DOSSIER SPÉCIAL

PANORAMA DE LA MENACE CYBER

SECTEUR DE L'ÉNERGIE / 2022

cert By xmco

Sommaire

Avant-propos

NOUS AVONS LE PLAISIR DE VOUS PRÉSENTER **LE PANORAMA DE LA MENACE CYBER** DU SECTEUR DE L'ÉNERGIE EN 2022. CE RAPPORT EST ISSU DU TRAVAIL DE VEILLE MENÉ PAR LES ANALYSTES DE CYBER THREAT INTELLIGENCE (CTI) AU SEIN DU CERT-XMCO.

Bien qu'étant principalement centré sur les attaques observées en 2022, les analyses et conclusions de ce rapport demeurent utiles pour les organisations du secteur de l'énergie qui cherchent à bénéficier d'une meilleur visibilité des menaces qui pèsent sur le secteur.

Ce rapport vise à fournir une analyse approfondie des menaces émergentes, des tendances observées et des attaques ayant ciblé le secteur de l'énergie en 2022. En cela, nous espérons renforcer la sensibilisation et la préparation de nos clients face aux menaces cyber.

Il est essentiel de souligner que la menace cyber est un défi commun, nécessitant une collaboration étroite entre les entités publiques et privées, expliquant notre approche proactive en matière d'anticipation de la menace.

Nous espérons que ce rapport puisse vous fournir des clés de compréhension, et permettre la mise en place des mesures de protection adéquates à votre secteur d'activités.

Executive Summary

CONTEXTE

L'invasion de l'Ukraine par la Fédération de Russie en février 2022 et ses implications sur l'approvisionnement énergétique en Europe ont eu des conséquences significatives sur l'écosystème cybercriminel, marqué notamment par la dislocation du groupe de ransomware russophone Conti et l'apparition de groupes hacktivistes pro-russes et pro-ukrainiens. Les tensions géopolitiques entre la Chine et l'Inde en 2022 ont alimenté une escalade des activités cyber à l'encontre du secteur de l'énergie devenant une cible privilégiée pour les modes opératoires APTs en Asie centrale et orientale. Certains d'entre eux se sont illustrés par leur capacité d'évasion, tirant profit des faiblesses des systèmes de contrôle industriel (ICS/SCADA) à des fins de collecte de renseignements et de sabotage. Au Moyen-Orient, plusieurs modes opératoires associés à l'Iran ont été observés ciblant le secteur de l'énergie. En effet, APT33 (connu sous le nom d'Elfin) et APT34 (connu sous le nom d'Hazel Sandstorm) ou encore APT35 (connu sous le nom de Mint Sandstorm) auraient ciblé des entreprises et des infrastructures critiques du secteur de l'énergie, participant à l'élaboration d'une stratégie de **blanchiment d'influence** (minimiser l'implication directe d'un acteur et à sous-traiter des intermédiaires non officiels, privés ou étrangers les activités offensives cyber).

La convergence continue des technologies de l'information (IT) et des technologies opérationnelles (OT) a conduit le secteur de l'énergie vers une augmentation de sa surface d'exposition. Au cours de l'année 2022, le nombre de vulnérabilités signalées par DRAGOS[3], dans les systèmes ICS/SCADA a augmenté de 27%, passant de 1703 CVEs identifiées en 2021 à 2 170 en 2022[4]. Enfin, le CERT-XMCO a recensé **49 attaques par ransomware** ayant ciblé le secteur de l'énergie en 2022, un nombre important et représentatif des augmentations observées ces **dernières années[5].**

POINTS CLÉS

L'invasion de l'Ukraine par la Russie en février 2022 a profondément fait évoluer le paysage de la menace, en particulier pour le secteur de l'énergie dont les enjeux sont au cœur de cette guerre.

Peu d'informations sur les **campagnes d'espionnage** ciblant des organisations du secteur de l'énergie sont disponibles et elles concernent des MOA chinois et russes. L'analyse géopolitique (corroborée avec le peu d'informations disponibles) est donc centrale pour proposer des analyses pertinentes. À cet égard les organisations les plus exposées sont :

- Entreprises implantées sur des zones géographiques en tension, tous sous-secteurs énergétiques confondus;
- Entreprises à fort patrimoine intellectuel;
- Multinationales stratégiques dont le positionnement géopolitique n'est pas en ligne avec les États-Unis et la Chine.

L'Ukraine est la principale cible **d'attaques de destruction** d'infrastructures énergétiques électriques, car il s'agit d'un territoire en guerre dont les frontières sont contestées par la Russie. Avec la multiplication des conflits territoriaux impliquant des États disposant de capacités cyber avancées, Taiwan, l'Inde, le Pakistan, l'Arabie Saoudite, l'Iran, l'Europe de l'Est et l'Asie du Sud-Est constituent des espaces de risques majeurs.

Les **attaques cybercriminelles** sont principalement des attaques de type ransomware, avec une victimologie, pour le secteur de l'énergie, principalement identifiée autour de deux pôles : Amérique du Nord/Europe de l'Ouest et Amérique latine/ Asie du Sud-Est. Aussi, le risque ransomware est accentué en Europe par le déclenchement de la guerre en Ukraine, avec des opérations susceptibles d'être alignées avec les intérêts russes. Cela étant, de nombreuses campagnes ne sont pas revendiquées pour ne pas reproduire la situation d'alerte des autorités après l'attaque contre Colonial Pipeline. Autrement, le risque ransomware demeure opportuniste.

Plus largement, on a observé la multiplication de **groupes hacktivistes** portant des revendications politiques et géopolitiques et qui prennent pour cibles des organisations publiques et privées, dont certaines appartiennent au secteur de l'énergie. Il s'agit d'un résultat de l'hybridation des affrontements géopolitiques, tant d'un point de vue de la nature de ces affrontements (vecteur cyber) que de la nature des acteurs qui y prennent part (collectifs hacktivistes informels). Cette dynamique doit être intégrée par les organisations du secteur de l'énergie dans le cas où des groupes hacktivistes d'un nouveau type (ex. groupes para-politiques radicaux) se constitueraient et les prendraient pour cibles.

Glossaire

APT - *Advanced Persistent Threat*	Une APT a le plus souvent recours à des TTPs sophistiquées, traditionnellement associées à des instances étatiques et poursuivant des objectifs divers.
CTI - *Cyber Threat Intelligence*	Discipline basée sur des techniques du renseignement, ayant pour objectif la collecte et l'organisation de toutes les informations liées aux menaces cyber, afin de dresser un portrait des MOA ou de mettre en exergue des tendances.
OT - *Operational Technology*	OT se rapporte aux composants matériels et briques logicielles qui contrôlent les équipements industriels, les processus et les alertes des outils de production.
SCADA - *Supervisory Control and Data Acquisition*	Un système de contrôle et d'acquisition de données permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.
ICS - *Industrial Control System*	Acronyme qui englobe le système industriel dans son ensemble. Il a pour finalité de tout contrôler, ce qui inclut le SCADA dans la vision européenne, et est souvent confondu avec celui-ci.

RAT - *Remote Access Trojan*	Outil d'accès à distance utilisé par les développeurs de malwares pour obtenir un accès complet à distance du système d'un utilisateur, y compris le contrôle de la souris et du clavier, l'accès aux fichiers et aux ressources du réseau.
Ransomware	Type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et exige le paiement d'une rançon en échange du rétablissement de l'accès.
MOA - *Mode Opératoire des Attaquants*	Défini par un ensemble des outils, tactiques, techniques, procédures et caractéristiques mis en œuvre par un ou plusieurs groupes d'attaquants dans le cadre d'une attaque informatique.
CVE - *Common Vulnerabilities and Exposures*	Dictionnaire des informations publiques relatives aux vulnérabilités de sécurité identifiées par le département de la Sécurité intérieure des États-Unis et maintenu par l'organisme MITRE.
IAB - *Initial Access Brokers*	Les courtiers en accès initial sont des acteurs de la menace qui vendent à d'autres acteurs l'accès aux réseaux d'entreprise. Ils sont hautement qualifiés dans leur domaine et possèdent un ensemble de compétences spécialisées qu'ils utilisent pour accéder à des réseaux sécurisés.
TTPs - *Tactiques, techniques et procédures*	Décrit le comportement d'un mode opératoire des attaquants. Une tactique est la description la plus élevée du MOA, tandis que les techniques donnent une description détaillée de la kill chain exploitée dans le contexte d'une tactique. Les procédures fournissent une étude encore plus détaillée des techniques exploitées par le MOA.
Payload - *Charge utile*	Constitue la partie fonctionnelle des données transmises. Les en-têtes et les métadonnées sont envoyés uniquement pour permettre la livraison de la charge utile.
Hacktivisme	Pratique subversive consistant à perturber ou saboter des services en ligne, à infiltrer de manière frauduleuse des systèmes ou des réseaux informatiques dans le but de les détourner, dans le cadre d'un combat militant ayant une dimension politique, religieuse ou sociale.
Wiper	Type de malware dont l'objectif est d'effacer tout ou partie des données qui se trouvent sur les ordinateurs compromis.
Infostealer	Malware conçu pour recueillir des informations sur une machine compromise. La forme la plus courante des infostealers recueille des informations de connexion stockées dans les navigateurs des postes compromis, qu'il envoie à un serveur C2.

Glossaire

Entrée en activité
des APT observées dans le cadre du Panorama

APT28 *(Mandiant)*
FOREST BLIZZARD *(Microsoft)*
Entrée en activité en 2004

En 2018, une inculpation du Conseiller spécial des États-Unis a identifié APT28 comme étant opérée depuis l'unité n°26165 du service de renseignement militaire russe (GRU). Le MOA serait actif depuis 2004[1].

Victimologie synthèse :
États-Unis • Ukraine • Brésil • Chine • Roumanie • Bulgarie • Italie • France *(Schneider Electric)*

APT LAZARUS
DIAMOND SLEET *(Microsoft)*
Entrée en activité en 2009

Le FBI a associé APT Lazarus (APT38) à une unité du service de renseignement de la Corée du Nord (Reconnaissance General Bureau - RGB). La première attaque associée à l'APT Lazarus est connue sous le nom «d'opération Troy», déroulée entre 2009 et 2012.

Victimologie synthèse :
États-Unis • Canada • Japon

APT41 *(Mandiant)*
BRASS TYPHOON *(Microsoft)*
Entrée en activité en 2009

Les activités d'APT41 ont été mises en lumière pour la première fois dans un rapport de FireEye publié en août 2019. Les experts de FireEye ont indiqué que ce groupe était impliqué à la fois dans des opérations de cyberespionnage pour le compte du gouvernement chinois et dans des intrusions visant à obtenir des avantages financiers personnels[2].

Victimologie synthèse : Inde

SANDWORM *(Trend Micro)*
SEASHELL BLIZZARD *(Microsoft)*
Entrée en activité en 2009

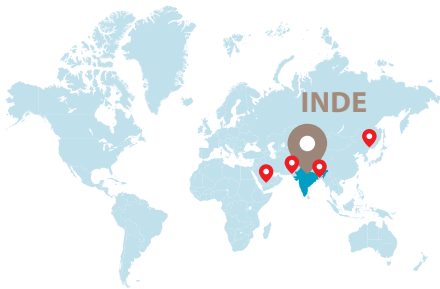
L'APT Sandworm est un MOA actif depuis au moins 2009 et associé à l'unité militaire 74455 du Centre principal des technologies spéciales (en russe : GTsST) du GRU. SANDWORM s'est principalement illustré par des campagnes d'attaques destructrices par wipers ciblant les infrastructures critiques du secteur de l'énergie en Ukraine.

Victimologie synthèse :
Ukraine

BITTER *(Forcepoint)*
T-APT-17 *(Tencent)*
Entrée en activité en 2013

APT Bitter est considérée comme active depuis au moins 2013 et a été signalée pour la première fois par Forcepoint Labs en 2016. Les opérateurs d'APT Bitter sont associés à l'Inde et se concentreraient sur des attaques ciblant le secteur de l'énergie au Pakistan, en Chine, au Bangladesh et en Arabie saoudite.

Victimologie synthèse :
Pakistan • Chine • Bangladesh • Arabie saoudite



RED LADON /
TA423 *(Proofpoint)*
Entrée en activité en 2013

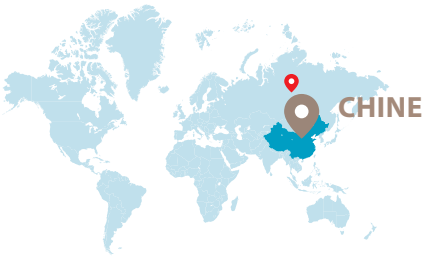
Associée à la Chine et active depuis 2013, elle cible diverses organisations en réponse à des événements politiques dans la région Asie-Pacifique, en mettant l'accent sur la mer de Chine méridionale. Les organisations ciblées comprennent des entrepreneurs de la défense, des fabricants, des universités, des agences gouvernementales, des cabinets juridiques impliqués dans des litiges diplomatiques et des entreprises étrangères impliquées dans la politique australasienne ou les opérations en mer de Chine méridionale.

Victimologie synthèse :
Inde • Australie

APT31 *(Mandiant)*
VIOLET TYPHOON *(Microsoft)*
Entrée en activité en 2016

Associée à la Chine, APT31 se concentre sur l'obtention de renseignements pouvant fournir au gouvernement chinois et aux entreprises publiques des avantages politiques, économiques et militaires.

Victimologie synthèse :
Russie



APT34 *(FireEye)*
HAZEL SANDSTORM *(Microsoft)*
Entrée en activité en 2014

La victimologie associée à APT34 favoriserait les intérêts de l'État iranien et le MOA serait opérationnel depuis au moins 2014. Un collectif hacktiviste nommé **Lab Dookhtegan** a divulgué les outils exploités par APT34 sur Telegram, poussant le mode opératoire à mettre à jour sa sécurité opérationnelle en 2019.

Victimologie synthèse :
Israël • États-Unis

APT LYCEUM *(Secureworks)*
HEXANE *(Dragos)*
Entrée en activité en 2018

APT Lyceum est associée à l'Iran et ciblerait des entreprises du secteur de l'énergie et des télécommunications au Moyen-Orient. Le MOA serait resté relativement discret depuis son identification en 2018.

Victimologie synthèse :
Moyen-Orient (Israel et Arabie Saoudite)

Méthodologie & Périmètre des observations

Le panorama de la menace que nous vous présentons repose sur une méthodologie prenant en compte plusieurs variables. Nous avons établi un cadrage chronologique précis, en nous concentrant exclusivement sur les attaques ayant ciblé le secteur de l'énergie au cours de l'année 2022. Cette approche nous a permis de fournir une analyse détaillée de l'activité des modes opératoires observés par le CERT-XMCO. Aucune limite géographique n'a été imposée dans la rédaction du panorama, permettant de prendre en compte les dynamiques géopolitiques ayant affecté les acteurs de la menace en 2022 et, par effet de cascade, le secteur de l'énergie.

