Club de la sécurité de l'information français

Panorama de la cybercriminalité année 2016

Paris, 11 janvier 2017

Evénement organisé avec le soutien de nos sponsors

Club de la sécurité de l'information français

Les nouvelles pratiques de la cybercriminalité underground

Adrien PETIT
Team Manager Cyber Threat Intelligence – CEIS

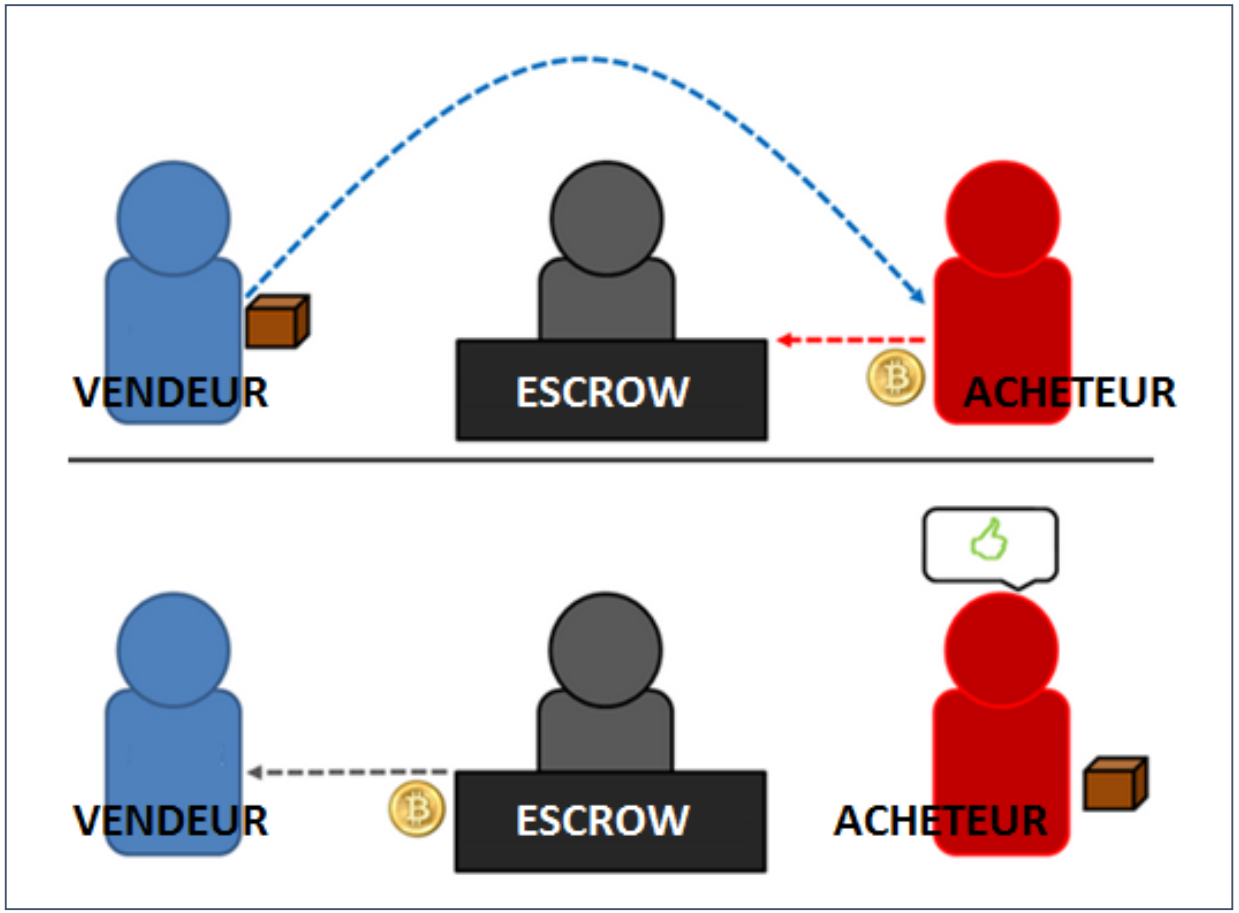
Principales communautés underground en 2016

