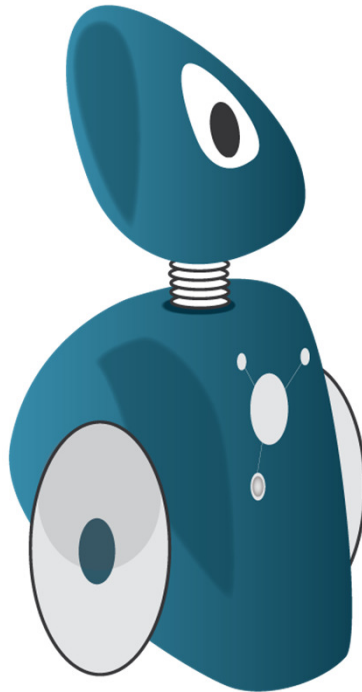


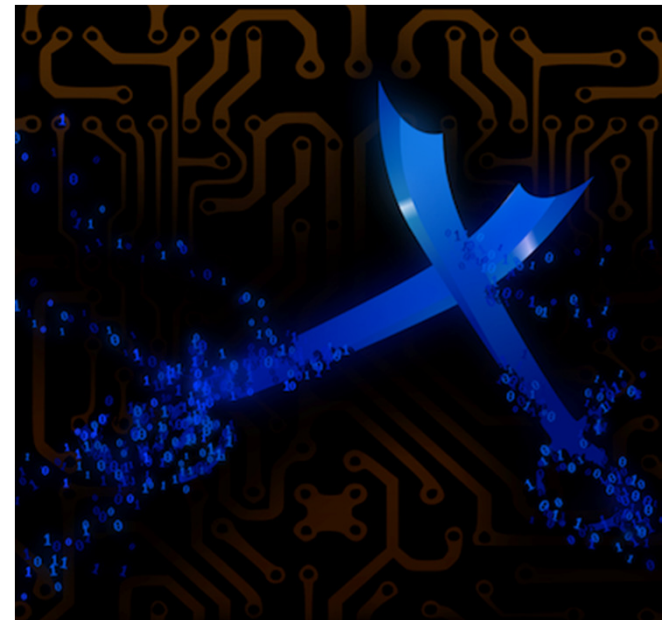
Botnets



Éric FREYSSINET

<http://blog.crimenumerique.fr> @ericfreyss

<https://www.botnets.fr> @botnets_fr



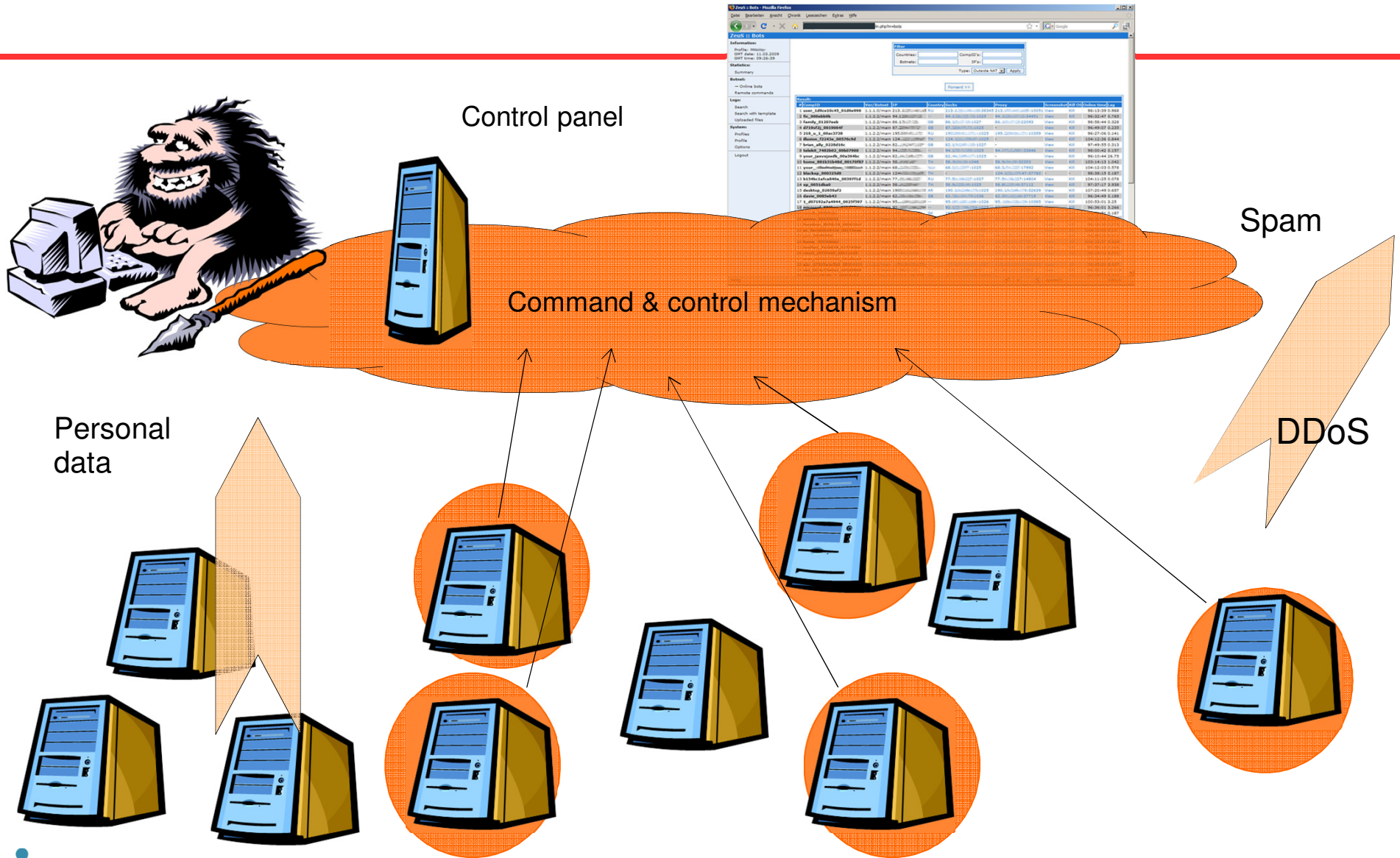
Why talk about *botnets* ?

- They are a major component of criminal infrastructures on the Internet
- It is not just about malware
 - At the same time known and not well known
- I am also carrying research towards a PhD on the fight against botnets

