Ransomware : de REvil à Black Basta, que sait-on de Tramp ?

lemagit.fr/actualites/366619807/Ransomware-de-REvil-a-Black-Basta-que-sait-on-de-Tramp

Septembre 2020. Un affidé de l'enseigne de rançongiciel REvil nous fait des révélations sur une cyberattaque qu'il a conduite quelques mois plus tôt contre le Français Elior. À ce moment-là, le ransomware est une menace déjà prégnante, mais loin de l'ampleur qu'elle s'apprête à prendre. C'est l'époque à laquelle nous commençons toutefois à en suivre mensuellement l'évolution.

Certains acteurs majeurs de cette menace actifs aujourd'hui l'étaient déjà à cette date. Le récit qui suit apporte un éclairage inédit sur la manière dont ils sont susceptibles de profiter de leurs gains, ainsi que du niveau de protection dont ils peuvent se faire valoir – à juste titre ou pas – pour échapper à la Justice.

Erevan, juin 2024

Le vendredi 21 juin 2024, sur l'American Street, à Erevan, l'aventure est sur le point de prendre un tournant inattendu pour celui qui apparaît être l'un d'entre eux.

Oleg Nefedov est arrêté par la police locale, à 11h du matin, sur cette rue de la capitale arménienne qui mène à l'ambassade des États-Unis, longeant la rivière Hrazdan.

Le lendemain, à 13h30, le procureur demande son placement en détention provisoire. Entre-temps, l'Arménie a obtenu et fait traduire les documents nécessaires à son extradition. Il ferait l'objet d'une notice rouge d'Interpol – non publique.

L'audience est prévue pour le lundi 24 juin 2024 à 10h du matin. Suffisant, en théorie. Le média arménien 168.am, qui a rapporté les faits, explique que la décision de placement en détention provisoire doit intervenir dans les 72h après l'interpellation, soit avant 11h du

matin, le 24 juin. Mais le délai est dépassé, pour des raisons non précisées. À 16h, Oleg Nefedov est remis en liberté. Le bureau du procureur général confirme les faits dans un communiqué du 20 septembre.

La nouvelle est passée inaperçue, ou presque. Le 16 décembre 2024, une source contacte LeMagIT. Elle est affirmative : celui qui utilise notamment le pseudonyme de *tramp* – un ancien de feu Conti et comptant parmi les leaders du gang de rançongiciels Black Basta – serait cet Oleg Nefedov qui a été arrêté à Erevan, à la fin du mois de juin précédent : « je connais aussi Tramp sous le nom d'Oleg Y. Nefedov », assure-t-il, ajoutant qu'il travaillait avec lui.

« Il a la meilleure protection [qui soit] en Russie. Il a des amis dans les services de sécurité. Il paie même le FSB et le GRU », nous dit cette source. Il s'agit des services du renseignement russe. « Personne n'a plus désormais ce genre d'argent ou ce niveau de sûreté », ajoute cette source.

C'est effectivement ce qu'affirme Tramp, aussi connu sous les pseudonymes de AA et GG, notamment, à l'un de ses partenaires, *dd*, le 14 novembre 2022 : « j'ai des gars de Loubianka [siège du FSB à Moscou, N.D.L.R.] et du GRU, je les alimente depuis longtemps », peut-on lire dans un journal d'échanges privés vraisemblablement survenus sur la messagerie chiffrée Tox. Ces échanges nous ont été fournis le 30 décembre 2024, ainsi qu'à nos confrères du *Spiegel* (voir encadré).

```
2022-11-14  14:15:15    AA  у менять есть с лубянки и гру ребята , кормлю давно их
2022-11-14  14:15:40    AA  они возьмут только на работу к себе
2022-11-14  14:15:49    AA  о сроках и тд речи даже идти не будет
2022-11-14  14:16:17    AA  просто будешь ходить как на белую работу каждый денб к 8 утра
и уходить в 18
2022-11-14  14:20:18    dd  это лучше
2022-11-14  14:20:22    dd  чем там быть
2022-11-14  14:20:26    dd  однозначно
```

Tramp se vante de contacts avec le FSB et le GRU.