Une structure commune

- Typologie des plateformes utilisées
  - Places de marché
  - Forums restrictifs

- Ces plateformes ont une double fonction
  - Communication
  - Commerciale → Généralisation du système « Escrow »

Système « Escrow »



Une communauté francophone en pleine mutation

- Exit-Scam de l'une des principales plateformes

- Conséquences
  - Apparition de nouvelles plateformes → Tentative de scam

→ Perte de confiance et paranoïa de la communauté

Une communauté francophone en pleine mutation

- Conséquences
  - Confirmation des plateformes historiques

Niveau de fiabilité des markets francophones actifs

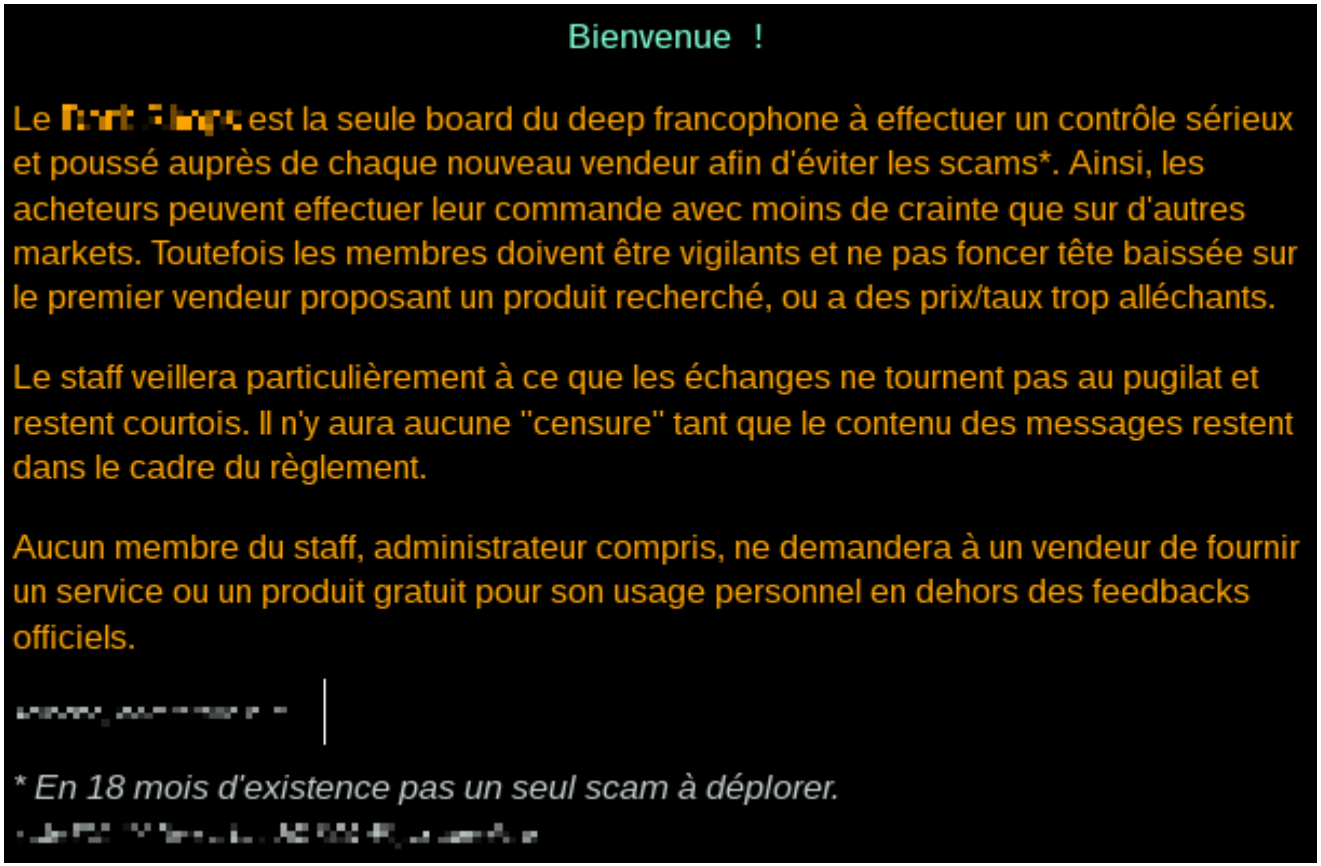
Exit scam : Se dit généralement d'un membre du staff (administrateur, modérateur, escrow) qui disparaît avec la totalité de l'argent qu'on lui a confié.