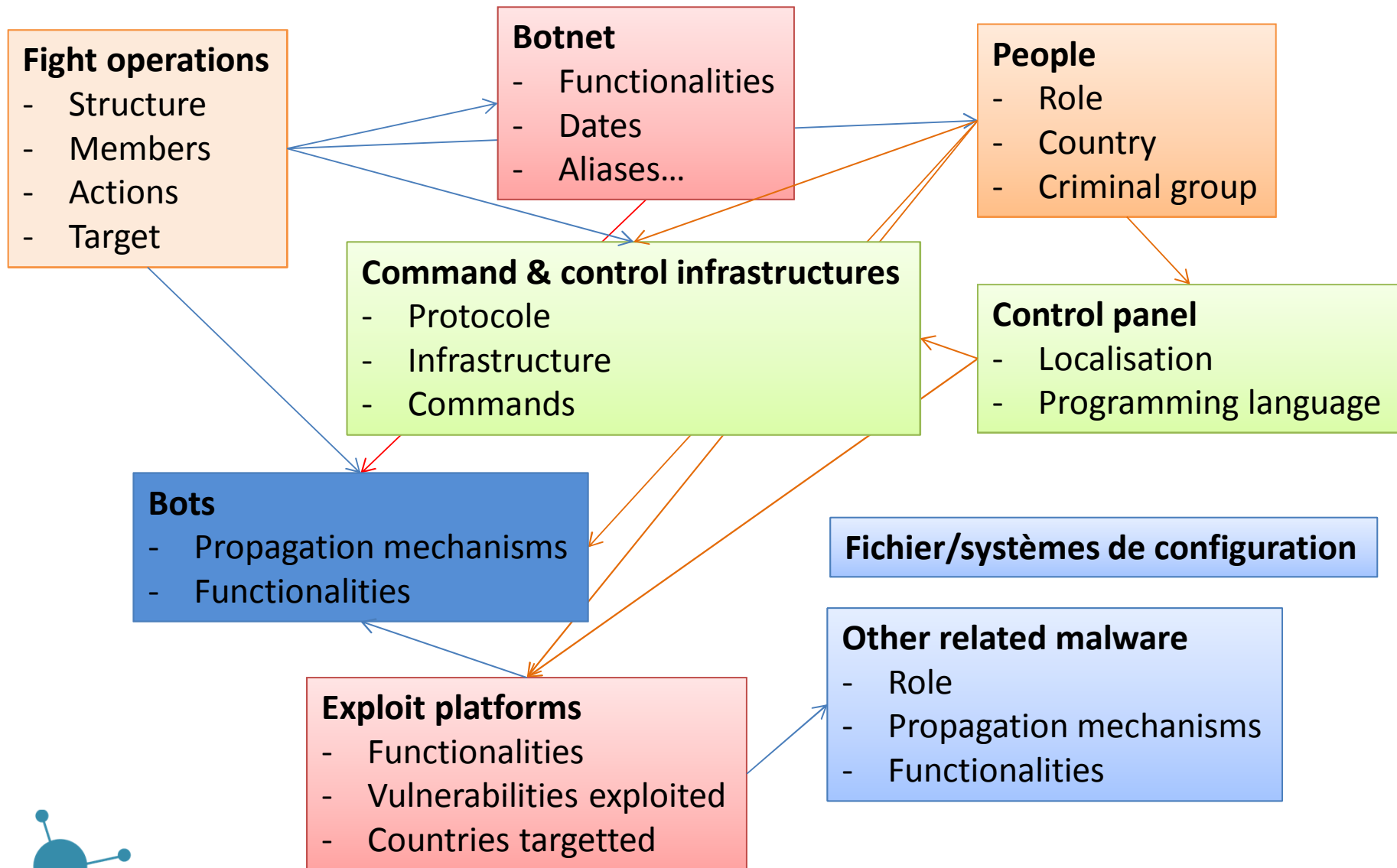


<http://www.complexnetworks.fr/>

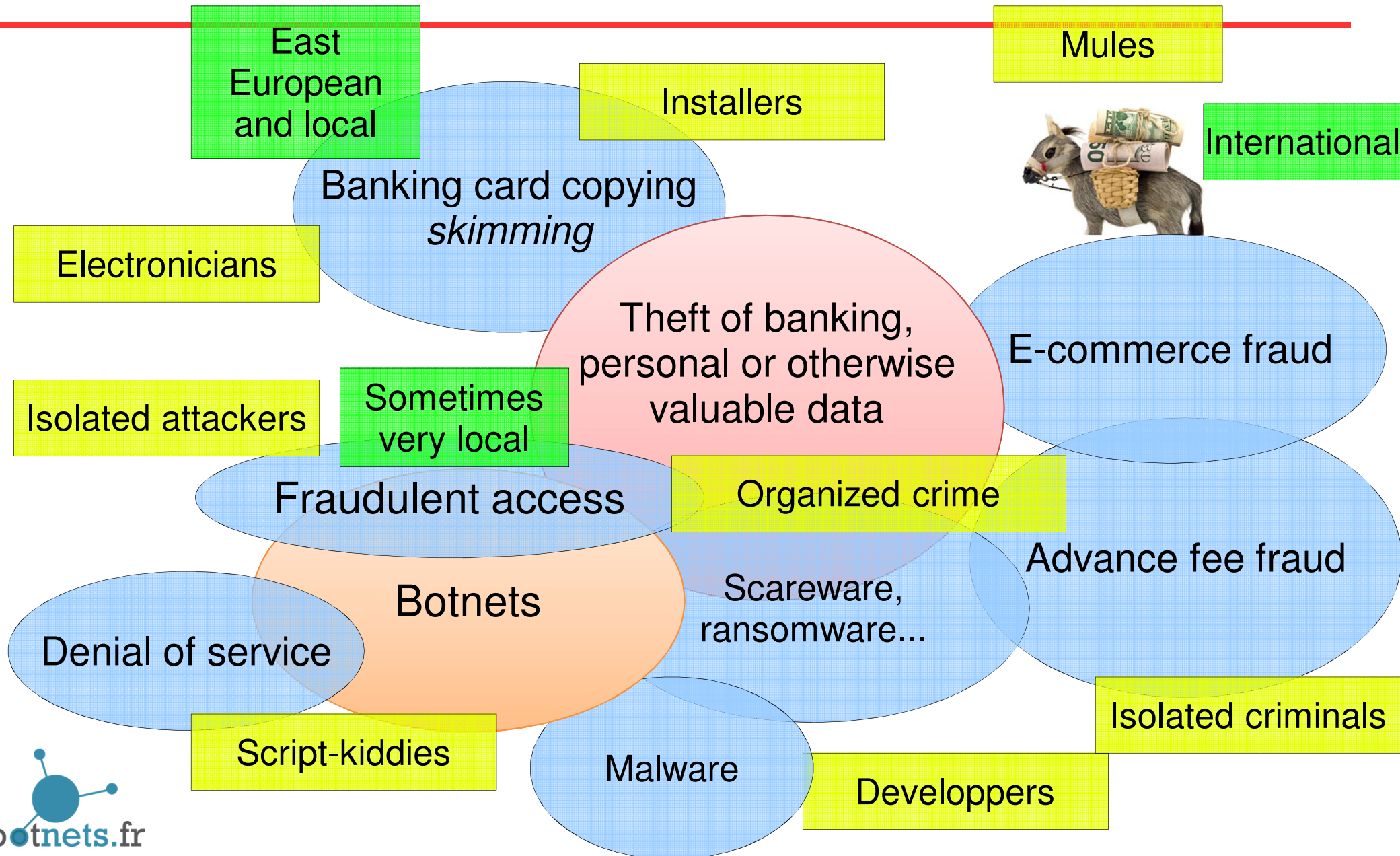
Botnets – General principles



The beginning of a more systematic approach



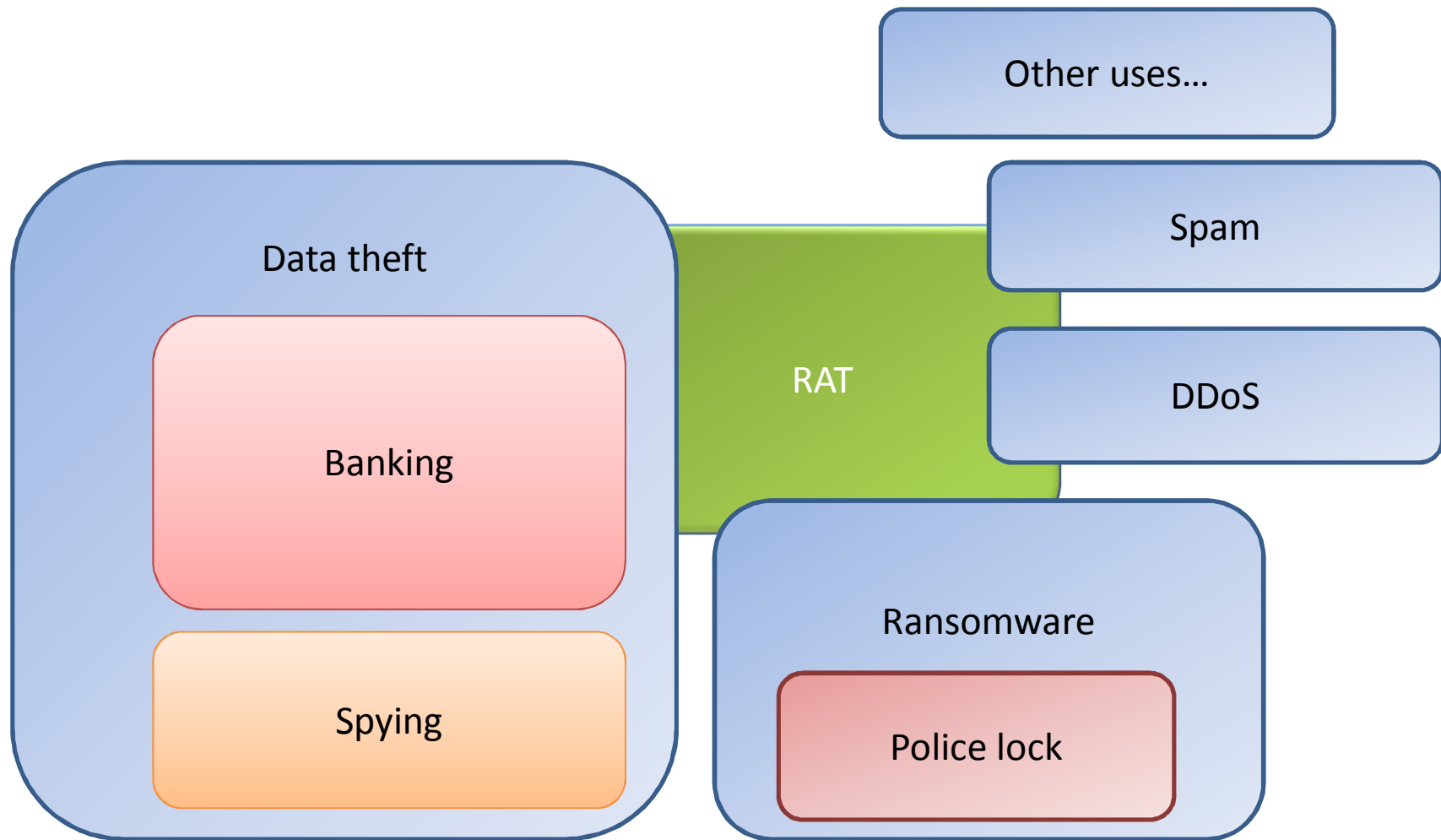
The cybercrime ecosystem



Classification

- I am convinced that:
 - Classification of malware, can be helped by classification of botnets, propagation mechanisms
 - This means collaborative work is a necessity
 - It will help and identify suspects behind malware and botnets more efficiently

