ANOZR WAY
PEOPLE-CENTRIC CYBER PROTECTION

CYBERCONFLIT UKRAINE-RUSSIE

Désinformation & Influence

Étude ANOZR WAY

11 mars 2022

Version 1.2.1 16/03/22

SOMMAIRE

Avant-propos

Cette analyse du cyberconflit lié à la guerre en Ukraine repose sur des observations et des bases de connaissances historiques d'ANOZR WAY.

Cette étude n'a pas pour objectif d'être exhaustive mais d'apporter des analyses inédites afin d'améliorer la compréhension de la menace cyber actuelle.

Synthèse

L'invasion de l'Ukraine par la Russie le 24 février a rapidement laissé planer l'hypothèse d'une cyber guerre ouverte en plus du conflit sur le terrain. Des transformations du cyber-espace ont bien été provoquées, mais les multiples revendications des groupes de hackers brouillent la réalité de la menace cyber. **Nous assistons plus à des actions de désinformation et d'influences qu'à de réelles cyberattaques d'ampleur.**

Avant le 24 février, des cyber-attaques contre les infrastructures ou sites de ministères ukrainiens[1] ont été remarquées. Ces actions peuvent être interprétées soit comme une préparation de l'invasion planifiée ou comme des actions de déstabilisation du fait de la montée des tensions.

Quinze jours après le début du conflit, des premières conclusions peuvent être avancées :

En l'état actuel, il n'y a pas de guerre cyber à proprement parler, dans le sens où aucune cyberattaque de grande ampleur n'a encore été observée. **Aucun des deux belligérants n'a encore mis en place d'offensives cyber majeures et organisées** pour paralyser les centres d'importances vitales et de commandement.

On assiste principalement à un affrontement numérique de cyber-hacktivistes réalisant **principalement des attaques à faibles impacts.** Leur réel cheval de bataille est avant tout la **désinformation, en réutilisant à de nombreuses reprises d'anciennes données fuitées** afin de faire croire à de nouvelles attaques. Ces opérations psychologiques sont protéiformes et massivement utilisées par les deux camps.

La sphère cyber s'est polarisée autour du conflit, brouillant et coupant l'accès aux canaux de communication jusqu'alors privilégiés. **Une restructuration des lieux d'échanges et de contacts est en cours.**

Tout en réfutant la thèse d'une guerre cybernétique, il est nécessaire de continuer à veiller sur les différents évènements et à en interpréter prudemment les signaux faibles tels que :

- L'annonce de l'isolement russe d'Internet dans la continuité des tests déjà réalisés de juin à juillet 2021 ;
- Les menaces d'interventions russes plus massives sur les câbles sous-marins de liaison intercontinentale ;
- Les récents événements comme ceux de mardi 8 mars de perturbations sur de nombreux médias tels que Discord, Facebook, TikTok, Spotifiy, Instagram, Youtube etc.

Les capacités cyber-russes doivent pousser à la retenue, à l'observation et à l'anticipation d'une deuxième phase de conflit, plus dévastatrice contre les États déclarés comme hostiles à la Russie.

[1] Notamment par les groupes russes SandWorm aka Fancy Bear sur la période du 16 au 23 février et par Actinium/Gamaredon le 14 janvier.

1. Forces en présence : motivations et allégeances des hackers

Alors que des hackers choisissent leur camp entre l'Ukraine et la Russie, d'autres se gardent bien de prendre position et assument des motivations purement financières.

Ces attaquants sont classés selon les quatre catégories suivantes :

- **Les cyber-hacktivistes** qui agissent au nom d'une cause politique ou sociale. Ils appartiennent souvent à des groupes peu structurés, qui agissent seuls ou se réclament de groupes de type *Anonymous*, *Againstthewest/Blue Hornet*, *Cyber partisans* etc.
- **Les cyber-mafieux** qui ont des motivations principalement financières et qui agissent au sein de groupes structurés tels que les groupes de ransomwares historiques *CONTI, LockBit2.0, Stormous* etc.
- **Les cybers-mercenaires** qui sont des hackers plus ou moins organisés utilisés ou coordonnés par un État à un moment T, tel que *l'IT Army of Ukraine*
- **Les hackers d'Etat** qui dépendent directement d'agences de renseignement étatiques tels que *Fancy Bear, Actinium* ou encore *Ghostwriter*.

1.1. Les hackers d'Etat et cyber-mercenaires

Les hackers d'Etat impliqués sont russes ou biélorusses et ont effectué la plupart de leurs cyberattaques en Ukraine entre mi-janvier et mi-février, c'est-à-dire en amont de l'invasion des troupes russes le 24 février. Ces attaques ont ciblé principalement des administrations et des organismes à importance vitale avec des **objectifs de déstabilisation ou d'espionnage**. Ces actions peuvent être interprétées soit comme une préparation de l'invasion planifiée soit comme des actions de déstabilisation du fait de la montée des tensions.