DÉFINITION DU SECTEUR DE L'ÉNERGIE

Secteur économique de première importance, qui comprend la production, le transport, la transformation, la distribution et la commercialisation des diverses sources d'énergie (fossiles, nucléaire et renouvelables).

COLLECTE DE DONNÉES

L'étape initiale de collecte de données par le CERT-XMCO a été effectuée sur l'ensemble des sources disponibles en accès libre (OSINT) : rapports d'investigations en CTI, bulletins d'information Yuno, revues spécialisées sur les questions de renseignement et déclarations publiques d'organisations gouvernementales.

ANALYSE DES TENDANCES

Une fois les données collectées, un long travail de mise en perspective a été effectué par les consultants du CERT-XMCO afin d'apporter des clés de compréhensions sur les modes observatoires observés au cours de l'année, leurs tactiques, techniques et procédures (TTPs), la nature de leurs objectifs, leur niveau de sophistication. En 2022, les tensions géopolitiques ont une incidence significative sur l'activité des modes opératoires APT et cybercriminels, aussi bien dans l'élaboration du vecteur de compromission initiale (recours massif aux techniques d'ingénierie sociale basées sur l'actualité) que dans les finalités recherchées (exploitation massive des wipers, campagnes d'attaques DDoS, pré-positionnement stratégique à des fins de sabotage, etc.).

1. L'énergie : un secteur sensible aux tensions géopolitiques

Sur la base des tactiques, techniques et procédures (TTPs) et de leur victimologie, plusieurs modes opératoires ayant ciblé le secteur de l'énergie en 2022 ont été associés à des entités étatiques. Le secteur de l'énergie comprend des infrastructures critiques, notamment des centrales électriques, des raffineries, des pipelines et des réseaux de distribution.

Ces infrastructures sont essentielles à la production, à la transmission et à la distribution de l'énergie. Leur compromission confère dès lors un avantage stratégique aux acteurs de la menace, ensuite en mesure d'influencer des négociations, d'exercer une pression ou de perturber un pays ou la santé économique d'une entreprise.

1.1 COLLECTE DE RENSEIGNEMENTS STRATÉGIQUES PAR LES MODES OPÉRATOIRES ÉTATIQUES

LA RUSSIE

En 2022, le secteur de l'énergie a été secoué par des campagnes d'espionnage d'une ampleur sans précédent, associées à des modes opératoires parrainés par la Fédération de Russie.
Ces cyberattaques ont principalement ciblé les infrastructures énergétiques ukrainiennes exacerbant les tensions en lien avec l'invasion russe en Ukraine en février 2022. Ces attaques sophistiquées ont également mis en évidence la vulnérabilité des infrastructures énergétiques en Europe occidentale.

En février 2022, une enquête de **ReSecurity Inc.** rendue publique par Bloomberg, a révélé une vaste opération d'espionnage visant les entités américaines spécialisées dans le la production et l'exportation de gaz naturel liquéfié (GNL)[6].

Le mode opératoire responsable de l'attaque a été baptisé **Forest Blizzard** par ReSecurity. Selon le rapport de Bloomberg, les opérateurs auraient essayé de rentrer en contact avec des *Initial Access Brokers* (IAB) pour obtenir des accès au sein des ordinateurs ciblés. L'opération aurait duré une quinzaine de jours au

cours desquels **Forest Blizzard** aurait réussi à compromettre plus de 100 ordinateurs appartenant aux employés de 21 grandes entreprises énergétiques américaines.

Parmi les cibles figuraient des entreprises telles que Cheniere Energy, Chevron, EQT Corp et Kinder Morgan. L'objectif de cette opération semblait être lié à un prépositionnement à des fins de collecte de renseignements stratégiques en vue de l'invasion en Ukraine, alors que les marchés de l'énergie étaient déjà perturbés par une pénurie d'approvisionnement.

En janvier 2022, le chercheur en cybersécurité William Thomas aurait identifié un mode opératoire ciblant des organisations du secteur des énergies renouvelables, ayant compromis depuis 2019 une quinzaine

d'entités à travers le monde[7]. Le mode opératoire aurait exploité un *toolkit* de phishing baptisé **MAIL BOX** et hébergé sur son infrastructure C2, ainsi que sur des sites web légitimes compromis. La plupart des pages de phishing étaient hébergées sur des domaines tels que **.eu3[.]biz**, **.eu3[.]org** et **.eu5[.]net**, tandis que la majorité des sites compromis étaient situés au Brésil. Parmi les organisations visées par les attaques de *phishing*, se trouvaient notamment : Schneider Electric ; Honeywell ; Huawei ; HiSilicon ; Telekom Romania ; la centrale hydroélectrique de Kardzhali (Bulgarie) ; CEZ Electro (Bulgarie) ; California Air Resources Board et la société italienne de recyclage Sorema.

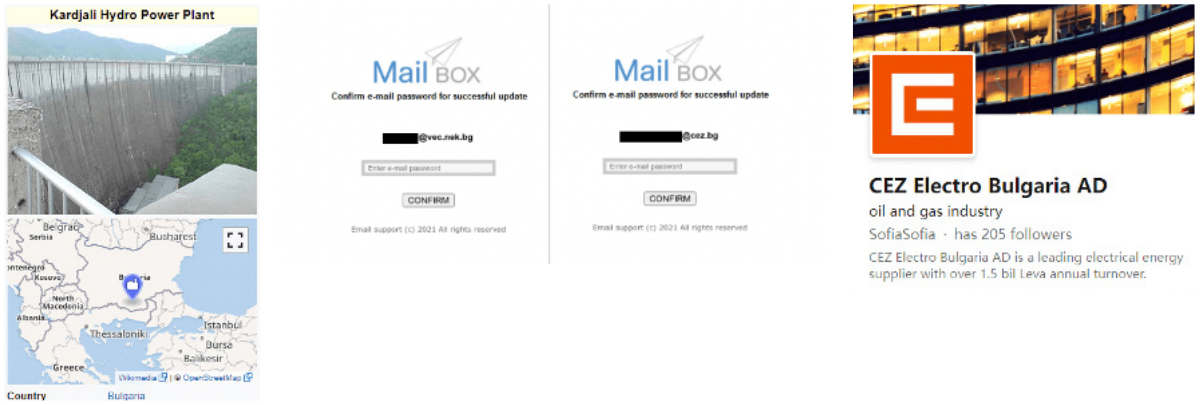


Figure 1 - Campagne de phishing via le toolkit « Mail Box » associée à APT28 (source : blog.bushidotoken.net)

Bien que le mode opératoire n'ait pas été associé à la Russie, les chercheurs du *Threat Analysis Group* (TAG) de Google ont observé l'exploitation de plusieurs domaines **eu3[.]biz** par **APT28** lors de campagnes de *phishing* distinctes. Ce cluster de TTPs permettrait d'envisager une association de l'attaque au 18ème Centre de Sécurité Informationnelle, créé après la réforme du renseignement russe de 2005 au sein de la Direction de la sécurité informationnelle (acronyme russe : УКИБ) du FSB[8].

Il n'est pas à exclure que le mode opératoire à l'origine de cette campagne d'attaques à des fins de sabotage soit un pays détenteur d'une source importante de combustibles fossiles et menacé par le secteur des énergies renouvelables.

ANALYSE DE NOS CONSULTANTS

Au cours de l'année 2022, les MOA associés à l'État russe ont démontré leurs capacités à saboter les infrastructures critiques du secteur ukrainien de l'énergie via la diffusion de wipers, bien que les conséquences de ces opérations soient largement minimisées par les autorités ukrainiennes.

LA CHINE

Dans la continuité des modes opératoires étatiques ayant ciblé le secteur de l'énergie, les chercheurs de Proofpoint et PwC ont publié en août 2022 une étude sur les attaques associées au mode opératoire **TA423 / Red Ladon** parrainé par la République Populaire de Chine[9]. Le mode opératoire aurait été identifié à travers d'une campagne de collecte de renseignements entre avril et juin 2022, ciblant diverses entreprises australiennes du secteur de l'énergie. En ciblant les infrastructures énergétiques essentielles de l'Australie, la Chine chercherait à identifier les vulnérabilités, les perturbations potentielles ou les faiblesses qui pourraient peser sur sa propre sécurité énergétique[10] dans un contexte marqué par l'alignement de la politique extérieure de Canberra sur celle de Washington [11].

La campagne observée aurait débuté avec du *spear-phishing*. En effet, les courriels malveillants renvoyaient vers un site d'informations australien en apparence légitime. La page *web* observée contenait du code JavaScript chargé d'installer le *malware* modulaire **ScanBox**. Les informations transmises à propos de l'utilisateur aux serveurs C2 permettaient de confirmer ou non l'intérêt de la cible pour le mode opératoire chinois, avant la diffusion d'un *keylogger*[12].

Le mode opératoire aurait été identifié pour la première fois en 2013, ciblant d'autres organisations siutées dans la région de la mer de Chine méridionale. Cette dernière constitue un passage logistique stratégique pour l'approvisionnement en hydrocarbures, notamment dans le cadre de l'initative des Routes de la Soie. Ceci expliquerait la victimologie du mode opératoire TA423/Red Ladon centrée sur les organisations étrangères situées dans cette région.

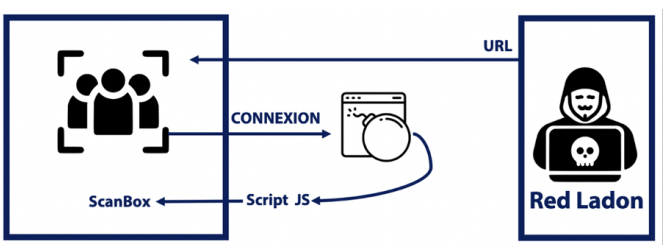


Figure 2 - Diffusion du malware modulaire ScanBox par Red Ladon (Production CERT-XMCO)

Un autre mode opératoire associé à la Chine (référencé comme **Red Echo**) aurait exploité plusieurs vulnérabilités présentes dans un serveur *web* Boa jusqu'en novembre 2022 pour cibler 7 infrastructures indiennes via la compromission du système électrique national d'intervention d'urgence[13], tous situés dans le nord de l'Inde, à proximité de la frontière disputée entre la Chine et l'Inde au Ladakh.

La présence prolongée des opérateurs chinois dans le réseau électrique indien offre des possibilités limitées de collecte de renseignements à des fins économiques et politiques. Cependant, les centres de distribution de charges synchrones (SLDC) restent essentiels pour assurer la stabilité et la fréquence du réseau électrique de New Delhi. L'exploitation abusive des serveurs Boa pour accéder au contrôle du réseau électrique indien permettrait à ***APT Red Echo*** de se pré-positionner pour mener des actions de sabotage ou de destruction en cas de conflit armé.

Figure 3 - Emplacements des victimes de Red Echo observées par Recorded Future[14]

Non maintenus à jour depuis 2005, les serveurs *web* Boa hébergent une solution logicielle **obsolète** encore utilisée par des composants permettant la connexion et l'accès aux consoles de gestion des dispositifs IoT, tels que les routeurs et les caméras de surveillance. Les vulnérabilités exploitées par le mode opératoire Red Echo, référencées **CVE-2017-9833** (CVSS 7.5) et **CVE-2021-33558** (CVSS 7.5), permettaient d'accéder de manière arbitraire aux fichiers des systèmes ciblés. Dans un rapport publié en novembre 2022, les chercheurs de Microsoft ont observé l'omniprésence des serveurs web Boa dans les appareils IoT qui pourrait s'expliquer par leur inclusion dans des SDK populaires[15].

En mai 2022, Cybereason a révélé une autre campagne d'espionnage associée au mode opératoire **APT41** (aussi référencé comme Winnti). Baptisée **CuckoBees**, la campagne aurait commencé en 2019 et visait à collecter des renseignements stratégiques pour le compte du ministère de la Sécurité d'État chinois (MSS)[16]. Selon les analystes de Cybereason, **APT41** aurait dérobé des centaines de giga-octets de données appartenant à de nombreuses multinationales non-référencées du secteur de l'énergie.

Reconnu pour son expertise en matière de sécurité opérationnelle et la sophistication de ses TTPs, le mode opératoire aurait exploité les vulnérabilités d'une plateforme ERP populaire, dont le nom n'a pas été divulgué, pour accéder aux systèmes d'information de ses victimes. Les opérateurs auraient ensuite déployé un *Web Shell* afin d'assurer la persistance sur les systèmes ciblés et collecter les informations d'identification pour se latéraliser dans le réseau de leurs victimes.

À des fins de discreton, **APT41** a également abusé du mécanisme Windows Common *Log File System (CLFS)*, permettant aux opérateurs de dissimuler leurs payloads et d'échapper à la détection par les produits de sécurité[17]. Enfin, Cybereason aurait identifié le déploiement d'autres *malwares* tels que **Spyder** (backdoor), **STASHLOG** (payload dans le service CLFS de Windows), **SPARKLOG** (pour obtenir une escalade des privilèges et parvenir à la persistance) et **WINNKIT** (rootkit).

Un rapport de *Positive Technologies* a révélé que l'État chinois avait ciblé le secteur de l'énergie russe en 2022 par l'intermédiaire du mode opératoire **APT31** dans le but de collecter des renseignements stratégiques[20].

L'attaque avait été détectée en avril 2022 ciblant plusieurs médias russes et entreprises du secteur de l'énergie via l'utilisation d'un document leurre appelé **list[.]docx** pour extraire une *payload* malveillante paquée avec **VMProtect**. L'analyse des échantillons, datant de novembre 2021 à juin 2022, aurait permis aux chercheurs d'associer l'attaque à **APT31**.

Cette dernière s'était inscrite dans un contexte marqué par des négociations entre la Russie et la Chine visant à renforcer leur alliance énergétique par le biais de la construction d'un nouveau gazoduc[21] et d'investissements chinois dans les sociétés énergétiques russes.

Figure 4 - Courriel de phishing diffusé par APT31 (source : Positive Technologies)

ANALYSE DE NOS CONSULTANTS

En 2022, la Chine a cherché à garantir sa sécurité énergétique en s'appuyant sur des fournisseurs en Asie centrale et au Moyen-Orient pour soutenir sa forte croissance économique[18]. L'acquisition de renseignements concurrentiels et de propriété intellectuelle étrangère constitue l'un des objectifs formulés par l'article 11 de la Loi sur le renseignement national chinois de 2017[19]. Dès lors, les modes opératoires APT chinois utiliseraient les informations collectées pour favoriser la croissance économique de la Chine dans les secteurs d'importance vitale.

