yuno By xmco

BILAN DES ACTIVITÉS 2023

par le CERT-XMCO

Avant-propos

Notre service de veille vous alerte en temps réel des nouvelles menaces du paysage Cyber, qu'il s'agisse de faille de sécurité (découverte de vulnérabilité, publication de correctif ou de code d'exploitation) ou d'attaque en cours. Ces informations vous aident à adapter la sécurité de votre entreprise au travers de nos recommandations ou de la fourniture d'iOC (Indicateur de Compromission), afin de vous protéger contre des menaces protéiformes.

Pour cette première édition du bilan annuel YUNO, le CERT-XMCO revient sur les évènements marquants de l'année passée. L'objectif de ce document est de fournir une vision globale du paysage et de l'évolution des cybermenaces, par un travail de synthèse et d'analyse des informations collectées au quotidien par nos analystes.

EN 2023, LE SERVICE YUNO A AINSI ENVOYÉ À CHACUN DE SES CLIENTS :

3694

C'est le nombre de **bulletins de type VULN** *(découverte de vulnérabilités)*, **PATCH** *(publication de correctifs)* et **EXPLOIT** *(publication de codes d'exploitation)*, en excluant tous les bulletins liés aux distributions Linux.

981

C'est le nombre de **bulletins de type INFO** *(identification de campagnes malveillantes, analyse de modes opératoires ou de malwares, explications de nouvelles normes ou de lois liées au domaine cyber, etc.)*.

12

C'est le nombre d'**observatoires des ransomware** *(analyses mensuelles de l'écosystème ransomware)*.

Au cours cette année, le CERT-XMCO a identifié plusieurs tendances structurantes ou émergentes relatives aux activités et modes opératoires des acteurs de la menace, aux vecteurs de distribution des codes malveillants ainsi qu'à la découverte et à l'exploitation de vulnérabilités. Ces différentes tendances peuvent être associées aux principales menaces pesant sur l'écosystème de la cybersécurité :

LA DÉCOUVERTE ET L'EXPLOITATION DE VULNÉRABILITÉS

Les vulnérabilités activement exploitées en 2023 ont été instrumentalisées directement après leur découverte démontrant une tendance à la réduction de leur délai d'exploitation, en particulier lorsqu'un code d'exploitation est disponible publiquement. Les technologies ciblées sont pour l'essentiel des services accessibles à distance et exposés sur Internet, ou des dispositifs réseau, permettant aux acteurs de la menace de prendre pied dans l'infrastructure d'une organisation et de se latéraliser en exploitant notamment de mauvaises configurations des politiques de gestion d'accès.

LES ATTAQUES RANSOMWARE

L'année 2023 a été marquée par des campagnes d'attaques exploitant des techniques sophistiquées et par l'émergence de nouvelles méthodes d'extorsion. En particulier, l'exploitation de vulnérabilités 0-day et le ciblage spécifique de fournisseurs de services managés (MSP) ont conduit à la compromission d'un nombre significatif de victimes. En parallèle, des actions de perturbations des activités cybercriminelles ont été menées par les forces de l'ordre, mais cet écosystème a une nouvelle fois su démontrer sa résilience.

LA DISTRIBUTION DE MALWARE

Les modes de distribution des malware se sont adaptés à l'évolution des mesures de sécurité, conduisant au recours accru à des vecteurs de compromission alternatifs comme le malvertising et le SEO Poisoning. Les malware ont également évolué pour étendre leurs opportunités de compromission en ciblant davantage les systèmes d'exploitation Linux et macOS. Enfin et à l'instar des ransomware, ils ont réussi à persister malgré les actions des forces de l'ordre, par la prolifération des codes malveillants et la création de nouvelles infrastructures.

LES MENACES APT

(ADVANCED PERSISTENT THREAT)

Les activités des modes opératoires APT ont généralement été caractérisées par une continuité vis-à-vis de l'année 2022. Le contexte géopolitique et les besoins en renseignement des États auxquels ils sont associés ont constitué les principaux facteurs orientant leurs opérations. Les évolutions observées sont de ce fait reliées à l'éclatement de la guerre entre Israël et le Hamas le 7 octobre 2023, entraînant une implication croissante de groupes associés à l'Iran ainsi qu'à la Russie, exploitant le conflit dans des attaques ciblant notamment des entités occidentales.

LES GROUPES HACKTIVISTES

Dans le continuum de l'année 2022, les opérations hacktivistes ont été particulièrement denses et ont principalement été rattachées à l'actualité géopolitique. Généralement caractérisés par des attaques à faible impact par déni de service distribué (DDoS), certains groupes se sont cependant démarqués par une évolution significative de leur sophistication et des impacts de leurs attaques, doublée d'une porosité croissante avec les menaces APT sponsorisées par des États, qui tendent à les exploiter pour dissimuler leurs activités et leurs objectifs réels. **Les éléments de détail et de chiffrage de cette thématique sont à retrouver dans le Panorama du CERT-XMCO sur la menace hacktiviste sur la France en 2023.**

Sommaire

Direction de la publication : XMCO
Date de publication : mai 2024

1. INFORMATIONS DÉLIVRÉES EN 2023

1.1 Vulnérabilités massivement exploitées

SÉLECTION DE VULNÉRABILITÉS MASSIVEMENT EXPLOITÉES EN 2023 ET INSTANTANÉMENT PUBLIÉES PAR YUNO.

L'exploitation de vulnérabilités logicielles est un des principaux vecteurs d'attaques exploités par les groupes d'attaquants. Parmi l'ensemble des failles identifiées en 2023, le CERT-XMCO revient sur quatre d'entre elles qui ont particulièrement impacté l'écosystème de la cybersécurité, en raison de leur criticité, de leur exploitation massive et des compromissions qu'elles ont entraînées.

CVE-2023-23397

Microsoft Outlook

Apparue le 14 Mars 2023 et publiée par YUNO le lendemain, la vulnérabilité 0-day référencée **CVE-2023-23397** (CVSS:3.1 de 9.8) affecte le client de messagerie électronique Microsoft Outlook. Corrigée par l'éditeur en mars 2023, elle permettait à un attaquant distant non authentifié de réaliser des attaques de type relais NTLM via l'envoi d'un e-mail spécifiquement conçu [150]. Cette vulnérabilité a été massivement exploitée par le groupe APT28 associé à la Russie pour cibler de nombreuses organisations stratégiques et critiques en Ukraine, mais aussi dans plusieurs pays membres de l'OTAN. [151][152][65]

Victimes connues :
Entités gouvernementales françaises, les entreprises, universités, ainsi que les instituts de recherche et groupes de réflexion situés en France, aussi 15 organisations gouvernementales, militaires, du secteur de l'énergie et des transports auraient également été visées.

Impacts :
Renseignement, espionnage.

CVE-2023-22515 & CVE-2023-22518

Atlassian Confluence Data Center et Server

Apparue le 4 Octobre 2023 et publiée par YUNO le lendemain, les vulnérabilités 0-day référencées **CVE-2023-22515** et **CVE-2023-22518** (CVSS:3.1 de 9.8) affectent Confluence Data Center et Server, une plateforme de travail collaborative éditée par Atlassian. Corrigées en octobre 2023, elles permettaient à un attaquant distant non authentifié d'élever ses privilèges au niveau administrateur.

Suite à la publication d'un code d'exploitation, les failles ont rapidement été exploitées pour déployer le ransomware Cerber et la backdoor Effluence[153][154]. Elles ont également été utilisées par le groupe APT associé à la Chine Storm-0062 ainsi que par le groupe hacktiviste pro-ukrainien Ukrainian Cyber Alliance pour compromettre les serveurs du ransomware Trigona.[155][156][131]

Impacts :
Espionnage et déploiement de ransomware

À partir 05/11/2023
Exploitation massive par le ransomware CERBER

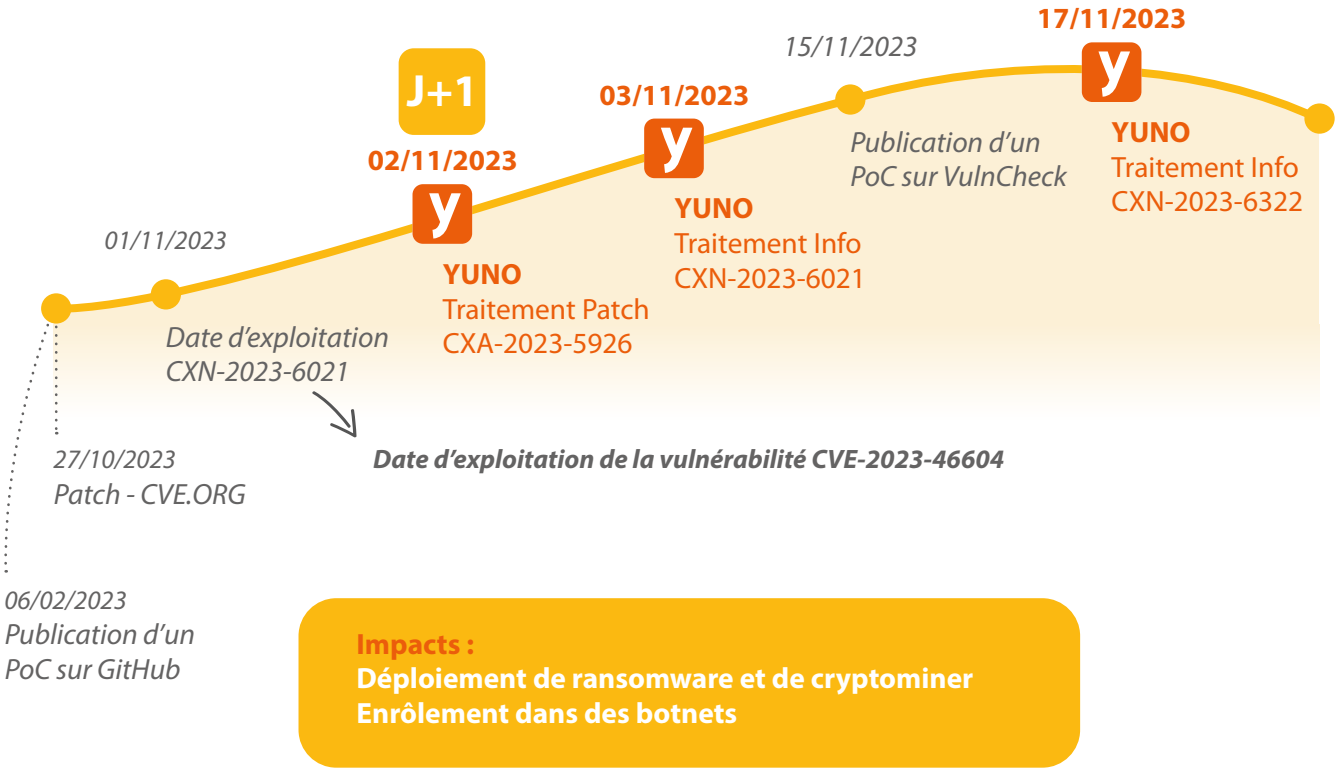
CVE-2023-46604

Apache ActiveMQ

Apparue le 27 Octobre 2023 et publiée par YUNO dans la semaine, la vulnérabilité critique référencée **CVE-2023-46604** (CVSS:3.1 de 9.8) affecte ActiveMQ, un service d'agent de messages édité par Apache.

Corrigée en octobre 2023, elle permettait à un attaquant distant non authentifié d'exécuter du code arbitraire[171].

Dès le mois de novembre, son exploitation active par le groupe de ransomware HelloKitty a été détectée. La publication d'un PoC le même mois a ouvert la voie à son exploitation massive par divers groupes d'attaquants tels que le groupe de cryptomining Kinsing, le groupe APT nord-coréen Andariel ainsi que d'autres cybercriminels déployant notamment les botnets GoTitan et le webshell Godzilla[172][173][174][175][176].



