OS OBJECTIF SÉCURITÉ
Architecte de la sécurité informatique

Démonstration pratique d'une infection

10 novembre 2017

Philippe Oechslin
Objectif Sécurité

Par où viennent les attaques ?

- La messagerie reste un canal privilégié pour les attaques
- Quelques exemples:
  - Hameçonnage (Phishing)
  - Rançongiciels (Ransomware)
  - Ingénierie sociale
  - Chevaux de Troie

Campagne de phishing du 9.02.16

De KANTONAL BANK <e-banking.sicherheit@kantonalbank.ch>
Sujet **e-BANKING SICHERHEIT - DRINGEND** 04:2
Réponse à e-banking.sicherheit@kantonal.ch
Pour Recipients <e-banking.sicherheit@kantonalbank.ch>

KANTONAL BANK
Postfach
8010 Zürich
10-02-2016

Sehr geehrter Kunde,

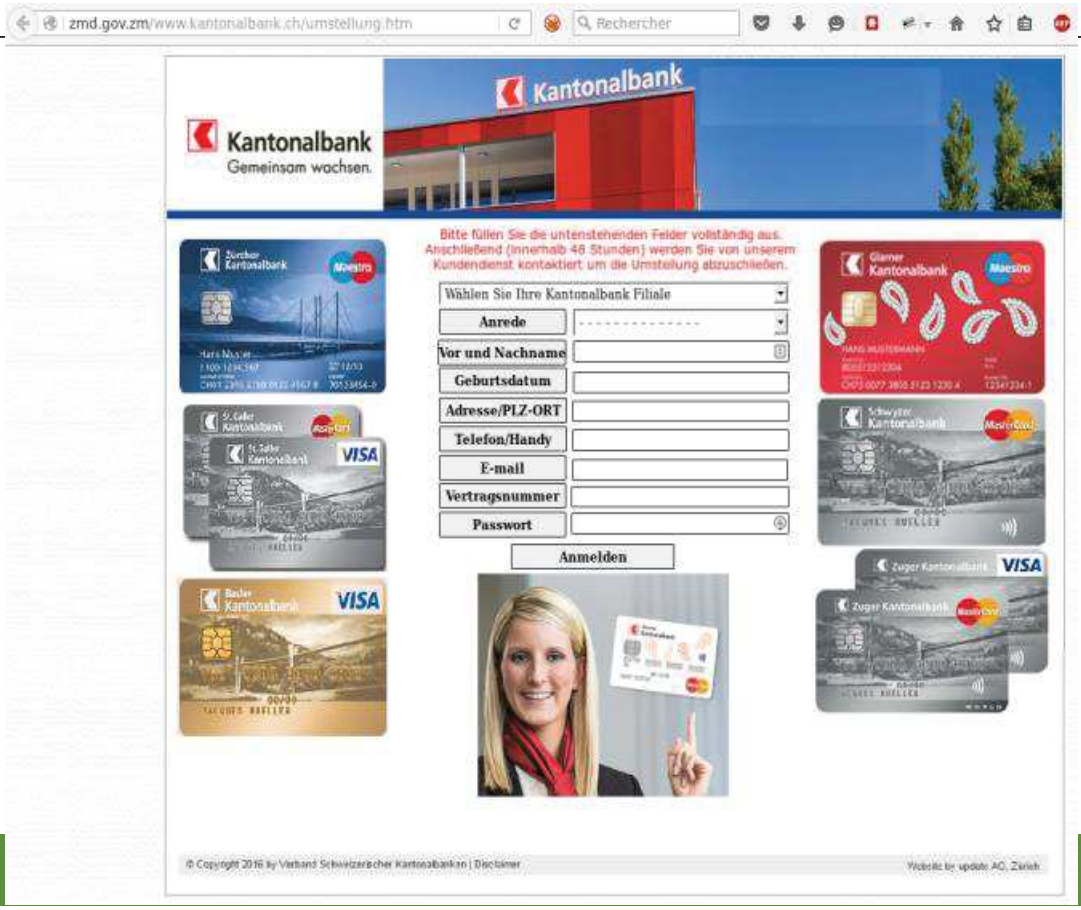
Bitte beachten Sie, dass Ihr e-banking-Zugang bald abläuft. Um diesen Dienst weiterhin nutzen zu können, klicken Sie bitte auf den untenstehenden Link um Ihren Zugang manuell mit unserem Sicherheits-Update zu aktualisieren:

klicken Sie hier

Nach Vervollständigung dieses Schrittes werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos kontaktiert.

Beim e-banking haben Sie per Mausklick alles im Griff! Mit dem komfortablen e-banking Ihrer Kantonal Bank haben Sie schnellen und problemlosen Zugang zu Ihrem Girokonto und erledigen Überweisungen und Daueraufträge bequem per Mausklick. Das e-banking
bietet aber noch viele weitere Vorteile.