L'INDE

Pour répondre aux préoccupations régionales de l'Union Indienne, le mode opératoire indien référencé comme **APT Bitter** aurait ciblé le secteur de l'énergie nucléaire en Chine, d'après une investigation menée par les chercheurs d'Intezer le 24 mars 2023. Actif depuis au moins 2021, le mode opératoire aurait ciblé de nombreuses organisations au Pakistan, en Chine, au Bangladesh et en Arabie Saoudite[22].

7 courriels de *phishing* diffusés lors de la phase de compromission initiale auraient été identifiés.

Les opérateurs d'**APT Bitter** se faisaient passer pour l'ambassade du Kirghizistan en Chine, invitant leurs cibles à participer à des conférences.

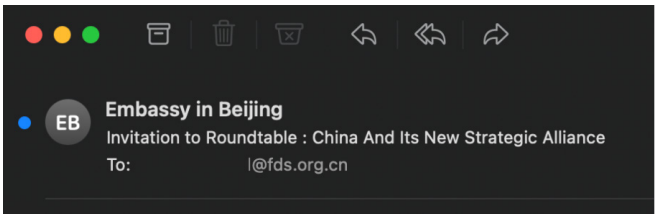


Figure 5 - Courriel de phishing associé à APT Bitter (source : Intezer)

Les *payloads* étaient diffusées par le mode opératoire par l'intermédiaire d'un fichier Excel® en apparence anodin, exécutant des bibliothèques DLL malveillantes après l'activation des macros par l'utilisateur ciblé.

Une tâche planifiée s'exécutait ensuite toutes les 15 minutes pour assurer la persistance sur le SI et communiquer avec les serveurs C2.

ANALYSE DE NOS CONSULTANTS

Plusieurs éditeurs de solutions de sécurité informatique soupçonnent l'Inde d'avoir développé des capacités offensives de lutte informationnelle, dans un contexte géopolitique tendu marqué par des relations complexes avec ses rivaux régionaux. L'étude des attaques attribuées à APT Bitter démontre que l'Inde cible régulièrement le secteur de l'énergie nucléaire en Chine à des fins de collecte de renseignement stratégique.

LA COREE DU NORD

Dans la continuité des modes opératoires asiatiques ayant ciblé le secteur de l'énergie en 2022, les opérateurs d'**APT Lazarus** se sont illustrés lors de la compromission de fournisseurs d'énergie implantés aux États-Unis, au Canada et au Japon entre février et juillet 2022.

Selon les données collectées par Talos[24], la killchain observée serait basée sur l'exploitation de la vulnérabilité **Log4j (CVE-2021-44228, CVSS 10)** sur des serveurs **VMWare Horizon** vulnérables.

Les opérateurs diffuseraient ensuite le *malware* **MagicRAT** disposant de diverses capacités, telles que l'exploration des ports, l'établissement de persistance, l'exécution de commandes à distance pour manipuler des fichiers, ainsi que l'utilisation d'un serveur de commandes et de contrôle (C2) pour l'exfiltration de données et l'hébergement de nouveaux variants développés par **APT Lazarus**, notamment **TigerRAT**.

APT Lazarus aurait ensuite déployé des *payloads* personnalisées référencées **VSingle** et **YamaBot** servant respectivement de *backdoor* et de *bot HTTP*.

YamaBot exécuterait du code arbitraire à partir d'un réseau distant, téléchargeant et exécutant également des *plugins* pour mener la reconnaissance, le déploiement de *malwares* et l'exfiltration des données.

Comme **VMWare Horizon** fonctionnerait avec des privilèges élevés, le mode opératoire ***Lazarus*** pourrait désactiver Windows®Defender en modifiant des clés de registre et en utilisant WMIC et des commandes PowerShell avant de déployer **VSingle**.

La victimologie d'**APT Lazarus** reste pour autant historiquement motivée par la recherche du gain financier et serait soupçonnée d'alimenter le financement des programmes d'armement du régime de Pyongyang[25].

ANALYSE DE NOS CONSULTANTS

Les opérateurs du MOA ont démontré la sophistication de leurs techniques d'ingénierie sociale lors de la phase initiale de phishing.[23]

L'IRAN

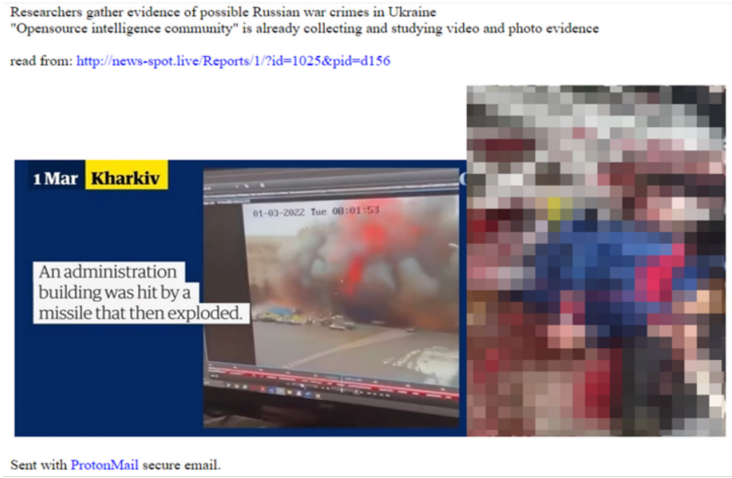
L'année 2022 fut marquée par de fortes tensions géopolitiques entre Israël et l'Iran[26], au cours de laquelle plusieurs infrastructures critiques en eau et en énergie ont fait l'objet d'attaques à des fins de collecte de renseignements.

Les entités liées à l'énergie basées en Israël et en Arabie saoudite ont été des cibles de choix pour les MOA iraniens en 2022. **APT Lyceum**, aurait notamment utilisé une nouvelle *backdoor* en .NET exploitant une technique de **DNS-tunneling** pour mener des attaques contre des entreprises des secteurs de l'énergie et des télécommunications au Moyen-Orient. Selon les analystes de Zscaler, la backdoor serait une version personnalisée de l'outil *Open Source* **DIG[.]net**.

Les opérateurs auraient personnalisé le code pour lui permettre d'exécuter des commandes système à distance et télécharger des fichiers depuis leurs serveurs C2 en exploitant une technique d'empoisonnement du cache DNS[27]. Celle-ci permet de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse et contrôlée par les serveurs C2 contrôlés par les opérateurs iraniens.

APT Lyceum serait actif depuis 2017 et serait motivé par la recherche de renseignements stratégiques pour le compte du Corps des gardiens de la révolution islamique (IRGC)[28].

Une entreprise énergétique israélienne aurait reçu un courriel provenant de l'adresse inews-reporter@protonmail[.]com avec pour objet «*Crimes de guerre russes en Ukraine*». Le courriel contenait quelques images tirées de sources médiatiques publiques et un lien vers un article hébergé sur le domaine news-spot[.]live. Responsable du téléchargement du binaire en .NET, le *malware* chargerait ensuite une *payload* abusant de la fonctionnalité **Password Filters**[29] de Microsoft® afin de récupérer les mots de passe des utilisateurs compromis grâce à un filtre mis en place par une DLL malveillante enregistrée dans une clé de registre. La *payload* déployée pourrait ensuite utiliser les mots de passe en argument, se connecter au serveur Exchange des utilisateurs compromis, et exfiltrer des données.


Researchers gather evidence of possible Russian war crimes in Ukraine
"Opensource intelligence community" is already collecting and studying video and photo evidence

read from: http://news-spot.live/Reports/1/?id=1025&pid=d156

1 Mar Kharkiv

An administration building was hit by a missile that then exploded.

Sent with ProtonMail secure email.

Figure 6 - Courriel de phishing utilisé par APT Lyceum (source : Zscaler)

D'autres compagnes ciblant des organisations du secteur de l'énergie auraient été attribuées à des APT iraniennes :

- Actif depuis 2014, **APT34** aurait mené des compromissions (https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html) contre le secteur de l'énergie au Moyen-Orient (Israël, Jordanie, Arabie saoudite, Liban, Qatar, Koweït, Émirats arabes unis, Turquie) et à l'international (principalement les États-Unis et la Chine).

- Avant 2022, des investigations menées par *Proofpoint*[30] suggèrent que des opérateurs iraniens auraient usurpé l'identité d'un physicien israélien et l'aurait utilisée comme *troll* pour cibler au moins 25 autres chercheurs aux États-Unis et en Israël. Le leurre utilisé - un rapport sur les capacités nucléaires d'Israël - aurait été diffusé par Charming Kitten (**APT35**) pour voler les identifiants de la victime.

L'analyse de la stratégie cyber de l'Iran par Citalid émet l'hypothèse que le différend maritime entre Israël et le Liban, notamment en ce qui concerne le champ gazier de Karish, ainsi que les discussions sur les pipelines entre Israël et la Turquie sont susceptibles de continuer à alimenter les activités d'espionnage menées par l'Iran au Moyen-Orient[31].

Figure 7 - Page de phishing suspectée d'être liée à Mint Sandstorm (source : Insikt Group)

ANALYSE DE NOS CONSULTANTS

Le ciblage des infrastructures énergétiques par l'Iran au Moyen-Orient contribue à l'élaboration d'une stratégie de « *blanchiment d'influence* ». Celle-ci repose sur la combinaison des moyens cyber déployés sur le territoire national et à l'étranger[32] dans le cadre de l'orientation prise par l'amiral Habibollah Sayyari, coordonnateur adjoint de l'armée de la République islamique d'Iran.
En termes de stratégie, l'Iran semble favoriser la confrontation indirecte avec les pays de la région qu'elle juge hostiles, en ayant notamment recours aux services des groupes hacktivistes comme l'*Iran Cyber Army* (ICA) et le collectif *Cyber Hezbollah* composés de spécialistes informatiques soupçonnés d'être coordonnés par les *Pasdaran*.

1.2. SABOTAGE ET DESTRUCTION DES INFRASTRUCTURES DU SECTEUR DE L'ÉNERGIE

En 2022, le secteur de l'énergie a été confronté à une augmentation significative des attaques à des fins de sabotage. La Russie et l'Ukraine ont respectivement cherché à perturber les infrastructures critiques de l'adversaire via un large spectre d'attaques[33]. Les capacités offensives de la Fédération de Russie en matière de destruction des infrastructures critiques de Kiev, largement éprouvées depuis 2015 avec la compromission du réseau électrique national ukrainien par **SANDWORM**[34], ont conduit le FBI, la CISA et la NSA à émettre un avertissement dès le 11 janvier 2022 concernant le niveau de risque élevé de perturbations, orchestrées par des modes opératoires parrainés par l'État russe[35].

Figure 8 - Avis publié par les autorités américaines le 11/01/2022

Néanmoins, les opérations de sabotage soutenues par la Russie en février 2022 n'ont pas eu les effets escomptés sur les infrastructures physiques et numériques ciblées en marge de l'invasion en Ukraine, malgré le déploiement d'au moins neuf wipers par les modes opératoires russes[36] :

- AcidRain
- WhisperGate
- HermeticWiper
- IsaacWiper
- CaddyWiper
- DoubleZero
- AwfulShred
- OrcShred
- SoloShred

En effet, lorsque la guerre a commencé en février 2022, l'Ukraine et ses partenaires s'attendaient à ce que les offensives d'APT Sandworm et des autres MOA associées à la Russie essaient de répéter les attaques réussies contre les centrales électriques ukrainiennes en 2014 pour plonger les villes dans l'obscurité. Toutefois, il s'est finalement avéré plus facile et plus efficace pour la Russie d'endommager le réseau électrique ukrainien à l'aide d'armes conventionnelles que par l'usage de wipers.

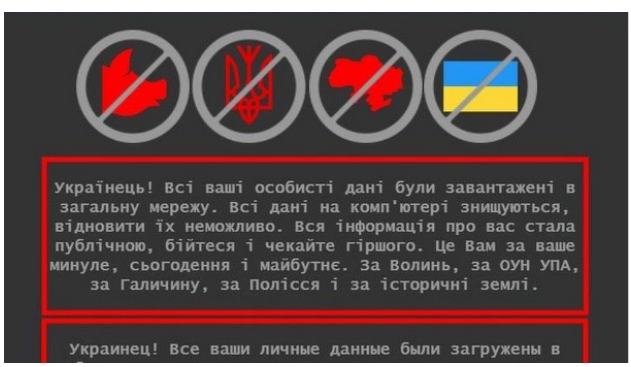


Figure 9 - Défiguration de sites web ukrainiens en parallèle de la diffusion de wipers au début de l'invasion russe (source : BBC)

Le 12 avril 2022, en collaboration avec le CERT-UA, les chercheurs d'ESET ont annoncé avoir identifié une attaque associée au mode opératoire **SANDWORM** lors de laquelle un fournisseur d'énergie basé en Ukraine avait été ciblé par la diffusion d'une nouvelle variante d'**Industroyer**[37].

Les investigations menées par les analystes d'ESET indiquent que le *malware* aurait été compilé le 23 mars 2022, suggérant que les opérateurs avaient planifié leur attaque deux semaines avant son lancement. Du fait de ses capacités de persistance et de son habilité à interférer directement avec le fonctionnement des systèmes SCADA, **Industroyer2 serait le malware le plus dangereux pour les systèmes de contrôle industriel du secteur de l'énergie**[38].

Industroyer2 serait capable de saboter les interrupteurs et les disjoncteurs des sous-stations électriques. Le *malware* utiliserait des protocoles de communication industriels **obsolètes** (norme IEC-104 de la Commission électrotechnique internationale), utilisés au sein des infrastructures d'alimentation électrique, des systèmes de contrôle des transports et d'autres systèmes d'infrastructures critiques hydrauliques. D'autres outils auraient été exploités lors de l'attaque, notamment le *script* PowerShell **PowerGap**, conçu pour télécharger des *payloads* supplémentaires, et **Impacket**, exécutant des commandes à distance[39].

Basé sur l'exploitation abusive des mêmes protocoles obsolètes, le *malware* **BlackEnergy** avait pourtant déjà été identifié sur des réseaux de distribution d'électricité ukrainiens en 2015 pour diffuser des RAT et compromettre des infrastructures hydrauliques ukrainiennes[40]. En avril 2022, les chercheurs de Mandiant ont observé un autre *malware* nommé **Incontroller** (aussi référencé comme **Pipedream**) ciblant le secteur de l'énergie ukrainien via la manipulation de protocoles **obsolètes** au sein des systèmes de contrôle industriels[41].

Le *framework* ciblerait spécifiquement les systèmes de contrôle industriel (ICS) et aurait été développé par un mode opératoire référencé **CHERNOVITE**, attribué à la Russie.

