SHA-256	de1bceb00c23e468f4f49a79ec69ec8ad3ed622a3ffc08f84c0481ad0f6f592b	Document Excel malveillant
TLP:CLEAR	SHA-256	83545b07d74087acd8408d7810cafdb6c2200a72ae7dd990af40b082ad533368	Document Excel malveillant
TLP:CLEAR	SHA-256	9ac5fa37f5cf3d0201f0e70a3e6527e58250ddcff77370262b8cb377e8c5995f	Document Excel malveillant
TLP:CLEAR	SHA-256	d90f6e12a917ba42f7604362fafc4e74ed3ce3ffca41ed5d3456de28b2d144bf	Chargeur DLL
TLP:CLEAR	SHA-256	08fa6aaf064470dbfac7894469457b2d78541adccba3f1bb278dd4c3f936131a	Chargeur DLL
TLP:CLEAR	SHA-1	18151b3801bd716b5a33cfc85dbdc4ba84a00314	temp.xlsx
TLP:CLEAR	SHA-1	2c06c01f9261fe80b627695a0ed746aa8f1f3744	Донесення 5 реч фонд зборів- зразок.xls
TLP:CLEAR	SHA-1	301ffdf0c7b67e01fd2119c321e7ae09b7835afc	Zrazok.xls
TLP:CLEAR	SHA-1	853da593d2a489c2bd72a284a362d7c68c3a4d4c	Додаток 8 реч новий.xls
TLP:CLEAR	SHA-1	9d110879d101bcaec7accc3001295a53dc33371f	Донесення 5 реч – зразок.xls
TLP:CLEAR	SHA-1	ebb30fd99c2e6cbae392c337df5876759e53730d	политзаключенные (по судам минска).xls
TLP:CLEAR	SHA-1	18bcc91ad3eed529d44926f4ae65acf44480f39d	Téléchargeur
TLP:CLEAR	SHA-1	64fca582cb69d9dc2afb1b432df58fb32ac18ca1	Téléchargeur
TLP:CLEAR	SHA-1	7261ad5d4e760aa88df94b734bc44598a090852a	Téléchargeur
TLP:CLEAR	SHA-1	9fa00a4ee4e95bc50a3919d2d3c0be2a567d8845	Téléchargeur

TLP	TYPE	VALEUR	DESCRIPTION
TLP:CLEAR	SHA-1	e5ebc7deca1ff1f0a4b1462d37ef813dad8413a6	Téléchargeur
TLP:CLEAR	Domaine	sweetgeorgiayarns[.]online	C2 - Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	Domaine	kitchengardenseeds[.]icu	C2 - Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	Domaine	punandjokes[.]icu	C2 - Campagne contre l'Ukraine de juillet 2025
TLP:CLEAR	Domaine	taskandpurpose[.]icu	C2 - Campagne contre la Pologne de mai 2025
TLP:CLEAR	Domaine	medpagetoday[.]icu	C2 - Campagne contre la Pologne de mai 2025
TLP:CLEAR	Domaine	pesthacks[.]icu	C2 - Campagne contre la Pologne d'avril 2025
TLP:CLEAR	Domaine	curseforge[.]icu	C2 potentiel enregistré
TLP:CLEAR	URL	hooks.slack[.]com/services/T08NWSF1L78/B08P91RQ1EW/ZQzZ7IvlT81VpQijneCR0iYa	C2 Slack - Campagne contre la Pologne d'avril 2025
TLP:CLEAR	URL	files.slack[.]com/files-pri/T08NWSF1L78-F08NQETU5M5/owjomlhoms.jpg	C2 Slack - Campagne contre la Pologne d'avril 2025
TLP:CLEAR	URL	hooks.slack[.]com/services/T08N1F1F64W/B08N1FMAN94/2QGu5K7wE3k6cVQ448Qa9n4W	C2 Slack - Campagne contre la Pologne d'avril 2025
TLP:CLEAR	URL	files.slack[.]com/files-pri/T08N1F1F64W-F08P2HJNU2F/ocnijrarcjvzenxyqhztf.jpg	C2 Slack - Campagne contre la Pologne d'avril 2025
TLP:CLEAR	Domaine	carpetmarker[.]pw	C2
TLP:CLEAR	Domaine	everything-everywhere.at.ply[.]gg	C2
TLP:CLEAR	IP	185[.]175.158.27	C2
TLP:CLEAR	Domaine	backstagemerch[.]shop	C2
TLP:CLEAR	Domaine	empoweringparents[.]shop	C2
TLP:CLEAR	Domaine	lauramcinerney[.]shop	C2
TLP:CLEAR	Domaine	ellechina[.]online	C2
TLP:CLEAR	Domaine	pedaily[.]link	C2
TLP:CLEAR	Domaine	goudieelectric[.]shop	C2
TLP:CLEAR	Domaine	thevegan8[.]shop	C2
TLP:CLEAR	Domaine	americandeliriumsociety[.]shop	C2
TLP:CLEAR	Domaine	cookingwithbooks[.]shop	C2
TLP:CLEAR	Domaine	everythingandthedog[.]shop	C2
TLP:CLEAR	Domaine	pigglywigglystores[.]shop	C2