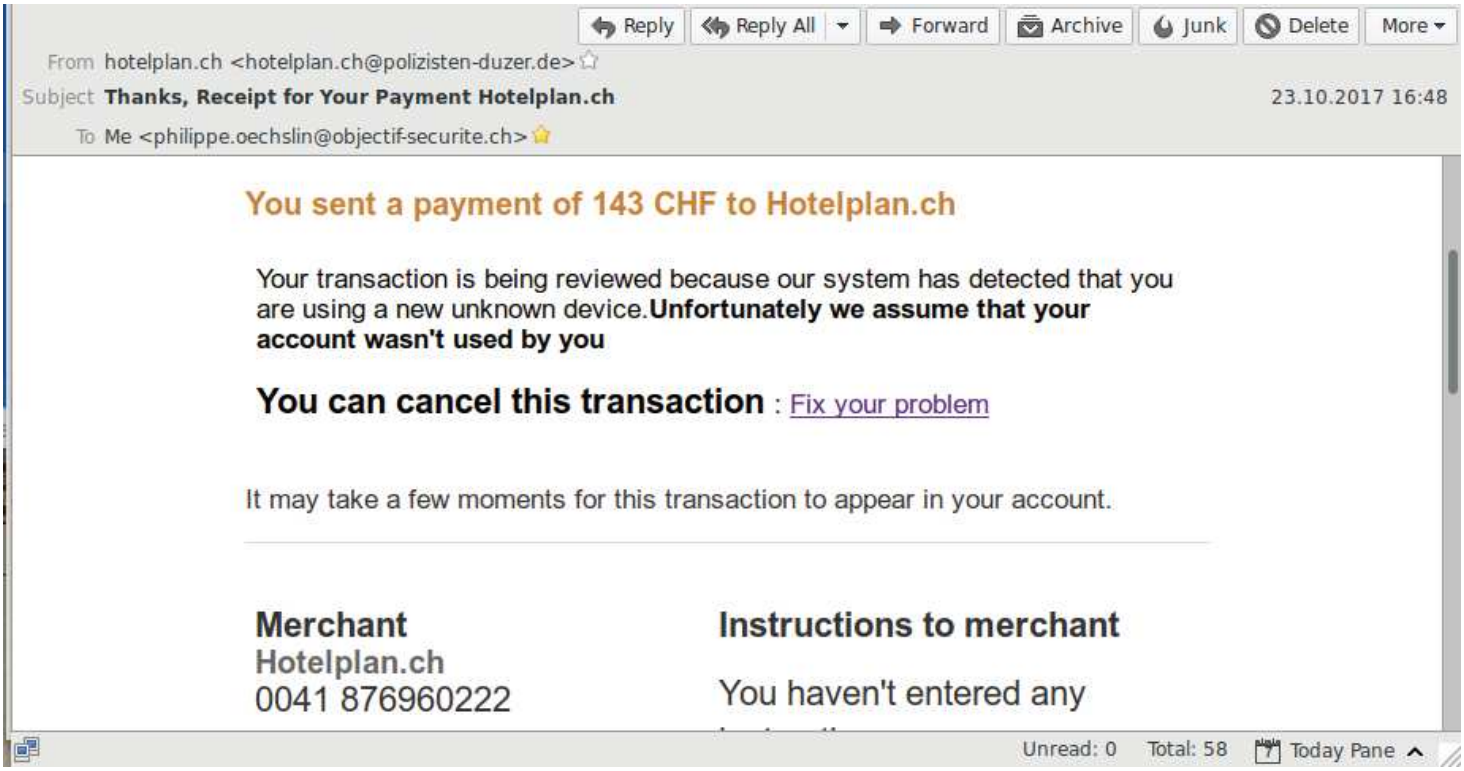
Campagne de phishing du 9.02.16



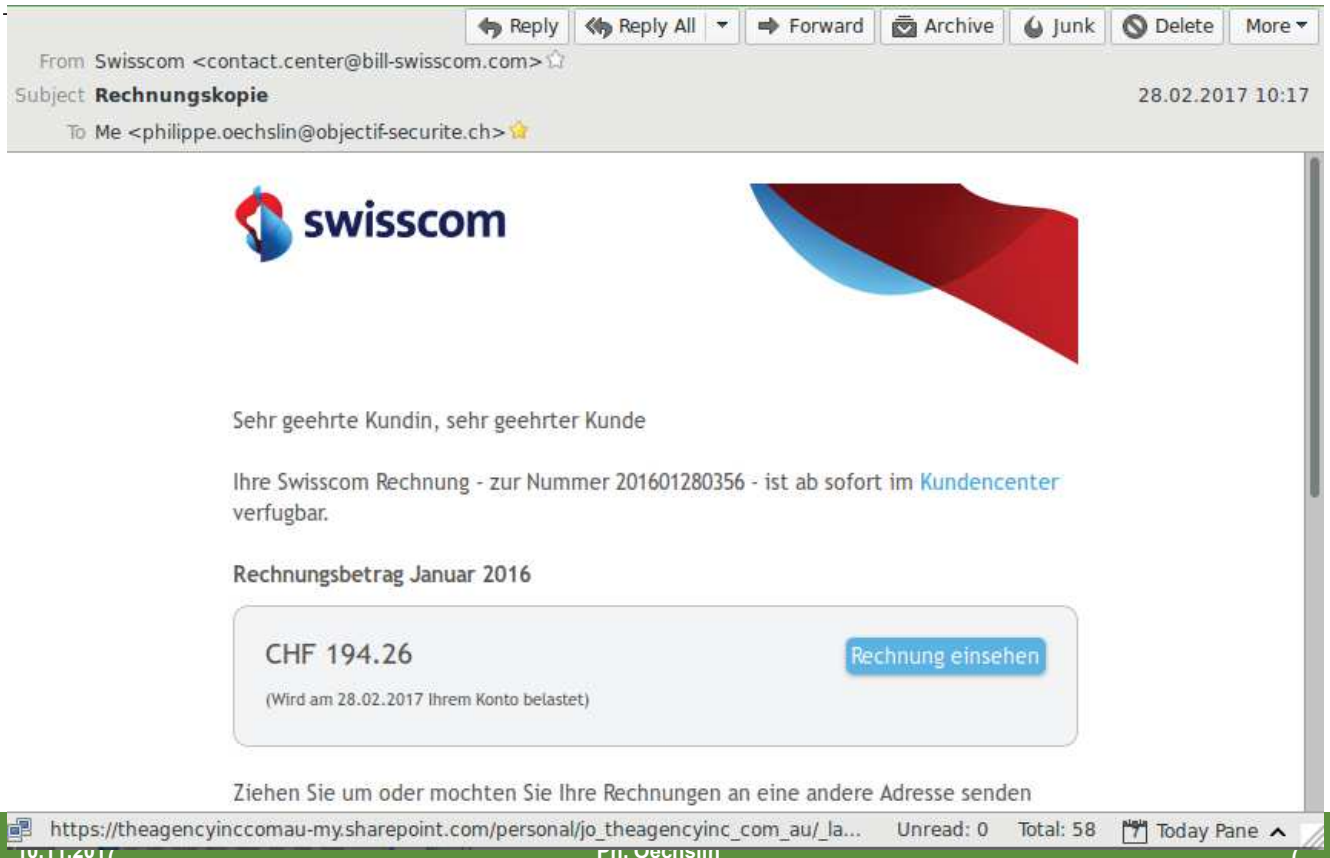
Campagne de phishing du 9.02.16

```
Received: from epfl.ch (128.178.50.68) by EWA8.intranet.epfl.ch
 (128.178.224.63) with Microsoft SMTP Server (TLS) id 14.3.248.2; Wed, 10 Feb
 2016 05:07:05 +0100
Received: by mailcleaner3 stage2 with id 1aTM3L-00080V-R8   for
 <oechslin@intranet.epfl.ch>; Wed, 10 Feb 2016 05:06:55 +0100
Received: from smtp1.epfl.ch ([128.178.166.2])  by epfl.ch stage1 with esmtp
    (Exim MailCleaner)  id 1aTM3L-00080E-Kl     for <oechslin@intranet.epfl.ch>
    from <e-banking.sicherheit@kantonalbank.ch>; Wed, 10 Feb 2016 05:06:55 +0100
Received: (qmail 16278 invoked by alias); 10 Feb 2016 04:06:55 -0000
X-MailCleaner-SPF: none
Delivered-To: spamf-philippe.oechslin@epfl.ch
Received: (qmail 16264 invoked by uid 107); 10 Feb 2016 04:06:55 -0000
X-Virus-Scanned: ClamAV
Received: from mail.karatay.edu.tr (HELO mail.karatay.edu.tr) (95.183.232.25)
 (TLS, DHE-RSA-AES256-SHA cipher)  by smtp1.epfl.ch (AngelmatoPhylax SMTP
 proxy) with ESMTPS; Wed, 10 Feb 2016 05:06:55 +0100
Received: from localhost (localhost.localdomain [127.0.0.1])    by
 mail.karatay.edu.tr (Postfix) with ESMTP id DB61015835D6;  Wed, 10 Feb 2016
 05:25:01 +0200 (EET)
Received: from mail.karatay.edu.tr ([127.0.0.1])    by localhost
 (mail.karatay.edu.tr [127.0.0.1]) (amavisd-new, port 10032)    with ESMTP id
 P0VGXy69Re5Z; Wed, 10 Feb 2016 05:25:01 +0200 (EET)
Received: from localhost (localhost.localdomain [127.0.0.1])    by
 mail.karatay.edu.tr (Postfix) with ESMTP id 3360515835F6;  Wed, 10 Feb 2016
 05:25:01 +0200 (EET)
```