Mais Tramp est-il véritablement Oleg ? D'autres sources nous l'ont affirmé, sous couvert d'anonymat, ainsi qu'à nos confrères. De nombreux éléments confortent ces assertions.

Tramp interpelé

L'analyse de l'activité associée au pseudonyme GG dans les échanges survenus sur l'instance Matrix de Black Basta est troublante : elle fait ressortir une absence totale d'activité du 21 juin 2024 au 2 juillet inclus.

Quand Tramp revient en ligne le 3 juillet, il dit avoir un nouvel ordinateur et changer de compte Telegram. Il explique avoir perdu son précédent ordinateur, « et pas uniquement. C'est une longue histoire », dit-il : « ça a été difficile dans la vraie vie. Je ne sais pas où commencer… ».

Mais, comme nous l'a pointé le chercheur et spécialiste du renseignement humain *liontamer*, Tramp se confie à un membre du gang, *chuck*, qu'il semble connaître depuis « tant d'années », quelques heures plus tard : « les flics m'ont pris ». Il fait état d'une récompense pour des « informations sur TR [potentiellement Trickbot, mais le pseudonyme Tramp a aussi été ouvertement désigné par la justice américaine, N.D.L.R.] : 10 millions ». Plus loin, il indique avoir vu son dossier, « mais ils ne m'ont pas tout montré ». Il devait être extradé.


```
    {
        "timestamp": "2024-07-03 15:50:06",
        "chat_id": "!FJNepzdTumLjULNYKA:matrix.bestflowers247.online",
        "sender_alias": "@usernamegg:matrix.bestflowers247.online",
        "message": "Remember I told you I have friends at a very high level, this is the
level of our first."
    },
    {
        "timestamp": "2024-07-03 15:50:12",
        "chat_id": "!FJNepzdTumLjULNYKA:matrix.bestflowers247.online",
        "sender_alias": "@usernamegg:matrix.bestflowers247.online",
        "message": "I just had time to call him."
    },
```


Tramp dit avoir fait appel à des soutiens haut placés pour échapper à l'extradition vers les États-Unis.

Le même jour, *chuck*, dit vouloir prendre des vacances : « ne va nulle part. Reste à la maison », lui conseille Tramp. *Chuck* dit avoir pris des billets pour Kaliningrad. Tramp insiste : « nous devons protéger tout le monde maintenant ». *Chuck* finira par renoncer à ses projets : « j'annule ; j'irai en Carélie ». Tramp explique avoir vu tous les pseudonymes des membres de Black Basta dans le dossier qui lui a été présenté.

Il dit avoir profité de protections très haut placées, « au niveau de notre numéro 1 » : « j'ai réussi à appeler. J'ai juste demandé un laissez-passer. Ils ont immédiatement décollé pour moi ».

Des relations très haut placées

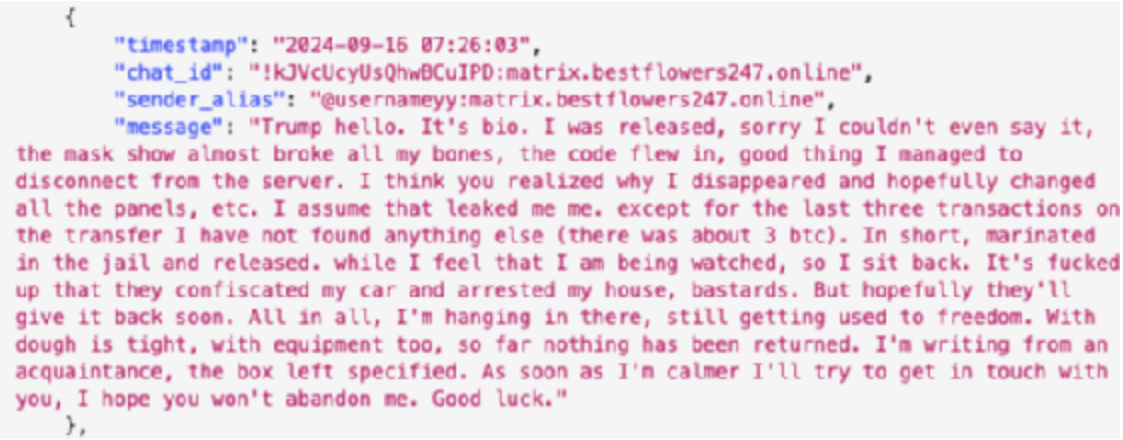
Des précisions ? « Je ne peux rien dire sur la façon dont on m'a sorti et qui a aidé. Mais on m'a dit que le numéro 1 me connaît et que, sans son accord, ils n'auraient rien fait », assure Tramp. *Chuck* demandera dans la foulée : « Poutine, c'est ça ? ». Tramp n'en dira pas plus.