Depuis le **24 février**, date de l'invasion en Ukraine de la Russie, aucune attaque vers ces cibles à haute valeur ajoutée ne semble avoir eu lieu. Attention cependant à certains signaux faibles qui doivent être surveillés. Rien n'exclut en effet une éventuelle seconde phase plus active.

Les cyber-mercenaires dans le conflit sont surtout représentés par *l'IT Army of Ukraine*, constituée en urgence au début de la guerre. Le lendemain de l'entrée en Ukraine de l'armée Russe, le président ukrainien Volodymyr Zelenski et son ministre en charge de la transformation digitale ont invité *via* Twitter les différents hackers ukrainiens à se mobiliser et à s'organiser pour défendre le pays. Ces professionnels de l'underground pourraient permettre de protéger les réseaux informatiques et d'apporter une éventuelle capacité de riposte sur certaines cibles stratégiques.

Pour rappel, l'Ukraine est dépourvue d'un commandement cyber offensif et défensif structuré, donc particulièrement vulnérable en cas d'intensification des attaques à son encontre.

Figure 1: Création de l'IT Army of Ukraine par le gouvernement ukrainien.
Source : Twitter, le 26 février 2022

Cependant leurs faits d'armes répertoriés semblent se limiter à des actions de désinformation et d'influence. Les attaques espérées mettant en péril les infrastructures russes n'ont pas eu lieu.

1.2. Les cyber- hacktivistes

Ces groupes constituent la majorité du « bruit » qui entretient l'illusion d'une « guerre cyber ».

De nombreux pirates isolés se sont ralliés au camp russe ou ukrainien en créant des groupes ou en ralliant des bannières de types *Anonymous*.

Le 25 février, le groupe d'hacktivistes *Anonymous* ouvre le bal et déclare la cyber guerre à la Russie en soutien au peuple ukrainien. En quelques jours, plus d'une cinquantaine de groupes se créent et s'engagent, la plupart utilisant Twitter ou Telegram comme canaux de communication.

Figure 2 Le groupe Anonymous pro-Ukrainien
Source : Twitter, le 24 février 2022

Figure 3 Le groupe Cobra pro-Russe
Source : Twitter, le 28 février 2022

Ces différents acteurs se présentent comme ayant la capacité de mener des attaques impactantes. Dans les faits, la plupart des attaques s'avèrent avoir un impact limité ou fausses (voir les exemples d'attaques analysées plus bas).

Ces groupes se révèlent cependant efficaces dans la guerre d'influence et de désinformation avec une propagande numérique massive.

Pour les groupes pro-russes, la propagande s'effectue autour de trois théories principales :

- La preuve irréfutable de la nazification de l'Ukraine.
- L'hypocrisie occidentale et ses politiques interventionnistes.
- La menace que représente l'OTAN pour le glacis de sécurité russe.

Figure 4: Désinformation du groupe pro-Russe cobra
Source : Twitter

Figure 5: Dénonciation de l'hypocrisie occidentale
Source : Twitter, le 24 février 2022

Pour les groupes pro-ukrainiens, la guerre de l'information met en avant :

- L'enlisement des troupes russes du fait de la résistance ukrainienne.
- La bienveillance des Ukrainiens à l'égard des soldats russes.
- La diabolisation et la solitude du personnage de Vladimir Poutine.

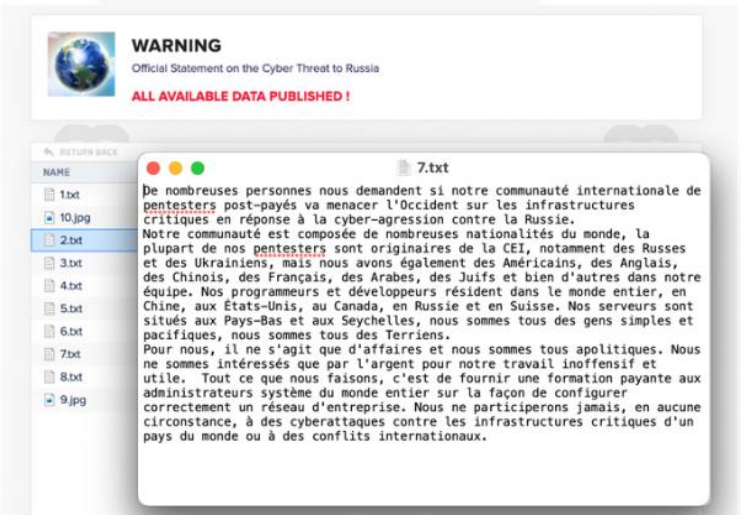
Figure 6: La solitude du président Poutine
Source : Twitter le 1er mars 2022