Pipedream serait initialement développé pour compromettre des dispositifs utilisés dans l'industrie électrique, ainsi que dans les secteurs pétroliers et gaziers. Trois conséquences ont été identifiées à l'issue des attaques menées par le *malware* :

Arrêt de la chaine d'approvisionnement

CHERNOVITE utilise des frameworks OMSHELL et/ou CODECALL pour bloquer les automates. La perte de disponibilité des automates obligerait l'organisation ciblée à arrêter sa chaîne de production, entrainant des retards de production et des pertes financières.

Sabotage des processus industriels

Les opérateurs envoient des commandes non autorisées à l'API pour modifier le comportement physique des SCADA/ICS et des infrastructures physiques, telles que les moteurs ou les pompes. Cette attaque pourrait entrainer une baisse de la production et/ou un dysfonctionnement des machines ciblées sur une période prolongée.

Destruction des infrastructures physiques

Le mode opératoire désactive les systèmes de sécurité ICS/SCADA pour provoquer la destruction physique des infrastructures industrielles, entrainant des impacts sur la sécurité environnementale et humaine.

Les attaques par wipers ont été accompagnées fin novembre 2022 par une série d'attaques visant des organisations en Ukraine menée par le mode opératoire **SANDWORM**. Ces compromissions auraient été réalisées en utilisant le *malware* **RansomBoggs**, distribué via un *script* PowerShell très similaire à celui utilisé par **SANDWORM** en avril 2022 lors d'autres attaques contre le secteur de l'énergie[42].

Ce *malware* prenant l'apparence d'un *ransomware* aurait pour fonction de chiffrer les fichiers présents sur les systèmes infectés à l'aide de l'algorithme AES-256. Par la suite, **RansomBoggs** ajouterait l'extension [.]chsch aux fichiers chiffrés avant d'extorquer les victimes[43].

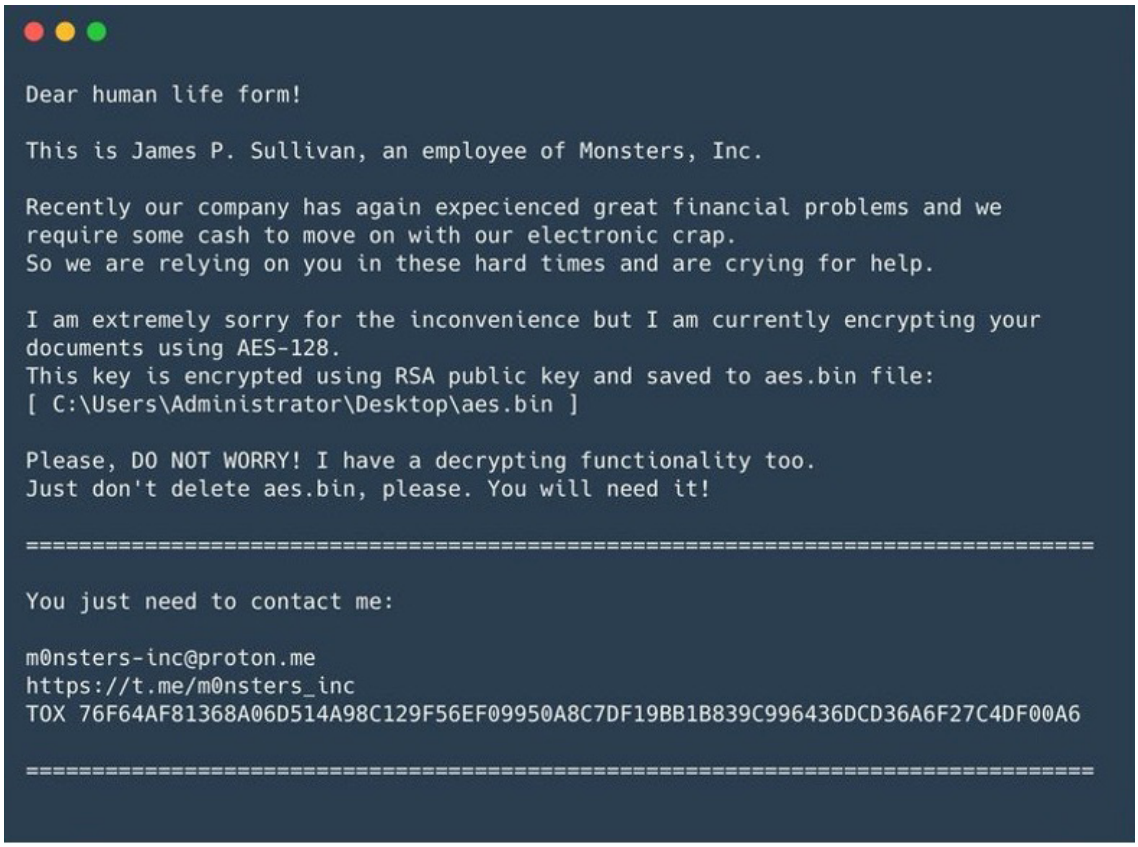


Figure 10 - Note de rançon du malware RansomBoggs (source : ESET)[44]

1.3. HACKTIVISME ET LUTTE INFORMATIONNELLE D'INFLUENCE

En 2022, la lutte informationnelle s'est intensifiée avec l'émergence de groupes hacktivistes ciblant les acteurs du secteur de l'énergie en soutien à la Russie ou l'Ukraine, en marge du conflit. Ces acteurs ont exploité un large spectre d'attaques (DDoS, désinformation, Hack and Leak) pour promouvoir leurs messages politiques, discréditer des personnalités publiques ou encore perturber les entreprises du secteur de l'énergie. Au cours de la dernière décennie, la Russie s'est engagée dans la capitalisation de l'espace informationnel afin d'en faire une caisse de résonance de son action diplomatique et le prolongement de ses activités offensives[45].

« La militarisation du cyberespace par la Russie s'est accompagnée par l'usage offensif de l'information, accélérant de surcroît l'avènement d'une ère de doute généralisé (conceptualisé dès l'époque soviétique sous la terminologie de « brillante incertitude »[46]) applicable au panorama de la menace ciblant le secteur de l'énergie. »

Les cadres sécuritaires russes auraient envisagé en octobre 2022 de mener des attaques clandestines contre les infrastructures européennes - gazoducs, oléoducs, navires pétroliers et câbles - en cas d'exacerbation de la confrontation énergétique avec l'Ukraine et ses alliés[47].
Bien que n'ayant entrainé que des perturbations temporaires sur les réseaux ciblés, les attaques par déni de service distribué (DDoS) menées en 2022 sont devenues une composante à part entière du conflit en pesant sur l'évolution des perceptions cognitives des populations.

Moscou a exploité l'ensemble de l'éventail des techniques de guerre informationnelle, de l'exploitation de l'audimat des médias classiques soutenus par l'État russe aux plateformes clandestines de l'*Internet Research Agency*, et des faux comptes sur les réseaux sociaux pour façonner la perception publique de la guerre. Le groupe pro-russe **KillNet** aurait revendiqué plusieurs dizaines d'attaques DDoS contre les entités du secteur de l'énergie en 2022, basées dans les États membres de l'Organisation du traité de l'Atlantique Nord (OTAN) ayant proposé leur aide matérielle et technique à l'Ukraine.

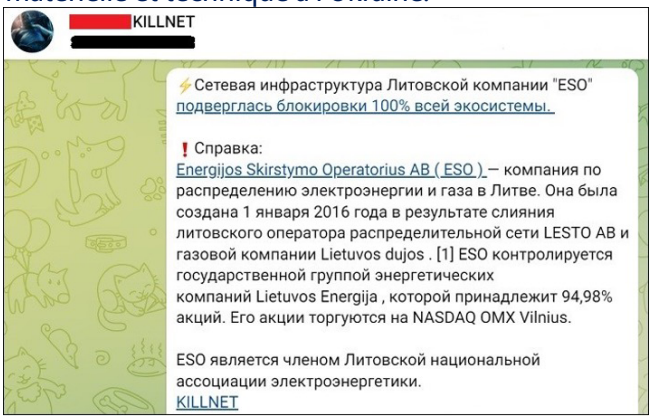


Figure 11 - Message sur le canal Telegram de KillNet décrivant l'attaque DDoS contre la filiale ESO d'Ignitis Group, entreprise énergétique lituanienne (Monitoring CERT-XMCO)[48]

Un autre groupe hacktiviste pro-russe nommé **Anonymous Sudan** a frappé de nombreuses organisations en Europe au cours de l'année 2022. Selon DARKReading, le partage de l'infrastructure C2 du groupe **Anonymous Sudan** avec **KillNet** laisse supposer que les mêmes opérateurs seraient derrière ces deux collectifs[49]. Ce n'est pas la première fois que des modes opératoires, soupçonnés d'être parrainés par l'État russe, dissimulent l'attribution de leurs attaques en prenant la forme d'une entité hacktiviste étrangère.

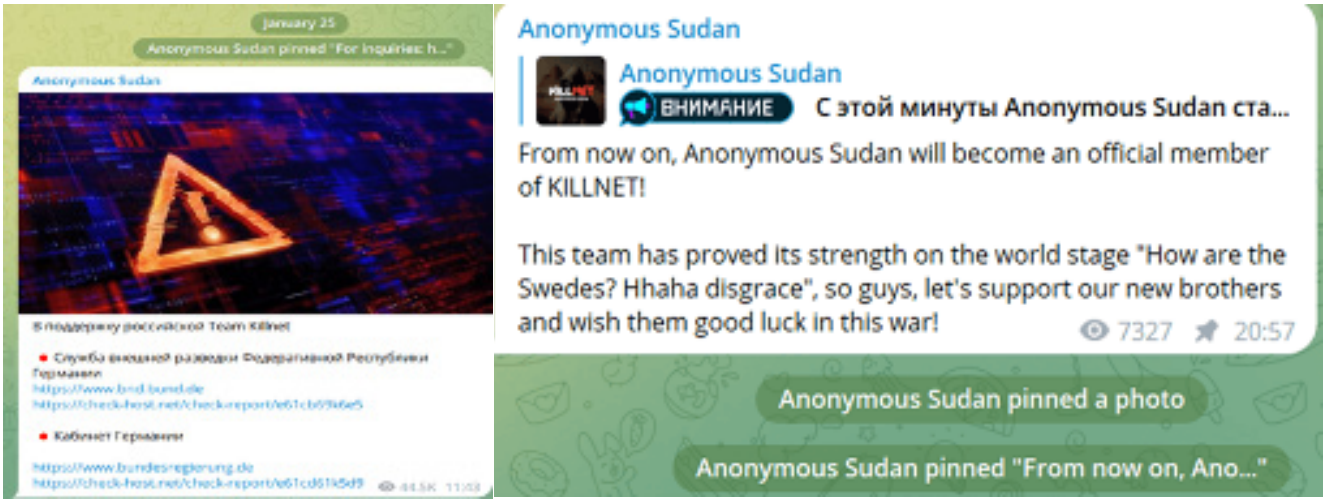


Figure 12 - Coopération entre Anonymous Sudan et KillNet (Monitoring CERT-XMCO)

En effet, en 2015, les TTPs et l'infrastructure C2 d'APT28 avaient été observées par FireEye lors d'une campagne d'attaques DDoS ayant ciblé TV5 Monde. Les attaques avaient pourtant été revendiquées par un groupe hacktiviste jusqu'alors inconnu, nommé **CyberCaliphate**[50].

Prenant cette fois-ci parti pour l'Ukraine, d'autres groupes hacktivistes ont profité de la guerre pour effectuer des campagnes d'attaques ciblant le secteur de l'énergie en Russie. Débutée quelques jours après l'invasion, l'**opération #OpRussia** visait à fédérer autour du collectif Anonymous des groupes hacktivistes politiques souhaitant prendre la défense de l'Ukraine. Cette opération menée tout au long de l'année 2022 aurait mis en lumière les vulnérabilités présentes au sein des infrastructures énergétiques russes et auraient démystifié les capacités cyber de la Russie, en semant la discorde au sein des groupes industriels russes, déjà divisés sur leur position concernant l'invasion en Ukraine[51].

Le 29 avril 2022, le collectif **Anonymous** a revendiqué la compromission de plusieurs entreprises russes du secteur de l'énergie, avant de diffuser publiquement leurs données sur la plateforme **DDoS Secrets**.

Figure 13 - Revendication d'attaques menées par le collectif Anonymous (Monitoring CERT-XMCO)[52]

Ces attaques s'inscrivent dans le modèle **Hack & Leak**, destinées à faire réagir l'opinion publique.

En 2022, le collectif hacktiviste aurait volé près de 5.8 To[53] de données aux entreprises russes.

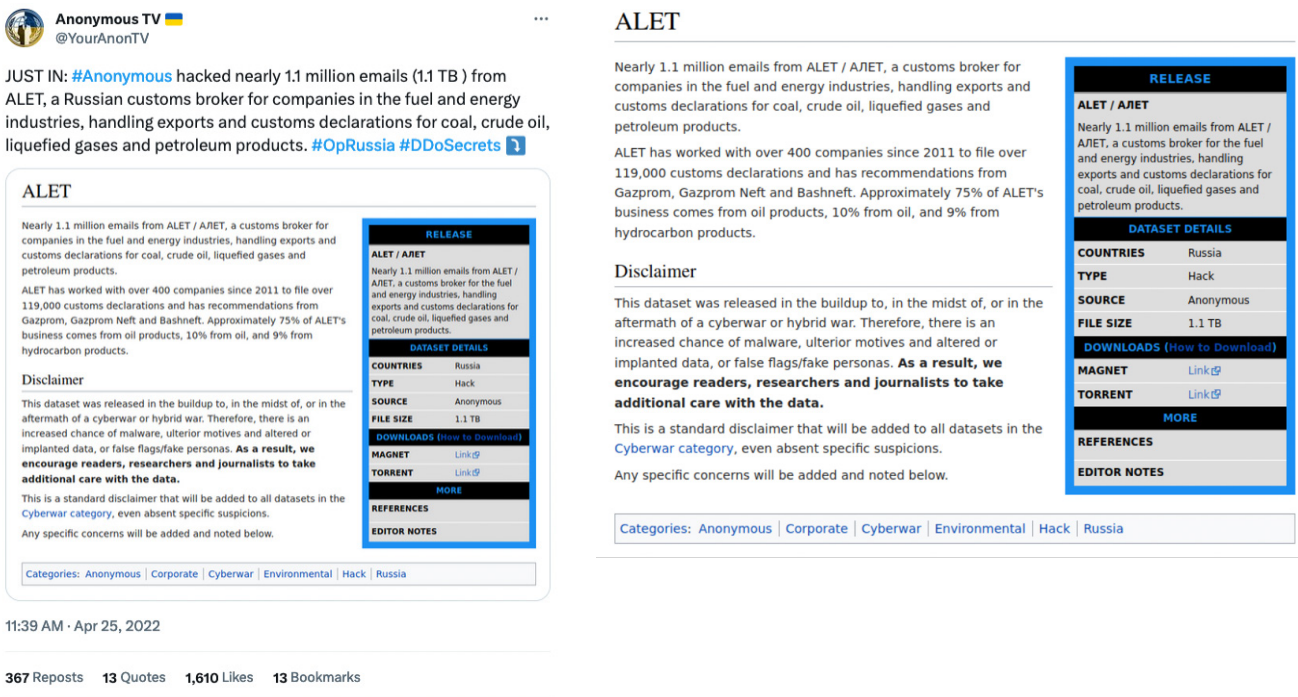


Figure 14 - Divulgation des données du service de douane russe ALET. (Monitoring CERT-XMCO)[54]

