Virus Gendarmerie : variante Office Centrale de Luttre contre la criminalité – controle informationnel

EDIT : Page plutôt ancienne.
Vous trouverez des versions plus récentes sur ces deux pages :

- Nymaim / Lyposit/Adneukine : https://www.malekal.com/2013/04/11/ransomware-office-centrale-de-la-lutte-contre-la-criminalite-variante-3-nymaim/
- Urausy / Reveton : https://www.malekal.com/2012/01/10/virus-gendarmerie-activite-illicite-demelee/

Une variante qui reprends l'identité de l'Office Central de Lutte contre la criminalité avec un message : **Votre ordinateur a été bloqué par le système de contrôle automatique informationnel**
La variante initial étant du Reveton : https://www.malekal.com/2012/01/10/virus-gendarmerie-activite-illicite-demelee/

Ce dernier prétend enregistrer l'activité à travers la Webcam :

Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication

TOUTE L'ACTIVITÉ DE CET ORDINATEUR A ÉTÉ ENREGISTRÉE

SI VOUS UTILISEZ UN WEBCAM, LES VIDÉOS ET LES DESSINS ONT ÉTÉ SAUVÉS POUR L'IDENTIFICATION

Votre ordinateur a été bloqué par le système de contrôle automatique informationnel

Pourquoi ?
Cela peut se passer à cause des raisons suivantes :

1. Votre ordinateur a été utilisé pour le visionnage des sites interdits
2. Votre ordinateur a été utilisé pour le visionnage des sites comportant des éléments de pornographie d'enfants
3. Votre ordinateur a été utilisé pour le transfert de l'information interdite
4. Votre ordinateur a été utilisé pour le stockage/le visionnage du contenu sans licence

Comment corriger cela ?
Conformément à la loi sur « le contrôle informationnel et la protection d'information » de 02.01.2012 Vous devez payer une amende de montant 100 euros. Pour la commodité de payement d'amende nous offrons une forme de payement protégée à l'aide des vouchers Ukash. Vous devez acheter un voucher (des vouchers) pour le montant total de 100 euros, en enregistrer dans la forme de payement et d'appuyer le bouton « envoyer le code ».

Qu'est-ce qui se passera après l'indication de code ?
Après l'indication de code il sera vérifié par notre système et votre ordinateur sera débloquer immédiatement. Si Vous voulez indiquer 2 codes de 50 euros, il Vous faut d'abord indiquer un code et après sa confirmation indiquer le deuxième code.

Qu'est-ce qu'il faut faire au cas d'apparition des problèmes ?
Si pour n'importes quelles raisons Vous n'êtes pas arrivés à payer une amende à l'aide d'une forme de payement protégée il faut nous écrire une lettre à ce courrier cyberpolice@fbi.gov et y indiquer votre adresse ip et un code (des codes) de vaucher (-s) Ukash pour le montant 100 euros.
Après la vérification du code par notre système Votre ordinateur sera débloqué immédiatement.

Où trouver Ukash?
Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques et GAB.

Tabac presse - Ukash est disponible dans des milliers Bureaux de tabac.
Toneo - Ukash est maintenant disponible avec la Carte Toneo.
Becharge - Utilisez Ukash en lign 24/7 avec Visa/MasterCard ou Carte Bancaire.

FBI

All activity of this computer has been recorded.
If you use a webcam, videos and pictures were saved for identification.

You can be clearly identified by resolving your IP address and the associated hostname.

Your Computer has been locked!

Furthermore, possession of illegally downloaded material is punishable under Section 184 paragraph 3 of the Criminal Code and may also lead to the confiscation of the computer, with which the files were downloaded.)

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

Take your cash to one of these retail locations:

Walmart

ELEVEN

Pick up a MoneyPak and purchase it with cash at the register.

McAfee SecurityAlliance

Come back and enter your MoneyPak code to unlock your Computer.

Illegally downloaded material (MP3's, Movies or Software) has been located on your computer.

By downloading, those were reproduced, thereby involving a criminal offense under Section 106 of the Copyright Act.

unlock computer:

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200.
Payable through GreenDot Moneypak.