Figure 7: La bienveillance des Ukrainiens
Source : Twitter le 2 mars 202

1.3. Les cyber-mafias

Ces groupes plus durablement installés dans le paysage de la cybercriminalité financière ont été peu impactés et se sont plus faiblement mobilisés. **Sur la trentaine de groupes actifs, seule une poignée ont communiqué sur le sujet.**

Cela s'explique par la diversité des membres constituant ces groupes. Une prise de position pourrait faire éclater l'unité et entacher leur activité économique. Pour rappel, les groupes de ransomware, s'ils peuvent s'allier à des Etats par opportunisme, ont des motivations encore principalement pécuniaires. C'est ce qu'explique *LockBit 2.0*, le groupe de ransomware le plus actif de 2021 et de 2022 dans un message publié sur son site le 27 février :



Cette absence de bouleversement dans le monde du ransomware peut également s'expliquer par le **temps nécessaire à la mise en place d'une attaque**, plus difficilement compatible avec le temps de guerre. Tout en étant plus impactantes, ces attaques s'inscrivent sur du moyen-terme du fait des phases d'analyse de l'environnement de la victime et d'identification de vulnérabilités. Le résultat de ces attaques n'est peut-être pas encore visible.

Deux groupes seulement ont officiellement pris parti et ce à des degrés très différents : le groupe ransomware *Conti* et le groupe ransomware *Stormous*.

Le groupe *Conti* est le premier à communiquer sur le sujet le 25 février en annonçant son soutien au gouvernement russe. **Deux jours plus tard, des données internes du groupe sont fuitées par un affidé[2] ce qui le contraint à faire marche arrière.** Dès lors, le groupe privilégie une attitude passive et ne semble pas avoir mené d'attaques spécifiquement en lien avec le conflit.

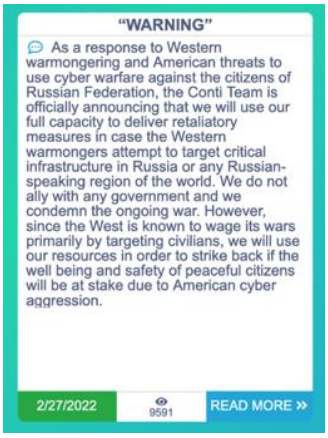


Figure 8 : message de Conti le 27 février
Source : site de Conti sur le darkweb

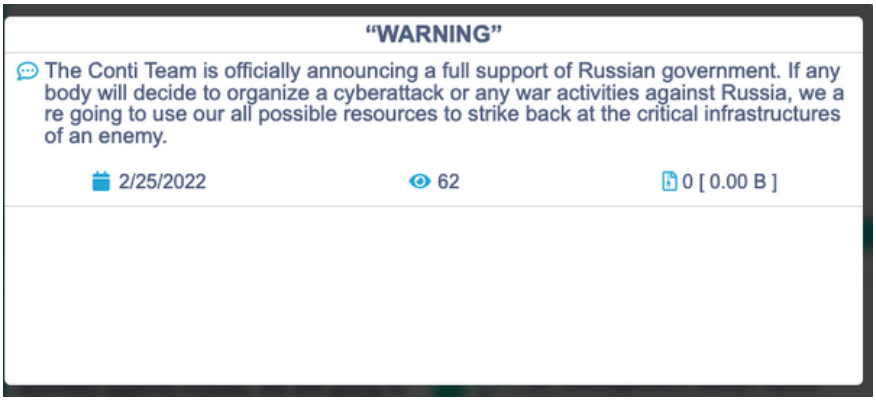


Figure 9 : message de Conti le 25 février
Source : site de Conti sur le darkweb

Cette déconvenue n'a cependant pas impacté son activité économique puisque le nombre d'attaques à son actif a bondi ces derniers jours. **Plus de 36 attaques ont été revendiquées depuis le début de la guerre contre seulement une dizaine au mois de janvier.** Deux explications peuvent être avancées :

- le groupe, attaqué en son sein, a démultiplié ses attaques pour démontrer qu'il n'a pas été affaibli par les différentes publications ;
- ces attaques datent d'avant-guerre et sont publiées par le groupe rapidement face à la crainte d'un éventuel démantèlement par les autorités.

[2] Affidé ou affilié : utilisateur d'un ransomware-as-a-service créé par un groupe de hackers

Le second groupe est **Stormous Ransomware** qui est lui beaucoup plus actif depuis le début de la guerre. Sur son fil Telegram, il est particulièrement véhément à l'encontre de l'Ouest et de l'Ukraine et mène une campagne d'attaques qui se veulent liées au conflit.