Impacts :
Déploiement de ransomware et de cryptominer
Enrôlement dans des botnets

CVE-2023-34362

Progress Software MOVEit Transfer

La vulnérabilité 0-day référencée **CVE-2023-34362** (CVSS:3.1 de 9.8) affecte MOVEit, une plateforme de transfert de fichiers éditée par Progress Software. Corrigée en juin 2023, elle permettait à un attaquant distant non authentifié d'accéder à des bases de données, d'élever ses privilèges et de faire le premier pas vers la mise en place d'un webshell[159].

La faille a été exploitée par de nombreux acteurs de la menace au-devant desquels le groupe de ransomware Cl0p depuis 2021[160][161][162].
Plus de 2500 victimes de compromission et vol de données par Clop parmi lesquelles : La BBC, British Airways, l'Etat du Maine, Shell, Radisson Hotels, Maximuss[163][164][165].

Déploiement de ransomware :
31/05/2023 - BORN Ontario - CXN-2023-3207
05/06/2023 - Zellis - CXN-2023-2927 / The Record
05/06/2023 - BBC - CXN-2023-2927 / The Record
05/06/2023 - British Airways - CXN-2023-2927 / The Record
06/06/2023 - Nova Scotia - CXN-2023-3207
06/06/2023 - ABIM - CXN-2023-3207
07/06/2023 - Extreme Networks - CXN-2023-3207
12/06/2023 - Ofcom - CXN-2023-3207
02/08/2023 - Maximus - CXN-2023-4061
09/11/2023 - Etat du Maine - CXN-2023-6221

1.2 Informations marquantes de 2023

YUNO COUVRE L'ESSENTIEL DE L'ACTUALITÉ DE L'ÉCOSYSTÈME CYBER À TRAVERS SES BULLETINS INFOS.

Chaque jour, nos clients reçoivent un concentré des évènements marquant de moment, qu'ils concernent des APT, des modes opératoires, des attaques, des organisations gouvernementales, etc. Le CERT-XMCO revient ici sur deux moments marquants de 2023.

[INFO] **Anonymous Sudan**

Campagne d'attaques contre le secteur hospitalier français

DATE DE PUBLICATION : 05/07/2023
LIEN DE LA PUBLICATION : https://leportail.xmco.fr/watch/advisory/**CXN-2023-3514**

Le collectif hacktiviste Anonymous Sudan a revendiqué sur Telegram une série d'attaques DDoS ciblant le secteur hospitalier français le vendredi 30 juin 2023, bloquant temporairement les sites web de :

- Assistance Publique-Hôpitaux de Paris
- Hôpital Pitié-Salpêtrière
- Hôpital Saint-Antoine
- Hôpital Américain de Paris
- Hôpital Universitaire de Marseille (AP-HM),
- Centre hospitalier universitaire (CHU) de Lyon.

D'après les investigations du CERT-XMCO sur le canal Telegram d'Anonymous Sudan, la campagne d'attaques a été revendiquée en réponse à la mort de Nahel M, décédé à Nanterre le mardi 27 juin 2023 lors d'un contrôle routier. La DGSI aurait été co-saisie d'une enquête contre les opérateurs du groupe le 21 mars 2023 à la suite d'attaques ayant ciblé les sites des aéroports de Paris (cf. CXN-2023-1500).

ASSOCIATION ET SOPHISTICATION D'ANONYMOUS SUDAN

Bien que les perturbations des attaques d'Anonymous Sudan restent limitées, le collectif hacktiviste s'inscrit dans une stratégie de lutte informationnelle conceptualisée par Vladislav Sourkov (ancien Vice-président du gouvernement russe).[2]

Ne requérant qu'un faible investissement en ressources techniques, ces attaques DDoS n'en restent pas moins dommageables par la dimension symbolique qu'elles impliquent : indisponibilité temporaire du service web, coûts de restauration et exposition médiatique dommageable pour l'image des services hospitaliers (cf. CXN-2023-2188). Selon les analystes de Cyfirma, la force des groupes hacktivistes pro-russes (dont Anonymous Sudan et KillNet font partie) ne résiderait pas dans la sophistication de leurs attaques, mais plutôt dans leur capacité à les coordonner à grande échelle.[3]

CAMPAGNES DE RANSOMWARE

Les campagnes d'attaques DDoS ne constituent qu'une partie marginale des activités cybercriminelles ciblant le secteur de la santé français.

En effet, selon le dernier rapport de l'ANSSI sur «l'état de la menace cyber sur les établissements de santé», les ransomwares sont la «menace la plus immédiate à l'encontre des établissements de santé» à la fois «en termes de volume, de fréquence des attaques et de conséquences». Cette tendance s'expliquerait selon les chercheurs de Sophos par le fait que les établissements de santé sont les plus susceptibles de payer la rançon, se classant au premier rang avec 61 % des organisations payant la rançon pour récupérer des données chiffrées, contre une moyenne mondiale de 46%.[4]

[INFO] **ANSSI**

État de la menace sur le secteur des télécommunications

DATE DE PUBLICATION : 20/12/2023
LIEN DE LA PUBLICATION : https://leportail.xmco.fr/watch/advisory/**CXN-2023-6984**

Le 18 décembre 2023, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié son état de la menace sur le secteur des télécommunications. Le rapport met en évidence la diversité des acteurs ciblant ce secteur d'activités qualifié de «supercritique» en raison des conséquences immédiates et systémiques qu'engendrerait un incident l'affectant. La préoccupation principale des organisations du secteur des télécommunications reste la disponibilité de leurs services, parfois au détriment de la confidentialité des données et de l'intégrité des systèmes d'information. **Au cours des 3 dernières années, l'ANSSI a été informée de plus de 150 événements de sécurité affectant des entités du secteur des télécommunications.**

MENACE À FINALITÉ PARTISANE

ESPIONNAGE

Les modes opératoires alignés sur les intérêts stratégiques chinois et iraniens sont documentés comme très actifs dans la collecte de renseignements à l'encontre du secteur des télécommunications. Leurs opérations d'espionnage ont pour principal objectif l'exfiltration de données, traitées en masse par les entités du secteur. Ces dernières années, l'ANSSI observe une hausse préoccupante de compromissions touchant des équipements, notamment des routeurs en cœur de réseau des opérateurs. Ces attaques, d'un haut niveau de sophistication, sont souvent menées dans une temporalité longue et difficilement détectées. Elles compromettent l'intégrité du réseau des opérateurs et permettent aux attaquants d'avoir un accès direct aux communications d'entités stratégiques et d'individus.

Parmi les campagnes d'attaques APT ayant ciblé le secteur des télécommunications au cours des dernières années, le CERT-XMCO tient à porter votre attention sur :

- L'APT **Volt Typhoon** distribuant KV-botnet dans le cadre d'une campagne d'attaques ciblant des dispositifs IoT (cf. CXN-2023-6919).
- Les acteurs de la menace ayant exploité une vulnérabilité dans **Dante Discovery** pour cibler le secteur des télécommunications en Asie (cf. CXN-2023-5582).
- L'APT **Sandman** ayant ciblé le secteur des télécommunications au Moyen-Orient, en Europe occidentale et en Asie du Sud (cf. CXN-2023-5101) .
- Le mode opératoire **ShroudedSnooper** ayant ciblé des entreprises du secteur des télécommunications au Moyen-Orient (cf. CXN-2023-5073).

DÉSTABILISATION & SABOTAGE

La menace à finalité de déstabilisation pèse également sur le secteur des télécommunications. Bien que les principales attaques recensées lors des 3 dernières années sont le fait de groupes hacktivistes, qui pratiquent du chantage au déni de service distribué (**DDoS**) et de l'exposition de données personnelles associée à des revendications politiques (**Hack&Leak**), les opérations de plus grande envergure et à des fins de sabotage restent une menace majeure du secteur.

L'attaque qui a ciblé le réseau satellitaire KA-SAT dans la nuit de l'invasion russe en Ukraine en février 2022 a démontré l'impact massif des opérations de sabotage menées contre le secteur des télécommunications (cf. CXN-2022-2338).

Parmi les campagnes perturbatrices ayant ciblé le secteur des télécommunications au cours des dernières années, le CERT-XMCO tient à porter votre attention sur :

- La compromission de l'opérateur mobile ukrainien **Kyïvstar** revendiquée par des hacktivistes pro-russes (cf. CXN-2023-6953).
- La mise hors service du réseau satellitaire de l'opérateur **Dozor Teleport** (cf. CXN-2023-3488).
- Les 11 entreprises de télécommunications compromises en Ukraine par APT **Sandworm** selon le CERT-UA (cf. CXN-2023-5613).

MENACE À FINALITÉ LUCRATIVE

Les attaques à finalité lucrative sont fréquentes dans le secteur des télécommunications.
Une part importante d'entre elles concerne la fraude aux communications, qui cible les opérateurs comme leurs clients et représente un préjudice financier et d'image important, notamment pour les opérateurs de téléphonie mobile. Les opérateurs de télécommunications sont également ciblés par des attaques opportunistes s'intéressant à la masse de données personnelles détenues par les opérateurs.
Les données alors exfiltrées sont revendues par des cybercriminels ou sont utilisées dans le cadre d'attaques par ransomware comme chantage à la divulgation de données.

Parmi les campagnes lucratives ayant ciblé le secteur des télécommunications au cours des dernières années, le CERT-XMCO tient à porter votre attention sur :

- Le rapport de **Microsoft** sur les tactiques, techniques et procédures (TTPs) du mode opératoire **Octo Tempest** (cf. CXN-2023-5945).
- La société chilienne de télécommunications **Grupo GTD** victime du ransomware **Rorschach** (cf. CXN-2023-5969).
- La campagne d'attaque ciblant les environnements **Jupyter Notebooks** afin de distribuer le malware **Qubitstrike** (cf. CXN-2023 -5824).

L'ANSSI propose un ensemble de recommandations à l'attention des entités du secteur des télécommunications.

1.3 Ransomware, évolutions des modes opératoires

RANSOMWARE
Évolutions des modes opératoires

EXPLOITATION DE VULNÉRABILITÉS COMME VECTEURS D'ACCÈS INITIAL ET LE CIBLAGE DE MSP

Les groupes ransomware ont continué à améliorer leurs techniques de compromission leur permettant de réaliser des attaques de grande envergure.

L'exploitation de vulnérabilités et notamment de 0-day dans des logiciels populaires comme vecteur d'accès initial a été particulièrement privilégiée par ces derniers[1][2][3]. Le groupe Cl0p s'est ainsi démarqué par l'exploitation de failles 0-day affectant GoAnywhere MFT, MoveIT et SysAid On-Prem, qui lui ont permis de compromettre des centaines d'organisations[4][5][6]. Toutefois, ce dernier s'est détourné du modèle de double extorsion, délaissant le chiffrement des données au profit de leur simple exfiltration.
Les groupes cherchent à maximiser leur impact et leur gain en essayant également de compromettre des infrastructures permettant de réaliser des attaques ciblant la chaîne d'approvisionnement. Les ransomware Play et LockBit par exemple, ont compromis des fournisseurs de services managés (MSP) et par extension, leurs clients[7][8].

ÉMERGENCE DE NOUVELLES TACTIQUES D'EXTORSION

Afin d'accroître la pression sur leurs victimes, les groupes ransomware ne se sont plus contentés de publier les données volées à leurs victimes sur leur site de publication de fuites de données sur le darkweb.
BlackCat/Alphv a exploité des techniques de typosquatting afin de cloner le site officiel de sa victime pour y publier les données compromises et a soumis une déclaration d'incident à l'organisme fédéral américain chargé de la réglementation et du contrôle des marchés financiers, la SEC, à la place d'une de ses victimes[9][10].

D'autres groupes comme LockBit et HarBit ont professionnalisé et industrialisé leurs stratégies d'extorsion par l'harmonisation de la valeur des rançons pour leurs affiliés ou l'ajustement de son montant en fonction du contrat d'assurance souscrit par la victime[11][12].

ACTION DES FORCES DE L'ORDRE ET RÉSILIENCE DE L'ÉCOSYSTÈME

ACTIONS DE DÉMANTÈLEMENT ET PERTURBATIONS

Différentes autorités qu'elles soient étatiques ou privées ont cherché à perturber le développement des activités ransomware.