Phishing



Phishing

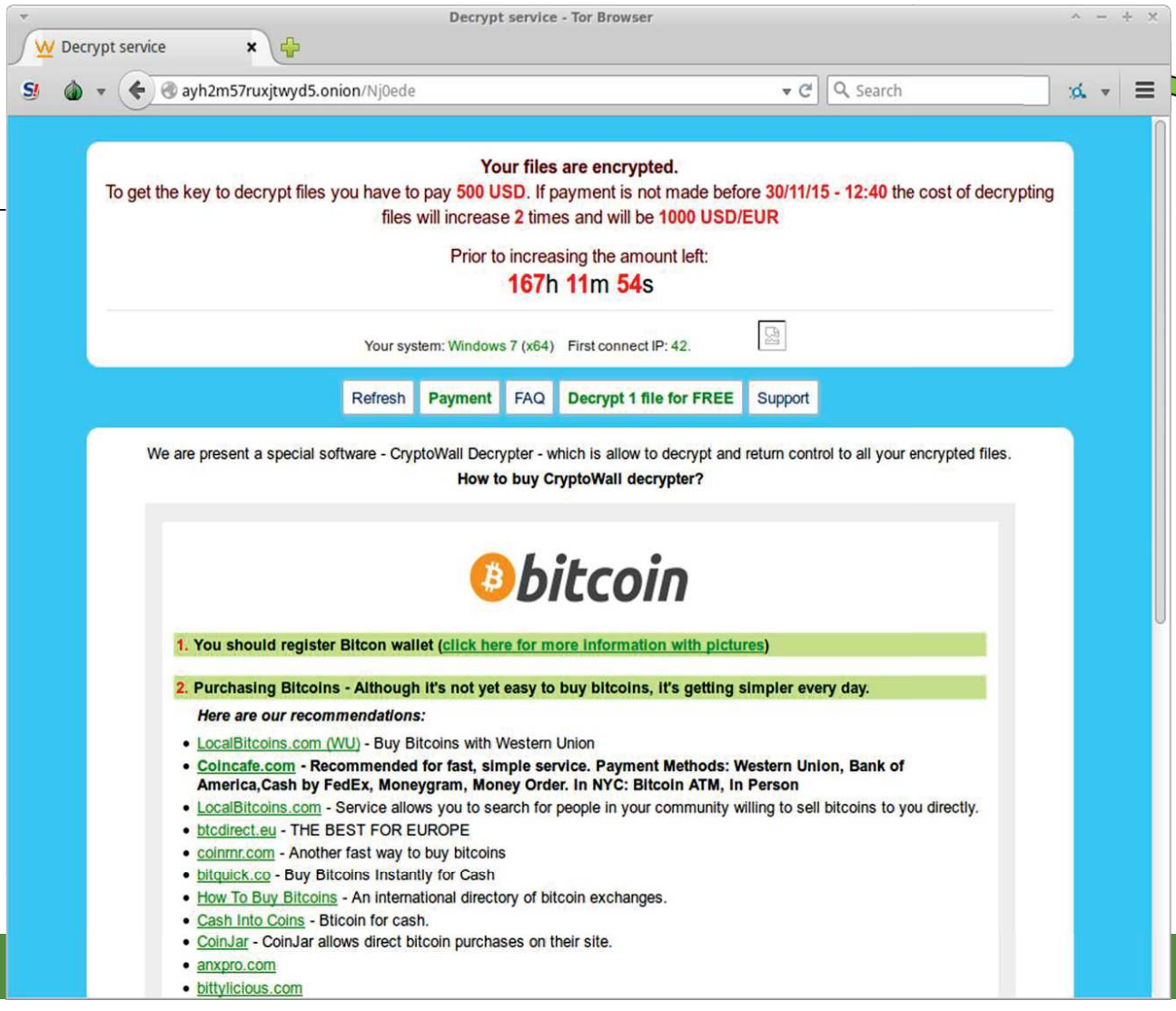


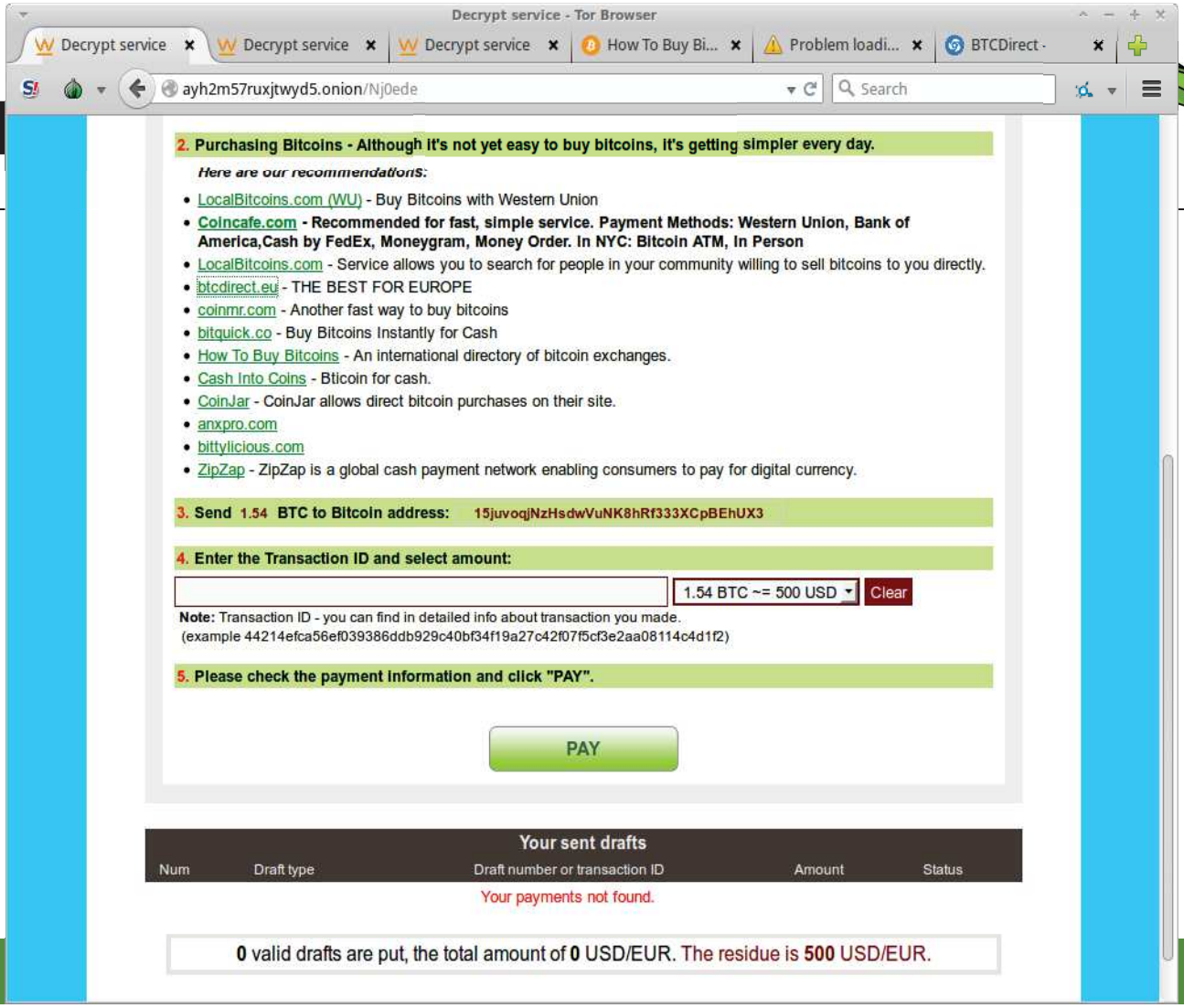
Rançongiciels

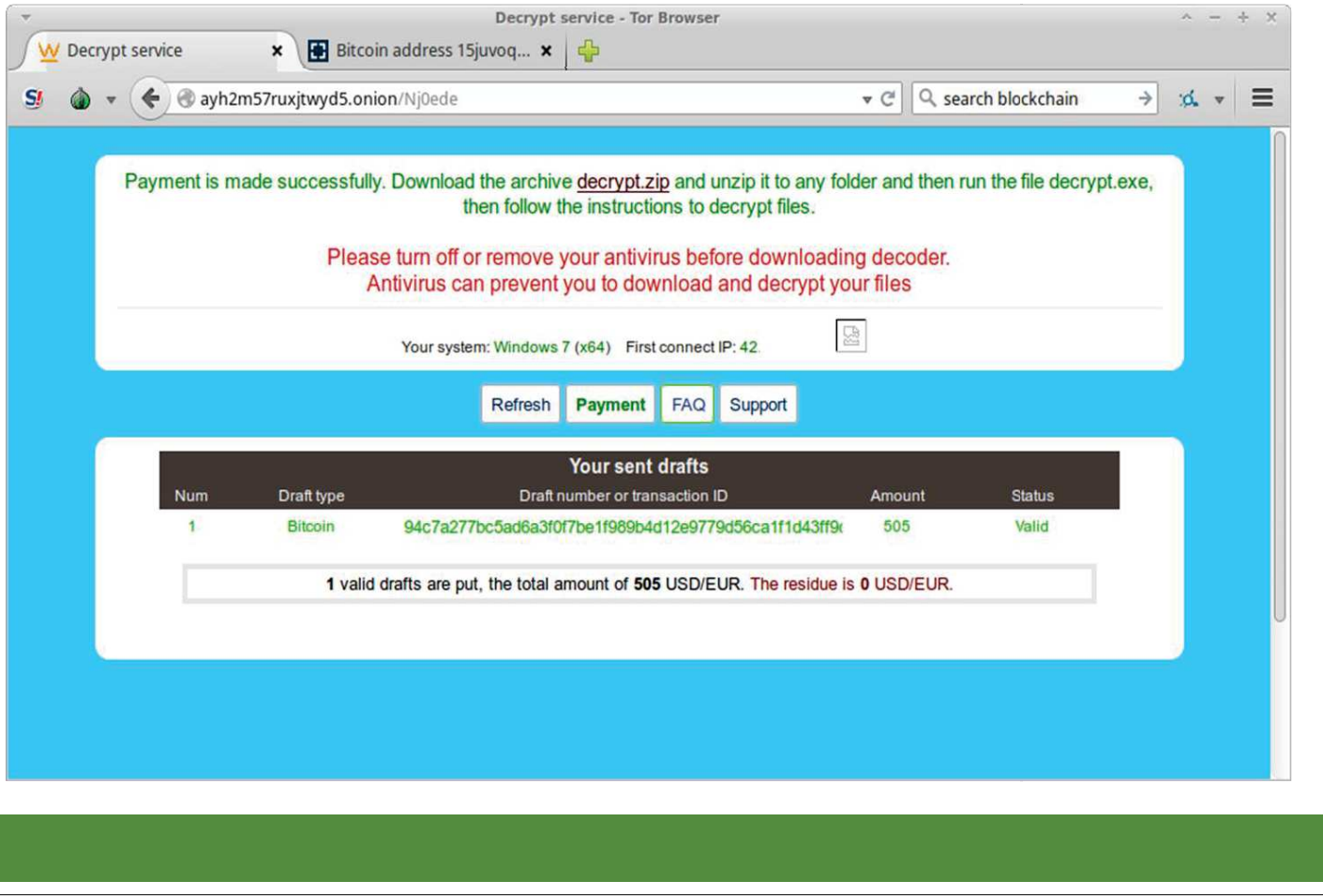
Le Matin

Rançongiciel

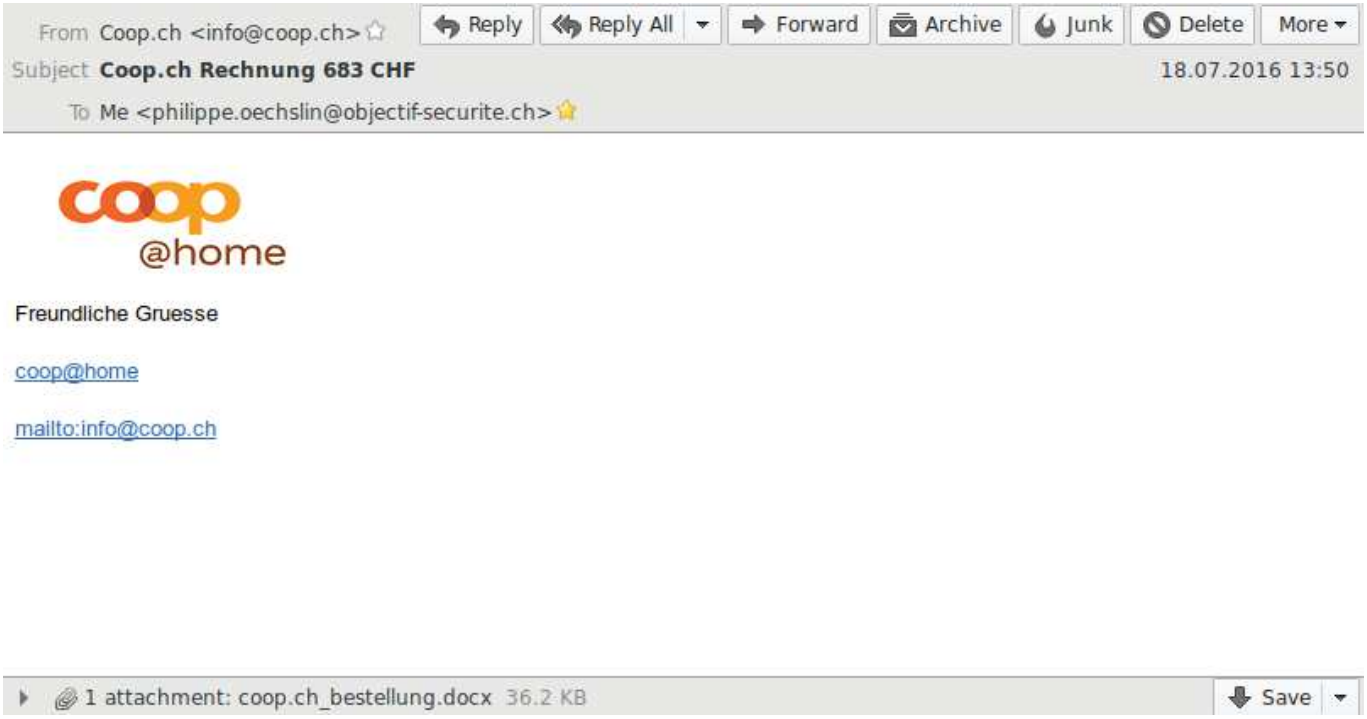
- Le logiciel chiffre tous vos fichiers
- Vous devez payer pour obtenir la clé de déchiffrement
- Un moyen simple pour les petits criminels de gagner de l'argent
- Efficace grâce
  - Au Bitcoin pour les transferts d'argent discrets
  - Au réseau TOR (darknet), pour les communications anonymes
- Le site nomoreransom.org contient des antidotes pour certains rançongiciels




Decrypt service - Tor Browser
Decrypt service
Decrypt service
Decrypt service
How To Buy Bi...
Problem loadi...
BTCDirect -
ayh2m57ruxjtwyd5.onion/Nj0ede
Search
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
btcdirect.eu - THE BEST FOR EUROPE
coinmr.com - Another fast way to buy bitcoins
bitquick.co - Buy Bitcoins Instantly for Cash
How To Buy Bitcoins - An international directory of bitcoin exchanges.
Cash Into Coins - Bticoin for cash.
CoinJar - CoinJar allows direct bitcoin purchases on their site.
anxpro.com
bittylicious.com
ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.54 BTC to Bitcoin address: 15juvoqjNzHsdwVuNK8hRf333XCpBEhUX3
4. Enter the Transaction ID and select amount:
1.54 BTC ~= 500 USD
Clear
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".
PAY
Your sent drafts
Num
Draft type
Draft number or transaction ID
Amount
Status
Your payments not found.
0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

