



Démonstration pratique d'une infection

10 novembre 2017

Philippe Oechslin
Objectif Sécurité

10.11.2017

Ph. Oechslin

1



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](#)

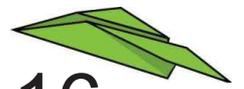
Nach Vervollständigung dieses Schrittes werden Sie von einem Mitarbeiter unseres Kundendienstes zum Status Ihres Kontos kontaktiert.

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.

10.11.2017

Ph. Oechslin

3



Campagne de phishing du 9.02.16

zmd.gov.zm/www.kantonalbank.ch/umstellung.htm

Rechercher

Kantonalbank
Gemeinsam wachsen.

Bitte füllen Sie die untenstehenden Felder vollständig aus. Anschließend (innerhalb 48 Stunden) werden Sie von unserem Kundendienst kontaktiert um die Umstellung abzuschließen.

Wählen Sie Ihre Kantonalbank Filiale

Anrede

Vor und Nachname

Geburtsdatum

Adresse/PLZ-ORT

Telefon/Handy

E-mail

Vertragsnummer

Passwort

Anmelden

© Copyright 2016 by Verband Schweizerischer Kantonalbanken | Disclaimer

Website by update AG, Zürich



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 ESMTPTS; Wed, 10 Feb 2016 05:06:55 +0100

Received: from localhost (localhost.localdomain [127.0.0.1]) by mail.karatay.edu.tr (Postfix) with ESMTPT 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 ESMTPT 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 ESMTPT id 3360515835F6; Wed, 10 Feb 2016 05:25:01 +0200 (EET)

10.11.2017

Ph. Oechslin

5



Phishing

From hotelplan.ch <hotelplan.ch@polizisten-duzer.de> ☆

Subject **Thanks, Receipt for Your Payment Hotelplan.ch** 23.10.2017 16:48

To Me <philippe.oechslin@objectif-securite.ch> ☆

You sent a payment of 143 CHF to Hotelplan.ch

Your transaction is being reviewed because our system has detected that you are using a new unknown device. **Unfortunately we assume that your account wasn't used by you**

You can cancel this transaction : [Fix your problem](#)

It may take a few moments for this transaction to appear in your account.

Merchant Hotelplan.ch 0041 876960222	Instructions to merchant You haven't entered any
---	--

Unread: 0 Total: 58 Today Pane ^

10.11.2017

Ph. Oechslin

6



Phishing

↩ Reply ↩ Reply All ➡ Forward 📁 Archive 🗑 Junk 🗑 Delete More

From Swisscom <contact.center@bill-swisscom.com> ☆
 Subject **Rechnungskopie** 28.02.2017 10:17
 To Me <philippe.oechslin@objectif-securite.ch> ☆



Sehr geehrte Kundin, sehr geehrter Kunde

Ihre Swisscom Rechnung - zur Nummer 201601280356 - ist ab sofort im [Kundencenter](#) verfügbar.

Rechnungsbetrag Januar 2016

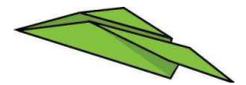
CHF 194.26

(Wird am 28.02.2017 Ihrem Konto belastet)

[Rechnung einsehen](#)

Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden

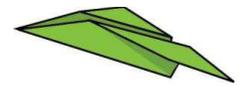
https://theagencyincomau-my.sharepoint.com/personal/jo_theagencyinc_com_au/_la...
Unread: 0 Total: 58 Today Pane



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

10.11.2017

Ph. Oechslin

9

The screenshot shows a web browser window titled "Decrypt service - Tor Browser". The address bar contains "ayh2m57ruxjtwyd5.onion/Nj0ede". The main content area has a blue background and contains the following text:

Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **30/11/15 - 12:40** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h 11m 54s

Your system: **Windows 7 (x64)** First connect IP: **42.**

Buttons: Refresh, Payment, FAQ, Decrypt 1 file for FREE, Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

bitcoin

1. You should register Bitcon wallet ([click here for more information with pictures](#))
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](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bitlyicious.com](#)

Decrypt service - Tor Browser

ayh2m57ruxjtwyd5.onion/Nj0ede

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](#) - Bitcoin 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 44214efca56ef039386ddb929c40bf34f19a27c42f07f5c3e2aa08114c4d1f2)

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

ayh2m57ruxjtwyd5.onion/Nj0ede

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	94c7a277bc5ad6a3f0f7be1f989b4d12e9779d56ca1f1d43ff9c	505	Valid

1 valid drafts are put, the total amount of 505 USD/EUR. The residue is 0 USD/EUR.