Des collaborations entre plusieurs États ainsi que des actions réalisées par les autorités américaines ont permis la saisie d'infrastructure des groupes ALPHV/BlackCat, Hive ou RagnarLocker ainsi que la publication d'outils de déchiffrement[13][14][15][16][17].

Des entreprises de cybersécurité ont également contribué à ces actions avec la publication de kits de déchiffrement pour des variantes de ransomware particulièrement actifs à l'instar de Cl0p, Conti, ou Akira[18][19][20].

DEMANTÈLEMENT DU RANSOMWARE HIVE

Le 26 janvier 2023, les serveurs et les clés de déchiffrement du groupe ransomware Hive ont été saisis à la suite d'une opération conjointe entre les États-Unis, Europol et 12 autres pays[14].

Une infiltration du groupe par le FBI pendant 6 mois a permis aux enquêteurs d'accéder à des communications internes, des condensats de fichiers

malveillants ainsi que des informations sur les 250 affiliés de la franchise Hive.
Bien que l'opération ait été un succès, aucun membre n'a été appréhendé, il est donc probable que les membres (opérateurs et affiliés) rejoignent d'autres groupes ransomware ou passent par une phase de rebranding[209].

Site de publication de fuites de données du ransomware Hive après la saisie de son infrastructure
Source : Europol[21]

UNE CAPACITÉ DE RÉSILIENCE SIGNIFICATIVE

Face à ces actions perturbatrices, les opérateurs de ransomware ont développé de nouvelles variantes en s'appuyant sur le recrutement d'affiliés, à l'instar d'Akira, ainsi que sur la publication d'outils de déchiffrement et la réutilisation du code source d'autres ransomware, comme l'ont fait LockBit et Hunters International. LockBit Green est ainsi basé sur celui de Conti qui avait été divulgué en 2022 et Hunters International a, pour sa part, acheté le code source de Hive[22][23][24][25][26].

Le système d'affiliation via le modèle de Ransomware-as-a-Service (RaaS) a également permis à des acteurs d'un même écosystème voire d'écosystèmes différents de s'allier afin d'étendre leur stratégie de monétisation.

Les groupes Mallox, TargetCompany, Tohnichi et Fargo se sont associés pour développer un RaaS commun et Scattered Spider, spécialisé dans l'extorsion de données via des techniques d'ingénierie sociale, s'est affilié au ransomware BlackCat/Alphv, pour compromettre notamment des Casinos à Las Vegas[1][27][28].

À noter que ce groupe continue de revendiquer des victimes en dépit de sa saisie annoncée par le FBI en décembre[13][29].

2. ANALYSE DES PRINCIPALES TENDANCES 2023

2.1 Principales tendances identifiées liées à l'exploitation de vulnérabilités

PRINCIPALES TENDANCES IDENTIFÉES
liées à l'exploitation de vulnérabilités

TIME-TO-EXPLOIT & RESPONSIBLE DISCLOSURE

Les vulnérabilités susmentionnées comprennent sept 0-day et deux vulnérabilités critiques, la **CVE-2023-27350** affectant PaperCut NG/MF ainsi que la **CVE-2023-46604** affectant Apache ActiveMQ.
Ces dernières ont été exploitées activement dans une temporalité très courte suivant la publication d'un correctif et de solutions d'atténuation, démontrant une tendance à la réduction du temps d'exploitation des vulnérabilités.

La publication rapide de codes d'exploitation publics a d'autant plus exacerbé leur instrumentalisation par des groupes d'attaquants, qui pouvaient les exploiter aisément sans nécessairement disposer de compétences techniques importantes[189][190].

Le choix de certains chercheurs de partager des codes d'exploitation ou des analyses techniques approfondies des vulnérabilités dans un délai très court après la publication d'un correctif apparaît alors comme un facteur aggravant des risques. Dans le cas de la vulnérabilité 0-day CVE-2023-0669 affectant GoAnywhere MFT, une analyse technique permettant de l'exploiter aisément a été publiée avant même qu'un correctif ne soit rendu disponible[191].

LE CIBLAGE DE SERVICES EXPOSÉS SUR INTERNET ET DE LA CHAÎNE D'APPROVISIONNEMENT LOGICIELLE

Les produits activement exploités par des acteurs de la menace sont diversifiés, dans l'objectif opportuniste d'élargir autant que possible la surface d'attaque qu'ils pourront exploiter. Cela étant dit, la majeure partie des technologies massivement ciblées comprend des services accessibles à distance et exposés sur Internet, tels qu'Atlassian Confluence Data Server & Center et Citrix NetScaler ADC & Gateway, ou des dispositifs réseau à l'instar des produits Cisco et Ivanti [192][193][194][195][196][192][197][198].

Leur compromission permet aux acteurs de la menace de prendre pied dans l'infrastructure d'une organisation et d'accéder à des données sensibles leur octroyant par la suite l'opportunité de se latéraliser en exploitant notamment de mauvaises configurations des politiques de gestion d'accès.

Autre fait notable, le groupe de ransomware cl0p a démontré sa capacité à développer des codes d'exploitation en interne, illustrant un degré de sophistication technique traditionnellement attribué à des groupes d'attaquants sponsorisés par des États.

Le ciblage spécifique de solutions tierces de partage de fichiers permet en outre aux attaquants de compromettre en cascade un nombre très important de victimes dans des attaques visant la chaîne d'approvisionnement logicielle, qui constituent par ailleurs un moyen de contourner efficacement les systèmes de sécurité sophistiqués de certaines organisations[5].

L'EXPLOITATION DE VULNÉRABILITÉS 0-CLICK PAR DES SPYWARE COMMERCIAUX

Les vulnérabilités 0-day sont souvent découvertes et exploitées par des acteurs disposant de ressources techniques et financières significatives. Des entités commerciales désignées par le terme « sociétés d'interception légales » se sont démarquées par la distribution d'outils de surveillance via l'exploitation de chaînes d'infection sophistiquées basées sur des vulnérabilités 0-day voire 0-click (i.e. : sans interaction de l'utilisateur) ciblant principalement les supports mobiles[61].

La publication des Predator Files en octobre 2023 a remis en évidence le risque associé à ces spyware commerciaux, exploités par différents pays pour cibler opposants politiques, journalistes, dirigeants

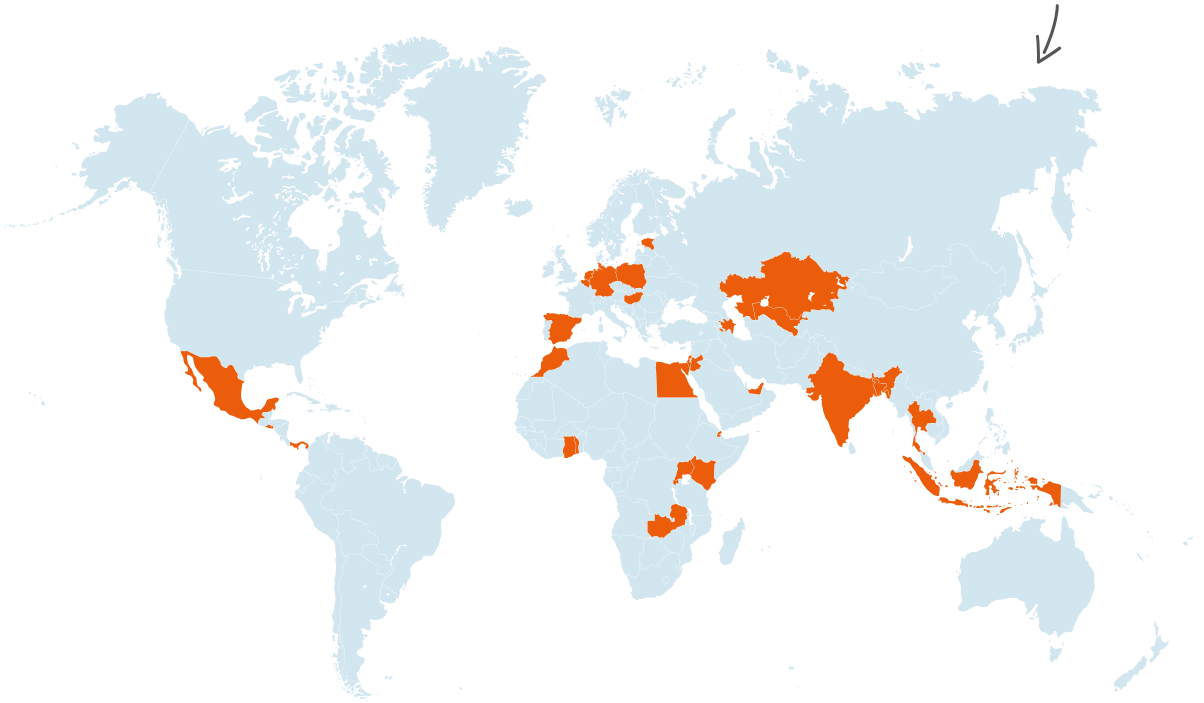
d'entreprises et activistes[199]. En 2023, des éditeurs comme Apple et Google ont corrigé plusieurs vulnérabilités exploitées par ces acteurs, mais leur prolifération s'appuyant sur un marché légal et cybercriminel de la vente de codes d'exploitation très concurrentiel, il est hautement probable que de nouveaux codes d'exploitation 0-day et 0-click soient découverts à l'avenir[200][201][202][203].

CORRECTION DE VULNÉRABILITÉS APPLE EXPLOITÉES PAR LE SPYWARE PEGASUS

Le jeudi 7 septembre 2023, Apple a publié des bulletins de sécurité d'urgence pour corriger 2 nouvelles vulnérabilités de type 0-day exploitées dans des attaques sophistiquées visant des utilisateurs des produits d'Apple[201]. Référencées **CVE-2023-41064** et **CVE-2023-41061**, ces 2 vulnérabilités ont été activement exploitées par la société israélienne NSO Group dans le cadre de leurs prestations commerciales de surveillance électronique. Les opérateurs ont eu recours à une chaîne d'exploitation 0-click dans iMessage (référencée BLASTPASS par CitizenLab) permettant de déployer le spyware Pegasus via l'exécution de code arbitraire[61].

Pays accusés d'avoir déployé le spyware Pegasus
Source : Carnegie[204]

Allemagne
Arabie Saoudite
Azerbaïdjan
Bahreïn
Bangladesh
Belgique
Djibouti
Egypte
Emirats Arabes Unis
Espagne
Estonie
Ghana
Hongrie
Inde
Indonésie
Israël
Jordanie
Kazakhstan
Kenya
Le Salvador
Mexique
Maroc
Ouganda
Ouzbékistan
Pays-Bas
Panama
Pologne
Rwanda
Thaïlande
Togo
Zambie



2.2 Malware, évolutions des modes opératoires

MALWARE
Évolutions des modes opératoires

ÉMERGENCE DE NOUVEAUX VECTEURS D'ACCÈS INITIAL

La désactivation des macros par défaut par Microsoft au début de l'année 2022 et l'introduction de nouvelles mesures de sécurité en 2023 ont encouragé l'exploitation croissante de nouveaux vecteurs de compromission.

Des attaquants ont ainsi exploité des techniques de malvertising via des publicités Google et de typosquatting par l'usurpation de logiciels populaires à l'instar des infostealers SYS01stealer, Raccoon, Vidar et Atomic Stealer[30][31][32][33][34][35]. D'autres campagnes de Qakbot et Emotet ont quant à elles privilégié l'utilisation de nouveaux formats de fichiers malveillants tels que OneNote ou add-in Excel[36][37].

En complément, les acteurs de la menace ont exploité la méthode de SEO Poisoning consistant à positionner les sites web malveillants dans les meilleurs résultats des moteurs de recherche. Le loader NullMixer, ayant ciblé la France, ou le groupe DEV-0569 ont employé cette technique[34][38][39].