Botnet categories

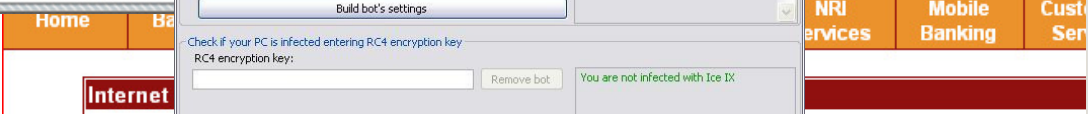
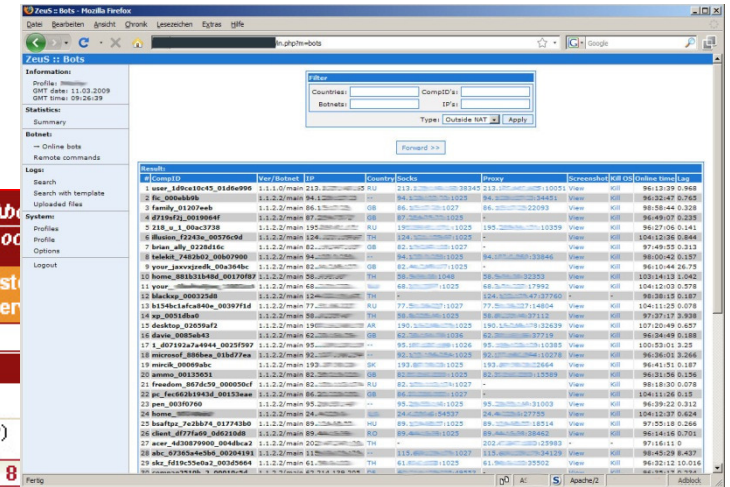
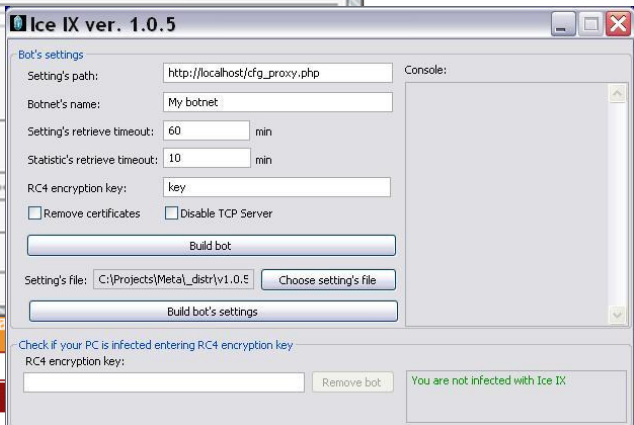


Banking botnets

- ZeuS, SpyEye, Torpig, Carberp, IceIX...

Parameters

Control panel (ZeuS)

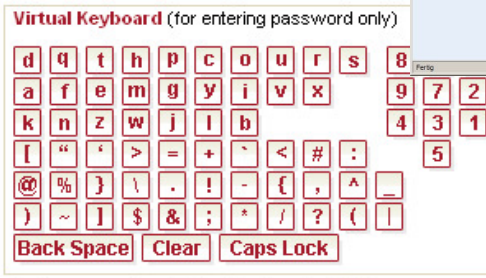


Important Security Notice:
 ICICI Bank does not ask you for any personal information other than your user ID and password when you log into www.icicibank.com.

User ID:

Password: Use virtual keyboard (Recommended)

Start in: My Accounts



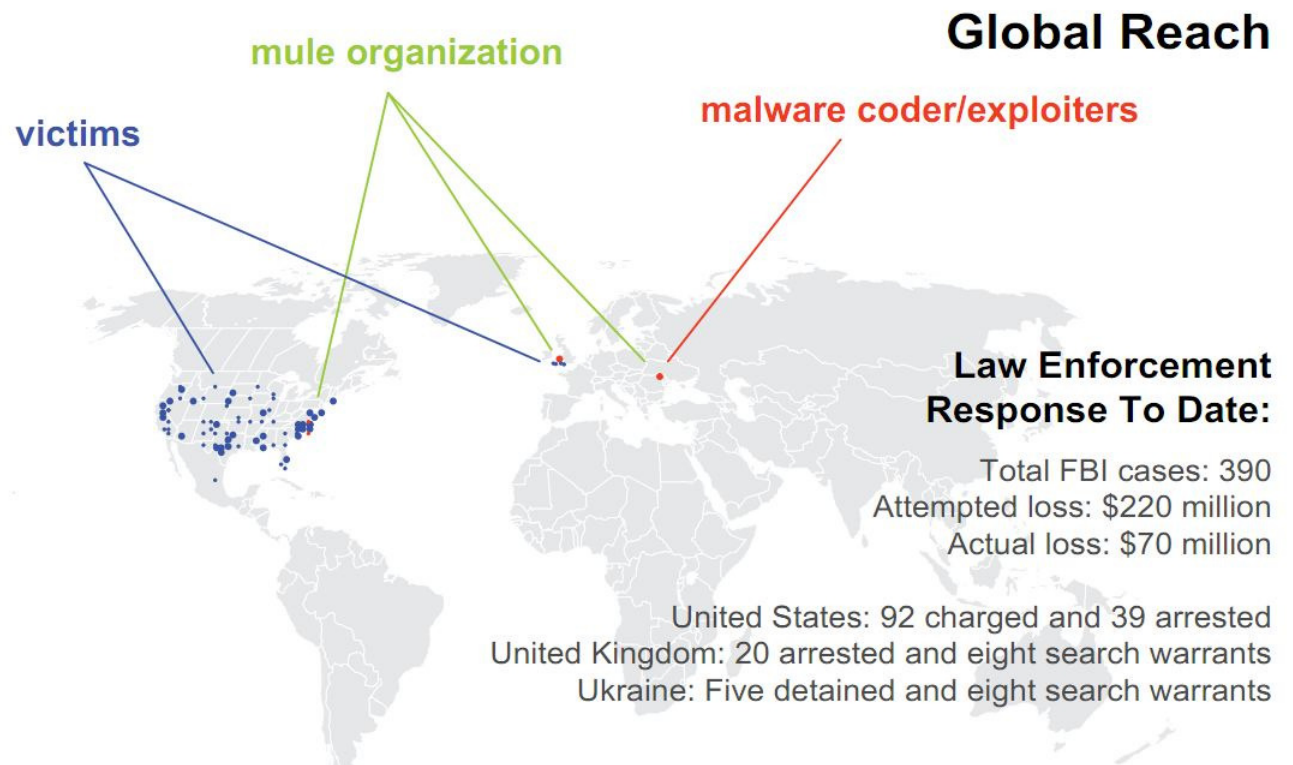
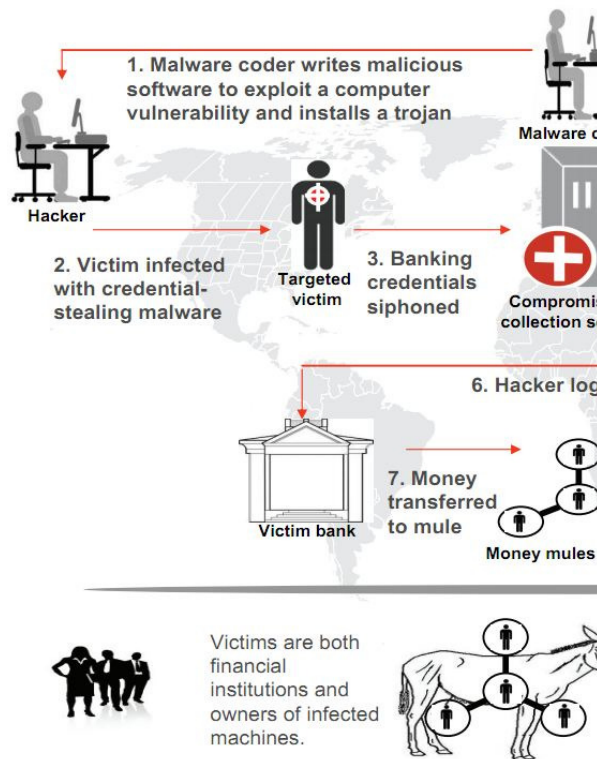
Theft of personal data, including from « secure » keypads