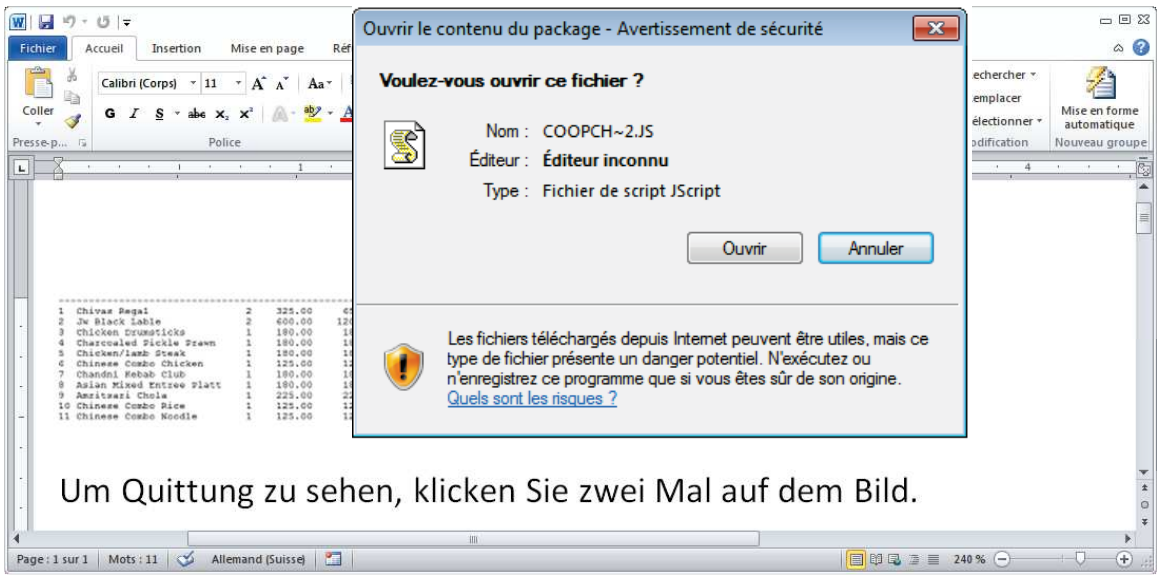

Decrypt service - Tor Browser
Decrypt service
Bitcoin address 15juvoq...
ayh2m57ruxjtwyd5.onion/Nj0ede
search blockchain
Payment is made successfully. Download the archive decrypt.zip and unzip it to any folder and then run the file decrypt.exe, then follow the instructions to decrypt files.
Please turn off or remove your antivirus before downloading decoder.
Antivirus can prevent you to download and decrypt your files
Your system: Windows 7 (x64) First connect IP: 42.
Refresh
Payment
FAQ
Support
Your sent drafts
Num
Draft type
Draft number or transaction ID
Amount
Status
1
Bitcoin
94c7a277bc5ad6a3f0f7be1f989b4d12e9779d56ca1f1d43ff9
505
Valid
1 valid drafts are put, the total amount of 505 USD/EUR. The residue is 0 USD/EUR.

Messages contenant des attachements

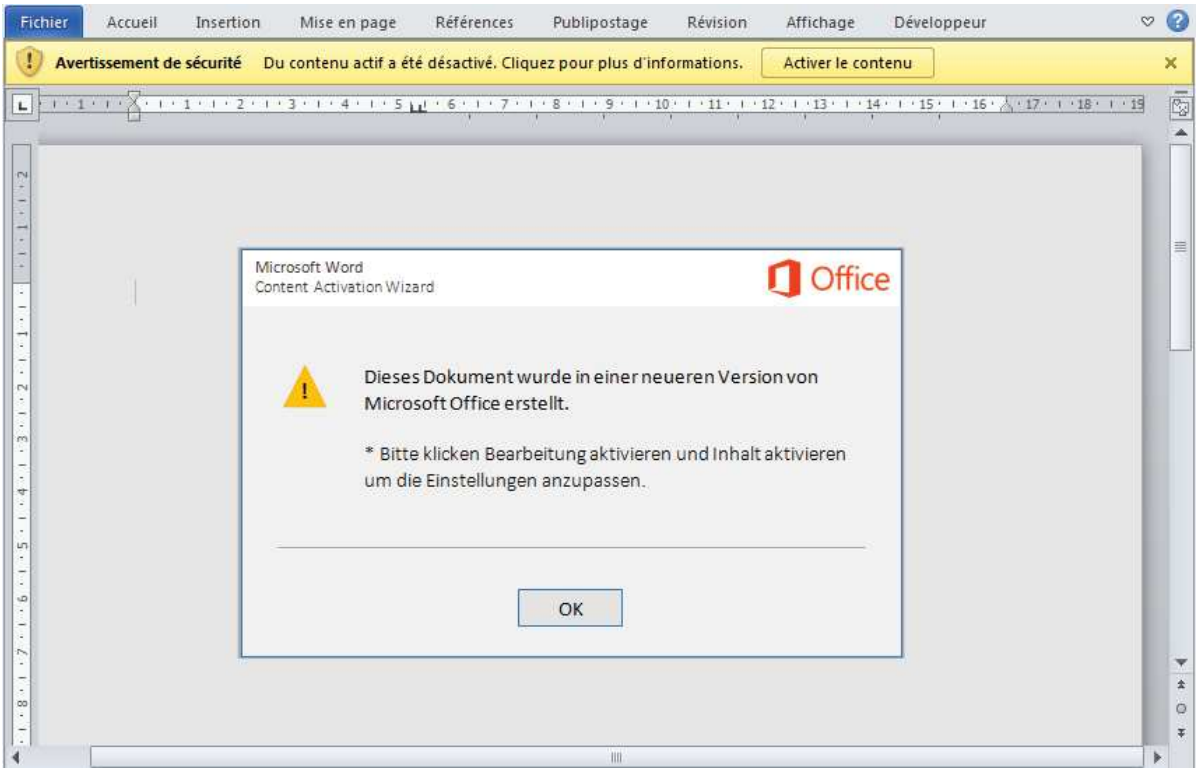


Document office contenant un maliciel

- Tous les documents Office peuvent contenir des programmes malicieux



Document office contenant une macro



Drive-by download

- Vous consultez un site web et vous êtes infecté à votre insu
  - C'est possible si vos logiciels ne sont pas à jour (ex. Flash Player, Acrobat Reader, Internet Explorer, …)
- En 2016, le site de 20 minutes contenait des publicités qui infectaient les internautes n'ayant pas mis à jour leur Flash Player

Les attaques ciblées

- Pour éviter d'être détectées, les attaques ciblées ne sont envoyées qu'a un nombre limité et choisi de victimes.
  - Elles sont inconnues des anti-virus
- Elle font usage d'**ingénierie sociale** (l'art de pirater votre esprit)

Exemple société genevoise

From: info.vergnier@impots.gouv.fr [mailto:ojiuxglk4us8jyu@s465261331.onlinehome.us]
Sent: mardi 7 mai 2013 13:58
To:
Subject: Facture n° 51700141 (derniere relance) (UPS)

Bonjour,

Suite à notre conversation téléphonique, veuillez trouver ci-joint la facture n° 51700141.
Vous pouvez la visualiser en cliquant ICI.
Nous ne pouvions pas joindre le fichier PDF du fait que notre logiciel UPS génère les factures automatiquement.
Merci de la traiter dans les plus brefs délais.