Scam : se dit d'un vendeur qui disparaît avec l'argent que vous lui avez confié lors d'une transaction.

[illegible]	60% BON	Administré par , la section market du ne comporte pas de risque majeur côté exit-scam. En revanche, il n'y a pas de filtrage des vendeurs ce qui augmente le risque de scam. Vous devrez donc passer par un escrow pour sécuriser vos transactions : l et . Ils sont fiables.	[illegible]	40% PRUDENCE	Inscription payante : 50€ Escrow auto (risque élevé). Trois escrows humains ont filé avec la caisse. Fort soupçon de scam de la part d'un administrateur. Pas de filtrage des vendeurs. Politique anti-scam ambiguë. Un Scam-exit n'est pas à exclure.
[illegible]	40% PRUDENCE	Inscription payante : 20 et 55€. Opaque dans son administration. Cms non open source, ce qui est dangereux. Tout comme l'incitation à utiliser JS. Risque d'exit-scam à moyen ou long terme. Pas de filtrage des vendeurs. Un des escrow est un scammeur. Compteur des membres connectés non conforme à la réalité.	[illegible]	50% PRUDENCE	Ouvert peu avant le scam-exit d'l l dont un des modérateurs est administrateur de . Opacité sur l'identité du second administrateur et d'un escrow. Pas de filtrage des vendeurs. Risque de scam-exit à moyen ou long terme.
[illegible]	20% DANGER	Board down.	[illegible]	10% DANGER	Le staff vient du qui a fermé suite au scam-exit de ses administrateurs. Tout laisse penser que se sont les mêmes aux commandes de ce nouveau market. Les risques de scam-exit et de scam de vendeurs sont très élevés. Ne placez aucun argent sur cette board. Compteur des membres connectés non conforme à la réalité.

Une communauté francophone en pleine mutation

- Conséquences
  - Conditions d'inscription plus strictes (1/2)



Bienvenue !

Le [redacted] est la seule board du deep francophone à effectuer un contrôle sérieux et poussé auprès de chaque nouveau vendeur afin d'éviter les scams*. Ainsi, les acheteurs peuvent effectuer leur commande avec moins de crainte que sur d'autres markets. Toutefois les membres doivent être vigilants et ne pas foncer tête baissée sur le premier vendeur proposant un produit recherché, ou a des prix/taux trop alléchants.

Le staff veillera particulièrement à ce que les échanges ne tournent pas au pugilat et restent courtois. Il n'y aura aucune "censure" tant que le contenu des messages restent dans le cadre du règlement.

Aucun membre du staff, administrateur compris, ne demandera à un vendeur de fournir un service ou un produit gratuit pour son usage personnel en dehors des feedbacks officiels.