Please enter your Code below.

OK

green dot MoneyPak

After successful payment, your computer will automatically unlock. Failure to adhere to this request could involve criminal charges and possible imprisonment.
[illegible] the acquired GreenDot Moneypak code in the field

The downloading of copyrighted material via the Internet or music-sharing networks is illegal and is in accordance with Section 106 of the Copyright Act subject to a fine or imprisonment for a penalty of up to 3 y[illegible]

GVU

Gesellschaft zur Verfolgung von Urheberrechtsverletzungen

Bundesamt
für Sicherheit in der
Informationstechnik

Ihr Computer wurde von der GVU gesperrt.

Die ganze Tätigkeit dieses Computers ist registriert worden

Auf Ihrem Computer wurden illegal heruntergeladene Medien ("Raubkopien") gefunden.

Diese sind in Form von Musik, Filmen oder Entertainmentsoftware vorhanden.Durch den Download wurden diese Medien vervielfältigt, so dass ebenfalls eine Strafbarkeit gemäß § 106 Urhebergesetz gegeben ist.

Der Download von urheberrechtlich geschützten Medien durch das Internet oder einer Dateitauschbörse (Filesharing) ist illegal und wird gemäß § 106 Urhebergesetz mit Geldstrafe oder Freiheitsstrafe von bis zu 3 Jahren bestraft. Weiterhin ist der Besitz nach § 184 Absatz 3 StGB strafbar und kann auch zur Einziehung des Rechners führen, mit dem die Dateien heruntergeladen wurden.

Eine eindeutige identifizierung Ihrer Person ist mit hilfe Ihrer IP-Adresse und des Hostnames problemlos möglich.

Die gefundenen Raubkopien wurden verschlüsselt und in ein geschütztes Verzeichnis kopiert.

Um die Sperre aufzuheben und v/eiteren Strafrechtlichen konsequenzen aus dem Weg zu gehen, sind Sie verpflichtet eine Mahngebühr in Höhe von € 50,- zu bezahlen. Zahlbar durch unseren Payment- Partner Ukash . Nach erfolgreicher Bezahlung wird Ihr Computer automatisch entsperrt.

Um die Bezahlung durchzuführen, geben Sie den erworbenen Ukash -Code in das dafür vorgesehene Zahlungsfeld ein, wählen Sie den Wert Ihres Codes und drücken Sie anschliessend auf "Absenden". Gutschein muss mit einem Nennwert von 50 C seinAchtung! Wenn die feinen nicht innerhalb von zwei Tagen zu bezahlen, werden alle Daten an das Gericht übermittelt werden

Wenn Sie eine Netzkamera verwenden, wurden Videos und Bilder für die Identifizierung gespart

ARAL Shell TOTAL Westfalen Ukash Netto Marken-Discount ROSSMANN

Weitere Verkaufsstellen

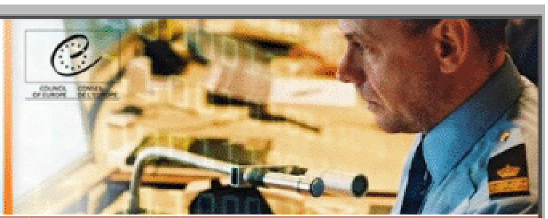
Sie bekommen Ihre paysafecard z.B. bei Rossmann Drogeriemärkten, Netto Marken-Discount, vielen Tankstellen sowie Lotto Annahmestellen und Handykartenautomaten.

1. Suchen Sie eine der angegebenen Verkaufsstellen auf
2. Fragen Sie den Händler nach einer Paysafecard im Wert von 50
3. Geben Sie den Code in das dafür vorgesehene Feld ein

Polisen

Polisen Enheten för databrott

REGERINGSKANSLIET



Datorn är låst

Datorn har blockerats

Din dator har blockerades av ett system för avtomatisk information kontroll. Varför?

Detta skulle kunna bero på en av följande skäl:

1. Datorn har använts for förbjudna websiter
2. Datorn har använts for websiter som innehåller barnpornografi
3. Datorn har använts for överforning av förbjuden information
4. Datorn har använts for att förvara/visa piratkopierat innehåll

Hur åtgärdar jag detta?