Parmi les victimes, Anonymous aurait publié une archive de 1,7 To contenant 1,23 million de courriels de la plus grande entreprise d'électricité de Russie, Elektrocentromontazh, chargée de concevoir, tester et entretenir les installations de production et de transmission d'électricité dans plus de 25 régions de Russie. Le collectif Anonymous aurait également publié une archive de 1,1 To contenant les échanges internes du courtier en douane ALET, spécialisé dans les exportations et les déclarations en douane pour le charbon, le pétrole brut, les gaz liquéfiés et les produits pétroliers. Le groupe russe ALET collabore activement avec Gazprom et Bashneft depuis 2011[55]. **Par effet de cascade, les industries occidentales implantées en Russie se voient ciblées par les collectifs hacktivistes pro-Ukraine.** Dans un tweet publié le 11 mars 2022, Anonymous a annoncé vouloir attaquer les sociétés françaises continuant à travailler avec les autorités russes[56] :

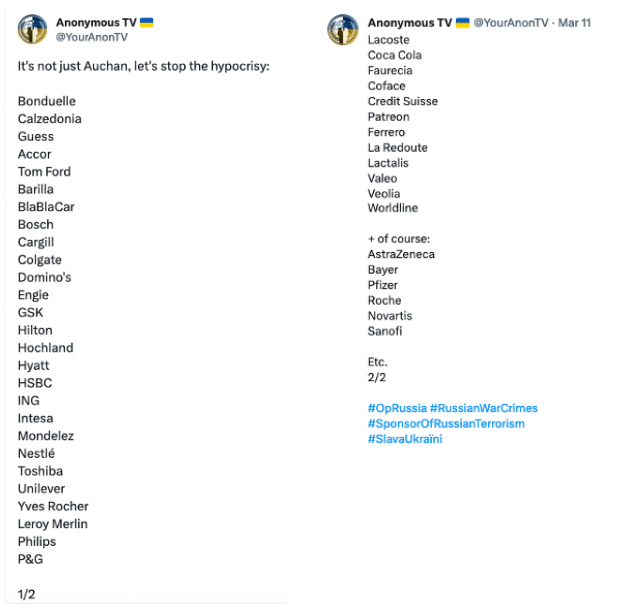


Figure 15 - Incitation d'Anonymous à prendre pour cible les entreprises françaises du secteur de l'énergie (CERT-XMCO)

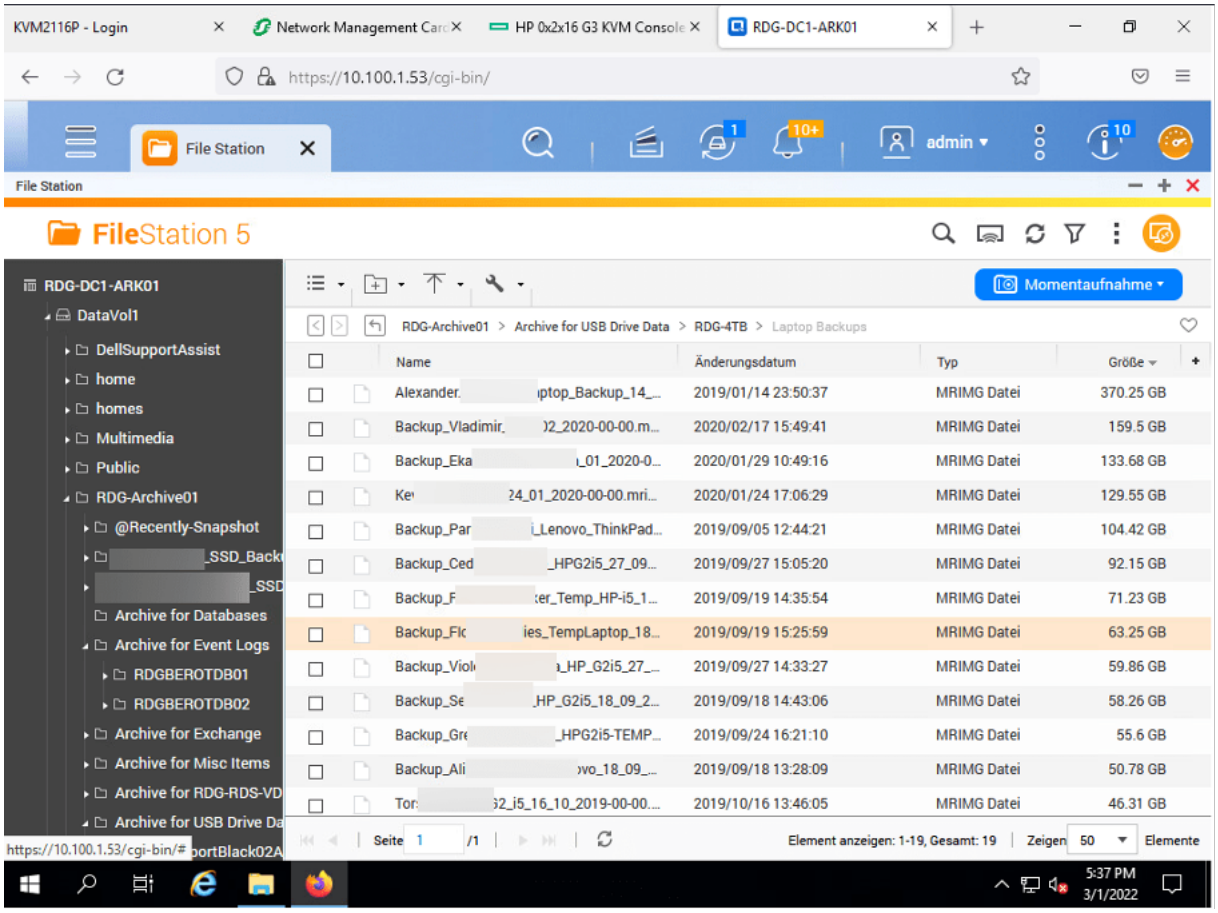
Loin d'endiguer le paysage de la menace, la polarisation de l'écosystème cybercriminel au début de l'année 2022 a entrainé une confusion généralisée des acteurs, de leurs motivations et de leurs TTPs. Cette situation explique les chevauchements de TTPs observés entre des acteurs aux motivations diverses, parfois même contradictoires.

En septembre 2022, les analystes du *Threat Analysis Group* de Google ont signalé qu'un groupe référencé **UAC-0098** exploitait le trojan **IceID** et des TTPs similaires à celles de **Conti** pour cibler l'Ukraine, laissant supposer que les anciens opérateurs du groupe travaillaient maintenant pour le compte de la Russie dans le cadre du conflit[57]. A l'inverse les opérateurs du ransomware LockBit ont plusieurs fois revendiqué leur position de neutralité. La coopération des acteurs de la menace russophones a été durablement endommagée par les désaccords politiques entre les groupes de ransomware concernant la position à adopter par rapport à la guerre en Ukraine.

Aussi, les campagnes d'attaques par déni de service distribué (DDoS) ont entrainé des perturbations temporaires pour les entreprises du secteur de l'énergie. En 2022, les groupes revendiquant leur affiliation au collectif «Anonymous» ont fait la promotion des opérations de type Hack&Leak, visant des entités occidentales du secteur de l'énergie. Le 14 mars 2022, **Anonymous** a revendiqué la compromission de la filiale allemande du géant énergétique russe Rosneft, volant 20 téraoctets de données à l'entreprise selon *Security Affairs*. Selon WELT, la compromission de la filiale allemande de Rosneft (**Deutschland GmbH**) aurait eu des « effets dommageables pour l'entreprise ». L'attaque a été confirmée par l'Office fédéral allemand de la sécurité de l'information[58]. Divers processus auraient été perturbés, y compris la plateforme de gestion des contrats de la filiale.

Figure 16 - Revendication de l'attaque contre Rosneft le 11 mars 2022 (source : Monitoring CERT-XMCO)

Rosneft avait déjà été touchée par le collectif Anonymous en février 2022 lors d'une attaque DDoS. La filiale allemande est responsable d'environ un quart des importations de pétrole brut en Allemagne.



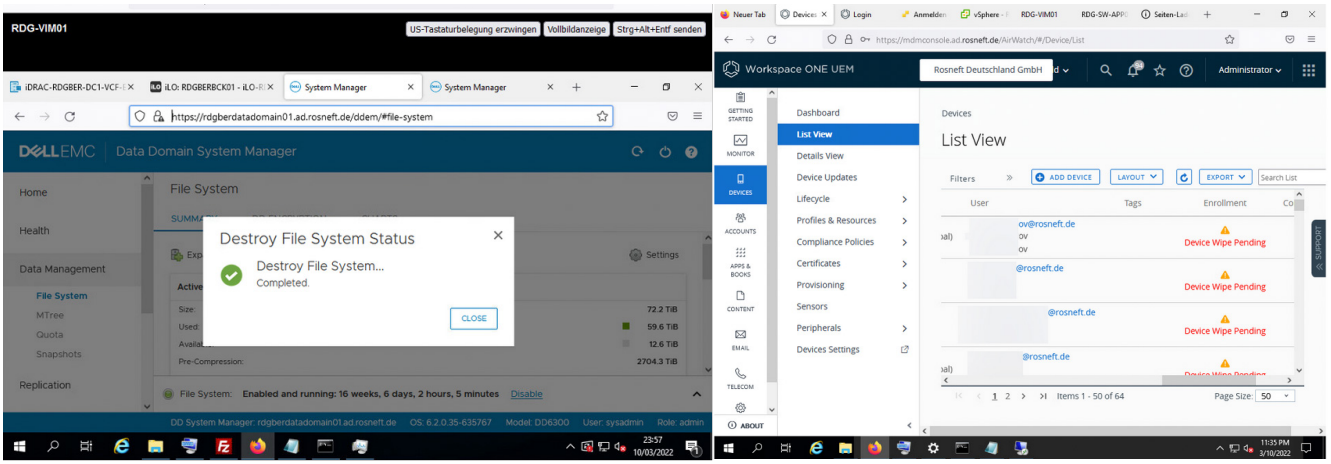


Figure 17 - Accès aux hyperviseurs de la filiale allemande de Rosneft (source : SecurityAffairs)[59]

Dernier exemple de campagne hacktiviste visant le secteur de l'énergie, en octobre 2022, l'Organisation iranienne de l'énergie atomique (**AEOI**) a confirmé la compromission d'une de ses bases de données, ayant ensuite été divulguée en ligne. Un serveur de messagerie électronique exploité par l'une des filiales de l'organisation iranienne aurait été attaqué par le groupe **Black Reward**. Ce dernier serait un groupe hacktiviste opposé au régime en place.

Le collectif aurait ensuite divulgué une collection de 14 archives RAR d'une taille de 27 Go, contenant prétendument 85 000 messages électroniques sur son canal Telegram.

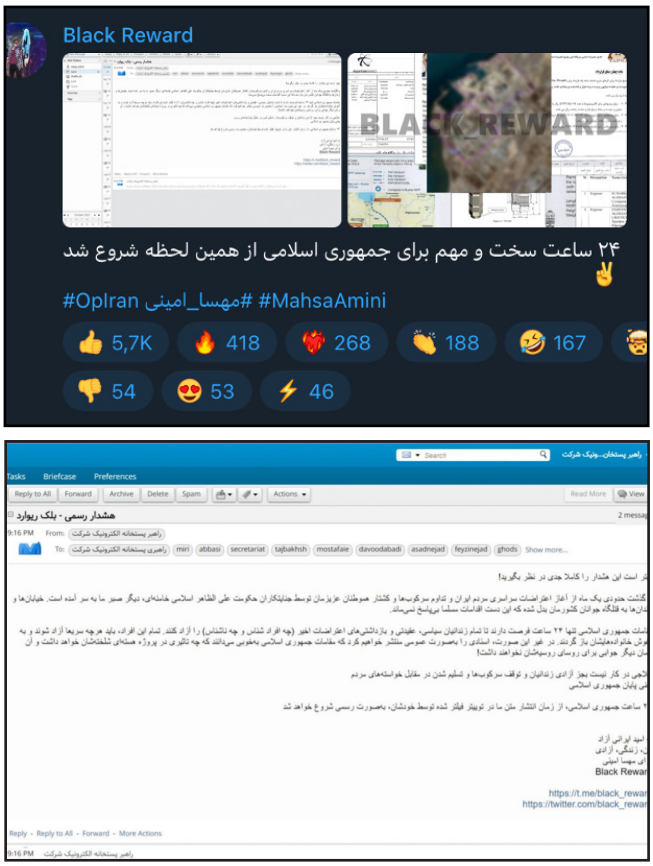


Figure 18 - Revendication de l'attaque par Black Reward sur Telegram (Monitoring CERT-XMCO)

« Les données volées comprenaient les passeports et les visas présumés d'Iraniens et de Russes travaillant avec l'AEOI. D'autres rapports scientifiques sur les performances des centrales électriques auraient été divulgués. La revendication de l'attaque par Black Reward était accompagnée par le message «Pour les femmes, la vie, la liberté», donnant à l'attaque un caractère hacktiviste[60]. »

2. L'énergie : un secteur d'activités vulnérable au cybercrime

En 2022, les acteurs de la menace cyber ont identifié le potentiel lucratif offert par le secteur de l'énergie. Étant donné les faiblesses structurelles (vulnérabilités présentes au sein des systèmes SCADA/ICS) et l'importance stratégique que revêt ce secteur, différents groupes aux motivations financières ont attaqué des entreprises du secteur de l'énergie en 2022.