DIVERSIFICATION DES SYSTÈMES D'EXPLOITATION CIBLÉS

Les opérateurs ont développé de nouveaux malware ou de nouvelles variantes afin d'étendre leurs opportunités de compromission, en particulier pour cibler les systèmes d'exploitation Linux et macOS.

C'est par exemple le cas du botnet Medusa, de la variante IZ1H9 de Mirai ou encore de P2Pinfect, qui cherchent à compromettre des appareils IoT ou des infrastructures de virtualisation basées sur Linux telles que les hyperviseurs VMware ESXi[40][41][42]. De même, les systèmes macOS sont de plus en plus ciblés et de nouveaux malware se sont spécialisés pour les compromettre, en particulier les infostealers tels qu'Atomic Stealer, MetaStealer ou MacStealer[43][44][45][46].

Cette tendance a également été observée chez les groupes APT comme Lazarus et APT27 ainsi que chez les groupes ransomware, à l'instar d'Akira et sa version Linux ou LockBit avec sa version macOS[47][48][49][50].

DÉCOUVERTE D'UN NOUVEL INFOSTEALER CIBLANT macOS

Le 3 mai 2023, un canal Telegram a fait la promotion d'un nouvel infostealer nommé Atomic macOS Stealer (AMOS), spécialisé dans la compromission de système d'exploitation macOS[46].

AMOS est destiné à des utilisateurs motivés par des gains financiers et permet de voler des mots de passe, des cookies de navigations et le contenu des portefeuilles de plus de 50 plateformes spécialisées dans les cryptomonnaies.

L'infostealer a notamment été observé dans une campagne de phishing faisant partie d'une opération à plus grande échelle appelée ClearFake. Cette dernière exploite des techniques de malvertising afin d'inciter les victimes à télécharger des mises à jour malveillantes pour Safari et Chrome[32].

L'apparition d'AMOS et de cette campagne rejoignent les observations des analystes du CERT-XMCO qui ont constaté une augmentation des infections par infostealer et une croissance de l'écosystème durant l'année 2023.

ACTION DES FORCES DE L'ORDRE ET RÉSILIENCE DE L'ÉCOSYSTÈME

DÉMANTÈLEMENT D'INFRASTRUCTURES ET DE MARKETPLACES

Différentes instances étatiques et de coopération ont cherché à neutraliser l'activité des malware. Parmi les actions notables, le FBI a annoncé en août et en novembre respectivement le démantèlement de l'infrastructure des botnets Qakbot (alias Qbot) et IPStorm[51][52].

D'autres opérations internationales ont permis la saisie de marketplaces cybercriminelles et forums utilisés notamment pour la commercialisation de malware ou la publication d'informations collectées par ces derniers, comme c'est le cas de Genesis Market, BreachedForum ou encore Monopoly Market[53][54][55].

DÉMANTÈLEMENT DE GENESIS MARKET

Le 5 avril 2023, une opération internationale menée par le FBI et intitulée «Operation Cookie Monster» a abouti à la saisie des infrastructures de la marketplace Genesis Market[53][215].

Les victimes avaient la possibilité de vérifier via la plateforme Have I Been Pwned (HIBP) si leurs données avaient été compromises[216]. La marketplace proposait à la vente des secrets dérobés par des infostealers. Ces derniers pouvaient être à la fois des identifiants, des cookies de session mais également l'empreinte numérique du navigateur permettant d'usurper l'identité de la victime. Genesis Market jouait un rôle majeur dans l'écosystème cybercriminel. Sa fermeture a ainsi entraîné la migration des membres vers d'autres plateformes existantes voire la création de nouvelles.

APPARITION DE NOUVEAUX MALWARE ET PLATEFORMES DE DIFFUSION

Le démantèlement d'infrastructures n'aboutit pourtant pas systématiquement à l'interruption des activités cybercriminelles.

Bien que celles de Qakbot aient été saisies, ses opérateurs sont restés actifs[56][57]. En outre, ses utilisateurs se sont également tournés vers de nouveaux malware modulaires comme Danabot et Darkgate[58][30]. Ce phénomène est également observable au niveau des marketplaces sur le darkweb, la saisie de BreachedForum ayant par exemple entraîné la migration de ses utilisateurs vers d'autres communautés[59].

Par ailleurs, les opérateurs de malware adoptant un modèle de Malware-as-a-Service (MaaS) se caractérisent également par une décentralisation croissante de leurs activités. Celle-ci s'appuie en particulier sur leur exploitation de réseaux sociaux, au-devant desquels Telegram, comme vecteur de communication, de promotion et de publication[60][61].

Marketplace Genesis Market saisie après une opération policière
Source : The Record[62]

2.3 Le piratage au service des États

1. LA RUSSIE

Renseignement et sabotage guidés par la guerre en Ukraine.

ACTIVITÉS D'ESPIONNAGE À DES FINS DE RENSEIGNEMENT

Les modes opératoires APT (Advanced Persistent Threat) associés à la Russie ont continué leurs activités alignées sur les besoins de renseignements stratégiques du régime, notamment liés à la guerre en Ukraine.

Pour ce faire, ils ont employé divers vecteurs de compromission, APT28 et Winter Vivern ayant exploité des vulnérabilités au sein du logiciel Roundcube et Microsoft Outlook pour espionner le secteur aéronautique ukrainien, des gouvernements européens et des membres de l'OTAN[63][64][65].

D'autres acteurs tels qu'APT29 ou Callisto ont ciblé des États occidentaux via l'exploitation de leurres de spear-phishing variés[66][67]. Une évolution notable réside dans l'utilisation de leurres basés sur le conflit israélo-palestinien par APT28 pour cibler des ONG et organisations gouvernementales européennes[68].

DES CAMPAGNES D'ATTAQUES OPÉRÉES PAR APT28 CIBLENT DES PAYS OCCIDENTAUX

Le mode opératoire APT associé à la Russie, APT28, a été particulièrement actif durant le mois de décembre avec la réalisation de multiples campagnes d'attaques.

Il a exploité les vulnérabilités, référencées **CVE-2023-23397** et **CVE-2023-38831**, affectant respectivement Microsoft Outlook et WinRAR dans des campagnes de phishing ciblant des organisations du secteur de la défense, de l'aérospatial, et du gouvernement au sein d'États membres de l'OTAN[65][152].
Il a également cherché à distribuer plusieurs Backdoor telles que OCEANMAP, MASEPIE ou Headlace, en particulier via une campagne de phishing exploitant le conflit israélo-palestinien comme leurre[217][68]. Ces dernières étaient capables de d'exécuter des commandes, de voler de nombreuses données de l'hôte et de ses navigateurs Internet ainsi que de les exfiltrer vers un serveur de commande et de contrôle (C2).

OPÉRATIONS DE SABOTAGE EN APPUI DES OPÉRATIONS MILITAIRES

La guerre en Ukraine a également vu les APT russes cibler des infrastructures ukrainiennes à des fins de sabotage et dans l'objectif de préparer des opérations cinétiques.
Le groupe Sandworm a continué d'exploiter des wipers afin de cibler des systèmes de contrôle industriels et provoquer des perturbations et des pannes à grande échelle[69][70]. Les chercheurs d'ESET et de Mandiant ont souligné la temporalité de ces attaques, coïncidant avec des frappes de missiles.

Des attaques attribuées à Sandworm ont également ciblé l'agence de presse ukrainienne Ukrinform ainsi que la firme de télécommunications Kyïvstar, dont la compromission a entraîné une perte de connexion à Internet massive ainsi que des répercussions sur des infrastructures bancaires et militaires[71][72][73].

2. LA CORÉE DU NORD

Vol d'argent et de renseignement pour alimenter le régime et ses programmes militaires.

VOL D'ARGENT POUR FINANCER LE RÉGIME

Les APT associés à la Corée du Nord ont continué leur stratégie de détournement de capitaux financiers afin de soutenir les objectifs de financement du régime de Pyongyang et le maintien de la dynastie Kim.

Le groupe Lazarus a mené des campagnes de phishing visant la communauté des cryptomonnaies ou usurpant des recruteurs pour cibler des développeurs et voler des fonds via des cryptominers, infostealers et downloaders comme KandyKorn et RustBucket[74][75][76][77].

Les APT nord-coréens ont également exploité des ransomware développés en interne comme Maui et H0lyGh0st, ou disponibles publiquement comme BitLocker et LockBit 2.0[78][79]. Ils se sont en outre démarqués par des attaques ciblant la chaîne d'approvisionnement via la compromission de 3CX, MagicLine4NX et Cyberlink[80][81][82][83].

VOL D'INFORMATIONS POUR DÉVELOPPER LES PROGRAMMES MILITAIRES

Le développement du programme d'armement nucléaire nord-coréen a été l'une des priorités des opérations de collecte de renseignement stratégique réalisées par les APT associés à Pyongyang.

Dans cette optique, des groupes comme Lazarus et APT37 ont ciblé des entités occidentales opérant dans les secteurs de la défense, de la recherche et de l'aérospatiale[84][85]. Kimsuky a pour sa part été observé dans une campagne ciblant un exercice militaire conjoint entre les États-Unis et la Corée du Sud[86].

Par ailleurs, ces modes opératoires ont ciblé de manière indiscriminée des entités localisées au sein de pays alliés de Pyongyang. Le groupe APT37 a par exemple compromis le groupe industriel de défense russe Mashinostroyeniya, spécialisé dans la conception de missiles balistiques intercontinentaux[87][88].

3. LA CHINE

Des opérations d'influence et de collecte de renseignement en Asie et en Occident.

ACTIVITÉS D'ESPIONNAGE ET OPÉRATIONS D'INFLUENCE EN ASIE-PACIFIQUE

Les contentieux territoriaux en mer de Chine méridionale ainsi que l'escalade des tensions avec Taïwan ont orienté les campagnes d'espionnage des modes opératoires APT associés à la Chine.

APT27, APT41, APT10 et Grayling ont ciblé des entités taïwanaises opérant dans des secteurs d'activité variés, avec un focus notable sur les fabricants de semi-conducteurs, à l'appui notamment du malware PlugX[89][90][91][92].
Des campagnes de désinformation ont également été observées à l'approche des élections de janvier 2024[93]. En Asie du Sud-Est, les organisations gouvernementales ont été la cible principale de la Chine dans l'objectif de collecter du renseignement sur la posture diplomatique et économique de ses voisins, à l'instar des opérations menées par Gelsenium, Mustang Panda, REF2924 et Gallium[94][95][96][97][98].

ESPIONNAGE INDUSTRIEL ET DIPLOMATIQUE EN EUROPE ET EN AMÉRIQUE DU NORD

Les tensions diplomatiques et commerciales avec les États-Unis et l'Europe ainsi que l'introduction de restrictions liées aux semi-conducteurs ont motivé des activités d'espionnage industriel et politique.

Le groupe Chimera a infiltré la firme de semi-conducteurs néerlandaise NXP pendant plus de 2 ans[99].

En France, l'ANSSI notait que la moitié des activités observées ciblant le secteur public et de l'industrie était attribuée à des modes opératoires associés à Pékin, en particulier APT31, Mustang Panda, RedDelta ou Ke3chang[100][101][102].

Outre-Atlantique, Storm-0558 a ciblé des fonctionnaires et Volt Typhoon a concentré ses opérations sur l'île de Guam, qui héberge des infrastructures militaires et de télécommunications, via l'exploitation de vulnérabilités Fortinet et Cisco[103][104].

Des opérations d'influence anti-américaines ont également été observées[105][106].

4. L'IRAN

Des opérations de renseignement, de sabotage et d'influence impactées par le conflit israélo-palestinien.

COLLECTE DE RENSEIGNEMENT STRATÉGIQUE EN OCCIDENT ET AU MOYEN-ORIENT

Les modes opératoires APT associés à l'Iran ont opéré des campagnes visant ses adversaires géopolitiques historiques, à savoir les pays occidentaux et des pays rivaux au Moyen-Orient tels qu'Israël et l'Arabie saoudite.