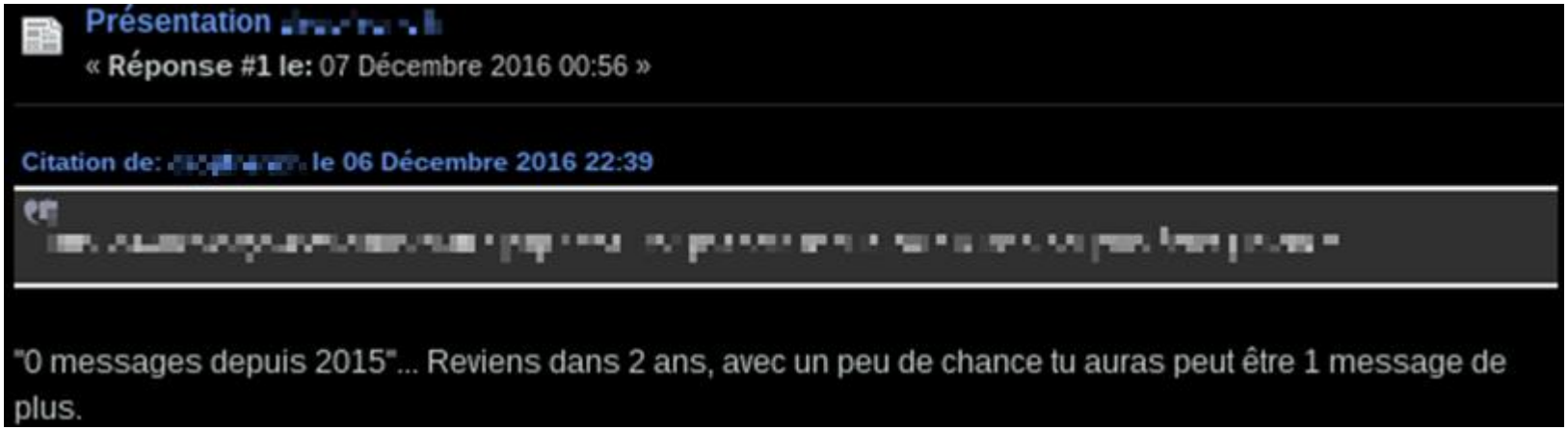
[redacted]

** En 18 mois d'existence pas un seul scam à déplorer.*

[redacted]

Une communauté francophone en pleine mutation

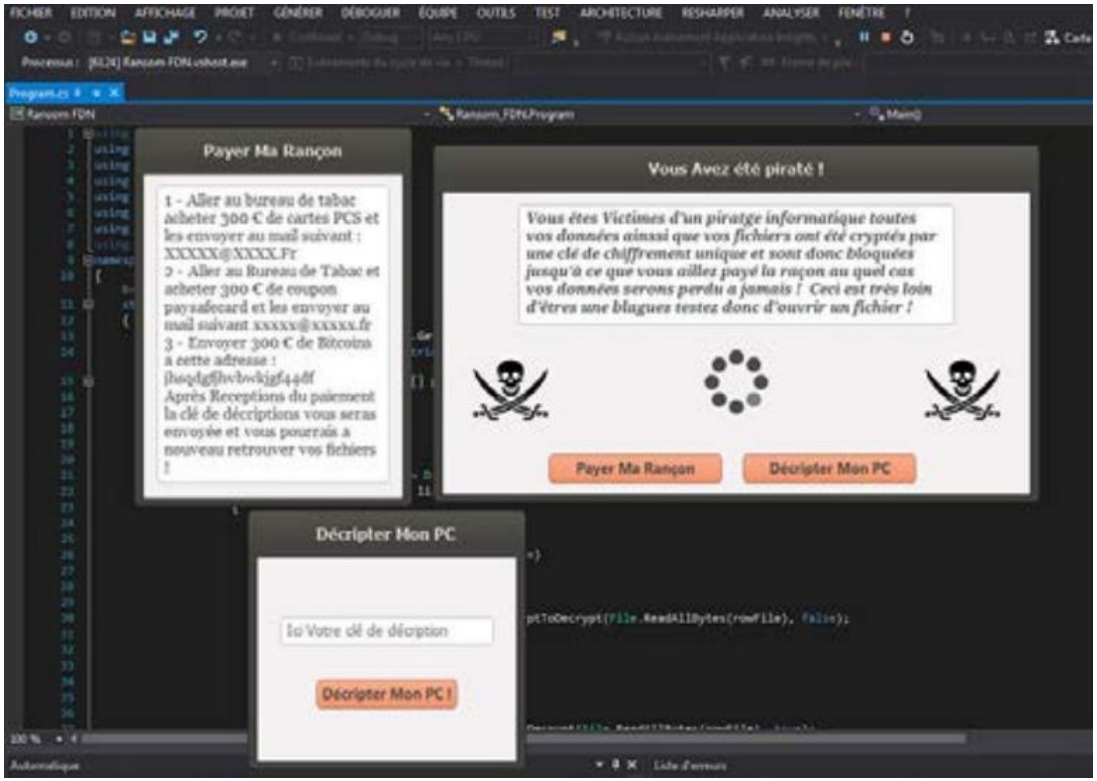
- Conséquences
  - Conditions d'inscription plus strictes (2/2)