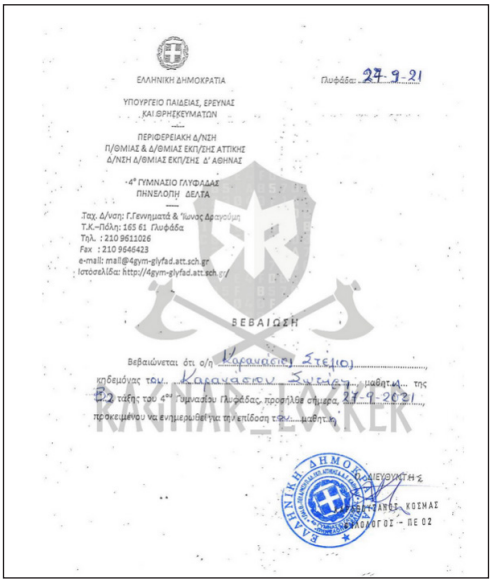
2.1. OPPORTUNISME DES GROUPES DE RANSOMWARE CIBLANT LE SECTEUR DE L'ÉNERGIE

En 2022, les attaques par ransomware ont continué de croître, perturbant les opérations de plusieurs organisations, fournisseurs et filiales du secteur de l'énergie par opportunisme. Au cours de l'année, les chercheurs de DRAGOS ont notamment observé le recours aux courtiers d'accès initiaux (IAB) comme vecteur de compromission initiale par les groupes de ransomwares. Ces groupes se sont aussi illustrés par l'exploitation de logiciels d'accès à distance légitimes détournés (de type RDP) comme Cobalt Strike et Brute Ratel RC4 pour contrôler les appareils à distance[61]. Selon les observations du CERT-XMCO, les groupes de ransomware LockBit et BlackBasta ont compromis respectivement 8 entreprises du secteur de l'énergie en 2022, suivis de près par BlackCat avec 6 attaques attribuées par des éditeurs de sécurité mais non revendiquées par ses opérateurs. La plupart de ces groupes opèrent selon le modèle de **Ransomware-as-a-Service** (RaaS) dans le cadre de campagnes lucratives.

En 2022, le groupe d'affiliés russophones BlackCat, aurait mené un nombre croissant d'attaques de ransomware ciblant des infrastructures énergétiques critiques en Europe de l'Ouest en 2022[62]. La victimologie du groupe inclurait notamment :

- Le fournisseur d'électricité et de gaz naturel Creos Luxembourg SA[63]
- La société allemande de stockage d'huile et de gaz Oiltanking[64]
- La société de négoce de pétrole Mabanaft[65]

Au cours du mois d'août 2022, les opérateurs du groupe de ransomware **Ragnar Locker** se sont illustrés par une fuite de données de 361GB ayant affecté le principal distributeur de gaz naturel en Grèce, DESFA.


ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ

ΠΕΡΙΦΕΡΕΙΑΚΗ Δ/ΝΣΗ Π/ΘΜΙΑΣ & Δ/ΘΜΙΑΣ ΕΚΠ/ΣΗΣ ΑΤΤΙΚΗΣ
Δ/ΝΣΗ Δ/ΘΜΙΑΣ ΕΚΠ/ΣΗΣ Δ' ΑΘΗΝΑΣ

4ο ΓΥΜΝΑΣΙΟ ΓΛΥΦΑΔΑΣ
ΠΗΝΕΛΟΠΗ ΔΕΛΤΑ

Πλυφάδα: 27-9-21

ΒΕΒΑΙΩΣΗ

Βεβαιώνεται ότι ο/η ... της τάξης του 4ου Γυμνασίου Γλυφάδας, προήλθε φοιτώσα 27-9-2021

ΔΙΕΥΘΥΝΤΗΣ

ΠΕ 02

Figure 19 - Documentation interne de DESFA divulguée par Ragnar Locker (Monitoring du CERT-XMCO)

En mars 2022, le FBI avait publié une alerte signalant que depuis 2020, au moins 52 entités appartenant à dix secteurs des infrastructures critiques aux États-Unis avaient été compromises par ce ransomware.

2.2. POPULARISATION DU MODÈLE MALWARE-AS-A-SERVICE

Les investigations menées sur le Deep/Dark Web par les consultants du CERT-XMCO ont mis en évidence les capacités d'innovation des acteurs de la menace, discutant notamment du fonctionnement des systèmes de contrôle industriel (ICS) et partageant des tutoriels, des documents et des rapports sur les automates programmables (PLC) et les unités terminales distantes (RTU) à des fins de reconnaissance.

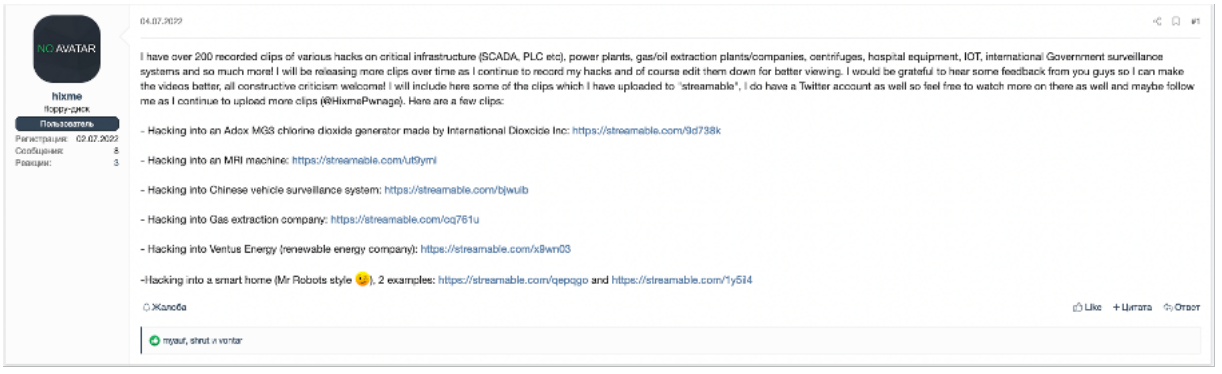


Figure 20 - Partage de vidéoclips réalisés lors d'attaques à l'encontre d'infrastructures du secteur de l'énergie (Monitoring du CERT-XMCO)

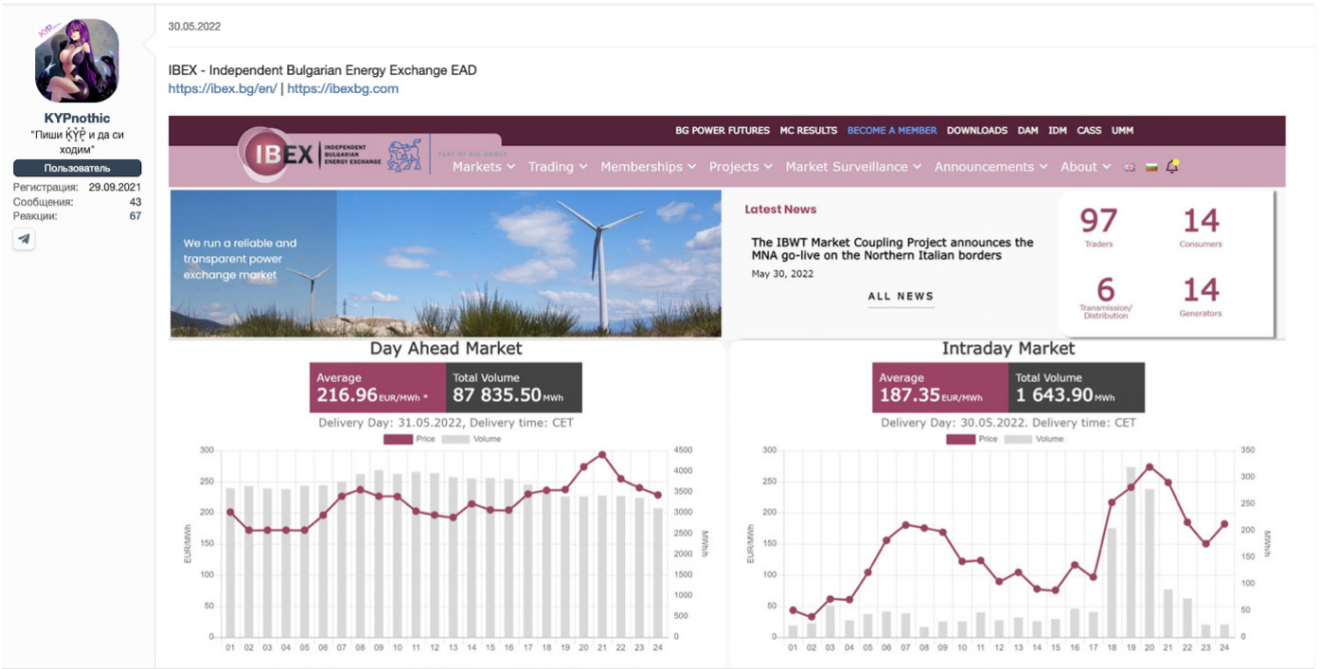


Figure 21 - Hack and Leak de la Bourse indépendante de l'énergie bulgare (source : Monitoring CERT-XMCO)

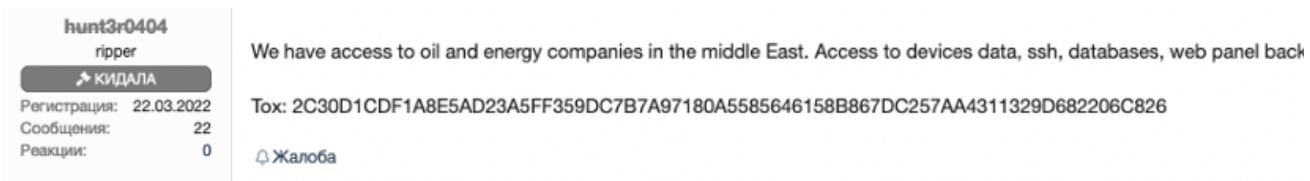


Figure 22 - Vente d'accès au sein de plusieurs sociétés du secteur de l'énergie localisées au Moyen-Orient (Monitoring CERT-XMCO)

Au cours de l'année 2022, les chercheurs d'Intezer ont mis au jour une campagne d'attaque sophistiquée ciblant des grandes entreprises du secteur de l'énergie. L'attaque observée par Intezer visait en particulier des fournisseurs de pétrole et de gaz[66].

Le contenu des courriels analysés démontrait une connaissance approfondie de l'acteur malveillant sur les interactions interentreprises (**B2B**). Les adresses de courriel des destinataires de ces courriels vont des adresses génériques telles que «info@target_company[.]com» ou «sales@target_company[.]com» à des personnes spécifiques au sein des entreprises ciblées.

Parmi les malwares identifiés lors de cette campagne figuraient notamment les MaaS **Formbook, Agent Tesla, Snake Keylogger, et AZORult**. Au cours de l'année 2022, les acteurs cybercriminels ont constamment cherché à exploiter les nouvelles vulnérabilités découvertes au sein de la chaîne d'approvisionnement afin de s'introduire dans les systèmes ou d'infecter les réseaux d'entreprises avec leurs malwares.

3. Analyses et conclusions

En résumé, nous sommes en mesure de tirer 4 grandes analyses de notre Panorama. Celles-ci sont divisées en :

- **Observations :** événements que nous avons identifiés au cours de nos investigations et notre veille ;
- **Enseignements :** mises en perspective effective des observations faites ;
- **Hypothèses :** déductions possibles des enseignements, sur lesquelles s'appuyer pour anticiper les risques et les menaces.

Analyses	Observations	Enseignements	Hypothèses
1	Seules quelques informations Open Source sur les **campagnes d'espionnages (APT)** ciblant des organisations du secteur de l'énergie sont disponibles. Elles concernent principalement des MOA chinois et russes.	La couverture des campagnes d'espionnage est facilitée par le peu d'informations disponibles qui permettent de réduire le niveau de bruit potentiel. Cependant, cette situation donne une visibilité très partielle des campagnes passées ou en cours et pousse à s'appuyer fortement sur les analyses géopolitiques (corroborées avec le peu d'informations disponibles) pour proposer des analyses pertinentes.	L'analyse géopolitique permet d'identifier 3 types d'organisations potentiellement visées au regard des enjeux géopolitiques: • Les organisations implantées sur des zones géographiques en tension, tous sous-secteurs énergétiques confondus (Europe, Asie de l'Est et du Sud-Est, sous continent indien, principalement) • Les entreprises à fort patrimoine intellectuel (nucléaire, construction de batteries électrique,etc.) • Les multinationales stratégiques au positionnement géopolitique ambigu (ex: TotalEnergies, Aramco, etc.).
2	Les **campagnes cyber de destruction d'infrastructure** ciblent principalement l'Ukraine (depuis 2014) et sont menées par des MOA alignés avec les intérêts de la Russie.	Jusqu'à ce jour les attaques destructrices ont touché des organisations, Stuxnet mis à part, implantées sur des zones territoriales contestées et/ou attaquées(ex. Ukraine).	Avec la multiplication des conflits territoriaux impliquant des États disposant de capacités cyber avancées, Taiwan, l'Inde, le Pakistan, l'Arabie Saoudite, l'Iran, l'Europe de l'Est et l'Asie du Sud-Est constituent des espaces de risques majeurs pour toute organisation implantée dans ces pays.
3	Les attaques **cybercriminelles** sont principalement des attaques de type **ransomware**, avec une victimologie identifiée autour de deux pôles principaux : • Amérique du Nord/Europe de l'Ouest • Amérique latine/ Asie du Sud-Est	• Amérique du Nord/Europe de l'Ouest : les organisations transport et stockage d'énergie (pétrole et gaz) et production de renouvelable sont principalement visées. • Amérique latine/ Asie du Sud-Est : les organisations de production de pétrole (plateformes, etc.) sont principalement visées.	Le risque ransomware est accentué en Europe avec le déclenchement de la guerre en Ukraine et tous les enjeux liés à l'approvisionnement énergétique qui en découlent. En effet, les opérations menées sont susceptibles d'être alignées avec les intérêts russes. Ceci étant de nombreuses campagnes de sont pas revendiquées (cf. les attaques de février 2022 contre Creos, Oiltanking et Mabnaft) pour les secteurs les plus sensibles comme le stockage et le transport de pétrole et gaz pour ne pas reproduire le schéma de Colonial Pipeline. Autrement, le risque ransomware demeure opportuniste et indiscriminé.
4	De nombreux groupes hacktivistes se sont constitués comme partie prenante à la guerre en Ukraine et ont notamment attaqué des organisations du secteur de l'énergie. Plus largement, on a observé ces dernières années la multiplication de groupes hacktivistes portant des revendications politiques et géopolitiques.	Le regain de tensions politiques et géopolitiques a poussé fortement à la création de groupes hacktivistes qui prennent pour cibles des organisations publiques et privées, dont certaines appartiennent au secteur de l'énergie, auxquelles ils s'opposent de manière directe ou indirecte.	Il faut voir la multiplication des campagnes hacktivistes comme un résultat l'hybridation des affrontements géopolitiques et politiques, tant d'un point de vue de la nature de ces affrontements (vecteur cyber) que de la nature des acteurs qui y prennent part (collectifs hacktivistes informels). Cette dynamique doit être en particulier prise en considération pour les organisations du secteur de l'énergie. En effet, la création de groupes hacktivistes para-politiques ou environnementalistes radicaux et contestataires (cf. augmentation brutale des prix de l'énergie) manipulés ou non par des intérêts étrangers, qui prendrait pour cibles des acteurs du secteur de l'énergie est une éventualité des prochaines années.