En occident, les activités d'espionnage ont principalement ciblé les secteurs de la défense et de l'éducation, illustrées par des campagnes attribuées à APT33, Mint Sandstorm et APT42[107][108][109][110][111].
Des attaques à visée politique ont également été identifiées, à l'instar de la compromission du journal français Charlie Hebdo attribuée au groupe Holy Souls[112].

Au Moyen-Orient, les groupes APT34, Imperial Kitten, APT35 et Agrius ont ciblé le secteur de la défense et des infrastructures stratégiques, exploitant notamment des vecteurs de spear-phishing ou l'exploitation de vulnérabilités pour distribuer des malware comme SideTwist, distribué à une organisation basée en Arabie saoudite, ou des wipers tels que PartialWasher en Israël[113][114][115][116][117].

L'IMPACT DE LA GUERRE ENTRE ISRAËL ET LE HAMAS

Depuis l'éclatement des affrontements armés entre Israël et le Hamas le 7 octobre dernier, des opérations de sabotage et d'influence associées à l'Iran ont été identifiées, en soutien à son allié.

Les premières activités d'APT iraniens en marge du conflit ont été attribuées au groupe MuddyWater, qui a conduit une campagne de spear-phishing ciblant des entités israéliennes avec son nouveau framework MuddyC2Go[118][119]. Une opération ultérieure conduite par APT42 a également été observée, avec comme objectif la collecte de renseignement militaire auprès de cibles israéliennes et américaines[120].

Par ailleurs, des groupes associés à l'Iran ont également distribué des wipers comme COOLWIPE dans des attaques à visée destructrice et ont opéré des opérations d'influence visant à polariser le débat public en Israël [120]. Enfin, l'Iran aurait ciblé Tel-Aviv via son soutien à des groupes attribués au Hamas, à l'instar d'AridViper[121][122][123].

2.4 Hacktivistes

HACKTIVISTES

Activités liées au contexte géopolitique

CONTINUITÉ DES ATTAQUES EN MARGE DE LA GUERRE EN UKRAINE

Le conflit en Ukraine continue d'être rythmé par des opérations de déstabilisation réalisées par des hacktivistes pro-russes ciblant l'Ukraine et ses alliés et par des hacktivistes pro-ukrainiens ciblant la Russie.

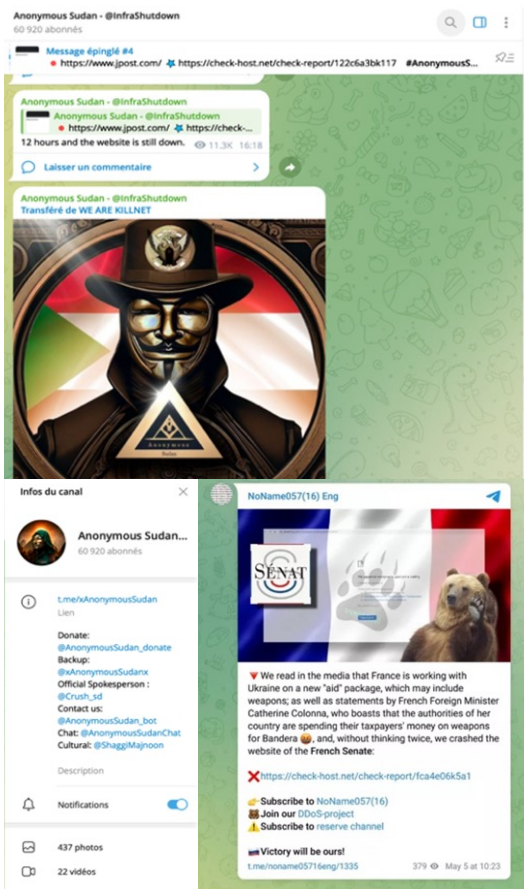
Sur cette thématique, le CERT-XMCO a publié son Panorama de la menace hacktiviste sur la France en 2023, qui présente de manière détaillée et chiffrée les dynamiques observées au cours de l'année passée.

Des hacktivistes pro-russes comme NoName057(16), Killnet et Anonymous Sudan ont conduit des attaques DDoS ciblant des entités occidentales, parmi lesquelles des CERTs européens, Eurocontrol ainsi que des entités des secteurs de la santé et des transports en France[124][125][126]. À noter également des attaques réalisées entre groupes pro-russes opposés ou partisans de la société militaire privée (SMP) Wagner suite à sa rébellion[127][128].

Les groupes pro-Ukraine ont quant à eux ciblé des entités russes à des fins de vol de données ou de sabotage. L'IT Army of Ukraine a notamment revendiqué la compromission de Gazprom et des aéroports russes et l'Ukrainian Cyber Alliance a compromis le ransomware Trigona, accusé d'entretenir des liens avec Moscou[129][130][131].

DES HACKTIVISTES PRO-RUSSES CIBLENT LA FRANCE

Durant tout le mois de mars 2023, des groupes hacktivistes comme Anonymous Sudan et NoName057(16) ont effectué de nombreuses opérations de déstabilisation. Dans le cadre de la guerre en Ukraine et de son soutien au pays, la France est devenue la cible récurrente d'attaques par DDoS réalisées par des groupes hacktivistes pro-russes.
Anonymous Sudan a revendiqué des attaques DDoS visant des aéroports, des compagnies aériennes, des universités, des établissements hospitaliers ainsi que le site Internet des services de renseignements intérieurs français (DGSI)[210][141][211][212][213]. NoName057(16) a également ciblé le secteur des services publics, notamment l'Assemblée nationale et le Sénat [214].



Revendications d'attaques DDoS contre la France par NoName057(16) et Anonymous Sudan
Source : Telegram[132] [133]

L'INTERNATIONALISATION DE LA MENACE HACKTIVISTE EN MARGE DU CONFLIT ISRAÉLO-PALESTINIEN

L'offensive du Hamas et l'opération militaire israélienne sur la bande de Gaza ont entraîné l'internationalisation des opérations hacktivistes en soutien aux deux parties en conflit.

Des groupes pro-russes comme Anonymous Sudan et Killnet, pakistanais tels que Team Insane PK, ou indonésiens comme AnonGhost Indonesia, se sont ralliés à la cause palestinienne et ont ciblé massivement des entités en Israël ainsi que des pays comme la France, accusés de lui apporter leur soutien[134]. L'impact de ces attaques restait cependant limité et essentiellement cantonné à du DDoS visant des entités de moindre envergure[135]. En contrepartie, des groupes soutenant Israël, en particulier associés à l'Inde à l'instar de l'India Cyber Force et Team UCC Ops, ont soutenu Israël en ciblant des entités à Gaza[136].

Le groupe pro-israélien Gonjeshke Darande pour sa part, a revendiqué des attaques ayant perturbé des stations d'essence en Iran[120].

ÉVOLUTIONS DES MODES OPÉRATOIRES ET POROSITÉS DES ACTEURS

SOPHISTICATION DES GROUPES

Certains groupes hacktivistes ont fait évoluer leur arsenal pour exploiter des modes opératoires plus sophistiqués, quand d'autres ont transformé leur mode d'action en ajoutant un aspect financier à leur motivation idéologique.

SiegedSec, présenté comme une faction du collectif Anonymous, a revendiqué par deux fois le vol de données à l'OTAN en suivant un modèle du Hack & Leak, les publiant ensuite sur leur canal Telegram[137] [138]. Anonymous Sudan et KromSec ont également adopté ce modèle, revendiquant notamment la compromission de données du gouvernement français et de Microsoft[139][140][141][142].

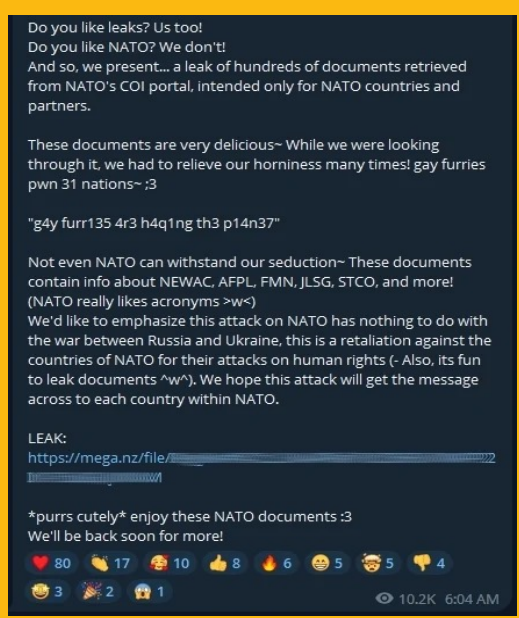
GhostSec quant à lui, a adopté le modèle de RaaS en faisant la promotion de son ransomware GhostLocker, alors que Gambling Hyena et Twelfth Hyena, soutenant l'Ukraine, ont démontré leur capacité à conduire des attaques de sabotage[143][144].

DIVULGATION DE DONNÉES SENSIBLES DE L'OTAN PAR LE GROUPE SIEGEDSEC

Le 24 juillet 2023, le groupe hacktiviste SiegedSec a revendiqué la compromission du portail de l'OTAN entrainant la fuite d'informations confidentielles (noms, adresses e-mails, numéros de téléphones et grades) d'au moins 70 responsables des 31 pays membres de l'organisation[137].

Entre septembre et octobre, le groupe a une fois de plus ciblé l'Organisation, revendiquant cette fois l'accès au portail de formations et de partage de documents[138].

Basées sur le modèle Hack & Leak, les activités de SiegedSec sont normalement centrées sur la recherche de gains financiers, ne soutenant que sporadiquement des actions à caractère hacktivistes. D'après les messages publiés sur Telegram par le groupe, l'attaque contre le portail aurait cependant été motivée par une violation des droits de l'homme attribuée par SiegedSec à l'OTAN.



Revendication du vol de données à l'OTAN par SiegedSec
Source : Telegram[218]

DES OPÉRATIONS D'ÉTATS-NATION DISSIMULÉES DERRIÈRE DES GROUPES HACKTIVISTES

Des APT associés à des États ont déguisé certaines attaques en opérations hacktivistes, complexifiant leur attribution ainsi que la lisibilité d'un écosystème qui devient de plus en plus poreux.

Des groupes hacktivistes pro-russes comme Solntsepyok et Free Civilian ont revendiqué des attaques, en particulier celle ayant ciblé la firme de télécommunications Kyïvstar en décembre 2023, qui auraient vraisemblablement été conduites par les APT Sandworm et DEV-0586 respectivement, attribués à la Russie[71][72][145].

Quant à l'Iran, des hacktivistes tels que Homeland Justice, que les autorités américaines ont attribué à l'Iran, ont ciblé des entités publiques et privées en Albanie[146][147]. Cyber Av3ngers qui s'est pour sa part démarqué par des attaques perturbant les infrastructures de traitement des eaux aux États-Unis, entretiendrait des liens avec le groupe Soldiers of Solomon attribué à l'Iran[148][149].

3. SOURCES

Sources

Page 6 / **CVE-2023-23397**, Microsoft Outlook

[65] CERT-XMCO, «[INFO] Le groupe APT28 attribué à la Russie a ciblé des pays membres de l'OTAN via l'exploitation de la CVE-2023-23397 dans Microsoft Outlook,» 08 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6787.

[150] CERT-XMCO, «[PATCH] [MICROSOFT] Prise de contrôle du système et élévation de privilèges via 6 vulnérabilités au sein de Microsoft Office (Word, Excel, PowerPoint, Outlook) (2023-Mar),» 15 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-1348 .

[151] CERT-XMCO, «[INFO] Un code d'exploitation tirant parti de la CVE-2023-23397 affectant Microsoft Outlook pourrait être réapproprié par des acteurs malveillants,» 17 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1420.

[152] CERT-XMCO, «[INFO] Exploitation active de la CVE-2023-23397 dans Outlook par le groupe APT28 attribué à la Russie,» 05 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6716.

Page 7 / **CVE-2023-22515 & CVE-2023-22518**, Atlassian Confluence Data Center et Server

[153] CERT-XMCO, «[INFO] Des acteurs malveillants exploitent les CVE-2023-22518 et CVE-2023-22515 dans les produits Confluence d'Atlassian,» 07 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6090.