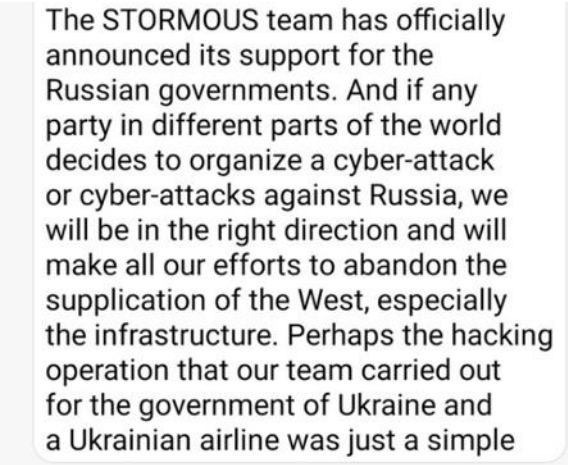


Figure 10: message du ransomware Stormous
Source : fil Telegram du groupe Stormous

Globalement, depuis le début du conflit en Ukraine le nombre de franchises de ransomware a réduit de 30%.

Cette diminution peut résulter :

- des interpellations conduites sur le sol ukrainien au cours de l'automne 2021 *(Europol & Interpol)* ;
- du conflit sur le territoire ukrainien tenant éloigné les pirates du pays des activités de rançonnage ;
- du repli d'affidés des groupes inactifs vers d'autres franchises ;
- du transfert des activités des hackers ukrainiens vers d'autres activités servant le conflit armé *(déstabilisation, sabotage, communication, propagande, piratage d'organisations étatiques russes, etc.)*.
- Du transfert des activités de hackers russes vers d'autres activités de soutien du régime (*déstabilisation, sabotage, propagande, piratage d'organisations étatiques ukrainiennes, etc.)*.

En tout état de cause, le phénomène ransomware ne faiblit pas à la faveur de la guerre en Ukraine:

- 164 faits répertoriés en janvier 2022 ;
- 247 faits répertoriés en février 2022 ;
- 49 faits répertoriés depuis début mars 2022 *(9 jours)*.

Quelques groupes, présentés comme opérateurs de ransomware apparaissent plus comme des groupes de hackers n'ayant pas recours au procédé habituel *(chiffrement puis*

extorsion). C'est le cas notamment de Lapsus$ *(apparu en janvier 2022)*, de Karakurt *(apparu en février 2022)*, ou encore de l'un des derniers arrivés : CRYP70N1C0D7 *(publication d'une liste de 11 leaks disponibles contre paiement)*.

Certains de ces derniers groupes peuvent utiliser une charge de type ransomware et préfèrent demander en contrepartie la libération de partisans, ou d'autres demandes idéologiques, plutôt que de l'argent.

2. Des opérations de désinformation & d'influence plus que des cyberattaques

2.1. Le front cyber : des attaques nombreuses mais peu efficaces

A en croire la quantité d'attaques revendiquées sur Twitter et sur Telegram, les premiers jours de guerre ont été marqués par des opérations cybers massives à l'encontre d'entités Russes. Des groupes comme *Against The West* et *Anonymous* annoncent les attaques de grandes administrations comme le Kremlin **le 27 février**, la ville de Saint Petersburg **le 28 février** ou encore le ministère du développement économique **le 1er mars**.

Rapidement, le nombre d'attaques présumées dépasse le millier.

Ce qui se joue dans le cyberespace est d'abord difficilement évaluable, tant en nombre qu'en qualité d'attaques. L'emballement médiatique général et sur tous les fronts, brouille volontairement l'identification des réels faits d'armes cybers.

Le recul révèle finalement une guerre d'information moderne car numérique plutôt qu'un conflit cyber.

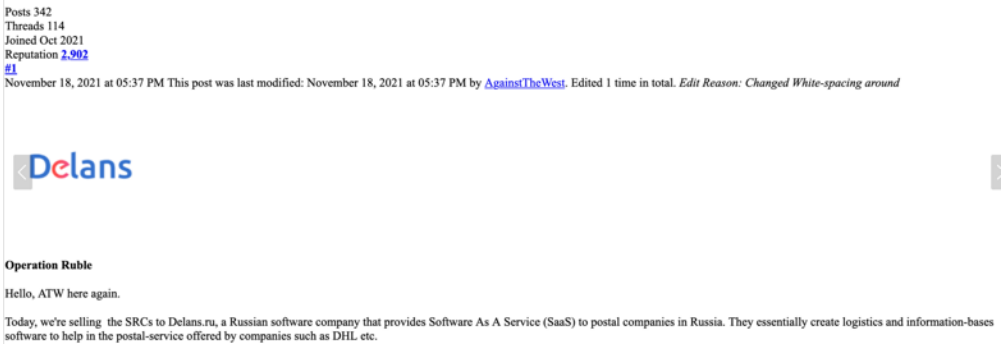
La plupart des attaques ont des impacts réels négligeables. Elles sont très souvent des DDoS de faible intensité, des défacements de sites et de médias russes ou des récupérations de codes sources de sites Internet sans récupération de données sensibles. L'*IT Army of Ukraine* suit la même ligne de conduite : face à son incapacité à se structurer dans l'urgence autour de charges virales agressives, elle encourage ses mercenaires à mener des attaques désordonnées en fournissant une liste de sites russes.