Au cours de l'année 2022, les différents modes opératoires observés par le CERT-XMCO ont tiré avantage de la zone grise existante en matière d'attribution pour mener des compromissions à l'encontre du secteur de l'énergie.

L'invasion de l'Ukraine par la Fédération de Russie a eu des répercussions significatives sur l'approvisionnement énergétique en Europe. Les attaques menées par les modes opératoires APT ont été une préoccupation majeure en 2022, démontrant leur capacité d'évasion et exploitant les faiblesses structurelles des systèmes de contrôle industriel (ICS/SCADA) pour collecter des renseignements et saboter les infrastructures. Les modes opératoires associés à la Chine ont eu recours à des TTPs sophistiquées lors des attaques ciblant le secteur de l'énergie en 2022. À des fins d'évasion, ces APTs ont eu recours à des outils sur mesure pour cibler le système électrique national d'intervention d'urgence indien. Les répercussions de la guerre en Ukraine sur les marchés européens et mondiaux de l'énergie, invitent à repenser la protection de la production, la transmission et la distribution des énergies contre le risque toujours croissant de cyberattaques.

Les attaques par ransomware ciblant les infrastructures critiques du secteur de l'énergie sont également restées un sujet préoccupant tout au long de l'année, avec 49 attaques recensées par les consultants du CERT-XMCO. Cette tendance sans précédent souligne la nécessité urgente de renforcer la cybersécurité dans le secteur de l'énergie pour protéger les infrastructures critiques et garantir un approvisionnement. En somme, l'état de la menace cyber ciblant le secteur de l'énergie en 2022 a mis en évidence la vulnérabilité de ce secteur stratégique qui reste susceptible d'être ciblé au cours des prochaines années.

De surcroit, la guerre en Ukraine a marqué un fort retour sur scène des groupes hacktivistes pour soutenir les parties prenantes du conflit à travers des opérations de déstabilisation (défacement, DDoS, fuite de données). Cette réapparition massive des groupes hacktivistes s'expliquant par un retour marqué des tensions géopolitiques devrait être considérée attentivement. En effet, avec le raidissement observé de nouveaux groupes environnementalistes, des entreprises du secteur pourraient d'être prises pour cibles par des organisations militantes qui choisiraient de faire évoluer leurs modes d'action vers des opérations hacktivistes.

Le secteur de l'énergie revêt une importance cruciale en raison de ses activités et de leurs conséquences sur les relations internationales. Il peut agir comme un vecteur de diplomatie et de coopération, tout en pouvant être utilisé comme un outil d'influence dans la guerre économique en suscitant des rivalités entre les puissances.

En raison de la sous-traitance de certaines de leurs activités ou de la délocalisation de leurs ressources humaines et infrastructures numériques, divers organismes du secteur de l'énergie ont subi une compromission de leurs données et infrastructures par effet de cascade en 2022.

Le CERT-XMCO recommande aux organismes du secteur de l'énergie de maintenir une veille constante de l'actualité internationale, en fonction de la nature respective de leurs activités et de leurs implantations géographiques.

Face à la nécessité des organismes du secteur de l'énergie d'assurer une disponibilité constante et une intégrité de leurs systèmes SCADA/ICS, nos consultants vous recommandent également de mettre en place un ensemble de mesures afin de vous protéger contre les acteurs de la menace, en mettant en place :

- Des mises à jour régulières de votre Système d'Information,
- Des sauvegardes régulières de votre Système d'Information,
- L'établissement d'une cartographie d'implantation de ses activités ainsi que de ses principaux partenaires,
- La cartographie votre périmètre d'exposition,
- La surveillance de votre surface d'exposition/attaque (surveillance du Deep et Dark Web, vente d'identifiants valides, exposition d'interfaces sensibles, etc.),
- L'identification des modes opératoires les plus susceptibles de vous prendre pour cible au regard de vos activités et de vos implantations géographiques,
- La réalisation d'exercice de crise cyber réguliers,
- Des séances de sensibilisation sur l'hygiène numérique pour vos collaborateurs.

Indices de compromission

Mail Box

domain:activate-suport-up-date-142i[.]eu5[.]net
domain:adm-up-da-te-x2020x89354[.]eu5[.]net
domain:i197--activate-up-date[.]eu5[.]net
domain:xt543-suport-up-date[.]eu5[.]net
domain:8xe3615-12-2019-up-date[.]eu3[.]org
domain:i131dere-up-date[.]eu3[.]biz
domain:jan-6543-up-date[.]eu3[.]biz
domain:x437-suport-up-dates[.]eu5[.]net
domain:e541-suport-up-date[.]eu5[.]net
domain:x914-suport-up-date[.]eu5[.]net
domain:4877-activate-up-date[.]eu5[.]net
domain:active-up-date-xk89si[.]eu5[.]net
domain:activate-suport-up-date-i754[.]eu3[.]biz
domain:activate-suport-up-date-i754[.]eu3[.]biz
domain:activate-suport-up-date-321i[.]eu3[.]biz
domain:adms-suport-up-datex8323[.]eu3[.]biz
domain:05-2019-up-date[.]eu5[.]net
domain:x07-2019-up-date[.]eu5[.]net
domain:08-2019-up-datex[.]eu5[.]net
domain:07-2019-up-datex[.]eu5[.]net
domain:adms-up-date-2020[.]eu5[.]net
domain:adm-up-date-2020x68293[.]eu5[.]net
domain:08-2019-up-da-tex[.]eu5[.]net
domain:06-2019-up-date1[.]eu5[.]net
domain:04-2019-upd[.]eu5[.]net

ipv4:185[.]176[.]43[.]106
ipv4:185[.]176[.]43[.]90
ipv4:185[.]176[.]43[.]98
ipv4:185[.]176[.]43[.]96
ipv4:185[.]176[.]43[.]94
ipv4:185[.]176[.]43[.]80
ipv4:185[.]176[.]43[.]84
ipv4:185[.]176[.]43[.]82
ipv4:185[.]176[.]43[.]80

url:hxxp://saleswarriorinc[.]com/aba/login/index[.]php
url:hxxp://armaghanteb[.]com/bul/login/index[.]php
url:hxxp://quadteximagery[.]com/veri/login/index[.]php
url:hxxps://primage[.]com[.]br/aa/update/index[.]php
url:hxxps://alphabitconsulting[.]com/veri/login/index[.]php
url:hxxps://centralinsumos[.]com[.]bo/update/index[.]php
url:hxxps://pwametalurgica[.]com[.]br/bb/update/index[.]php
url:hxxps://cercoselectricos[.]cl/aa/update/index[.]php
url:hxxps://flammaautomoveis[.]com[.]br/bul/update/index[.]php
url:hxxp://englishlessons-houston[.]com/les/welcome/?user=
url:hxxp://saojoaodaurtigars[.]com[.]br/malaysia/login/?user=

ScanBox de Red Ladon

url:hxxp://australianmorningnews[.]com/?p=23-7
url:hxxp://australianmorningnews[.]com/?p=23-11
url:hxxp://australianmorningnews[.]com/?p=23-24
url:hxxp://australianmorningnews[.]com/?p=23-27

RedEcho

ipv4:122[.]117[.]212[.]65
ipv4:103[.]58[.]93[.]133
ipv4:125[.]141[.]38[.]53
ipv4:14[.]45[.]33[.]239
ipv4:14[.]55[.]86[.]138
ipv4:183[.]108[.]133[.]29
ipv4:183[.]99[.]53[.]180
ipv4:220[.]94[.]133[.]121
ipv4:58[.]76[.]177[.]166

APT31

file:5897e67e491a9d8143f6d45803bc8ac8
file:91965ee08504eeb01e76e17007497852
file:0c1e1fd94383efc5a3de8f0117c154b2
file:85f8bfb3b859a35e342e35d7c35e8746
file:0c993a406be04b806222a130fb5a18e8
file:dfaa28a53310a43031e406ff927a6866
file:0c4540f659d3942a28f158bce7be1143
file:1d65ef16d1f161ae3faa5ed7896734cd
file:176d11c9bafac6153f728d8afb692f6f
file:5897e67e491a9d8143f6d45803bc8ac8
file:50eb199e188594a42262a5bbea260470
file:c89eaa7f40fc75f9a34e0f0a3b59b88b
file:0c1e1fd94383efc5a3de8f0117c154b2
file:640e6ecad629bd33c09ccec52f4aa6da
file:11010e139010697a94a8feb3704519f9
file:099c7d85d0d26a31469465d333329778
file:8b4c1f0ff1cee413f5f2999fa21f94f9

Indices de compromission

APT Bitter

file:5f663f15701f429f17cc309d10ca03ee00fd20f733220cc9d2502eff5d0cd1a1
file:eb7aebded5549f8b006e19052e0d03dc9095c75a800897ff14ef872f18c8650e
file:cac239cf09a6a5bc1f9a3b29141336773c957d570212b97f73e13122fe032179
file:8d2f6b0d7a6a06708593cc64d9187878ea9d2cc3ae9a657926aa2a8522b93f74
file:33905e2db3775d2e8e75c61e678d193ac2bab5b5a89d798effbceb9ab202d799
file:5c85194ade91736a12b1eeeb13baa0b0da88c5085ca0530c4f1d86342170b3bc
file:Ef4fb1dc3d1ca5ea8a88cd94596722b93524f928d87dff0d451d44da4e9181f1
file:b2566755235c1df3371a7650d94339e839efaa85279656aa9ab4dc4f2d94bbfa
file:33a20950e7f4b2191706ddf9089f1e91be1e5384cca00a57cf6b58056f70c96b
file:7e7e90b076ef3ea4ef8ed4ef14fb599a2acb15d9ce00c78e5949186da1e355cf
file:07504fcef717e6b74ed381e94eab5a9140171572b5572cda87b275e3873c8a88
file:06b4c1f46845cee123b2200324a3ebb7fdbea8e2c6ef4135e3f943bd546a2431
file:ded0635c5ef9c3d63543abc36a69b1176875dba84ca005999986bd655da3a446

APT Lazarus

file:586F30907C3849C363145BFDCDABE3E2E4688CBD5688FF968E984B201B474730
file:8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
file:c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
file:dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
file:90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
file:226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
file:16F413862EFDA3ABA631D8A7AE2BFFF6D84ACD9F454A7ADAA518C7A8A6F375A5
file:05732E84DE58A3CC142535431B3AA04EFBE034CC96E837F93C360A6387D8FAAD
file:6FBB771CD168B5D076525805D010AE0CD73B39AB1F4E6693148FE18B8F73090B
file:912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9
file:CAF6739D50366E18C855E2206A86F64DA90EC1CDF3E309AEB18AC22C6E28DC65
file:2963a90eb9e499258a67d8231a3124021b42e6c70dacd3aab36746e51e3ce37e
file:plink2AA1BBBE47F04627A8EA4E8718AD21F0D50ADF6A32BA4E6133EE46CE2CD13780
file:5A73FDD0C4D0DEEA80FA13121503B477597761D82CF2CFB0E9D8DF469357E3F8
file:C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3

ipv4:104[.]155[.]149[.]103
ipv4:40[.]121[.]90[.]194
ipv4:185[.]29[.]8[.]162
ipv4:146[.]4[.]21[.]94
ipv4:46[.]183[.]221[.]109
ipv4:84[.]38[.]133[.]145
ipv4:109[.]248[.]150[.]13
ipv4:155[.]94[.]210[.]11
ipv4:192[.]186[.]183[.]133
ipv4:54[.]68[.]42[.]4
ipv4:84[.]38[.]133[.]145
ipv4:213[.]180[.]180[.]154

url:hxxp[://]104[.]155[.]149[.]103/2-443[.]ps1
url:hxxp[://]104[.]155[.]149[.]103/8080[.]ps1
url:hxxp[://]104[.]155[.]149[.]103/mi64[.]tmp

(suite) **APT Lazarus**

url:hxxp[://]104[.]155[.]149[.]103/mi[.]tmp
url:hxxp[://]104[.]155[.]149[.]103/mm[.]rar

Indices de compromission

url:hxxp[://]104[.]155[.]149[.]103/pd64[.]tmp
url:hxxp[://]104[.]155[.]149[.]103/rar[.]tmp
url:hxxp[://]104[.]155[.]149[.]103/spr[.]tmp
url:hxxp[://]104[.]155[.]149[.]103/t[.]tmp
url:hxxp[://]104[.]155[.]149[.]103/update[.]tmp
url:hxxp[://]109[.]248[.]150[.]13:8080/1
url:hxxp[://]146[.]4[.]21[.]94/tmp/data_preview/virtual[.]php
url:hxxp[://]185[.]29[.]8[.]162:443/1[.]tmp
url:hxxp[://]40[.]121[.]90[.]194/11[.]jpg
url:hxxp[://]40[.]121[.]90[.]194/300dr[.]cert
url:hxxp[://]40[.]121[.]90[.]194/b[.]cert
url:hxxp[://]40[.]121[.]90[.]194/qq[.]cert
url:hxxp[://]40[.]121[.]90[.]194/ra[.]cert
url:hxxp[://]40[.]121[.]90[.]194/Rar[.]jpg
url:hxxp[://]40[.]121[.]90[.]194/tt[.]rar
url:hxxp[://]84[.]38[.]133[.]145/board[.]html
url:hxxp[://]84[.]38[.]133[.]145/header[.]xml
url:hxxp[://]www[.]ajoa[.]org/home/manager/template/calendar[.]php
url:hxxp[://]www[.]ajoa[.]org/home/rar[.]tmp
url:hxxp[://]www[.]ajoa[.]org/home/tmp[.]ps1
url:hxxp[://]www[.]ajoa[.]org/home/ztt[.]tmp
url:hxxp[://]www[.]orvi00[.]com/ez/admin/shop/powerline[.]tmp

C2:xxps[://]tecnojournals[.]com/review
C2:xxps[://]semiconductboard[.]com/xml
C2:xxp[://]cyancow[.]com/find
C2:xxp[://]155[.]94[.]210[.]11/news/page[.]php
C2:xxp[://]192[.]186[.]183[.]133/bbs/board[.]php
C2:xxp[://]213[.]32[.]46[.]0/board[.]php
C2:xxp[://]54[.]68[.]42[.]4/mainboard[.]php
C2:xxp[://]84[.]38[.]133[.]145/apollom/jeus[.]php
C2:xxp[://]mudeungsan[.]or[.]kr/gbbs/bbs/template/g_botton[.]php
C2:xxp[://]www[.]easyview[.]kr/board/Kheader[.]php
C2:xxp[://]www[.]easyview[.]kr/board/mb_admin[.]php
C2:xxp[://]213[.]180[.]180[.]154/editor/session/aaa000/support[.]php