[New users? Register here.](#) [Forgot password? Cyber Cafe Security](#) [Trouble logging in? About e-mail fraud](#)

Customer Service | Internet Banking FAQ's | Internet Banking Demo
 Privacy | Online Security | Terms and Conditions | Disclaimer

JabberZeus

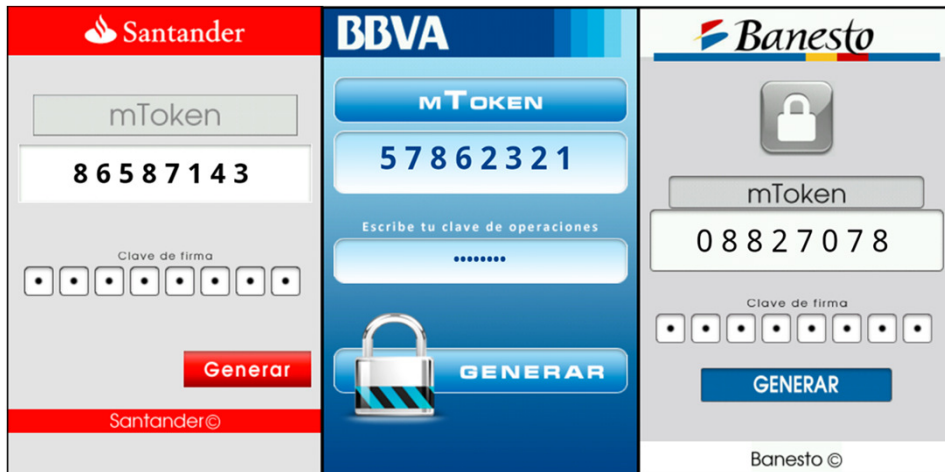
<http://krebsonsecurity.com/tag/jabberzeus/>



<http://garwarner.blogspot.fr/2012/03/microsoftdcu-fs-isac-and-nacha-vs-zeus.html>

<http://zeuslegalnotice.com/>

A mobile botnet




- FakeToken (Android)
- Communication through SMS & HTTP
- Logical evolution of banking malware

Distribution by SMS spam

- <http://blog.fortiguard.com/android-malware-distributed-by-malicious-sms-in-france/>

• mato [redacted] Posté [redacted] 2012 - 08:53 #1

Newbie



Membre
1 messages
Marque: [redacted]
Modèle: STAR ADDICT

Bonjour,

Ce matin je reçois un message du 10052

*" Pour le bon fonctionnement de votre appareil, téléchargez la nouvelle mise à jours ANDROID Flash Player ci-dessous :
[http://tinyurl.com/\[redacted\]](http://tinyurl.com/[redacted])
"*

J'ai un [redacted] Star Addict, je ne sais pas si c'est un virus. Quand j'ai vérifié l'uri du téléchargement sa venait d'un serveur mail, et le whois me disais que sa venait d'arable.

Je les téléchargez puis je les ouvert on aurait dit une image flash. Puis je l'ai désinstaller.

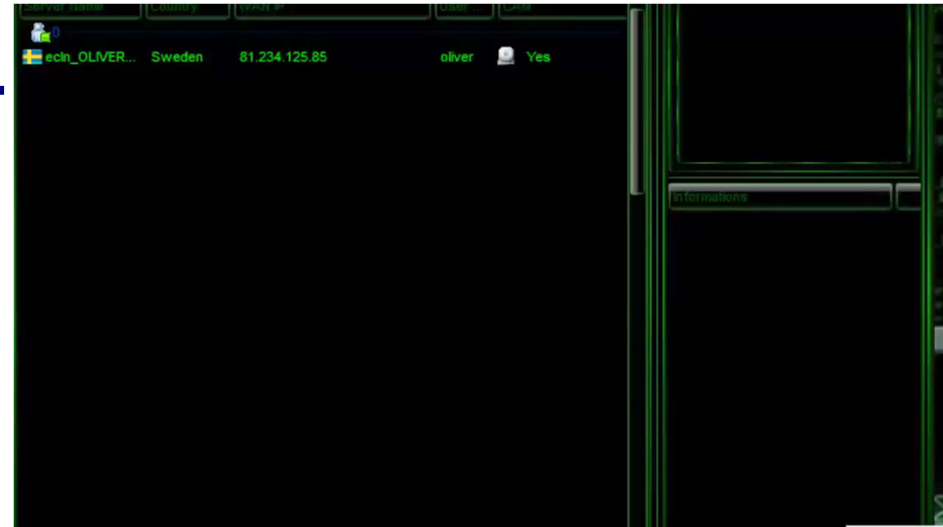
J'ai des chances d'avoir un virus ?

Car les permissions, prennait le réseau envoyez des sms etc...

Merci beaucoup!

RAT – Remote administration trojans

- Everybody remembers BackOrifice
- Other are very popular today
- Very often script kiddies will use their own IP address and dynamic DNS redirectors
- Xtreme RAT Video...



Bredolab

[Nederlands](#) | [English](#)



[Home](#) ♦ [Report Crime](#) ♦ [Press Release](#) ♦ [About Dutch Police](#)

Your computer is infected!

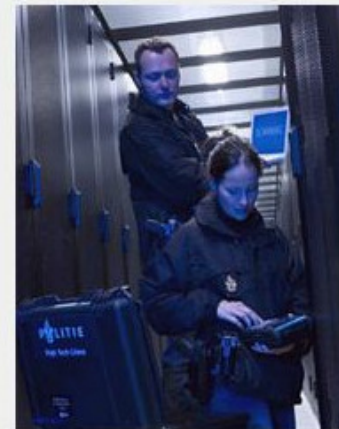
If this Browser has opened automatically then your computer has been infected with malware. Your computer has become part of a bot network.

This message has been sent to you by the High Tech Crime Team of the Dutch National Crime Squad and aims to notify all owners of infected computers.

Dutch National Crime Squad takes down infamous botnet

On October 25th 2010, the High Tech Crime Team of the Dutch National Crime Squad took down a very large botnet, containing at least 30 million infected computer systems worldwide since July 2009. These computers were infected with the malicious Bredolab trojan, through infected websites. Through these botnets, cybercriminals can spread large amounts of other viruses and create new botnets.

In close cooperation with a Dutch hosting provider, The Dutch Forensic Institute (NFI), the internet security company Fox-IT and GOVCERT, the computer emergency response team of the Dutch government, shut down 143 computer servers today.



More information:

For more information about removing Bredolab from your computer, visit:

<https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html>



Dorifel

.....Refresh

.....Exit

ALL:2429

BE	2
NL	2257
GB	2
IT	2
US	18
FR	2
DK	103
DE	5
PH	26
FI	1
EU	8
RO	1
ES	1
KE	1

Title: Loaded: Max: Action:

Clear Stats

Title: Country: (XX or ALL) Max:

Task:

SetUp

NCSC publishes Dorifel factsheet

News | 19-08-2012

An outbreak of the Dorifel virus primarily infecting systems in the Netherlands was seen in early August 2012. The virus is being spread through the Citadel botnet. This factsheet will take a closer look at the relationship between Dorifel and Citadel, describe the impact of an infection and recommend steps to take if you are infected. We conclude with providing a number of tips to avoid infection.

The most important things about Dorifel

- > Dorifel is a virus that actively seeks out Office documents on network drives and external media (USB sticks, external hard drives, etc.).
- > The **Citadel botnet is used to distribute Dorifel.**
- > Activating the Dorifel virus has revealed previous Citadel infections.
- > Multiple antivirus vendors have released updates that can identify Dorifel and restore files.
- > Citadel was originally designed to attack users of internet banking services.
- > Cybercriminals are also using the Citadel botnet for other purposes.
- > Computers may have been infected with the Citadel botnet malware for some time.

<http://www.damnthoseproblems.com/?lang=en>

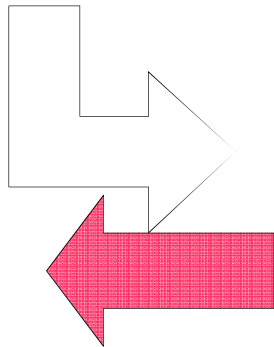
Duqu



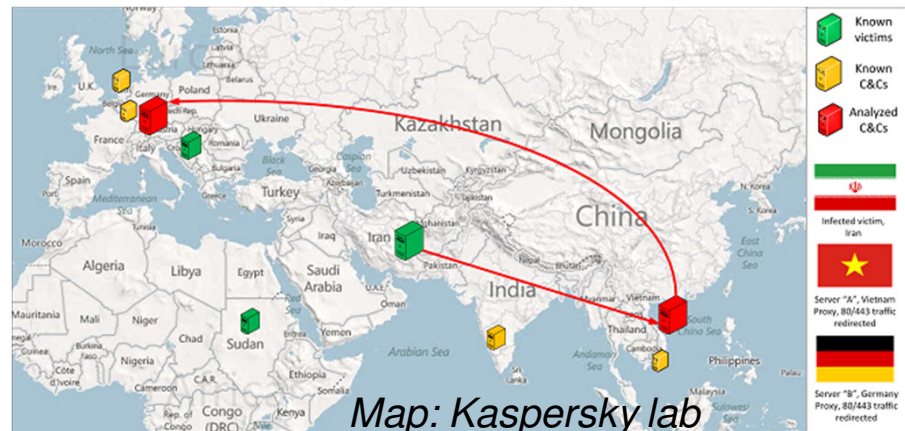
CVE-2011-3402

Local network contamination

Screen copies
Keystrokes
Configuration
Web history
...