TLP	TYPE	VALEUR	DESCRIPTION
TLP:CLEAR	Domaine	sciencealert[.]shop	C2
TLP:CLEAR	Domaine	backstagemerch[.]shop	C2
TLP:CLEAR	Domaine	bryndonovan[.]shop	C2
TLP:CLEAR	Domaine	chaptercheats[.]shop	C2
TLP:CLEAR	Domaine	clairedeco[.]shop	C2
TLP:CLEAR	Domaine	connecticutchildrens[.]shop	C2
TLP:CLEAR	Domaine	disneyfoodblog[.]shop	C2
TLP:CLEAR	Domaine	eartheclipse[.]shop	C2
TLP:CLEAR	Domaine	empoweringparents[.]shop	C2
TLP:CLEAR	Domaine	foampartyhats[.]shop	C2
TLP:CLEAR	Domaine	ikitas[.]shop	C2
TLP:CLEAR	Domaine	jackbenimblekids[.]shop	C2
TLP:CLEAR	Domaine	kingarthurbaking[.]shop	C2
TLP:CLEAR	Domaine	lansdownecentre[.]shop	C2
TLP:CLEAR	Domaine	lauramcinerney[.]shop	C2
TLP:CLEAR	Domaine	medicalnewstoday[.]shop	C2
TLP:CLEAR	Domaine	moonlightmixes[.]shop	C2
TLP:CLEAR	Domaine	penandthepad[.]shop	C2
TLP:CLEAR	Domaine	physio-pedia[.]shop	C2
TLP:CLEAR	Domaine	semanticscholar[.]shop	C2
TLP:CLEAR	Domaine	simonandschuster[.]shop	C2
TLP:CLEAR	Domaine	thevegan8[.]shop	C2
TLP:CLEAR	Domaine	twisterplussize[.]shop	C2
TLP:CLEAR	Domaine	utahsadventurefamily[.]shop	C2

4. RÉFÉRENCES

CVE-2025-49844

- https://www.cve.org/CVERecord?id=CVE-2025-49844
- https://www.sysdig.com/blog/cve-2025-49844-redishell
- https://redis.io/blog/security-advisory-cve-2025-49844/
- https://www.wiz.io/blog/wiz-research-redis-rce-cve-2025-49844

CVE-2025-48983

- https://www.cve.org/CVERecord?id=CVE-2025-48983
- https://www.veeam.com/kb4771

CVE-2025-55754

- https://www.cve.org/CVERecord?id=CVE-2025-55754
- https://lists.apache.org/thread/j7w54hqbkfcn0xb9xy0wnx8w5nymcbqd

Biélorussie : le groupe APT GHOSTWRITER

- WILDE Gavin, SHERMAN Justin, Belarus: Cyber upstart, or Russian staging ground? [En ligne] CYBERSCOOP 13/01/2022, Disponible sur : https://cyberscoop.com/belarus-cyber-upstart-or-russian-staging-ground/
- TASS, Belarus, Russia will step up security cooperation, Lukashenko pledges [En ligne] 13/11/2021, Disponible sur : https://tass.com/world/1361041
- Pierre GASTINEAU, Maître-espion | Biélorussie : Ivan Tertel, le maître-espion le plus courtisé d'Europe [En ligne] INTELLIGENCE ONLINE 29/08/2025, Disponible sur : https://www.intelligenceonline.fr/europe-russie/2025/08/29/ivan-tertel-le-maitre-espion-le-plus-courtise-d-europe,110513791-art
- Lee FOSTER, Sam RIDDELL, David MAINOR, Gabby RONCONE, Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests [En ligne] MANDIANT 28/07/2020, Disponible sur : https://cloud.google.com/blog/topics/threat-intelligence/ghostwriter-influence-campaign?
- Université de Cardiff, Ghostwriter Campaign as a multi-vector operation: Attempts to control its influence & the limitations of current counter-measures [En ligne] 2023, Disponible sur : https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf
- CERT-UA, Цільова кібератака UAC-0057 у відношенні державних органів із застосуванням PicassoLoader/njRAT (CERT-UA#6948) [En ligne] 07.07.2023, Disponible sur : https://cert.gov.ua/article/5098518
- CERT-UA, Кібератака групи UAC-0057 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109) [En ligne] 07.03.2022, Disponible sur : https://cert.gov.ua/article/37626
- CERT-UA, Точковий сплеск активності UAC-0057 (CERT-UA#10340) [En ligne] 24.07.2024, Disponible sur : https://cert.gov.ua/article/6280159
- FortiGuard Labs Threat Research, Ukrainian Military-Themed Excel File Delivers Multi-Stage Cobalt Strike Loader [En ligne] FORTINET 11/10/2022, Disponible sur : https://www.fortinet.com/blog/threat-research/ukrainian-excel-file-delivers-multi-stage-cobalt-strike-loader
- Vanja SVAJCER, Malicious campaigns target government, military and civilian entities in Ukraine, Poland [En ligne] CISCO TALOS 13/07/2023, Disponible sur : https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/
- Tom HEGEL, Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition [En ligne] SENTINELONE 25/02/2025, Disponible sur : https://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/
- HarfangLab Cyber Threat Research Team, UAC-0057 keeps applying pressure on Ukraine and Poland [En ligne] HARFANGLAB 20/08/2025, Disponible sur : https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/
- Cyble Research and Intelligence Labs, UNC1151 Strikes Again: Unveiling Their Tactics Against Ukraine's Ministry of Defence [En ligne] CYBLE 04/06/2024, Disponible sur : https://cyble.com/blog/unc1151-strikes-again-unveiling-their-tactics-against-

ukraines-ministry-of-defence/

- Kerstin ZETTL-SCHABATH, Jakob BUND, Lena ROTTINGER, Camille BORRETT, UNC1151 Fusing Technical and Social Vulnerabilities [En ligne] European Repository of Cyber Incidents [En ligne] 13/05/2023, Disponible sur : https://eurepoc.eu/wp-content/uploads/2023/05/EuRepoC-APT-profile-UNC1151.pdf