Cordialament.

Louis Vergnier

United Parcel Service France S.N.C.
Siège social
460 Rue du Valibout
78370 Plaisir
France
Tél.: 0821-233-007 (0,12€/min + surcoûts éventuels selon opérateurs)

Démonstration: *Dark Comet*

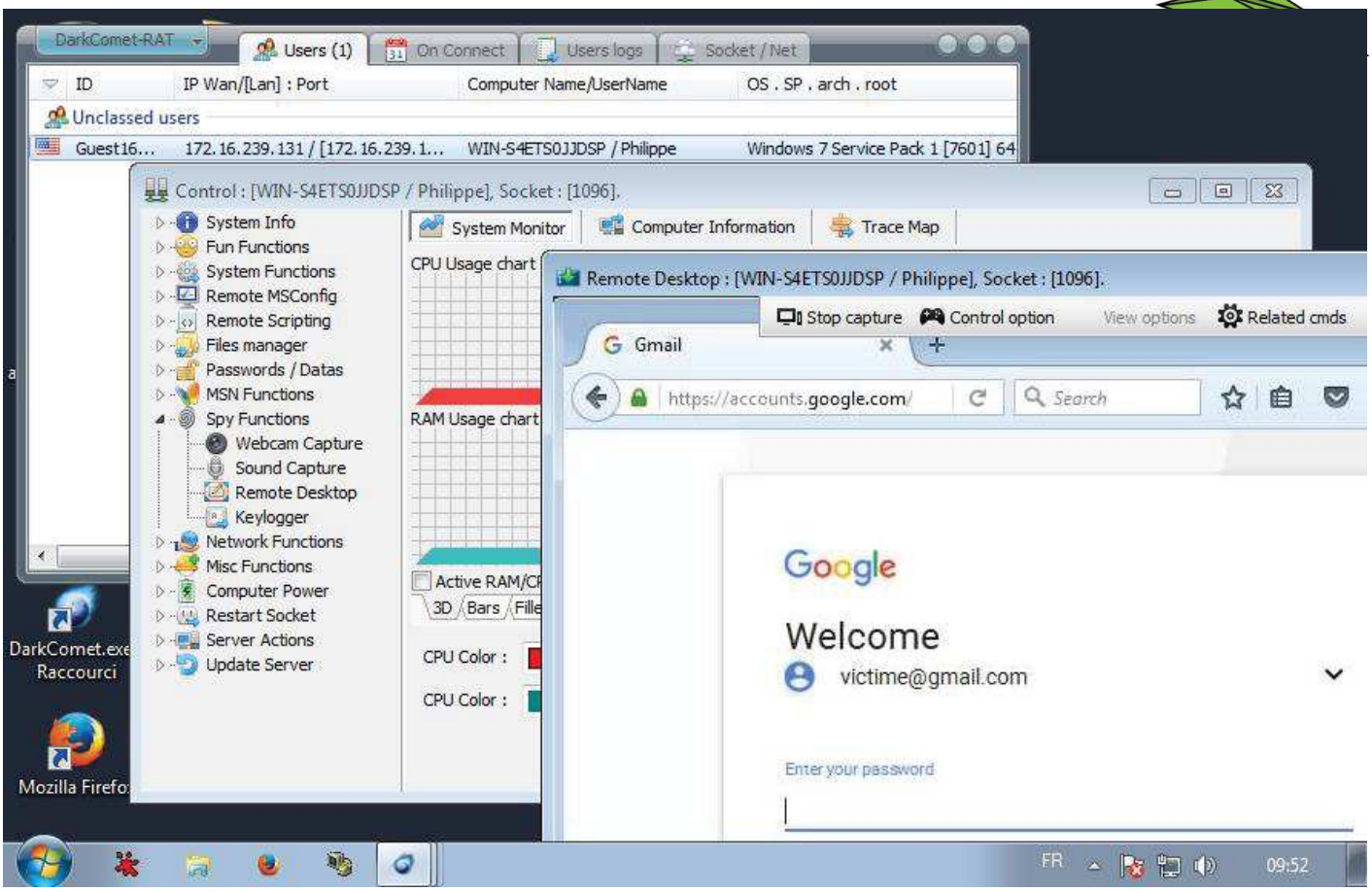
Computer spyware is newest weapon in Syrian conflict

By **Ben Brumfield**, CNN

Feb 23

DarkComet Surfaced in the Targeted Attacks in Syrian Conflict

7:24 pm (UTC-7) | by Kevin Stevens and Nart Villeneuve (Senior Threat Researchers)



Conclusions

- Vos meilleurs alliés
  - Une sauvegarde *hors-ligne* de vos données
  - Des logiciels mis à jour
  - Un antivirus à jour
  - Un esprit critique
  - De bons mots de passe (pourquoi pas un gestionnaire de mdp)
- Les bons réflexes
  - Prudence avec les emails, attachements, macros, sites inconnus
  - Informez votre service informatique en cas de doute

Conclusions

- Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants

Thucydide