[154] CERT-XMCO, «[INFO] Distribution de la web shell Effluence dans Confluence Data Center et Server d'Atlassian,» 15 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6222.

[155] CERT-XMCO, «[INFO] Le CISA fournit des informations supplémentaires sur l'exploitation de la CVE-2023-22515 dans Atlassian Confluence,» 23 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5785.

[156] CERT-XMCO, «[INFO] Exploitation active de la CVE-2023-22515 dans Confluence par le mode opératoire APT Storm-0062,» 12 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5516.

[131] CERT-XMCO, «[INFO] Le groupe hacktiviste Ukrainian Cyber Alliance a revendiqué la compromission du ransomware Trigona,» 20 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5747.

Page 8 / **CVE-2023-46604**, Apache ActiveMQ

[171] CERT-XMCO, «[PATCH] [APACHE] Prise de contrôle d'un système via une vulnérabilité dans Apache ActiveMQ,» 02 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-5926.

[172] CERT-XMCO, «[INFO] Exploitation de la CVE-2023-46604 dans Apache ActiveMQ pour distribuer le botnet GoTitan et d'autres malware,» 29 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6598.

[173] CERT-XMCO, «[INFO] Exploitation de la vulnérabilité CVE-2023-46604 affectant Apache ActiveMQ pour distribuer la webshell Godzilla,» 22 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0393.

[174] CERT-XMCO, «[INFO] Détection de nouvelles attaques exploitant la CVE-2023-46604 dans Apache ActiveMQ,» 20 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7040.

[175] CERT-XMCO, «[INFO] APT Andariel distribue 2 backdoors sur des serveurs de messagerie Apache ActiveMQ vulnérables à la CVE-2023-46604,» 27 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6543.

[176] CERT-XMCO, «[INFO] Des acteurs malveillants exploitent une vulnérabilité critique dans Apache ActiveMQ pour distribuer le ransomware HelloKitty,» 03 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6021.

Page 9 / **CVE-2023-34362**, Progress Software MOVEit Transfer

[159] CERT-XMCO, «[PATCH] [IPSWITCH] Manipulation de données et divulgation d'informations via une vulnérabilité au sein d'IPSwitch MOVEit,» 27 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-3384 .

[160] CERT-XMCO, «[INFO] Une vulnérabilité «0-day» massivement exploitée au sein de la plateforme MOVEit Transfer,» 02 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2887.

[161] CERT-XMCO, «[INFO] Exploitation de la «0-day» dans MOVEit Transfer par le groupe de ransomware Cl0p,» 06 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2927.

[162] CERT-XMCO, «[INFO] Retour sur l'exploitation de la «0-day» dans MOVEit Transfer par le groupe de ransomware Cl0p,» 12 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3045.

[163] CERT-XMCO, «[INFO] Compromission de l'État fédéral du Maine via l'exploitation de la vulnérabilité MOVEit,» 15 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6221 .

[164] CERT-XMCO, «[INFO] Compromission des données clients de Maximus par le groupe de ransomware Cl0p,» 02 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4061.

[165] CERT-XMCO, «[INFO] La liste des victimes de Cl0p s'allonge alors que des chercheurs découvrent une nouvelle vulnérabilité dans MOVEit Transfer,» 16 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3207.

Pages 11 à 13 / [INFO] **Anonymous Sudan**, campagne d'attaques contre le secteur hospitalier français

[2] CERT-XMCO, «[INFO] Le groupe de ransomware Akira cible les produits VPN de Cisco comme vecteur de compromission initiale» 24 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4553.
[3] CERT-XMCO, «[INFO] Le groupe de ransomware Cuba cible des infrastructures critiques aux États-Unis et en Amérique latine en exploitant les CVE-2023-27532 et CVE-2020-1472,» 23 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4515.
[4] CERT-XMCO, «[INFO] Retour sur l'exploitation de la «0-day» dans MOVEit Transfer par le groupe de ransomware Cl0p,» 12 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3045.

Pages 15 à 16 / **RANSOMWARE**, évolutions des modes opératoires

[1] CERT-XMCO, «[INFO] Rapport sur le ransomware Mallox ciblant les serveurs MS-SQL,» 25 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3920.
[2] CERT-XMCO, «[INFO] Le groupe de ransomware Akira cible les produits VPN de Cisco comme vecteur de compromission initiale,» 24 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4553.
[3] CERT-XMCO, «[INFO] Le groupe de ransomware Cuba cible des infrastructures critiques aux États-Unis et en Amérique latine en exploitant les CVE-2023-27532 et CVE-2020-1472,» 23 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4515.
[4] CERT-XMCO, «[INFO] Retour sur l'exploitation de la «0-day» dans MOVEit Transfer par le groupe de ransomware Cl0p,» 12 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3045.
[5] CERT-XMCO, «[INFO] Des affiliés du ransomware Cl0p affirment avoir compromis le SI de 130 organisations en exploitant la faille 0-day affectant GoAnywhere MFT,» 16 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0838.
[6] CERT-XMCO, «[INFO] Exploitation d'une 0-day par les opérateurs de Cl0p dans le logiciel SysAid On-Prem,» 09 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6140.
[7] CERT-XMCO, «[INFO] Des affiliés utilisent des outils RMM pour distribuer le ransomware LockBit,» 25 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5082.
[8] CERT-XMCO, «[INFO] Le groupe de ransomware Play cible les fournisseurs de services managés (MSP),» 18 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4451.
[9] CERT-XMCO, «[INFO] L'usurpation de site : nouvelle méthode des attaques ransomware pour augmenter la visibilité des données volées,» 04 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0026.
[10] CERT-XMCO, «[INFO] Le ransomware ALPHV/BlackCAT soumet une déclaration d'incident à la SEC pour accroître la pression sur l'une de ses victimes,» 17 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6346.
[11] CERT-XMCO, «[INFO] Les opérateurs du ransomware LockBit imposent de nouvelles règles à leurs affiliés pour la négociation des rançons,» 21 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6389.
[12] CERT-XMCO, «[INFO] Le groupe ransomware HardBit demanderait le détail des cyberassurances de ses victimes pour maximiser ses profits,» 24 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1005.
[13] CERT-XMCO, «[INFO] Les autorités américaines saisissent l'infrastructure du ransomware ALPHV/BlackCat,» 20 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7039.
[14] CERT-XMCO, «[INFO] Hive Ransomware : une opération coordonnée des forces de l'ordre démantèle les serveurs du groupe cybercriminel,» 27 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0479.
[15] CERT-XMCO, «[INFO] Une opération internationale a saisi le site d'extorsion du ransomware RagnarLocker,» 20 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5752.
[16] CERT-XMCO, «[INFO] Arrestation d'un membre du groupe de ransomware RagnarLocker à Paris,» 27 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5882.
[17] CERT-XMCO, «[INFO] La CISA publie un script permettant aux entreprises affectées par le ransomware ESXiArgs d'automatiser la récupération de leurs machines,» 08 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0643.
[18] CERT-XMCO, «[INFO] SentinelLabs a identifié une faille dans le variant Linux du ransomware Cl0p et propose un kit de déchiffrement,» 09 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0668.
[19] CERT-XMCO, «[INFO] Kaspersky publie un déchiffreur pour le ransomware de Conti,» 17 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1415.
[20] CERT-XMCO, «[INFO] Outil de déchiffrement proposé par Avast contre le ransomware Akira,» 05 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3489.
[21] Europol, «Cybercriminals stung as HIVE infrastructure shut down,» 26 Janvier 2023. [En ligne]. Available: https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.

[22] CERT-XMCO, «[INFO] LockBit utilise un nouveau logiciel de chiffrement basé sur Conti nommé LockBit Green,» 03 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0556.
[23] CERT-XMCO, «[INFO] LockBit Green utiliserait des éléments de code du ransomware Conti,» 29 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3382.
[24] CERT-XMCO, «[INFO] Identification du nouveau groupe de ransomware «Hunters International», aux liens supposés avec Hive,» 30 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5947.
[25] CERT-XMCO, «[INFO] Des affiliés de Conti ont rejoint le groupe de ransomware Akira,» 21 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5056.
[26] CERT-XMCO, «[INFO] Le responsable de LockBit tente de récupérer les affiliés et les développeurs des ransomware BlackCat/ALPHV et NoEscape,» 14 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6918.
[27] CERT-XMCO, «[INFO] Scattered Spider affilié du RaaS BlackCat/Alphv,» 20 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5008.
[28] CERT-XMCO, «[INFO] Le groupe de ransomware APLHV/BlackCat revendique la compromission de MGM Resorts,» 15 09 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4979.
[29] CERT-XMCO, «[INFO] Les autorités américaines alertent sur des attaques du ransomware BlackCat/ALPHV ciblant le secteur de la santé,» 28 Février 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1186.
[209] CERT-XMCO, «[INFO] Confirmation des liens entre le ransomware Hunters International et Hive,» 13 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6175.

Pages 19 à 20 / **PRINCIPALES TENDANCES IDENTIFIÉES**

[5] CERT-XMCO, «[INFO] Des affiliés du ransomware Cl0p affirment avoir compromis le SI de 130 organisations en exploitant la faille 0-day affectant GoAnywhere MFT,» 16 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0838.
[61] CERT-XMCO, «ACTUSÉCU #61 - Hors-Série spécial Dark Web,» Janvier 2024. [En ligne]. Available: https://www.xmco.fr/wp-content/uploads/2024/02/XMCO-ActuSecu-61-Dark-Web-Spyware.pdf.
[189] CERT-XMCO, «[EXPLOIT] [APACHE] Prise de contrôle du système via une vulnérabilité au sein d'Apache ActiveMQ,» 07 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-6070.
[190] Horizon3.ai, «CVE-2023-27350,» Avril 2023. [En ligne]. Available: https://github.com/horizon3ai/CVE-2023-27350.
[191] Frycos Security Diary, «GoAnywhere MFT - A Forgotten Bug,» 06 Février 2023. [En ligne]. Available: https://frycos.github.io/vulns4free/2023/02/06/goanywhere-forgotten.html.
[192] CERT-XMCO, «[INFO] Compromission d'Ivanti Endpoint Manager (anciennement MobileIron Core) par des acteurs de la menace ciblant 12 ministères norvégiens,» 25 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3934.
[193] CERT-XMCO, «[VULN] [CISCO] Prise de contrôle du système et élévation de privilèges via une vulnérabilité au sein de Cisco IOS XE (cisco-sa-iosxe-webui-privesc-j22SaA4z),» 17 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-5609.
[194] CERT-XMCO, «[INFO] Exploitation active d'une vulnérabilité critique dans l'interface utilisateur de gestion Web du logiciel Cisco IOS XE,» 17 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5606.
[195] CERT-XMCO, «[INFO] Mise à jour de l'implant distribué sur les appareils Cisco IOS XE vulnérables aux CVE-2023-20198 et CVE-2023-20273,» 25 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5817.
[196] CERT-XMCO, «[INFO] Cisco publie une nouvelle vulnérabilité zero-day dans IOS XE,» 23 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5780.
[197] CERT-XMCO, «[PATCH] [IVANTI] Contournement de sécurité et manipulation de données via une vulnérabilité au sein d'Ivanti Endpoint Manager Mobile (MobileIron Core),» 25 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2023-3931.
[198] CERT-XMCO, «[INFO] Exploitation active d'une vulnérabilité de Cisco Adaptive Security Appliance (ASA) et Cisco Firepower Threat Defense (FTD) pour distribuer des ransomware,» 12 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4853.
[200] CERT-XMCO, «[INFO] Apple corrige une vulnérabilité exploitée par le spyware Triangulation,» 25 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3942.
[201] CERT-XMCO, «[INFO] Apple corrige 2 vulnérabilités de type «0-day» exploitées par le spyware Pegasus,» 08 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4820.
[202] CERT-XMCO, «[INFO] La société russe «Operation Zero» augmente les récompenses financières pour les découvertes de «0-day»,» 29 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5212.
[203] CERT-XMCO, «[INFO] Google corrige une vulnérabilité de type «0-day» activement exploitée dans Chrome,» 29 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5225.
[204] CERT-XMCO, «Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses,» 14 Mars 2023. [En ligne]. Available: https://carnegieendowment.org/2023/03/14/why-doesglobal-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