Le bâtiment dit Loubianka, siège du FSB à Moscou.

Le 7 juillet, il devient toutefois plus bavard, indiquant que son téléphone a été saisi. Pour lui, un « ils » non précisé dispose d'un « accès total à Apple. Ils sont branchés sur toute la planète. Ils savent tout ». Du coup, « foutu pour foutu, Apple, c'est mort. […] Il faut tout nettoyer là-bas ».

Mais *chuck* est inquiet : quelqu'un lui a dit qu'il est recherché par les forces de l'ordre américaines. Une personne qu'il paie chaque mois pour le protéger au cas où le FSB viendrait le chercher. Il craint que les services russes ne « commencent à [les] extorquer ou [les] forcent à travailler pour eux, en échange de protection ». Il n'a peut-être pas tort.

Car le 16 septembre 2024, *YY* interpelle Tramp. Il révèle au passage un pseudonyme sous lequel il est connu pour ses activités avec feu Conti : « salut Tramp, c'est *bio*. On m'a relâché, désolé de ne pas avoir pu prévenir. Le raid des masqués a failli me briser tous les os quand ils ont débarqué, heureusement, j'ai eu le temps de me déconnecter du serveur ».



Bio, un ex-Conti, évoque ses démêlés avec les forces de l'ordre avec Tramp.

Selon lui, c'est un *exchange* de cryptomonnaies qui l'a trahi : « ils n'ont rien trouvé d'autre que mes trois dernières transactions (environ 3 btc). Bref, ils m'ont fait mariner en détention provisoire, puis m'ont relâché. Pour l'instant, je sens qu'on me surveille donc je me fais discret. C'est la merde qu'ils aient confisqué la bagnole et saisi la maison […], mais j'espère les récupérer bientôt ».

Bio demandera ensuite plusieurs paiements de quelques centaines de dollars à Tramp. Le 10 novembre 2024, il consolidera 20 bitcoins chez Kraken.

Un train de vie somptueux

Oleg fêtera prochainement ses 35 ans. Il est originaire de Iochkar-Ola, une ville de plus de 260 000 habitants située à 850 km à l'est de Moscou et à 60 km de la Volga, capitale de la république des Maris.

Ioshcar-Ola, capitale de la république des Maris.

Il semble avoir depuis longtemps un intérêt prononcé pour les cryptomonnaies. Un compte sur btc-e.com lui a été associé. Ce service de change a été victime d'une brèche de données en 2014.

En 2017, il travaille chez Bitsoft, qui se présentait alors comme « la plus grande entreprise russe dans le domaine du cloud-mining d'Ethereum, de Litecoin, et de Zcash ». Il en enregistre plusieurs noms de domaine, dont un en juillet 2017. Nous les avons retrouvés à partir de données Whois historiques et d'un numéro de téléphone. L'adresse ? À Iochkar-Ola.

À partir de ces données, nous avons également trouvé un numéro de téléphone qui fut, un temps, directement lié au nom de « Mr Tramp » dans TrueCaller, mais aussi référencé ailleurs sous celui d'Oleg Nefedov, ainsi que l'adresse associée à son compte Apple iCloud.