Industroyer2

file:D9C17C35A68FC505235E20C6E50C622AED8DEA0
file:6FA04992C0624C7AA3CA80DA6A30E6DE91226A16
file:9CE1491CE69809F92AE1FE8D4C0783BD1D11FBE7
file:0090CB4DE31D2D3BCA55FD4A36859921B5FC5DAE
file:D27D0B9BB57B2BAB881E0EFB97C740B7E81405DF
file:3CDBC19BC4F12D8D00B81380F7A2504D08074C15
file:8FC7646FA14667D07E3110FE754F61A78CFDE6BC

Prestige ransomware

file:5dd1ca0d471dee41eb3ea0b6ea117810f228354fc3b7b47400a812573d40d91d
file:5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57
file:6cff0bbd62efe99f381e5cc0c4182b0fb7a9a34e4be9ce68ee6b0d0ea3eee39c
file:a32bbc5df4195de63ea06feb46cd6b55

Indices de compromission

Campagne cybercriminelle non identifiée[66]

file:1c85618ef82808c9bcc6deddf93b66d6ee7a81b82c03341ecbf61d3ee4975bb3
file:74109522b38c609b4c576eecde644ffe544fcdc9a6494a9683f8eea6fb9e0bc7
file:cd77a054500efdac4d39d743ad83f963c738d6f2b6b53f5c4b5818d34742f02b
file:3da25300ec711385344467823ae229bbc25a9a5a7caeccd911875994ed74c5b9
file:8877b6a829967924063e85120bf22b2ccc511fa25e376b479213020a15482bf6
file:0dc594a10793d93e26584d8dcd4d811c4b2ccb017b86eb1119380f17e3606f85
file:b51e83fd2583c8e92ef34f6b8d23e07aaa82eedcf2db4b68e667f3a52c8862f5
file:079c7d83465481952407f3da954e08a5f165ff5480e2a51c32505088e78750f5
file:53e3ae371a3e329c6ed4942eb6cc51007c53008e3b9da6fccaecbed8f68f2ffa
file:96ff156bd7b09ec5a6216f43c0de578aafa9a8103832a401ce156e2ee918f580
file:ff5be1c9c0ee11ceca68c10a9bcd1f8a995be8e3f89ed17a4933adde010ac3ad
file:d5080a9391b2ad1a75deeee81db15be47be2b0742378f633081eb4c9f81226ad
file:a722bde3892eeaafdd285b6e9aabc67f0ad8dc8abe4035a8ff11671a7c2a68b1
file:01970569f16e4adfdd4afb50d7a85327e8eb6abd7cb61a446e4a6f1010835968
file:0ab00782d02cb0e817b0237007b6b7f81139ff6ded17bc42fbf277e929b77ccf
file:3d8d4fbf52301ea8dca5602d6c86da3d82fd659074d7868938064e84c7ad424a
file:ee7a4274d02042c8e516de2695ced13f4623c96377762f088d7795d5b0b2bd6f
file:0ea3575eed95cf60b1efb487a350a9fa24fd77482e881020a9a0f77220a6ad33
file:102adafddb589d6739ce8a489054825a9a958baa01e87b95eebdc302675a3bd9
file:9644169dee32d60f41d8d4e1f3dfb45a930ad3efd993fe941647549cf5e924dd
file:e2adb897c29a67295a2b411c47ee76e1e9ce1e27dccf259bc42a84c481ae41ce
file:a03c0a2b6458cf55ee800291cf6b4698d1450bddd6d9e3e02f963c465004ac5c
file:f1e85b9f7b1c2a6ce9da528dbfe2c66f0a0f513f39411dbf7bb7d4d917e1ba99
file:0840cff0a98daa3962236913952b7b16896cae63af24fa99e46f3371c0e1ca49
file:6a99c482b1634f3d0c775f4c8a0d1bb04cd24a0f54f1f48d1ee2697f5bf1c6c3
file:86ebf42301074e2907578e98dc20c46f6ecf9789503c625e2b2abfcb2af847b2
file:079c7d83465481952407f3da954e08a5f165ff5480e2a51c32505088e78750f5
file:53e3ae371a3e329c6ed4942eb6cc51007c53008e3b9da6fccaecbed8f68f2ffa
file:96ff156bd7b09ec5a6216f43c0de578aafa9a8103832a401ce156e2ee918f580
file:5384a56a7d814aea903c33fbd602a3e3d5bc637b6e3bc0bd4568d4b7b99db2ad
file:f873b017cb3063a499db2874275e4797b8412ccd1300d29f4f1af03d66ee6700
file:8620f85ffd045187ffbc5d7e70df01d8a04e7fc5c69048b152f2b7284d20caf1
file:06a3fe74ff3dd352db742ac96c6fbd0da1a0d98164dda2a6637e809ec0f48b35
file:b552939890305a0a0d2c9af8973a7d04b1593d9f512c0cc485a0b987f4293d97
file:8e2c23037b36f558920f626e7ef8767daa55734551238eb8816abd144f27db45
file:9c55cc8f7acc09b5de745ec99b0c60862f7975eab77420e41b5c9d1351114cd9
file:d90f2a4a97cf6523e868f67356df7fc08581912c37e8f1f6ee16f2220eabdbb6
file:5db134f3aa187e74903a732b1bd55419977d66c63a55ae8952d908b8b0bc2616
file:713da8a5f0b2ee6a477a57b90834d4ae4637723ad817ffc5a53e5c86792e8ba4
file:7b57b59d06c7ef6cc6fa09fafdf427f2db5969d1b49041d1b7a992e47a9a2726
file:b06cfcc8fabebb1bc83a4dfc91c0f9ba4e23c539018bb94fef1431745c0a2506
file:87b197032a6976c18f7f3df1df6e09cf9fd6a8e4cce3f35f51b2cf521b9ca278
file:7aacd968f2cfb23a8369712c0dc60bcabc7b7d7c0ebf69863f7643e6b90e656f
file:9e9ea32799bf9a246d76b11131abf71bbcffd3b79e026e440b221f6b1bdffe90
file:75ce82077ab9b2e18df87dae0e52270ae49fe20ec22f66fa3698b6fb75452e95
file:14ae4b4b66588af22cf569a90c94e9dd6e2af708ad9dc0efde0cd7d2a809fb51
file:60dc089158d86e9fb10ace29eb6afd7f23d001181e8a4a6ba5083c3597733a71

CVEs

L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) a mis en garde les organisations industrielles qui utilisent des produits vulnérables de mySCADA Technologies :

CVE-2023-28400 https://leportail.xmco.fr/vulndb/CVE-2023-28716 **CVSS 9.9**
CVE-2023-28716 https://leportail.xmco.fr/vulndb/CVE-2023-28716 **CVSS 9.9**
CVE-2023-28384 https://leportail.xmco.fr/vulndb/CVE-2023-28384 **CVSS 9.9**
CVE-2023-29169 https://leportail.xmco.fr/vulndb/CVE-2023-29169 **CVSS 9.9**
CVE-2023-29150 https://leportail.xmco.fr/vulndb/CVE-2023-29150 **CVSS 9.9**

Nexx :
CVE-2023-1749 https://leportail.xmco.fr/vulndb/CVE-2023-1749 **CVSS 6.5**
CVE-2023-1750 https://leportail.xmco.fr/vulndb/CVE-2023-1750 **CVSS 7.1**
CVE-2023-1751 https://leportail.xmco.fr/vulndb/CVE-2023-1751 **CVSS 7.5**
CVE-2023-1752 https://leportail.xmco.fr/vulndb/CVE-2023-1752 **CVSS 8.1**

Hitachi Energy :
CVE-2022-3682 https://leportail.xmco.fr/vulndb/CVE-2022-3682 **CVSS 9.9**
CVE-2022-3683 https://leportail.xmco.fr/vulndb/CVE-2022-3683 **CVSS 7.7**
CVE-2022-3684 https://leportail.xmco.fr/vulndb/CVE-2022-3684 **CVSS 7.5**
CVE-2022-3685 https://leportail.xmco.fr/vulndb/CVE-2022-3685 **CVSS 7.5**
CVE-2022-3686 https://leportail.xmco.fr/vulndb/CVE-2022-3686 **CVSS 4.8**

Sources

(Sources, pages 5 à 8)
Méthodologie & Périmètre des observations

(1) Société spécialisée dans la protection des infrastructures industrielles
(2) https://www.dragos.com/blog/industry-news/2022-dragos-year-in-review-now-available/

(Sources, pages 11 à 28)
L'énergie : un secteur sensible aux tensions géopolitiques

(3) https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report
(4) https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/
(5) https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation
(6) https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine#xj4y7vzkg
(7) https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/
(8) https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
(9) https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
(10) https://www.lopinion.fr/international/en-australie-et-en-nouvelle-zelande-la-chine-redevient-frequentable
(11) https://www.francetvinfo.fr/monde/asie/crise-des-sous-marins-australiens/defense-australie-etats-unis-et-royaume-uni-s-associent-pour-une-nouvelle-generation-de-sous-marins_5709599.html
(12) https://www.proofpoint.com/uk/blog/threat-insight/chasing-currents-espionage-south-china-sea
(13) https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/
(14) https://www.recordedfuture.com/redecho-targeting-indian-power-sector
(15) https://www.itbrew.com/stories/2022/12/07/discontinued-for-17-years-boa-web-server-still-used-for-iot-devices-exposing-massive-security-vulnerabilities
(16) https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation
(17) https://therecord.media/operation-cuckoobees-apt41-cybereason-winnti-group
(18) https://ifrimaps.org/Competition-Chine-Etats-Unis/sublayer/securite-des-approvisionnements-energetiques-la-volonte-chinoise-de-maitriser-ses-dependances
(19) https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/la-chine-a-lere-de-la-rivalite-strategique/la-loi-sur-le-renseignement-national-de-la-chine-et-lavenir-des-rivalites-avec-le-pays-sur-le-plan-du-renseignement.html
(20) https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
(21) https://www.lefigaro.fr/conjoncture/gazoduc-force-de-siberie-2-accord-conclu-entre-la-chine-et-la-russie-20230321
(22) https://intezer.com/blog/research/phishing-campaign-targets-nuclear-energy-industry/
(23) https://citalid.com/analyse-de-la-strategie-cyber-et-geopolitique-indienne/
(24) https://blog.talosintelligence.com/lazarus-three-rats/
(25) https://www.reuters.com/world/asia-pacific/exclusive-nkorea-grows-nuclear-missiles-programs-profits-cyberattacks-un-report-2022-02-05/
(26) https://www.marianne.net/monde/proche-orient/israel-iran-la-cyber-guerre-est-declaree
(27) https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor
(28) https://www.clearskysec.com/siamesekitten/
(29) https://learn.microsoft.com/en-us/windows/win32/secmgmt/installing-and-registering-a-password-filter-dll
(30) https://go.recordedfuture.com/hubfs/reports/cta-2022-0330.pdf
(31) https://citalid.com/analyse-de-la-strategie-cyber-iran/
(32) https://lerubicon.org/publication/la-strategie-de-cyber-influence-de-la-republique-islamique-diran/
(33) https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
(34) https://www.wired.com/story/russian-hackers-attack-ukraine/
(35) https://www.cisa.gov/news-events/alerts/2022/01/11/cisa-fbi-and-nsa-release-cybersecurity-advisory-russian-cyber-threats
(36) https://www.bbc.com/news/technology-60500618

Sources

(37) https://www.eset.com/int/industroyer/
(38) https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
(39) https://www.bleepingcomputer.com/news/security/sandworm-hackers-fail-to-take-down-ukrainian-energy-provider/
(40) https://www.kaspersky.fr/resource-center/threats/blackenergy
(41) https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool
(42) https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/
(43) https://www.cyberthreat.report/ransomboggs-ransomware-linked-to-russian-sandworm-apt-targeted-several-ukrainian-organizations/
(44) https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/
(45) https://www.senat.fr/rap/r22-334/r22-33410.html
(46) https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D1%91%D0%BC%D1%8B_%D0%BF%D1%80%D0%BE%D0%BF%D0%B0%D0%B3%D0%B0%D0%BD%D0%B4%D1%8B
(47) https://www.intelligenceonline.fr/grands-contrats/2022/10/25/moscou-fourbit-ses-armes-en-vue-d-une-guerre-energetique,109837343-eve
(48) https://www.bankinfosecurity.com/lithuanian-energy-firm-experiences-ddos-a-19555
(49) https://www.darkreading.com/attacks-breaches/pro-islam-anonymous-sudan-hacktivists-front-russia-killnet-operation
(50) https://www.lexpress.fr/societe/piratage-de-tv5-monde-la-plus-grosse-operation-de-cybercaliphate_1669568.html
(51) https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/en-ukraine-la-cyberguerre-a-bien-eu-lieu-mais-avec-des-effets-assez-limites-1-2-946720.html
(52) https://twitter.com/youranonnews/status/1514277626969575428?
(53) https://twitter.com/YourAnonTV/status/1516882645338234882
(54) https://twitter.com/YourAnonTV/status/1518525076286676993
(55) https://www.capital.fr/entreprises-marches/anonymous-pirate-des-entreprises-russes-du-secteur-de-lenergie-1434947
(56) https://twitter.com/YourAnonTV/status/1634669231303282688
(57) https://therecord.media/google-conti-repurposing-tools-for-ukraine-attacks-using-follina-bug-musk-impersonation
(58) https://www.welt.de/politik/deutschland/article237518665/Rosneft-Deutsche-Tochter-wurde-Ziel-eines-Cyberangriffs.html
(59) https://securityaffairs.com/129052/hacktivism/anonymous-hacked-german-subsidiary-rosneft.html
(60) https://www.i24news.tv/fr/actu/international/moyen-orient/1666464860-un-groupe-de-hackers-publie-des-documents-confidentiels-sur-le-programme-nucleaire-iranien

(Sources, pages 29 à 32)
L'énergie : un secteur d'activités vulnérable au cybercrime

(61) https://www.dragos.com/blog/ransomware-attack-analysis-q1-2023/
(62) https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/
(63) https://heimdalsecurity.com/blog/blackcat-ransomware-says-its-behind-the-attack-on-creos-luxembourg-s-a/
(64) https://www.computerweekly.com/news/252512876/BlackCat-crew-supposedly-behind-OilTanking-ransomware-heist
(65) https://www.lemondeinformatique.fr/actualites/lire-allemagne-un-ransomware-perturbe-la-distribution-de-petrole-85673.html
(66) https://intezer.com/blog/research/global-phishing-campaign-targets-energy-sector-and-its-suppliers/

yuno By XMCO

Le Panorama de la Menace Cyber 2022 sur le secteur de l'énergie a été réalisé dans le cadre de **yuno**, 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