Plutôt que la qualité des attaques, c'est donc leur nombre qui est mis en avant. Les hackers publient de longues listes de victimes pour créer artificiellement des écrans de fumée. En temps de guerre, ces opérations psychologiques permettent de démoraliser l'adversaire et de nourrir l'enthousiasme des alliés.

2.2. Etude de cas : l'utilisation massive de la désinformation

Afin de gonfler artificiellement les chiffres, les deux camps réutilisent des anciennes attaques ou les créent de toutes pièces.

Le 4 mars 2022, le groupe d'hacktivistes *Against The West* (ATW) revendique l'attaque de l'entreprise russe Delans. La veille sur les données a permis à ANOZR WAY de révéler que celle-ci date en réalité de **novembre 2021**. Le groupe en vendait les données sur Raidforums. [3]



Posts 342
Threads 114
Joined Oct 2021
Reputation 2,902
#1
November 18, 2021 at 05:37 PM This post was last modified: November 18, 2021 at 05:37 PM by AgainstTheWest. Edited 1 time in total. *Edit Reason: Changed White-spacing around*

Delans

Operation Ruble

Hello, ATW here again.

Today, we're selling the SRCs to Delans.ru, a Russian software company that provides Software As A Service (SaaS) to postal companies in Russia. They essentially create logistics and information-bases software to help in the postal-service offered by companies such as DHL etc.

Figure 11: Publication par le groupe ATW sur Raidforums (page en cache)
Source : Raidforums le 18 novembre 2021

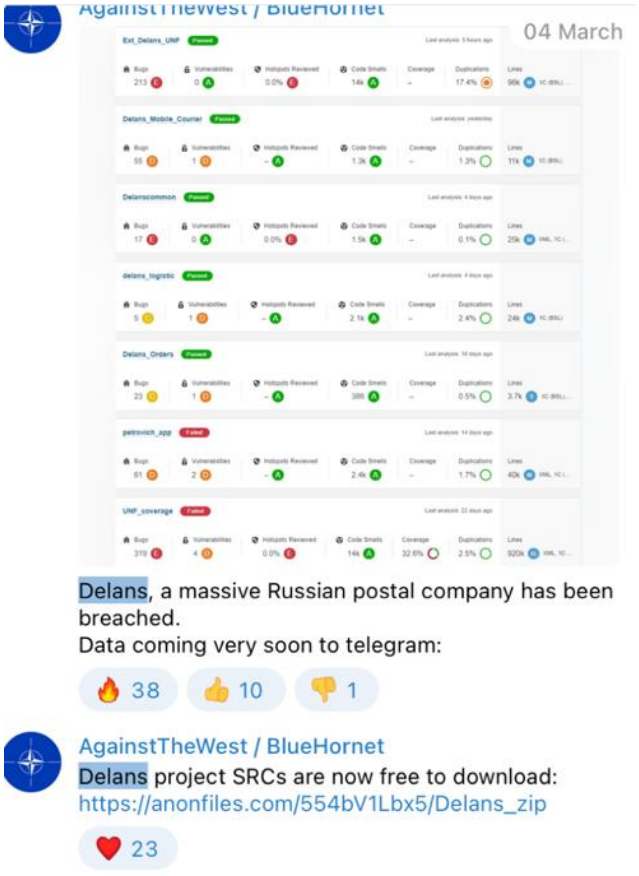


Figure 12: Publication par Against the West
Source : Telegram le 4 mars 2022

[3] Raidforums : forum central d'échange entre hackers

Début mars, *Anonymous* revendique l'attaque du réseau Yandex[4]. Les données publiées correspondent à des emails déjà fuités par le passé. Le groupe aurait récupéré les informations pour en faire un conglomérat et les publier comme preuve d'une nouvelle attaque.