Messages contenant des attachements

From Coop.ch <info@coop.ch> ☆ Reply Reply All Forward Archive Junk Delete More

Subject **Coop.ch Rechnung 683 CHF** 18.07.2016 13:50

To Me <philippe.oechslin@objectif-securite.ch> ☆



Freundliche Gruesse

coop@home

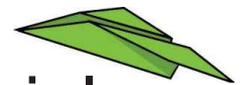
<mailto:info@coop.ch>

1 attachment: coop.ch_bestellung.docx 36.2 KB Save

10.11.2017

Ph. Oechslin

13



Document office contenant un maliciel

- Tous les documents Office peuvent contenir des programmes malicieux

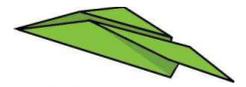
Um Quittung zu sehen, klicken Sie zwei Mal auf dem Bild.

1	Chivan Regal	2	325.00	61
2	Jw Black Lable	2	600.00	120
3	Chicken Drumsticks	1	190.00	18
4	Charcoal'd Pickle D'rawn	1	190.00	18
5	Chicken/Lamb Steak	1	150.00	14
6	Chinese Combo Chicken	1	125.00	12
7	Chandni Kebab Club	1	190.00	18
8	Asian Mixed Entree platt	1	150.00	14
9	Ameritari Chola	1	225.00	22
10	Chinese Combo Rice	1	125.00	12
11	Chinese Combo Noodle	1	125.00	12

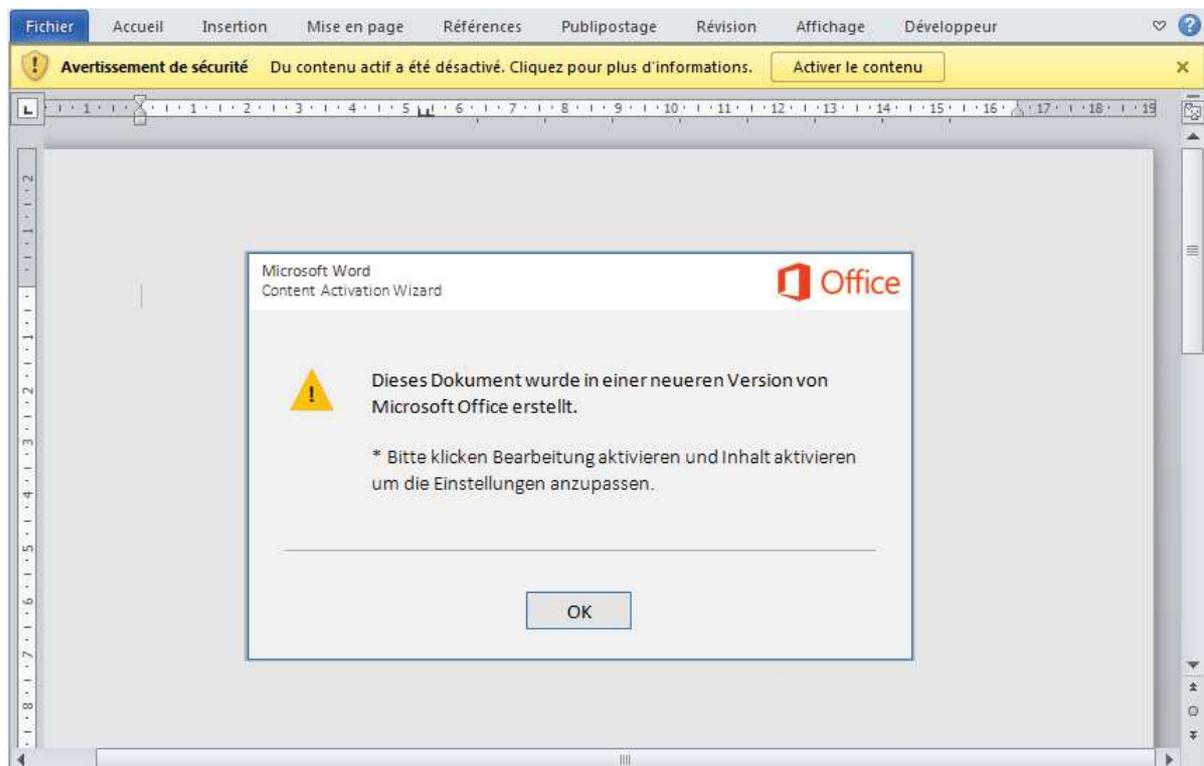
10.11.2017

Ph. Oechslin

14



Document office contenant une macro



10.11.2017

Ph. Oechslin

15



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

10.11.2017

Ph. Oechslin

16



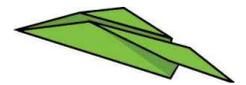
Les attaques ciblées

- Pour éviter d'être détectées, les attaques ciblées ne sont envoyées qu'à 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)

10.11.2017

Ph. Oechslin

17



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 pouvons pas joindre le fichier PDF du fait que notre logiciel UPS génère les factures automatiquement.

Merci de la traiter dans les plus brefs délais.

Cordialement.

Louis Vergnier



United Parcel Service France S.N.C.