Enligt lag, om Information kontroll och skydd av information' från den 2012/01/02 skyldig måste betala böter på 100 euro.För att underlätta betalning av böterna, erbjuder vi en säker form av utbetalning med hjälp av Ukash kuponger. Allt du behöver är att köpa en voucher (ar) for totalt 100 euro, och skriva dem i formen for avbetalning, sedan klicka på 'Skicka koden'.

Vad händer när jag skickat koden?

När koden har verifierats av vårt system din dator kommer omedelbart upp. Om du anger två kodar for € 50, då måste du först ange en kod, efter att ha fått bekräftelse -nästa.

Vad händer om jag har problem?

Om du av någon anledning inte kan betala böterna via en säker form av betalning, måste du skriva ett brevvia e-post info@online-cyber-police.com och ange i brevet din adress och IP-numret (er) kupongen (ar) Ukash i mängden 100 euro. När koden har verifierats av vårt system din dator kommer omedelbart upp.

All aktivitet på den här datorn har registrerats

Pressbyrån - Nu Ukash kuponger kan köpas på mer än 300 kiosker i butiksnätet «Pressbyrån» runt om hela Sverige.

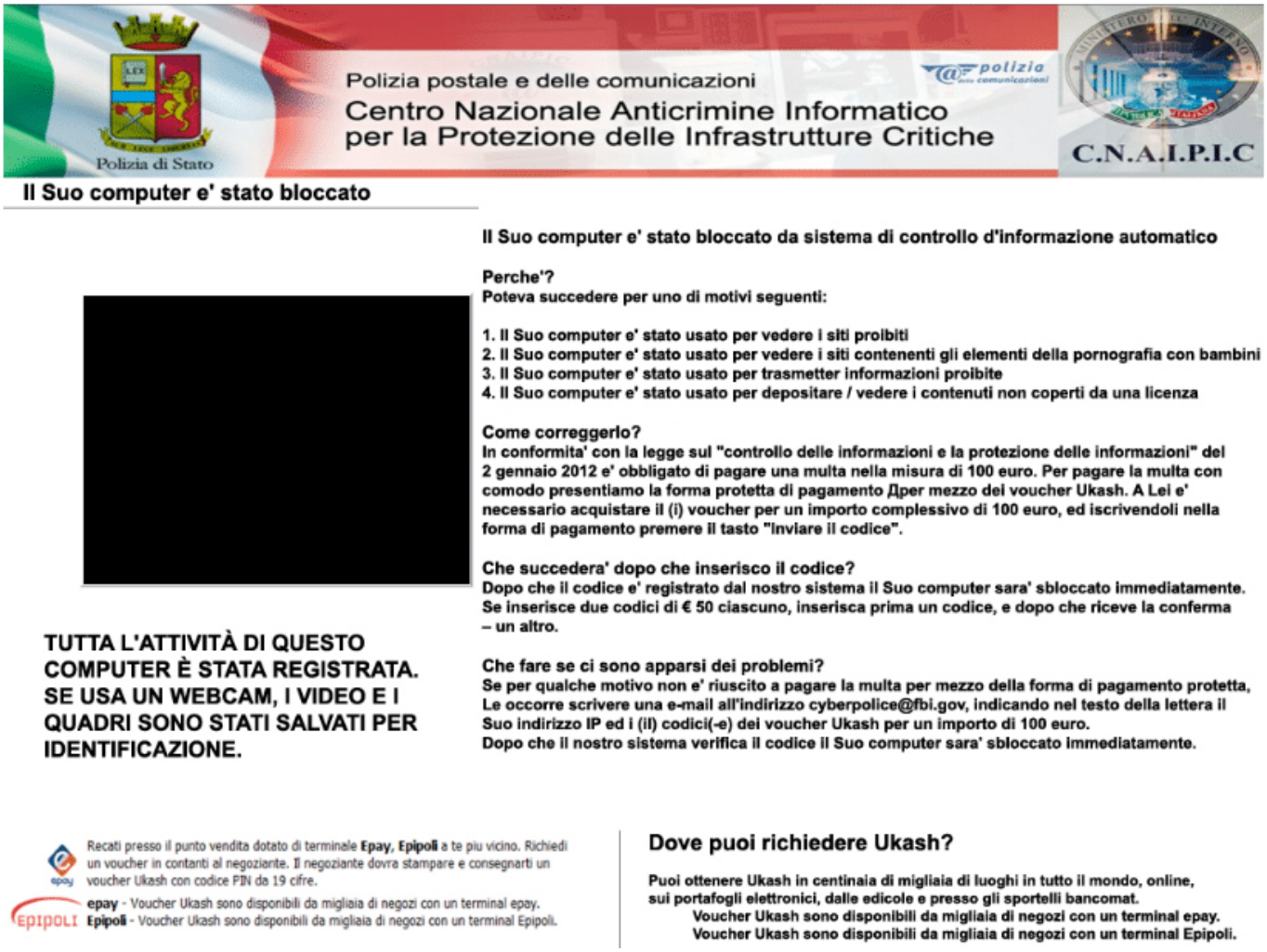
7Eleven - Ukash kuponger kan köpas på mer än 200 butiker «7Eleven», som ligger på bensinstationer Shell.