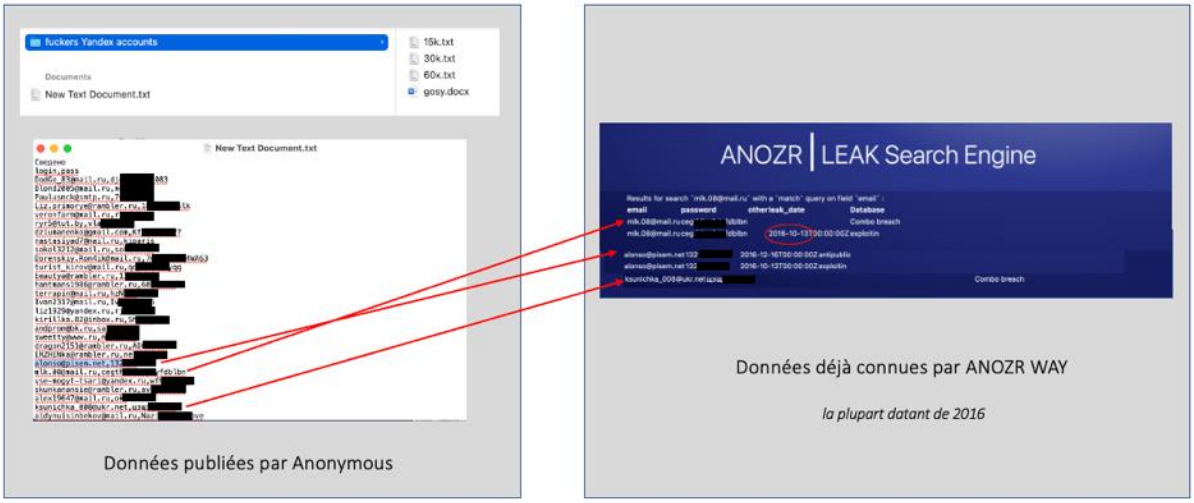


Figure 13: Soi-disante attaque d'Anonymous contre Yandex

Cette désinformation se fait cependant parfois de manière plus insidieuse et révèle un réel potentiel de nuisance.

Le 28 février, le groupe de ransomware Stormous pro-russe revendique l'attaque d'Ivchenko Progress, une entreprise aéronautique d'Etat en Ukraine. Le groupe poste plusieurs captures d'écran sur son fil Telegram pour apporter la preuve du vol de données. **Les informations sont en fait celles d'une entreprise française ciblée l'année dernière par le groupe de ransomware Grief et qui ont été réinjectées dans un montage.**

Cette observation vient nourrir la propagande russe : compromettre des entreprises occidentales pour montrer qu'Etats-uniens et Européens manigancent contre la sécurité de la Russie.

Cet épisode vient confirmer la nécessité de mener une veille active des fuites de données françaises pour identifier ces trucages et accusations infondées.

[4] Yandex est le plus important et le plus utilisé des moteurs de recherches sur le réseau web russophone