[30] CERT-XMCO, «[INFO] Le mode opératoire UNC2975 distribue DarkGate et DanaBot via du malvertising,» 21 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7015.
[31] CERT-XMCO, «[INFO] Utilisation abusive du service Google Ads par des acteurs de la menace pour distribuer des malwares,» 27 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2144.
[32] CERT-XMCO, «[INFO] Atomic Stealer distribué aux utilisateurs Mac dans le cadre de la campagne de phishing ClearFake,» 24 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6496.
[33] CERT-XMCO, «[INFO] Une campagne de phishing et de malvertising distribue PikaBot, notamment en France,» 18 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6981.
[34] CERT-XMCO, «[INFO] Découverte d'une vaste infrastructure de distribution des infostealers Raccoon et Vidar,» 10 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0105.
[35] CERT-XMCO, «[INFO] SYS01stealer : un nouvel infostealer diffusé à partir de publicités sur Google et Facebook,» 14 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1235.
[36] CERT-XMCO, «[INFO] Une nouvelle campagne d'attaques du trojan Qbot utiliserait des fichiers vérolés OneNote,» 15 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0803.
[37] CERT-XMCO, «[INFO] Face au blocage par défaut des macros Office, des attaquants utiliseraient des add-in Excel,» 04 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0041.
[38] CERT-XMCO, «[INFO] Des opérateurs de ransomware utilisent Google Ads pour compromettre leurs cibles,» 25 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0436.
[39] CERT-XMCO, «[INFO] Security Affairs publie une analyse technique d'une campagne infectant la France avec NullMixer,» 05 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1696.
[40] CERT-XMCO, «[INFO] Cyble publie l'analyse technique d'une variante du botnet Medusa incluant un module ransomware,» 08 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0642.
[41] CERT-XMCO, «[INFO] Détection d'une nouvelle variante du botnet P2Pinfect ciblant des appareils embarqués,» 05 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6718.
[42] CERT-XMCO, «[INFO] Nouvelle campagne d'une variante du botnet Mirai nommée IZ1H9,» 16 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5560.
[43] CERT-XMCO, «[INFO] Rapport d'Accenture sur l'augmentation des attaques ciblant macOS,» 21 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4481.
[44] CERT-XMCO, «[INFO] MacStealer : Un nouveau infostealer ciblant MacOS a été identifié,» 03 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1660.
[45] CERT-XMCO, «[INFO] Identification d'un nouvel infostealer ciblant les instances macOS de professionnels,» 13 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4897.
[46] CERT-XMCO, «[INFO] Un nouvel infostealer nommé « Atomic MacOS » serait en vente sur Telegram,» 03 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2294.
[47] CERT-XMCO, «[INFO] Le ransomware Akira ciblerait les hyperviseurs VMware ESXi avec un chiffreur Linux,» Avril Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3460.
[48] CERT-XMCO, «[INFO] LockBit diversifie ses capacités en développant un ransomware ciblant MacOS,» 19 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2032.
[49] CERT-XMCO, «[INFO] Le malware SysUpdate évolue et possède maintenant une version Linux,» 03 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1132.
[50] CERT-XMCO, «[INFO] LAZARUS développe RustBucket afin de cibler davantage de systèmes d'exploitation dont macOS,» 28 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2263.
[51] CERT-XMCO, «[INFO] Le FBI a annoncé le démantèlement du botnet Qakbot,» 29 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4664.
[52] CERT-XMCO, «[INFO] Le FBI saisit l'infrastructure du Botnet-as-a-Service IPStorm,» 16 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6309.
[53] CERT-XMCO, «[INFO] La marketplace cybercriminelle Genesis a été saisie par les forces de l'ordre,» 05 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1723.
[54] CERT-XMCO, «[INFO] Le FBI saisit BreachForums, 3 mois après avoir appréhendé son administrateur Pompompurin.,» 27 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3365.
[55] CERT-XMCO, «[INFO] Europol et 9 pays saisissent la marketplace Monopoly Market et arrêtent 288 vendeurs,» 09 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2381.
[56] CERT-XMCO, «[INFO] Les opérateurs de Qakbot distribuent le ransomware Ransom Knight en dépit du démantèlement de leur infrastructure,» 10 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5397.
[57] CERT-XMCO, «[INFO] Retour de Qakbot dans une campagne de phishing ciblant le secteur du tourisme aux Etats-Unis,» 18 Décembre 2023. [En ligne]. Available: https:/leportail.xmco.fr/watch/advisory/CXN-2023-6982.

[58] CERT-XMCO, «[INFO] Analyse du Malware-as-a-Service DarkGate,» 23 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6493.
[59] CERT-XMCO, «[INFO] Divulgation d'une base de données des utilisateurs de RaidForums par l'administrateur Impotent du forum Exposed,» 30 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2812.
[60] CERT-XMCO, «[INFO] La plateforme Telegram est le nouveau hub de la cybercriminalité,» 07 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0614.
[61] CERT-XMCO, «ACTUSÉCU #61 - Hors-Série spécial Dark Web,» Janvier 2024. [En ligne]. Available: https://www.xmco.fr/wp-content/uploads/2024/02/XMCO-ActuSecu-61-Dark-Web-Spyware.pdf.
[62] The Record, «Genesis Market, one of world's largest platforms for cyber fraud, seized by police,» 04 Avril 2023. [En ligne]. Available: https://therecord.media/genesis-market-takedown-cybercrime.
[215] CERT-XMCO, «[INFO] Publication d'un rapport détaillé sur la compromission des victimes de Genesis Market,» 04 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1919.
[216] CERT-XMCO, «[INFO] Les données saisies par le FBI lors de la fermeture de la marketplace cybercriminelle Genesis Market sont consultables dans Have I Been Pwned,» 06 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1748.

Page 25 / **LA RUSSIE** [le piratage au service des États]

[63] CERT-XMCO, «[INFO] Observation du mode opératoire APT BlueDelta ciblant les organisations ukrainiennes,» 23 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3293.
[64] CERT-XMCO, «[INFO] APT Winter Vivern cible des entités gouvernementales européennes via une «0-day» dans les serveurs Roundcube Webmail,» 26 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5877.
[65] CERT-XMCO, «[INFO] Le groupe APT28 attribué à la Russie a ciblé des pays membres de l'OTAN via l'exploitation de la CVE-2023-23397 dans Microsoft Outlook,» 08 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6787.
[66] CERT-XMCO, «[INFO] APT29 exploite des fichiers PDF malveillants pour cibler des instances diplomatiques de membres de l'OTAN,» 21 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4428.
[67] CERT-XMCO, «[INFO] Winter Vivern cible les portails webmail des institutions de pays alignés avec l'OTAN,» 06 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1727.
[68] CERT-XMCO, «[INFO] APT28 cible 13 pays dans une campagne de phishing utilisant le conflit israélo-palestinien comme leurre,» 14 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6875.
[69] CERT-XMCO, «[INFO] Le groupe APT russe Sandworm a conduit une attaque de sabotage visant une organisation critique en Ukraine,» 10 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6168.
[70] CERT-XMCO, «[INFO] L'APT Sandworm ciblerait le secteur énergétique ukrainien avec NikoWiper, une nouvelle souche de wiper,» 03 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0544.
[71] CERT-XMCO, «[INFO] Les services de sécurité ukrainiens confirment l'implication du groupe APT russe Sandworm dans l'attaque ayant ciblé Kyïvstar,» 05 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0079.
[72] CERT-XMCO, «[INFO] Retour sur la compromission de l'opérateur mobile ukrainien Kyïvstar revendiquée par des hacktivistes pro-russes,» 15 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6953.
[73] CERT-XMCO, «[INFO] Un nombre croissant de wipers a été utilisé dans le cadre du conflit en Ukraine,» 02 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0521.
[152] CERT-XMCO, «[INFO] Exploitation active de la CVE-2023-23397 dans Outlook par le groupe APT28 attribué à la Russie,» 05 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6716.
[217] CERT-XMCO, «[INFO] Détection d'une campagne de phishing d'APT28 ciblant l'Ukraine et la Pologne,» 28 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7197.

Page 26 / **LA CORÉE DU NORD** [le piratage au service des États]

[74] CERT-XMCO, «[INFO] Chevauchement d'infrastructures entre les campagnes RustBucket et KandyKorn opérées par des APTs attribués à la Corée du Nord,» 29 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6577.
[75] CERT-XMCO, «[INFO] Distribution du malware macOS Kandykorn par l'APT associé à la Corée du Nord Lazarus,» 06 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6031.
[76] CERT-XMCO, «[INFO] Les opérateurs de Lazarus ciblent des développeurs et des chercheurs en cybersécurité sur GitHub,» 24 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3901.
[77] CERT-XMCO, «[INFO] Des APTs attribuées à la Corée du Nord ciblent les développeurs et les firmes du secteur informatique à des fins d'espionnage et de gain financier,» 24 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6498.
[78] CERT-XMCO, «[INFO] L'agence américaine de cybersécurité publie un bulletin sur la menace ransomware émanant de Corée du Nord,» 14 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0741.
[79] CERT-XMCO, «[INFO] Rapport de Kaspersky sur les modes opératoires asiatiques de type APT,» 13 Novembre 2023.

[En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6141.
[80] CERT-XMCO, «[INFO] Un groupe nord-coréen serait à l'origine de l'attaque par supply chain de 3CX,» 13 Avril 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1904.
[81] CERT-XMCO, «[INFO] L'APT nord-coréenne Diamond Sleet exploite une version malveillante d'un logiciel Cyberlink,» 24 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6497.
[82] CERT-XMCO, «[INFO] Le Royaume-Uni et la Corée du Sud alertent sur les attaques supply chain attribuées à des APTs nord-coréennes,» 24 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6516.
[83] CERT-XMCO, «[INFO] Exploitation de la CVE-2023-42793 dans les serveurs TeamCity par des modes opératoires associés à la Corée du Nord,» 20 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5722.
[84] CERT-XMCO, «[INFO] APT Lazarus a ciblé une entreprise aérospatiale espagnole avec la backdoor LightlessCan,» 04 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5295.
[85] CERT-XMCO, «[INFO] Les secteurs de l'énergie et de la défense d'Europe de l'Est ciblés par une mise à jour du framework MATA,» 26 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5823.
[86] CERT-XMCO, «[INFO] Détection du mode opératoire APT Kimsuky ciblant l'exercice militaire conjoint entre les États-Unis et la Corée du Sud,» 23 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4517.
[87] CERT-XMCO, «[INFO] Compromission des serveurs de Mashinostroyeniya par APT ScarCruft,» 09 Août 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4182.
[88] CERT-XMCO, «[INFO] La majorité des attaques ciblant la Russie seraient réalisées par des APTs associés à la Chine et la Corée du Nord,» 22 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6419.