Relay



Police ransomware

Gendarmerie



ATTENTION!
Votre ordinateur a été bloqué pour violation de la loi Française

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs.
- Spam
- Utilisation des logiciels en infraction avec les droits d'auteur
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquent votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.



ATTENTION!
Votre ordinateur a été bloqué pour violation de la loi Belgique

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs
- SPAM
- Utilisation des logiciels en infraction avec les droits d'auteur
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquent votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.


Vous pouvez payer l'arrêté avec aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer arrêché», rempli le forme avec les codes et valeurs des vouchers, et cliquez sur le bouton «Payer arrêché». Votre ordinateur sera débloquent dans les 24 heures suivantes.

Après le débloquent, nous suggérons que vous:

- Supprimez toutes les fichiers multimédia en infraction avec les droits d'auteur.
- Supprimez des logiciels en infraction avec les droits d'auteur.
- Installez un logiciel anti-virus, si vous n'en avez pas encore.
- Faire un scan anti-virus.

Votre SE: Windows Seven Votre FAL:
Votre adresse IP: Votre ville:

Gema



Access to your computer was denied.

Illegally downloaded music tracks in other words "pirated copies" have been detected at your PC. While being downloaded the before mentioned tracks were copied - But it is a criminal offense in conformity with §106 of the Digital Millennium Copyright Act.

Both copyrighted music tracks downloaded in the Internet and music files exchange are illegal subject to compliance with §106 of the Digital Millennium Copyright Act and punished by either imposition of monetary fines or up to three years of imprisonment. Moreover, following a § 114 of the Criminal Code the property is subject to seizure - it can carry forth of the computer has been formally used for the above mentioned files downloading.

Your IP address: IP: [REDACTED]


The legitime identification both of your person and that who uses your IP address and HostName poses no problem anyway. The detected pirated copies were copied and copied to password-protected directory. For unblocking and commission of any other actions resulted from infringement of rule of law you should pay a penalty equal to €50. The payment should be delivered through our financial partner - Paysafecard. When the payment procedure is complete successfully your PC will be unblocked automatically. For the completion of the above mentioned payment insert enter Paysafecard's password in proper box and press "Enter".

GEMA holds legal rights and permanently contacts with state legislation.

payment System: Paysafecard
File:
Value: 50 €
[Buttons: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, -, =]

Selling spots:
For instance: pharmacy and other websites, phone cards. More variants are available at www.paysafecard.com

Other selling spots:
1. Refer to nearest local dealer for Paysafecard equal to €50.
2. Receive your personal Paysafecard password by post.
3. Enter your Paysafecard password to proper box.



Gimemo



Police Nationale

Vous pouvez être victime d'un escroquerie...

Des messages de messages (spam) ont été localisés sur votre ordinateur. En téléchargement, ces messages de messages visent à effectuer une infraction pénale en vertu de l'article 106 de la loi sur le droit d'auteur.

Le téléchargement des copies de musique protégées qui via l'Internet ou via les réseaux de partage de musique ne légitime ni en conformité avec l'article 106 de la loi, sous réserve du droit d'auteur d'une personne qui a intentionnellement copié ou diffusé des copies protégées de contenu numérique.

Le non respect de cette demande pourrait entraîner des accusations criminelles et l'emprisonnement.

Pour effectuer le paiement, connectez le code Paysafecard ou le code de paiement déposé, sélectionnez le valeur de votre code puis appuyez sur le bouton «Entrer».

SACRE est légitimé par la loi - et est en contact direct avec les législateurs et la justice.

Voici un exemple de formulaire de paiement:

Votre adresse IP: [REDACTED]

Vous avez 100 euros de paiement offerts par la résolution de votre adresse IP et le nom d'hôte associé. Les données produites en relation ont été diffusées et ont été diffusées dans un dossier protégé pour empêcher des escroqueries.

Pour débloquent votre ordinateur et d'autres ordinateurs connectés, vous devez d'abord débloquer votre ordinateur en utilisant le code de paiement. Les données produites en relation ont été diffusées et ont été diffusées dans un dossier protégé pour empêcher des escroqueries.

Le non respect de cette demande pourrait entraîner des accusations criminelles et l'emprisonnement.

Pour effectuer le paiement, connectez le code Paysafecard ou le code de paiement déposé, sélectionnez le valeur de votre code puis appuyez sur le bouton «Entrer».

SACRE est légitimé par la loi - et est en contact direct avec les législateurs et la justice.

Code: [REDACTED] 50 €
[Buttons: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, -, =]

Pays de vente: [Options: Total, Torneo, Paysafecard]

Plus de points de vente: [List of locations]



Goldenbaks



Activité illicite décelée!

Ce message de l'ordinateur sert à la protection de vos actes illicites. Le système d'exploitation a bloqué à cause de la détection de bits de la République Française! Ou indirectement l'adresse de votre IP adresse qui correspond au matériel informatique, la pornographie, le matériel, la violence et des actes de violence envers les enfants. Egalément on a récupéré un virus avec les données de violence et la pornographie d'enfant. De même on a enregistré l'envoi ou transfert d'éléments non autorisés de données.

Pour lever le blocage de l'ordinateur vous devez payer le montant de 100 euros.

Il y a deux possibilités d'effectuer le paiement:
1) Si vous devez remplir le formulaire de paiement avec le code donné, appuyer sur OK (ce cas de données disponibles, vérifiez les données avant l'appui sur le bouton OK)
2) Si vous devez remplir le formulaire de paiement avec le code donné, appuyer sur OK (ce cas de données disponibles, vérifiez les données avant l'appui sur le bouton OK)
3) Si l'application d'un virus, vous devez envoyer le code à l'adresse indiquée info@p-g.org

Où puis-je acheter un voucher Ukash?
Acheter Ukash dans plus de 20 000 points de vente en France. Vous pouvez obtenir Ukash dans des commerces de détail et en ligne, au supermarché, au magasin, des pharmacies, banque GABY, et auprès des bureaux de tabac.
Point de vente: Ukash est maintenant disponible dans des milliers de points de vente.
Tabac presse: Ukash est maintenant disponible avec la Carte Torneo.
Recharge: Ukash est disponible en ligne 24/7 sur www.ukash.com.
Chaque: Ukash est maintenant disponible avec la Carte Torneo.
Recharge: Ukash en ligne 24/7 sur www.ukash.com.



Silence locker



ATTENTION!

Pour des raisons de sécurité, votre système Windows a été bloqué.

La raison peut être la visite des sites infectés ou pornographiques. L'ordinateur est dans un état critique, en cause de cela le système peut perdre tous vos documents et fichiers. Pour avoir la possibilité de restaurer le système, vous aurez besoin de télécharger la mise à jour complémentaire pour le système de sécurité.

Cette mise à jour payée est destinée également pour les systèmes infectés. Cette mise à jour va protéger complètement votre système contre les virus et les logiciels malveillants, va stabiliser votre système informatique et va éviter la perte de données.

Selectionnez la méthode préférable de paiement

Ukash POSSIBLE ✓
paysafecard POSSIBLE ✓

Votre système informatique sera restauré (quart) bientôt, pour ce faire vous avez besoin d'entrer un code pour le transfert de 100 euros dans les systèmes de Paysafecard ou de Ukash. Vous pouvez acheter (code) à n'importe quelle station de gaz ou à l'automate. Ces codes peuvent également être achetés sur les cartes de recharge sont vendus.

Immédiatement après avoir entré un code et la vérification de son exactitude, votre système informatique sera mis à jour et protégé - tous les chevaux de Troie et les virus seront supprimés.



Activité illicite décelée!

Un message de votre ordinateur sert à la protection de vos actes illicites. Le système d'exploitation a bloqué à cause de la détection de bits de la République Française! Ou indirectement l'adresse de votre IP adresse qui correspond au matériel informatique, la pornographie, le matériel, la violence et des actes de violence envers les enfants. Egalément on a récupéré un virus avec les données de violence et la pornographie d'enfant. De même on a enregistré l'envoi ou transfert d'éléments non autorisés de données.

Pour lever le blocage de l'ordinateur vous devez payer le montant de 100 euros.