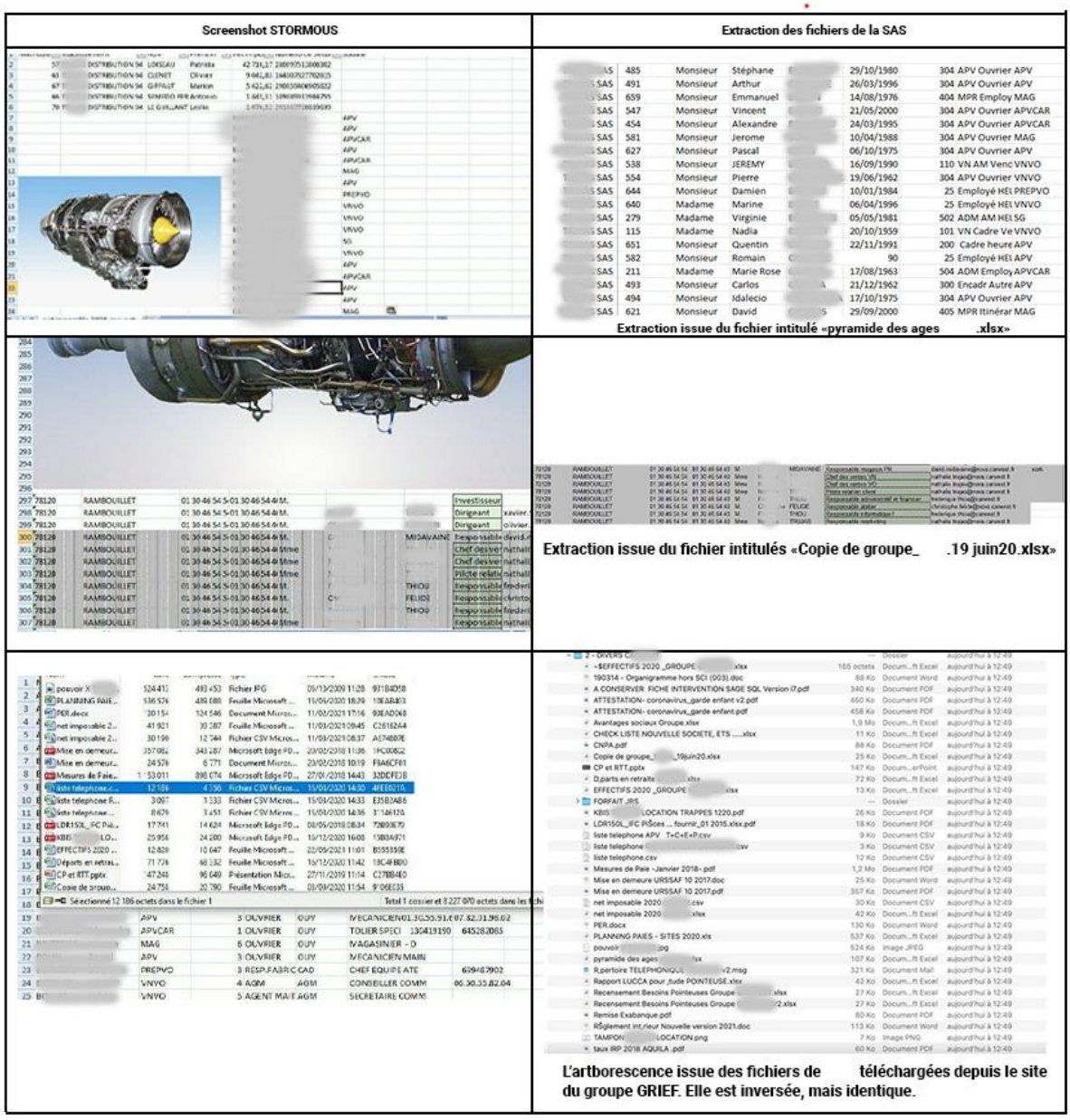


Figure 14 : Publication de Stormous où l'on peut apercevoir des fichiers français A gauche la soi-disante nouvelle attaque effectuée par Stormous Ransomware, à droite le fichier original de 2021 suite au Ransomware Grief

3. L'éclatement des canaux de communication des hackers

Le conflit en Ukraine a entrainé une polarisation extrême de la communauté cyber avec des tensions et des ruptures brutales au sein de certains canaux de communication.

3.1. La fermeture de Raidforums

Le 27 février, le premier site de revente et de partage de données Raidforums prend position en faveur de l'Ukraine. Quelques heures plus tard, le site n'est plus accessible.

Début mars, un message annonce qu'il a été saisi par le FBI.

Actions simultanées ou simple coïncidence, sa fermeture entraine une désorganisation au sein de la communauté du Dark et du Deep Web qui cherche des canaux de communication alternatifs.

Face à la recrudescence des demandes d'inscription, d'autres forums comme le russe XSS ferment leurs accès aux nouveaux arrivants.

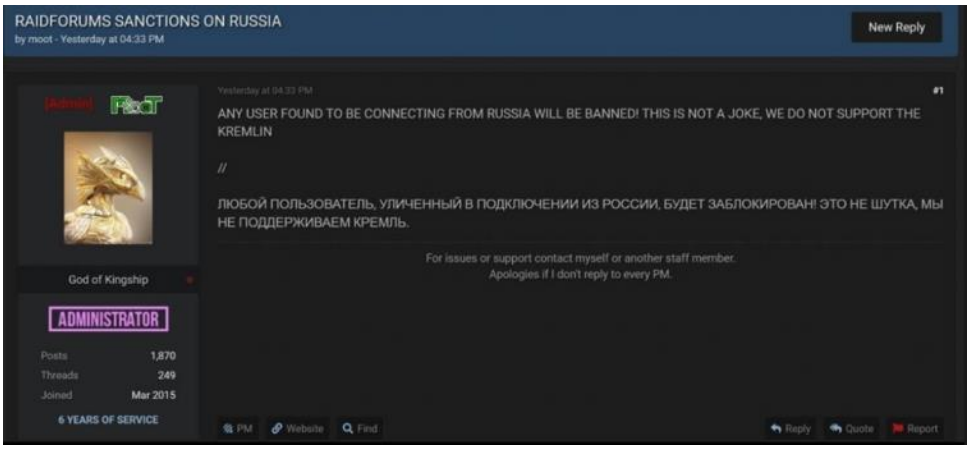


Figure 15: mise en garde par un administrateur de Raidforums le 27 février, juste avant qu'il devienne inaccessible
Source : Raidforums le 27 février

3.2. Twitter et Telegram : les nouveaux canaux

Un regroupement s'effectue autour des réseaux sociaux libres d'accès pour reconstituer les groupes de discussions et de partages instantanés. La plupart des utilisateurs actifs de Raidforums se retrouvent sur Twitter et Telegram où ils tentent de reformer leurs réseaux.

La discussion instantanée de Telegram permet aux différents hackers de publier leurs vols de données ou de communiquer sur leurs attaques. **Cette migration vers Telegram avait déjà été entamée il y a plusieurs mois, mais le conflit a vu une explosion de son utilisation par les groupes d'attaquants.**

Face au déferlement de propagande pro-russe ou pro-ukrainienne, ces deux réseaux sociaux se voient dans l'obligation de fermer certains comptes, aussitôt recréés.

Le 9 mars, Twitter annonce sa prochaine disponibilité sur le Deep et le Dark via Tor[5]. Cette alternative peut être intéressante pour les Russes qui se voient radiés de nombreux canaux de communication occidentaux.

Cette multiplication des sources d'information complexifie la veille et l'analyse de l'état actuel de la menace.

4. Des signaux faibles qui appellent à la vigilance

Si la guerre est encore loin d'être cyber et reste pour le moment une guerre de l'information, certains signaux faibles doivent cependant être attentivement surveillés.