  - De plus en plus d'espaces privés

Une communauté francophone en pleine mutation

- Développement de malwares francophones



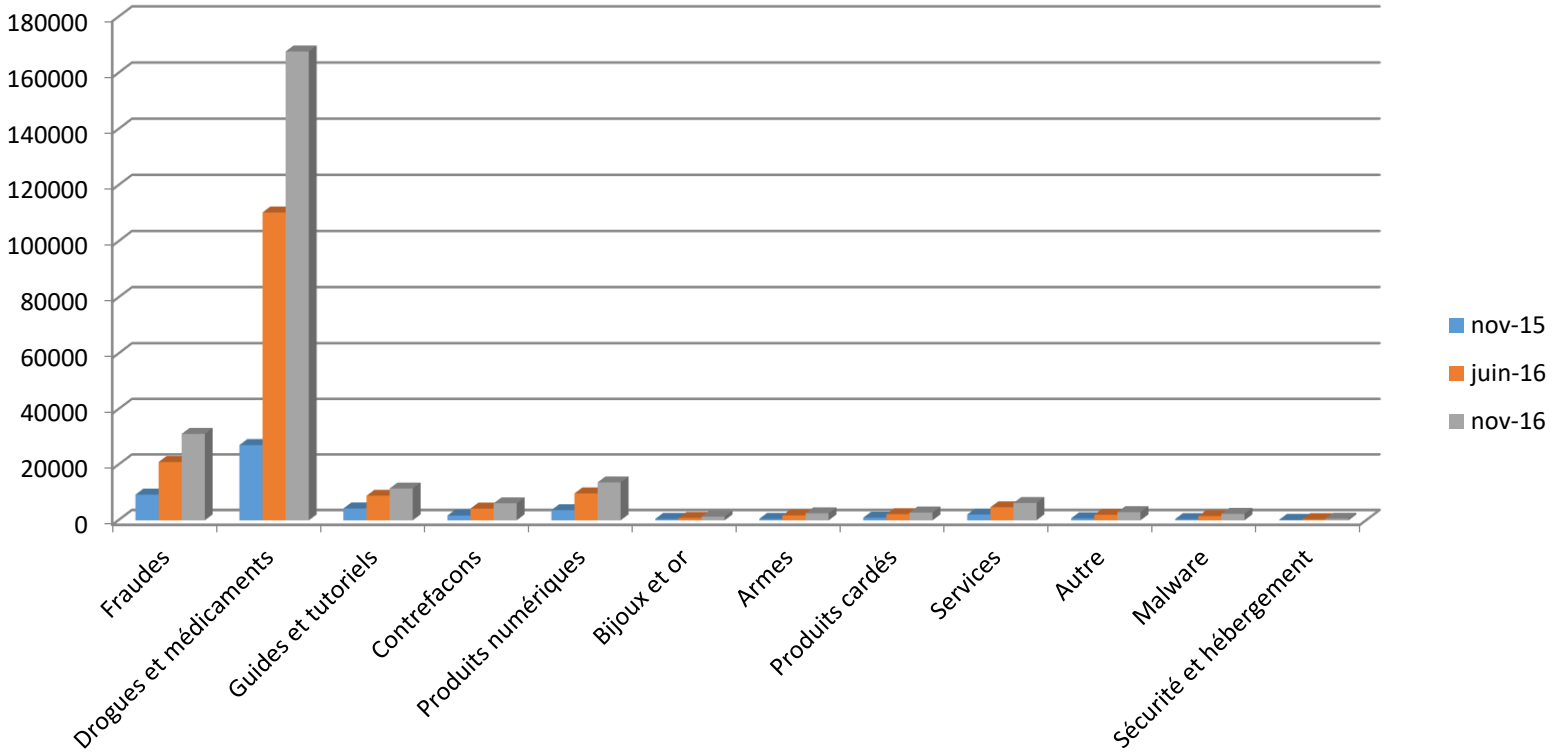
Communauté anglophone : confirmation de la suprématie d'AlphaBay