Il y a deux possibilités d'effectuer le paiement:
1) Si vous devez remplir le formulaire de paiement avec le code donné, appuyer sur OK (ce cas de données disponibles, vérifiez les données avant l'appui sur le bouton OK)
2) Si vous devez remplir le formulaire de paiement avec le code donné, appuyer sur OK (ce cas de données disponibles, vérifiez les données avant l'appui sur le bouton OK)
3) Si l'application d'un virus, vous devez envoyer le code à l'adresse indiquée info@p-g.org

Ukash POSSIBLE ✓
paysafecard POSSIBLE ✓

Reveton



Achtung!!!


Die Betriebssysteme wurden im Zusammenhang mit Verdacht gegen die Geräte der Bundespolizei Deutschland gesperrt! Es wurde folgende Verstoß festgestellt: Das IP-Adresse lautet mit einer IP-Adresse mit pornographischen Inhalten, Kinderschutzprogramme, Systeme und Gerate gegen Kinder aufgerufen. Auf Ihrem Computer werden ebenfalls Videodateien mit pornographischen Inhalten, Elementen von Gewalt und Kinderschutzprogrammen gespeichert.

Es werden auch Emails in Form von Spams, mit pornographischen Inhalten, verschickt. Diese Sperre des Computers dient dazu, Ihre Regeln Aktivieren zu unterstützen.

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen.

Ukash POSSIBLE ✓
paysafecard POSSIBLE ✓

AlertLock



Warning! Access to your computer is limited.

Why? From your computer was detected mailing (spam) advertisements illegal sites with child pornography, which contradicts law and harm other network users.

Probably your computer has been infected and as a result our service blocked access to your computer, including a fully networked access (except for our staff).

As the virus sends the illegal spam mail to many different users and modifies itself every 48 hours, including removing our program protection, you have 48 hours, otherwise we will remove all protection program data including the operating system and all your files without the possibility of recovery.

To solve this problem you need to buy and send sms with MoneyPark or Paysafecard or Ukash code (100€ or 100€) and your Reference Number: **471981781100** to the special service phone number: **+18722161446** or email: antispam@cyberservices.com

You can buy MoneyPark card at the nearest stores: Walgreens, Walmart, CVS pharmacy, Kmart, Seven-Eleven, Rite Aid or go to www.moneypark.com to find location stores near you.

To find Paysafecard location stores near you visit www.paysafecard.com or Ukash at www.ukash.com

After that our experts within 1-3 hours Will do audit and clean up your computer from viruses sending out spam and send you sms on the cell phone or email (from which you send card code and your reference number) control code (which unlock your PC) that must be enter here.

[Buttons: Send Control Code, Unusable]

"Do not attempt in any way to remove the protection program, because if you try to do this, your operating system Windows will be unusable"

Anti-Cyber Crime Department of Federal Internet Security Agency (ACCFD/FISA)

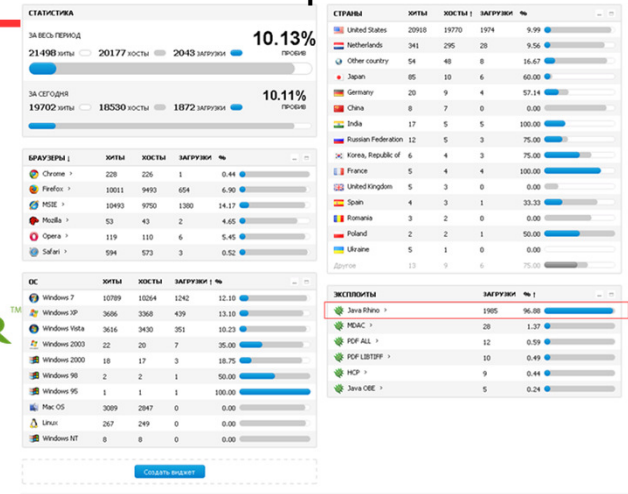
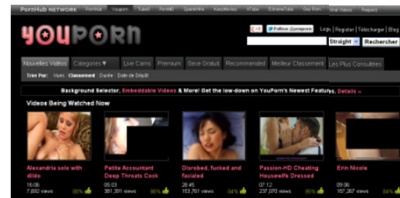
General scheme (first cases)

Exploit kits

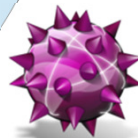
- Malicious Javascript
- On hacked websites
- Inside advertising banners



CLICKSOR™



Drive-by download



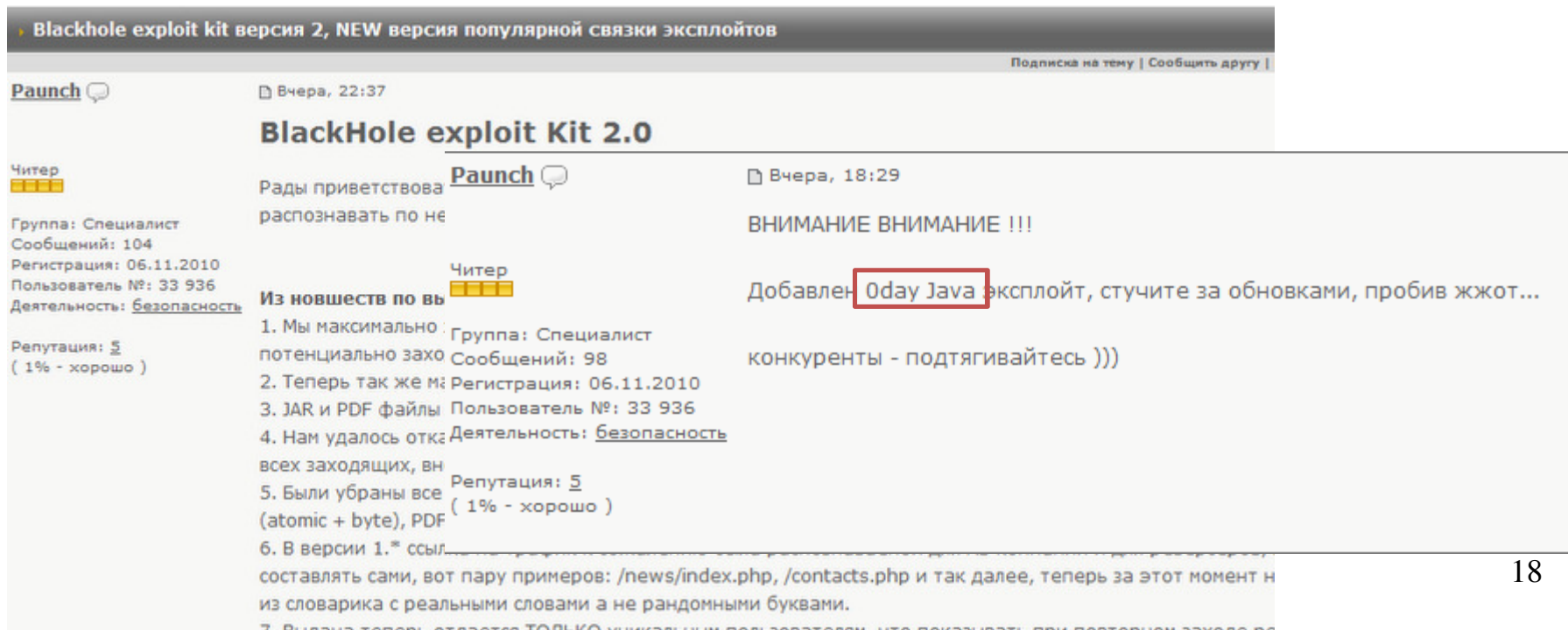
- Ransomware
- Other malware



Payment ticket + personal data

Exploit kits


- Nuclear Pack, BlackHole, Sweet Orange, Phoenix,... (https://www.botnets.fr/index.php/Catégorie:Exploit_kits)
- A real business model, marketing attitude, customer management, ... introduction of the latest 0days





The screenshot shows a forum post titled "BlackHole exploit Kit 2.0" on the botnets.fr website. The post is from a user named "Paunch" and is dated "Вчера, 22:37". The post content includes a list of updates and a warning about "Oday Java" exploits. The "Oday Java" text is highlighted with a red box. The forum interface includes a user profile for "Читер" (Chiter) on the left, a user profile for "Paunch" on the right, and a list of updates in the main content area.