Page 27 / **LA CHINE** [le piratage au service des États]

[89] CERT-XMCO, «[INFO] Les attaques cyber intensifient les tensions entre la Chine et Taïwan,» 23 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2665.
[90] CERT-XMCO, «[INFO] Le groupe Earth Longzhi ciblerait les pays d'Asie Pacifique en utilisant des techniques avancées,» 05 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2335.
[91] CERT-XMCO, «[INFO] Campagne d'attaques ciblant des entreprises de semi-conducteurs basées à Taïwan, Hong Kong et Singapour,» 09 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5388.
[92] CERT-XMCO, «[INFO] Identification du nouveau mode opératoire APT Grayling,» 12 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5479.
[93] CERT-XMCO, «[INFO] Campagne de désinformation pro-chinoise ciblant Taïwan en marge des élections présidentielles de janvier 2024,» 27 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7174.
[94] CERT-XMCO, «[INFO] Détection du mode opératoire APT Gelsemium ciblant un gouvernement d'Asie du Sud-Est,» 25 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5131.
[95] CERT-XMCO, «[INFO] Des APTs associés à la Chine ciblent des entités cambodgiennes à des fins d'espionnage,» 09 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6126.
[96] CERT-XMCO, «[INFO] Les modes opératoires APTs chinois ciblent l'Asie à des fins d'espionnage,» 28 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5183.
[97] CERT-XMCO, «[INFO] Identification d'une nouvelle backdoor exploitée par le mode opératoire Camaro Dragon,» 16 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3176.
[98] CERT-XMCO, «[INFO] Identification d'une backdoor associée au mode opératoire APT REF5961 attribué à la Chine,» 19 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5717.
[99] CERT-XMCO, «[INFO] APT Chimera, attribué à la Chine, a compromis la société de semiconducteurs NXP pendant plus de 2 ans,» 28 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6574.
[100] CERT-XMCO, «[INFO] La France serait particulièrement ciblée par le cyberespionnage chinois d'après l'ANSSI,» 27 Janvier 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0467.
[101] CERT-XMCO, «[INFO] Deux agences européennes de cybersécurité mettent en garde contre les attaques de groupes chinois,» 21 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0918.
[102] CERT-XMCO, «[INFO] Des attaques associées à RedDelta cibleraient diverses instances étatiques en Europe,» 06 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3512.
[103] CERT-XMCO, «[INFO] APT Volt Typhoon distribue KV-botnet dans le cadre d'une campagne d'attaques ciblant des dispositifs IoT,» 14 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6919.
[104] CERT-XMCO, «[INFO] APT Volt Typhoon aurait ciblé plusieurs infrastructures critiques américaines,» 29 Mai 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2750.
[105] CERT-XMCO, «[INFO] Identification d'une campagne d'influence pro-chinoise sur YouTube,» 20 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7032.
[106] CERT-XMCO, «[INFO] Nouvelles campagnes d'influence russes et chinoises sur les réseaux sociaux de Meta,» 04 Décembre 2023.

[En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6694.

Page 28 / **L'IRAN** [le piratage au service des États]

[107] CERT-XMCO, «[INFO] APT42 exploiterait la payload NokNok pour cibler des systèmes macOS,» 13 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3602.
[108] CERT-XMCO, «[INFO] Le groupe APT attribué à l'Iran Peach Sandstorm cible le secteur de la défense avec la nouvelle backdoor personnalisée FalseFont,» 22 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7114.
[109] CERT-XMCO, «[INFO] APT33 a ciblé des milliers d'organisations via une attaque de type «password spraying»,» 15 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4977.
[110] CERT-XMCO, «[INFO] Compromission d'une organisation aéronautique américaine par un mode opératoire associé à l'Iran,» 08 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4823.
[111] CERT-XMCO, «[INFO] Le groupe APT associé à l'Iran Mint Sandstorm cible des organismes de recherche et des universités avec de nouvelles TTPs,» 18 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0347.
[112] CERT-XMCO, «[INFO] Microsoft attribue la cyberattaque de janvier 2023 contre Charlie Hebdo à un acteur sponsorisé par le régime iranien,» 06 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0601.
[113] CERT-XMCO, «[INFO] Identification d'une nouvelle backdoor associée au mode opératoire Charming Kitten,» 12 Septembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4864.
[114] CERT-XMCO, «[INFO] Le mode opératoire APT34 exploite une variante du malware SideTwist,» 03 Octobre 2023. [En ligne]. Available: https://eportail.xmco.fr/watch/advisory/CXN-2023-5285.
[115] CERT-XMCO, «[INFO] Exploitation du framework LIONTAIL par APT Scarred Manticore pour cibler des entités au Moyen-Orient,» 06 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6036.
[116] CERT-XMCO, «[INFO] Le mode opératoire APT Crambus a compromis une instance gouvernementale au Moyen-Orient pendant 8 mois,» 24 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5787.
[117] CERT-XMCO, «[INFO] APT Agonizing Serpens cible le secteur de l'éducation et des technologies en Israël avec des wipers,» 08 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6109.
[118] CERT-XMCO, «[INFO] Détection du mode opératoire APT MuddyWater ciblant des entités israéliennes,» 06 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6039.
[119] CERT-XMCO, «[INFO] L'APT iranien MuddyWater utilise le nouveau framework MuddyC2Go,» 15 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6167.
[121] CERT-XMCO, «[INFO] Analyse de l'infrastructure d'une application du Hamas qui serait liée aux acteurs de la menace palestiniens,» 23 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5753.
[122] CERT-XMCO, «[INFO] L'APT Gaza Cybergang associée au Hamas cible des entités palestiniennes et israéliennes avec la porte dérobée Pierogi++ et le malware Micropsia,» 18 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6956.
[123] CERT-XMCO, «[INFO] Étude du mode opératoire APT AridViper en marge des affrontements dans la bande de Gaza,» 31 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5949.

Pages 30 à 32 / **HACKTIVISTES**, activités liées au contexte géopolitique

[120] CERT-XMCO, «[INFO] Synthèse des opérations cyber en marge du conflit armé entre Israël et le Hamas,» 14 Février 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0881.
[124] CERT-XMCO, «[INFO] Campagne d'attaque d'Anonymous Sudan contre le secteur hospitalier français,» 05 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3514.
[125] CERT-XMCO, «[INFO] Le groupe hacktiviste NoName057(16) cible le ministère de l'Économie et des Finances français,» 03 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5268.
[126] CERT-XMCO, «[INFO] Killnet revendique des attaques DDoS sur plusieurs aéroports européens dont certains en France,» 16 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5584.
[127] CERT-XMCO, «[INFO] Attaque DDoS du groupe Noname057(16) contre les sites de la SMP WAGNER,» 28 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3406.
[128] CERT-XMCO, «[INFO] Campagne d'attaques menée par les partisans de la SMP WAGNER,» 04 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3488.
[129] CERT-XMCO, «[INFO] Les aéroports russes touchés par une campagne d'attaques DDoS de l'IT Army of Ukraine,» 02 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5244.
[130] CERT-XMCO, «[INFO] L'IT Army of Ukraine revendique la compromission de Gazprom et l'accès à 1,5GB d'archives,» 03 Février 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0538.
[131] CERT-XMCO, «[INFO] Le groupe hacktiviste Ukrainian Cyber Alliance a revendiqué la compromission du ransomware Trigona,» 20 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5747.

[132] Telegram, «NoName057(16),» [En ligne]. Available: https://t.me/s/noname05716.
[133] Telegram, «Anonymous Sudan,» [En ligne]. Available: https://t.me/s/xAnonymousSudan.
[134] CERT-XMCO, «[INFO] Focus sur les opérations hacktivistes visant la France en marge du conflit israélo-palestinien,» 31 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5951.
[135] CERT-XMCO, «[INFO] Opérations d'influence pro-iraniennes en marge du conflit dans la bande de Gaza,» 08 Février 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0717.
[136] CERT-XMCO, «[INFO] Israël-Palestine : Intensification des attaques DDoS en marge de l'affrontement armé,» 10 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5393.
[137] CERT-XMCO, «[INFO] Divulgations de données sensibles de l'OTAN par le groupe SiegedSec,» 27 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3974.
[138] CERT-XMCO, «[INFO] Le groupe hacktiviste SiegedSec revendique une fuite de données sensibles de l'OTAN,» 10 Octobre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5401.
[139] CERT-XMCO, «[INFO] Ministère de la Justice français : divulgation de données personnelles par le groupe hacktiviste KromSec,» 04 Juillet 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3509.
[140] CERT-XMCO, «[INFO] Le groupe hacktiviste KromSec revendique une cyberattaque contre l'Assemblée nationale,» 21 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6412.
[141] CERT-XMCO, «[INFO] Anonymous Sudan revendique de nouvelles attaques DDoS et fait fuiter des données de compagnies aériennes françaises,» 20 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1436.
[142] CERT-XMCO, «[INFO] Attaques par DDoS sur OneDrive revendiquées par Anonymous Sudan,» 09 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3021.
[143] CERT-XMCO, «[INFO] Chevauchements de TTPs entre 2 groupes hacktivistes ciblant des entités en lien avec les autorités russes,» 29 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7212.
[144] CERT-XMCO, «[INFO] Le groupe hacktiviste GhostSec fait la promotion de leur RaaS GhostLocker,» 08 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6095 .
[145] CERT-XMCO, «[INFO] Attribution d'attaques par wipers au mode opératoire Cadet Blizzard,» 16 Juin 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3180.
[146] CERT-XMCO, «[INFO] Analyse de l'attaque du groupe hacktiviste pro-Iran Homeland Justice contre l'Albanie,» 08 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0087.
[147] CERT-XMCO, «[INFO] Le groupe hacktiviste pro-iranien Homeland Justice revendique une campagne d'attaques contre l'Albanie,» 02 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0014.
[148] CERT-XMCO, «[INFO] Le groupe hacktiviste pro-iranien Cyber Av3ngers exploite des automates Unitronics dans les systèmes de traitement des eaux usées aux États-Unis,» 29 Novembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6603.
[149] CERT-XMCO, «[INFO] Analyse du mode opératoire du groupe Cyber Av3ngers, ciblant les systèmes de traitement des eaux aux Etats-Unis,» 04 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6690.
[210] CERT-XMCO, «[INFO] Anonymous Sudan revendique des attaques DDoS visant les sites Internet d'aéroports et d'établissements hospitaliers français,» 16 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1390.
[211] CERT-XMCO, «[INFO] Anonymous Sudan revendique des attaques DDoS visant les sites Internet d'universités françaises,» 17 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1409 .
[212] CERT-XMCO, «[INFO] Anonymous Sudan annonce de nouvelles attaques DDoS visant des établissements hospitaliers et des aéroports français,» 22 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1478.
[213] CERT-XMCO, «[INFO] Ouverture d'une enquête sur les récentes attaques du collectif prorusse Anonymous Sudan,» 23 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1500 .
[214] CERT-XMCO, «[INFO] L'Assemblée nationale victime d'une attaque DDoS par le groupe prorusse NoName057(16),» 28 Mars 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-1580.
[218] CERT-XMCO, «SiegedSec,» [En ligne]. Available: https://t.me/s/SiegedSecurity.
[71] CERT-XMCO, «[INFO] Les services de sécurité ukrainiens confirment l'implication du groupe APT russe Sandworm dans l'attaque ayant ciblé Kyïvstar,» 05 Janvier 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0079.
[72] CERT-XMCO, «[INFO] Retour sur la compromission de l'opérateur mobile ukrainien Kyïvstar revendiquée par des hacktivistes pro-russes,» 15 Décembre 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6953.

yuno By XMCO

Ce bilan des activités **yuno** en 2023 a été réalisé par le service de veille en menace cyber du CERT-XMCO.

yuno propose 2 types de services pour répondre aux besoins de ses clients :

Une veille quotidienne sur les vulnérabilités et les menaces cyber du moment.

- Plus de 1500 technologies et éditeurs suivis.
- Plus de 1000 sources d'informations différentes.

Une veille récurrente (hebdomadaire, mensuelle ou trimestrielle) et ciblée sur des menaces spécifiques.

- Focus par géographie, secteur ou type de menace.
- Approche et analyse Cyber Threat Intelligence.

À propos du

cert By xmco

Le CERT-XMCO met à votre disposition son équipe d'experts, afin de vous aider à protéger votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité.

Le CERT-XMCO est le CSIRT de la société XMCO. Il est reconnu par le CERT gouvernemental français (le CERT-FR), ainsi que par la TF-CSIRT et le Trusted Introducer, ce qui lui permet d'obtenir les informations et de collaborer avec les autres CERT français et européens.

Le CERT-XMCO protège votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité (veille en vulnérabilités, Cyber Threat-Intelligence, Réponse à Incident, Accompagnement à la remédiation, etc.).

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à cœur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le cœur de métier historique : l'audit et les tests d'intrusion.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

info@xmco.fr

01 79 35 29 30