Payzone - Ukash kuponger kan köpas vid terminaler «Payzone» runt om hela Sverige.

Ukash

Var kan jag köpa Ukash?

Du kan köpa Ukash kuponger i tusentals platser runt globen, online, med hjälp av online börsan, i olika kiosker och bankomater.



Dans mon cas le malware s'installe dans C:/Documents and Settings/Mak/Application Data/System/winlogon.exe

Le malware ne touche pas les clefs Safeboot, le redémarrage en mode sans échec est donc possible.

Ce dernier est relativement simple à éradiquer.

- Redémarrer en mode sans échec : pour cela, redémarre l'ordinateur, avant le logo Windows, tapotez sur la touche F8, un menu va apparaître, choisissez Mode sans échec avec prise en charge du réseau
- Télécharger RogueKiller
- Après le pre-scan, Lancer un Scan par le bouton Scan à droite.
- Le bouton Suppression devrait être dégrisé. Cliquez

dessus.

- Redémarrer l'ordinateur

- Télécharger et installer Malwarebyte : https://www.malekal.com/tutorial_MalwareBytes_AntiMalware.php
- Mettre le à jour, fais un scan rapide, supprime tout et poste le rapport ici.
- !!! Malwarebyte doit être à jour avant de faire le scan !!!
- Supprimer bien ce qui est détecté : bouton supprimer sélection.

Après la désinfection – Tres important

Des PUPs/LPIs sont certainement installés sur votre ordinateur, ces derniers étant très répandus.
Il est conseillé de faire un scan de suppression (bouton

suppression) avec AdwCleaner.

Votre ordinateur est vulnérable car vos logiciels ne sont pas à jour – Un site hacké ou une publicité malicieuse qui conduit à un exploit sur site WEB peux infecter votre ordinateur (si votre antivirus est dans le vent, ce qui est souvent le cas).
La source de l'infection est d'avoir sur son ordinateur des logiciels non à jour.
Des logiciels permettent de vous y aider => **https://forum.malekal.com/logiciels-pour-maintenir-ses-programmes-jour-t15960.html**

Pensez à maintenir à jour vos logiciels (notamment Java, Adobe Reader et Flash), ces programmes non à jour permettent l'infection de votre système.
Plus globalement pour sécuriser son ordinateur : Sécuriser son ordinateur (version courte)

Afin de vous protéger des sites distribuant les PUPs/LPIs et Adwares et pour filtrer les régies de publicités qui distribuent des malvertising, vous pouvez installer HOSTS Anti-PUPs/Adwares : https://www.malekal.com/2012/01/10/hosts-anti-pupsadware/

Aucune aide ne sera donnée en commentaire, si vous avez besoin d'aide, créer votre propre sujet sur le forum partie VIRUS

: https://forum.malekal.com/virus-aide-malwares-vers-trojans-spywares-hijack.html