Siège social

460 Rue du Vallbout

78370 Plaisir

France

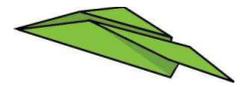
Tél.: 0821-233-007 (0,12€/min + surcoûts éventuels selon opérateurs)



10.11.2017

Ph. Oechslin

18



Démonstration: *Dark Comet*

Computer spyware is newest weapon in Syrian conflict

By Ben Brumfield, CNN



AFP/GETTY IMAGES

Feb

23

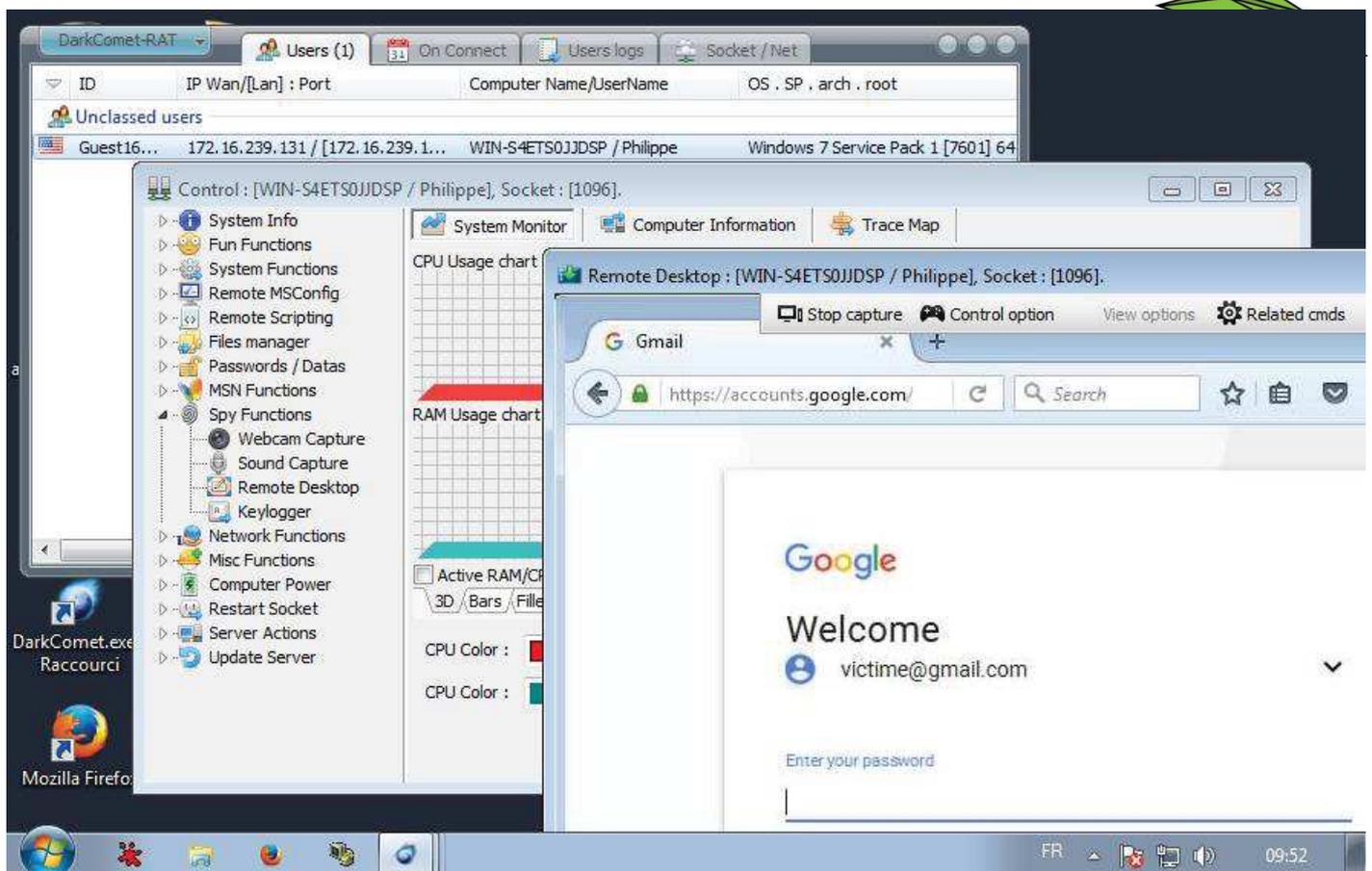
DarkComet Surfaced in the Targeted Attacks in Syrian Conflict

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

10.11.2017

Ph. Oechslin

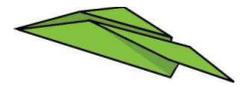
19



10.11.2017

Ph. Oechslin

20



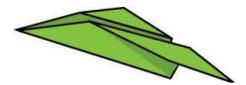
Conclusions

- o 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)

- o Les bons réflexes

- Prudence avec les emails, attachements, macros, sites inconnus
- Informez votre service informatique en cas de doute



Conclusions

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

Thucydide