4.1. Une possible déconnexion russe de l'Internet mondial

Le premier signal faible est les manœuvres de la Russie pour déconnecter son réseau de l'Internet mondial à l'horizon annoncé du 11 mars - non suivi d'effet au moment où nous écrivons ces lignes – comme entrepris lors d'un exercice grandeur nature entre juin et juillet 2021. Cela lui permettrait de se protéger plus efficacement contre des cyberattaques de grandes ampleurs et de maitriser encore plus facilement l'information qui circule sur les réseaux.

Si la Russie anticipe des attaques massives dans le cyberespace, c'est peut-être parce qu'elle se prépare elle-même à en provoquer. Les perturbations du 8 mars derniers sur des géants comme Discord, Spotify, YouTube, Google, Amazon etc. ne doivent donc pas être sous-estimées.

4.2. La problématique des câbles sous-marins

Le second est la menace de la coupure des câbles sous-marins qui relient l'Europe à Internet. La Russie sait en effet que les pays européens, s'ils ont massivement investi dans la cybersécurité pour protéger leurs Opérateurs d'Importance Vitale (OIV), ont tout autant négligé la protection des infrastructures physiques dont leur Internet dépend. Une coupure massive des câbles provoquerait une perturbation importante des communications et de l'Internet occidental.

Si cette pratique est courante en temps de guerre et ce depuis le XIX^{e} siècle, les conséquences aujourd'hui seraient démultipliées par l'indépendance de nos sociétés aux technologies de l'information et de la communication.

[5] euronews.com. 2022. Twitter launch new 'onion' version to bypass Russian censorship. [en ligne] Disponible à : https://www.euronews.com/my-europe/2022/03/10/twitter-launch-new-onion-version-to-bypass-russian-censorship [Consulté le 10 mars 2022].

4.3. Vers un durcissement du cyberconflit ?

Même si cette première phase semble être limitée à de la désinformation et cible les principaux protagonistes (Ukraine, Russie, Biélorussie), une deuxième phase pourrait avoir lieu une fois le territoire et les infrastructures ukrainiennes mieux maîtrisés par la Russie.

Les groupes liés à la Russie pourraient alors rediriger leurs attaques contre les pays déclarés hostiles par Vladimir Poutine. La France pourrait alors se retrouver plus ciblée par des attaques liées à l'Etat russe.

Il convient de rappeler qu'en 2021, la France était le premier pays de l'Union européenne dans le TOP 3[6] des pays les plus attaqués par les groupes de ransomwares principalement hébergés en Russie.

La France est déjà une cible de choix pour les cyberattaques et pourrait le devenir encore plus par des actions russes de plus grande ampleur et plus impactantes au fur et à mesure de l'avancée dans le conflit.

La mise à mal d'Internet par la Russie semblant capable de vivre en quasi autonomie[7] sur son Runet[8], impacterait fortement l'économie occidentale et serait une revanche contre les sanctions économiques.

[6] Baromètre ANOZR WAY du Ransomware - Bilan annuel 2021 & Perspectives 2022, janvier 2022. https://anozrway.com/fr/barometre-ransomware/

[7] La Russie avait déjà annoncé pouvoir se couper de l'Internet mondial en 2021. Cependant, elle semble rencontrer des problèmes de certificat TLS en étant coupé des autorités de certification tierces. Cela permet de s'interroger sur la possibilité réelle de couper son Runet du monde.

[8] Runet : communauté russophone sur Internet et les sites Web. Runet n'est pas complètement synonyme de l'Internet en Russie ni des sites Internet en russe, pas même avec l'ensemble des sites dans le TLD.ru, mais se réfère plus précisément à la sphère des sites Internet principalement visités par les utilisateurs russophones, qui font partie de la culture russe contemporaine.

A propos

ANOZR WAY est une startup française spécialisée dans l'analyse des données exposées sur le web, darkweb et la protection des personnes face aux risques cyber. Fondée à Rennes en 2019 par Alban ONDREJECK, ancien officier des services de renseignement français, et Philippe LUC, ancien dirigeant dans le secteur de l'assurance. ANOZR WAY a développé une technologie propriétaire innovante multi-récompensée à base d'Intelligence Artificielle et « Data Science ». Les solutions logicielles ANOZR WAY permettent aux dirigeants d'entreprise et à leurs collaborateurs d'être protégés face à des menaces d'ingénierie sociale, d'usurpation d'identité, d'espionnage, de ransomware, de vol de données etc.

Avec une première levée de 2M€ en 2021, BPI, Breizh Up et BNP Développement sont au capital. ANOZR WAY est en phase d'accélération avec une croissance de +271% et compte 30 collaborateurs.

Site web : https://www.anozrway.com/

LinkedIn : linkedin.com/company/anozrway/

Twitter : twitter.com/anozrway