Blackhole exploit kit версия 2, NEW версия популярной связки эксплойтов

Подписка на тему | Сообщить другу |

Paunch  Вчера, 22:37



BlackHole exploit Kit 2.0

Читер 
Группа: Специалист
Сообщений: 104
Регистрация: 06.11.2010
Пользователь №: 33 936
Деятельность: [Безопасность](#)
Репутация:  5
(1% - хорошо)

Рады приветствовать **Paunch** 
распознавать по не

Из новшества по версии 2.0:

1. Мы максимально потенциально захотим
2. Теперь так же мы добавили
3. JAR и PDF файлы
4. Нам удалось отключить
5. Были убраны все (atomic + byte), PDF
6. В версии 1.0 мы добавили
7. Выдана теперь ссылка ТОЛЬКО уникальным пользователям, что показывает при повторном заходе на сайт

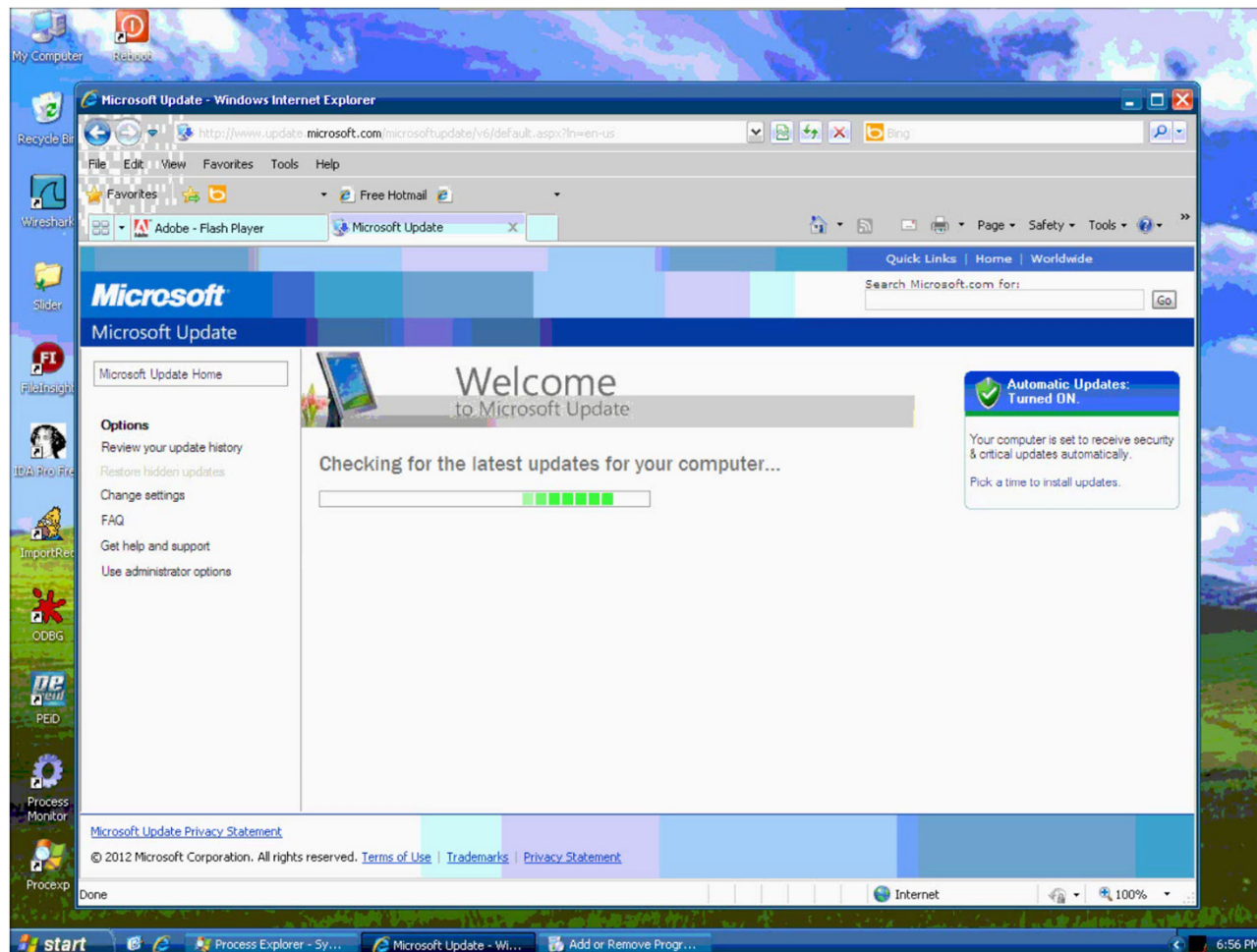
Читер 
Группа: Специалист
Сообщений: 98
Регистрация: 06.11.2010
Пользователь №: 33 936
Деятельность: [Безопасность](#)
Репутация:  5
(1% - хорошо)

ВНИМАНИЕ ВНИМАНИЕ !!!

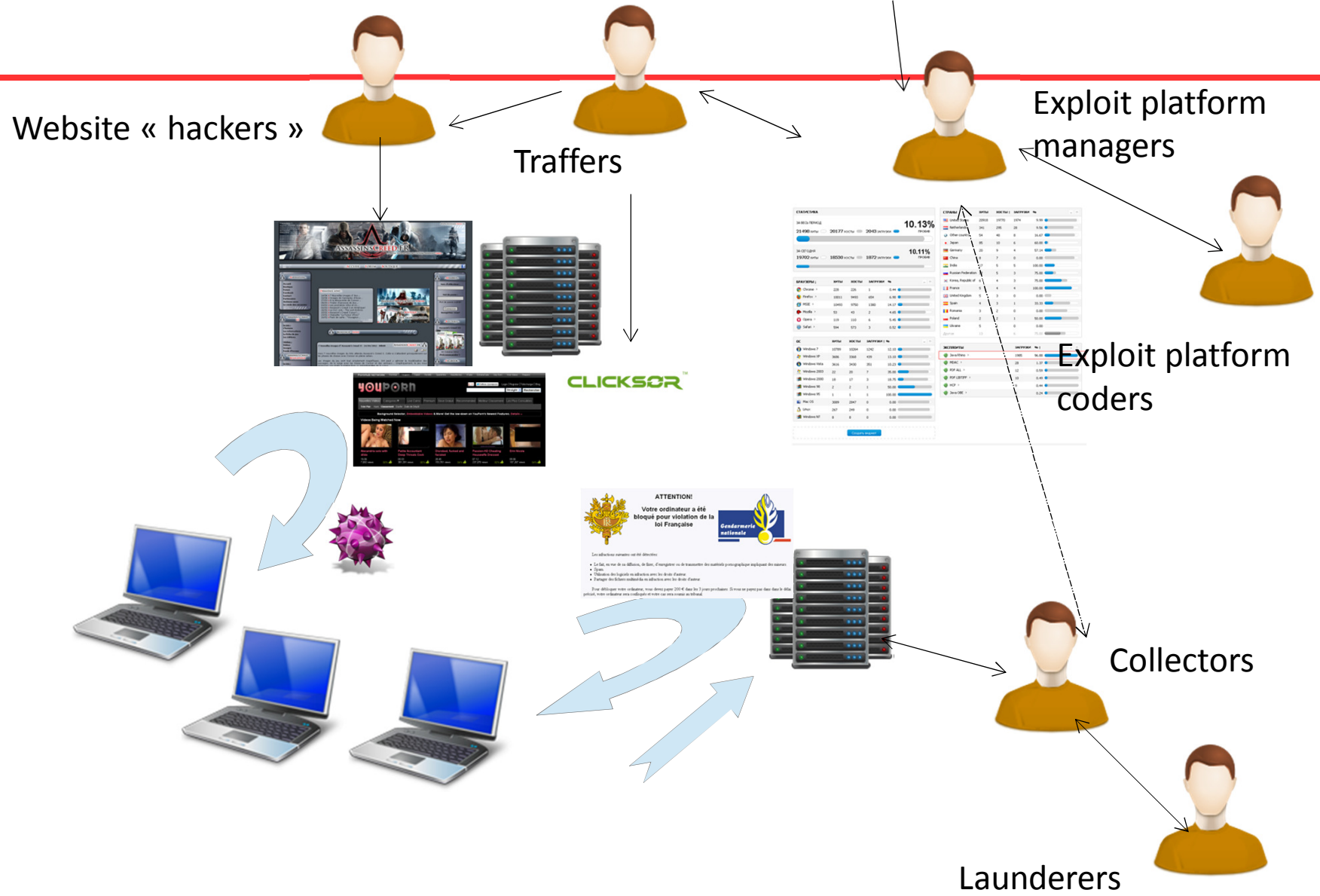
Добавлен **Oday Java** эксплойт, стучите за обновлениями, пробив жжот... конкуренты - подтягивайтесь)))

Exploit kits

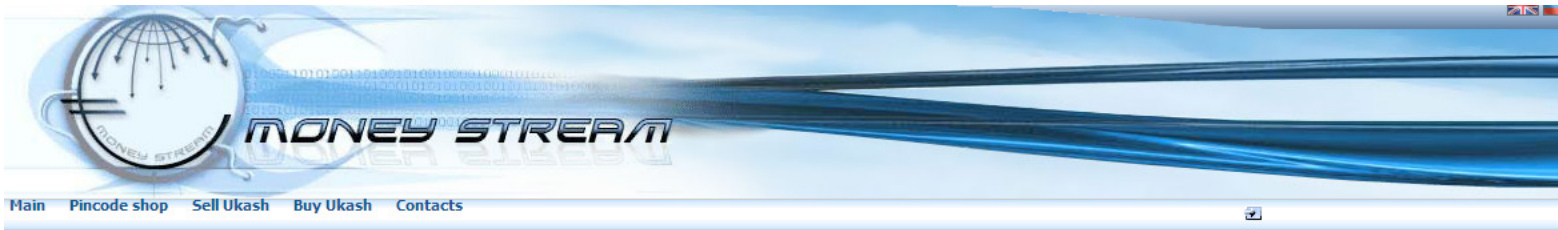
- <http://www.youtube.com/user/kafeineify>