- Fermeture de 2 places de marché
  - Août 2015 : Agora se met en « pause » le temps de sécuriser la plateforme
  - Avril 2016 : Exit Scam de Nucleus

→ Migration des acheteurs et vendeurs

- Alphabay leader incontesté
  - Juin 2015 : 25 000 annonces
  - Juin 2016 : 167 000 annonces
  - Novembre 2016 : 249 000 annonces

Répartition et évolution des annonces sur le marché noir Alphabay



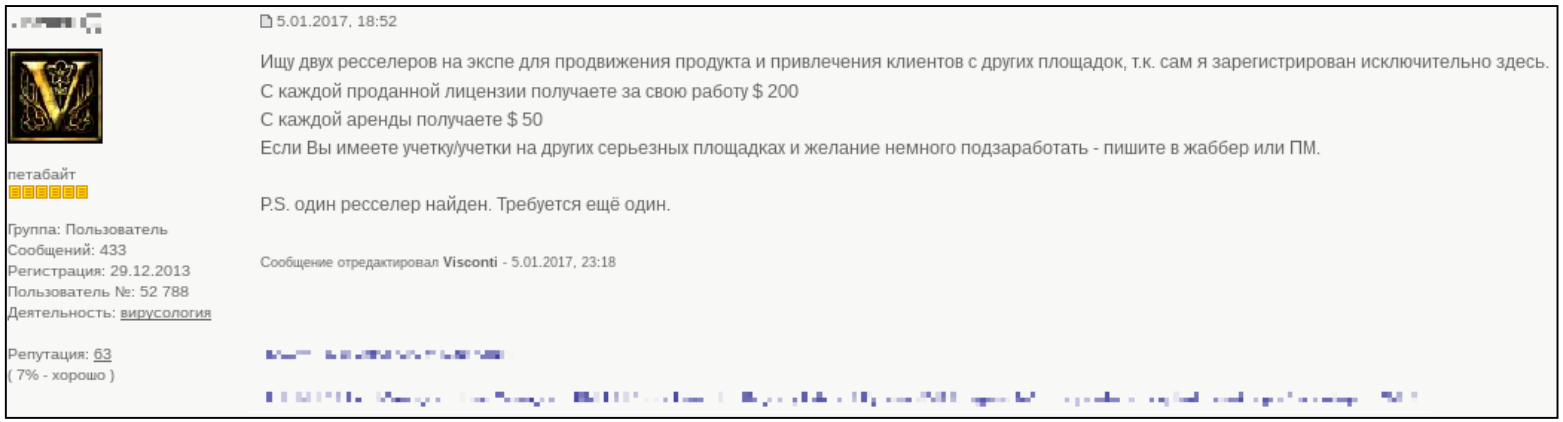
Source : Étude CEIS (novembre 2016)

Communauté anglophone : de nouvelles évolutions

- Introduction de Monero
- Généralisation du As-A-Service (Ransomware, DDoS, hacking, etc.)

De plus en plus d'intéractions entre les communautés

- Principal forum russophone pris en exemple
- Développement de "connecteurs" entre les différentes communautés underground



Sources

- Cybercrime and the Deep Web
  http://www.trendmicro.fr/media/wp/cybercrime-and-the-deep-web-whitepaper-en.pdf
- Dark Net Markets Comparison Chart
  https://www.deepdotweb.com/dark-net-market-comparison-chart/
- The French Underground: Under a Shroud of Extreme Caution
  http://www.trendmicro.fr/media/wp/the-french-underground-whitepaper-fr.pdf
- Flashpoint and Talos Analyze the Curious Case of the flokibot Connector
  https://www.flashpoint-intel.com/flokibot-curious-case-brazilian-connector/