Oleg déclare des revenus de Bitsoft jusqu'en 2021. Sur la période, ces revenus ne sont guère impressionnants : 60 000 roubles en 2017 et 2018, soit environ… 900 euros par an. C'est un peu mieux en 2019, avec plus de 261 000 roubles, soit de l'ordre de 3 600 euros au taux de change moyen cette année-là. Après cela, il recevra des revenus de Polis, une entreprise liquidée fin 2023. Bitsoft connaîtra le même sort en août 2024.

Mercedes-Benz G 63 AMG, un SUV à plus de 80 000 €.

Cela ne l'empêche pas de rouler en BMW X6 M50D en 2019. En 2021, il est pris en excès de vitesse au volant d'une Mercedes AMG S63 4MATIC – à plus de 60 km/h au-dessus de la limite. Il a également roulé en Porsche Macan.

Début 2024, il fait remplacer les papiers de son van Mercedes classe V. À cette date, il dispose également d'une Mercedes GLE 400 D 4MATIC. Quelques mois plus tôt, il faisait changer l'adresse pour son SUV classe G AMG G63.

Depuis au moins 2022, Oleg investit notamment dans des bars lounges haut de gamme, sous une marque dont il détient une part de propriété intellectuelle. L'enseigne est présente dans le monde entier, jusqu'à Dubaï et Abu Dhabi en passant par Baku, Moscou, voire encore Bali. Fin août 2024, il fonde une organisation caritative du nom de Rodina – mère-patrie, en Russe.

Tramp, golden boy du ransomware

Selon nos analyses, Tramp dispose d'au moins 20 bitcoins de côté et en contrôlait au moins 2 000 en janvier 2023. Une demi-surprise. À l'automne 2021, LeMagIT avait suivi les millions de dollars de paiements de rançons obtenus par Conti au cours des mois précédents. En novembre 2023, Elliptic et Corvus Insurance estimaient que Black Basta n'avait pas fait moins bien, encaissant plus de 100 millions de dollars de rançons en près de deux ans d'activité.

En France, Black Basta s'est notamment attaqué à Oralia en avril 2022, puis H-Tube, l'étude Villa Florek, Envea, Dupont Restauration, et Baccarat. Au total, plus de 520 victimes de Black Basta sont publiquement connues, contre plus de 350 pour Conti.

Dans les échanges qui nous ont été fournis fin décembre dernier, des paiements en bitcoins sont demandés à Tramp par deux fois. Au moins l'un des paiements est bien provenu d'une adresse connue pour être contrôlée par lui.

Mais Tramp, qui est aussi connu sous le pseudonyme « p1ja », n'est pas arrivé dans le monde du ransomware avec l'apparition de Conti, cette PME de la cyberextorsion qui a volé en éclats en 2022, peu après l'invasion de l'Ukraine par la Russie.

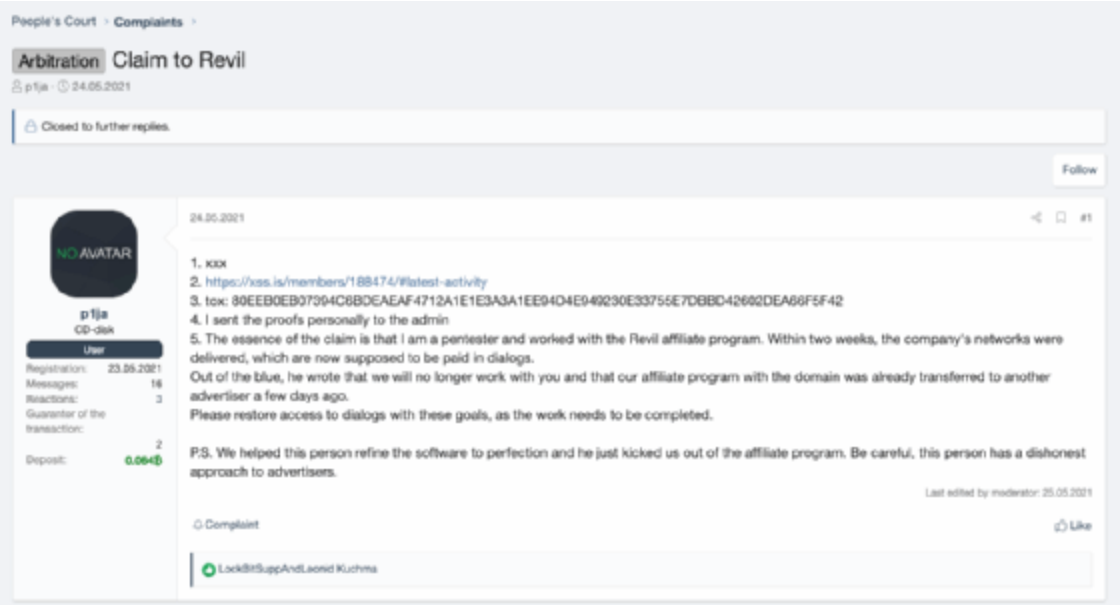
Selon nos informations, il est en effet impliqué dans de telles activités depuis bien plus longtemps. Dans les extraits de discussions privées entre Tramp et *ssd*, on trouve, en novembre 2022, la référence à un nom de système Windows : WIN-7PV24JSN83C.