Potential actors



Reselling platforms



On this site you can:

- Exchange ukash, cashu
- Top-up your betamax account
- Purchase Skype credit and Skype In
- Get your consultation about digital money for free

Pincode Shop:

- 10\$ skype = 11 USD Liberty Reserve
- 10 EUR Betamax = 15.50 wnz

We accept:

Working hours

Monday - Saturday
08:00 - 22:00 GMT

Sell \ Get	Liberty Reser USD
Ukash 20...49 EUR voucher value	0.76
Ukash 50...100 EUR voucher value	0.79
Ukash 20...49 GBP voucher value	0.97
Ukash 50...100 GBP voucher value	1.00
Cashu USD	0.85

UKASHX.COM
SELL UKASH - PAYSAFECARD

Ukash exchange

Information

paysafecard
pay.cash, paysafe.

Sell PaySafeCard instant to
wmz, wmr, wme, wmu, lr, pm, liqpay, visa, paypal, okpay, moneybookers, paxum, alertpay.

Psc convert rates

- 1 EUR = 0.79 WM WMZ
- 1 EUR = 0.61 WM WME
- 1 EUR = 6.18 WM WMU
- 1 EUR = 25.46 WM WMR
- 1 EUR = 0.82 PM USD
- 1 EUR = 0.61 PM EUR
- 1 EUR = 0.80 LR USD
- 1 EUR = 0.61 LR EUR
- 1 EUR = 0.76 LiqPay USD
- 1 EUR = 24.187 LiqPay RUR
- 1 EUR = 5.871 LiqPay UAH
- 1 EUR = 0.76 Visa USD
- 1 EUR = 24.187 Visa RUR
- 1 EUR = 0.76 Visa VIR
- 1 EUR = 0.76 PayPal USD
- 1 EUR = 0.76 Paxum USD
- 1 EUR = 0.76 Alertpay USD
- 1 EUR = 0.76 Oknav USD

english

Paysafecard Ukash Cashu FAQ Register Login

PaySafeCard

SELL UKASH **SELL PAYSEFECARD** **SELL CASHU**

Paysafecard Instant exchange - Selling of Paysafecard for PayPal, WebMoney etc

How to exchange?

1. Enter pin's data. The voucher consists of 16 numbers and face value (sum), begins on «0». For example 0123-1234-1234-1234
2. Enter the value of voucher and select pin's currency (amount of exchange will be appeared automatically).
3. Select preferable ecurrency and enter your purse/account/visa number along with e-mail for confirmation.
4. Push "Submit vouchers". Usually exchange takes up to 24 hours, but we can take some time (48 hours) to process it

PIN: 1

Value * Currency: EUR Password (if exists)

Add voucher

WebMoney WMR You get: 0	WebMoney WMZ You get: 0	WebMoney WME You get: 0	WebMoney WMU You get: 0
PerfectMoney USD You get: 0	PerfectMoney EUR You get: 0	Liberty Reserve USD You get: 0	Liberty Reserve EUR You get: 0
VISA USD You get: 0	VISA RUR You get: 0	VISA VIRTUAL You get: 0	PayPal USD You get: 0

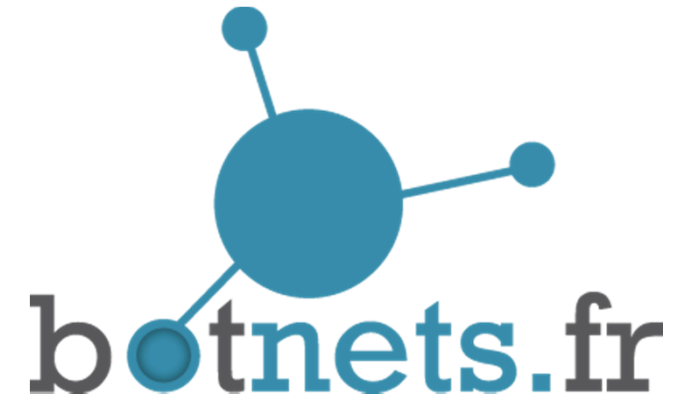
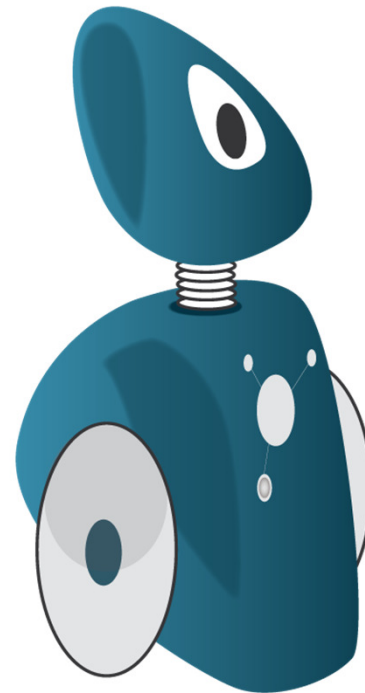
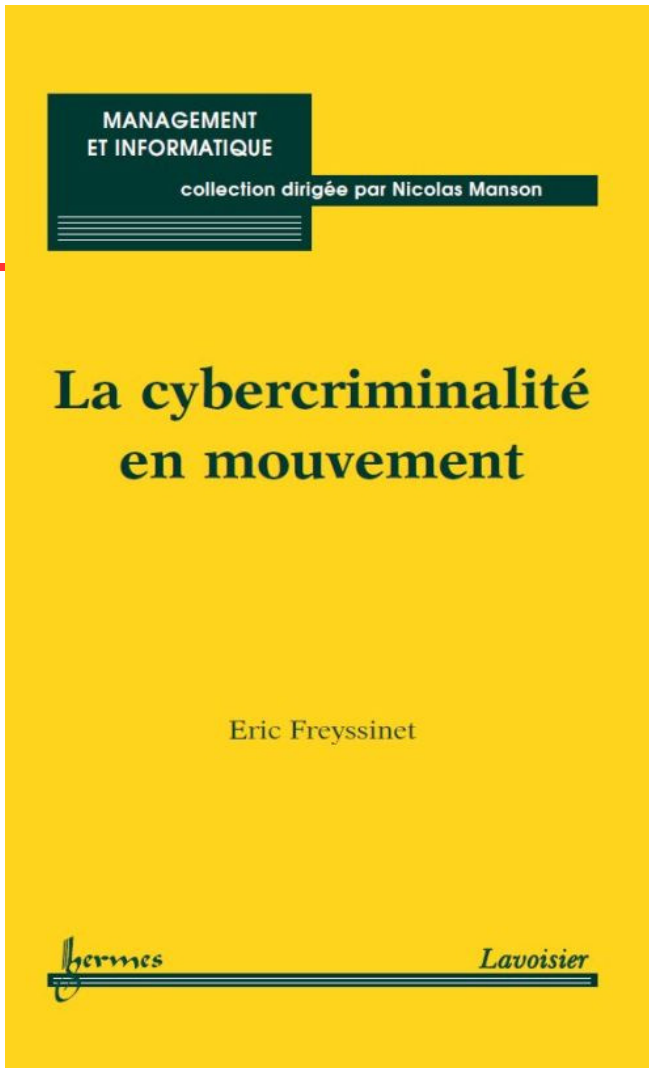
A vivid ecosystem

- Distribution of a ransomware through Skype
 - <http://techcrunch.com/2012/10/08/ransomware-worm-now-spreading-on-skype/>
 - “lol is this your new profile pic?
h__p://goo.gl/{BLOCKED}5q1sx?img=username”
- The Sality botnet was used to scan the whole IPv4 address space for SIP servers (02/2011, presented 2012 by UCSD)
 - <http://www.h-online.com/security/news/item/Botnet-maps-the-entire-internet-1725674.html>
- Botnets distributing other botnets
- Disposable botnets
- The exploit kit war (latest around... Cool Exploit Kit (<http://malware.dontneedcoffee.com/2012/10/newcoolek.html>))

Work to come

- Refine the classification
- Comparison of operations against botnets (public, private, working groups, etc.)
 - Technical issues
 - Legal issues
- National and international mitigation projects
- Detection of malware activity inside networks
 - By operators
 - By companies

Questions



The logo and the robot are a creation of @sopicgraph

[@botnets_fr](#)

[@ericfreyss](#)

<http://blog.crimenumerique.fr/>