Nos confrères de *Red Hot Cyber* avaient relevé ce nom de machine en août 2022. Nous l'avons-nous-mêmes observé pour 28 victimes revendiquées sous l'enseigne LockBit – 2.0 et 3.0 – tout au long de cette même année. Correspondant vraisemblablement à une machine virtuelle hébergée, ce nom n'étant pas très répandu à l'époque : en août 2022, le moteur de recherche spécialisé Shodan en avait compté environ 200 occurrences, dont plus de 190 sur des adresses IP géolocalisées en Russie.

Un conflit avec REvil

Ce n'est pas tout. Que ce soit dans les échanges divulgués en ce mois de février 2025 ou dans ceux qui nous ont été transmis fin décembre 2024, Tramp apparaît utiliser très régulièrement le mot de passe 123123 pour protéger des fichiers relativement peu sensibles ou très temporairement disponibles. Et c'est, à très peu de choses près, le seul.

Nous avons observé ce comportement dans deux négociations sous la bannière de REvil début 2021, puis deux autres sous la marque de Conti quelques mois plus tard. Avant cela, le code source de Crysis 3 divulgué par Egregor en 2020 l'avait été dans une archive protégée par le même mot de passe.



Quand Tramp travaillait avec REvil.

En mai 2021, *p1ja* demandera, sur l'un des forums bien connus pour être notamment fréquentés par les cybercriminels, un arbitrage pour conflit avec un autre utilisateur : « je suis *pentester* et j'ai travaillé avec le programme d'affiliation de REvil ». Ses accès à l'interface de négociation avec ses victimes venaient de lui avoir été retirés.

Sur ce même forum, Tramp a également été actif sous le pseudonyme « washingt0n32 ». Il s'y était inscrit ainsi en août 2020. Il revendiquait alors « plus de 10 ans » d'expérience dans le test d'intrusion.

Nos confrères du *Spiegel* et nous-mêmes avons conjointement sollicité les commentaires d'Oleg Nefedov, sans succès. Le site vitrine et l'interface de négociation de Black Basta sont inaccessibles au moment où sont publiées ces lignes, depuis près de deux semaines. De sources concordantes, certains membres du groupe sont déjà passés chez Akira ainsi que chez Cactus, notamment.

En coulisses

En décembre 2024, LeMagIT et Hakan Tanriverdi, du *Spiegel* et *Paper trail media*, ont été approchés par un individu assurant disposer d'informations sur Tramp. Depuis ce moment, la rédaction a été en étroit contact avec Hakan Tanriverdi et Hannes Munzinger, partageant et vérifiant de manière croisée les résultats de nos recherches. À de nombreuses reprises, nous avons pu confirmer que les mêmes informations nous avaient été confiées.

À ce jour, rien n'indique que l'individu nous ayant mis sur la piste d'Oleg Nefedov soit le même que celui ayant divulgué des conversations internes à Black Basta début février, connu sous le pseudonyme « ExploitWhispers ».