

Week 7: Supposed order confirmation delivers malware and new variants in fake extortion emails

 ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/wochenrueckblick_7.html

Navigation

22.02.2022 - Last week, the NCSC received a persistently high number of reports. Hackers are attempting to distribute remote access malware by means of bogus order notifications. In addition, there has been an increase in the spread of fake extortion emails being sent in the name of prosecution authorities, and they are now written in German as well.



Bogus order confirmations contain remote access malware

The way people shop has changed since 2019, with a shift towards online shopping. Fraudsters are taking advantage of this trend by sending bogus parcel notifications. In most cases, the emails sent involve credit card phishing or ask the recipient to purchase paysafecards and provide the codes.

A suspicious email was forwarded to the NCSC last week, and an analysis of it revealed a new modus operandi: The email contained a notification that an order had been received and that it was now being processed. Intentionally, the fraudsters did not include any references to any seller or items purchased; only a meaningless order number was listed.

Von: Pasha Shiva [REDACTED]
Gesendet: Dienstag, 1 [REDACTED]
An: [REDACTED]
Betreff: HomeRechnung

Lieber Kunde:

Ihre Bestellung wurde erfolgreich aufgegeben und Ihre Bestellung wird jetzt bearbeitet.

Sobald Ihre Bestellung bestätigt ist, wird sie versendet.

Einzelheiten :

Bestelldaten: 2/15/2022
Bestellnummer:# 049-4818-93869-216409
Zahlungsmethode: Kreditkarte

Hinweis : Ihre Bestellung wird innerhalb weniger Stunden bestätigt und versandt .
Wenn Sie diese Bestellung stornieren möchten, laden Sie bitte die Stornierung herunter und füllen Sie sie sofort aus!

Wärmste Grüße,
Danke schön
Wir hoffen, Sie wiederzusehen.

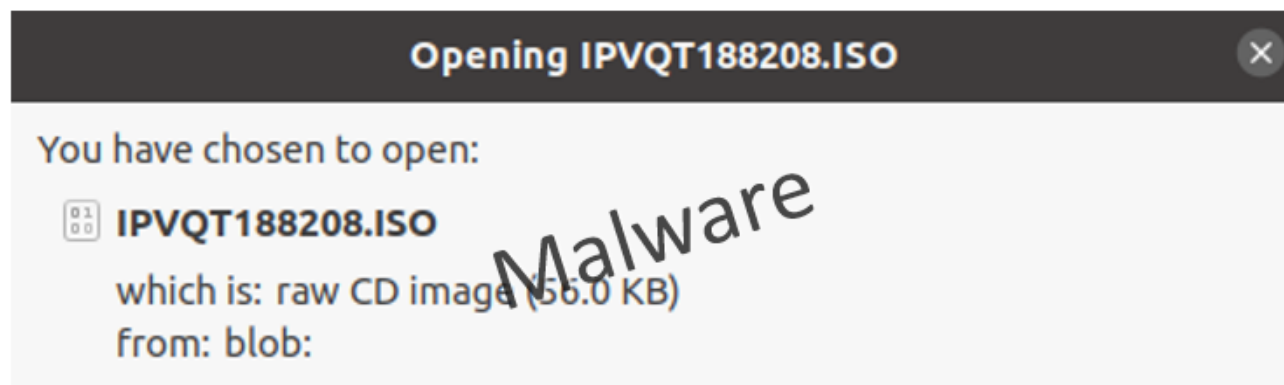
Unterstützung
Zinedine Wendall

> 1 attachment: IPVQT188208.html 76.3 KB

Generic email with the HTML attachment that leads to the malware

The attachment is an HTML file with a cryptic name. When this file is executed, the download of an additional ISO file must be permitted. This is when all alarm bells should be ringing, at the very latest.

ISO files are treated by computers like executable CDs and DVDs, and often contain installation media for games or office programmes, for example.



When the HTML file is opened, information about downloading an ISO file is displayed

In this case, the program contained malware called AsyncRAT. RAT stands for "remote access tool", which allows an attacker to access the infected computer remotely.

Target
IPVQT188208.vbs



MD5
44[REDACTED]1



Filesize
5KB

Score

10/10

SHA1

306[REDACTED]



SHA256

44a[REDACTED]



SHA512

f21[REDACTED]



Tags

asyncrat

rat

suricata

Signatures

AsyncRat



suricata: ET MALWARE Observed Malicious SSL Cert (AsyncRAT Server)



Async RAT payload



Analysis of the ISO file with an appropriate tool indicated the presence of AsyncRAT malware

Remote access to the computer gives an attacker the opportunity to steal data stored on it and also to upload and install other malware in order to be able to intercept passwords when they are entered, for example.

- **Be wary all unsolicited email notifications you receive.**
- **Be especially suspicious if you are asked to open or download a file.**
- **Never allow your computer to execute files obtained in this way.**
- **Report such cyberincidents to the NCSC and, if possible, send us the email in question.**

[NCSC-Reporting form](#)

Fake extortion emails in the name of various police authorities are now also being sent in German

In recent weeks, thousands of fake extortion emails written in French in the name of almost a dozen different law enforcement agencies were found in the email inboxes and spam folders of Swiss citizens. In France, this form of fraud has been known for years. At the end of last year, the fraudsters began to focus on the French-speaking part of Switzerland and now more and more emails of this type are appearing in Ticino (with Italian authority logos) and in German-speaking Switzerland (with German authority logos).



STRUCTURES EN COLLABORATION FEDPOL - POLICE DE SURETE & GENDARMERIE - DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Nous engageons à votre rencontre, des poursuites judiciaires peu après une saisie informatique de Cyber-infiltration pour : **Pédopornographie, Pédoophilie, Cyberpornographie et Exhibitionisme**

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal sont réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

Après enquête, nous attestons que vous avez commis ces infractions, à savoir l'acquisition, la détention, la visualisation, la transmission et la consultation d'images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d'internet (sites d'annonces, sites à caractère pornographiques, sites de rencontres, réseaux sociaux).

Lors de l'investigation, nous avons également observé que des contenus obscènes de vous étaient diffusés sur des sites web ou réseaux à forte audience, regroupant de nombreux mineurs de 16 ans.

Il est préférable de rappeler que lorsque la nudité est exposée d'une telle sorte, cela constitue un délit d'exhibition sexuelle aux regards du public et des mineurs de moins de 16 ans. Cette infraction est sévèrement punie par la Loi.


Des historiques d'images, de vidéos dénuées de vous et de mineurs, enregistrées par la Cyber-infiltration constituent des preuves de vos infractions

Vous êtes prié(e) de vous faire entendre par mail, en écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions : ceci dans un délai strict de 48 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport au Tribunal Judiciaire de votre Région, pour l'établissement d'un mandat d'arrêt à votre rencontre, qui s'ensuivra d'une arrestation immédiate par la police de votre lieu de résidence.

Vous serez ensuite fiché(e) au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias pour publication de votre personne fichée au **RNSD**.

* Veuillez adresser votre réponse à l'adresse e mail
Nicolletta.della.valle21@gmail.com

Madame NICOLETTA DELLA VALLE,
 DIRECTRICE DE FEDPOL,
 OFFICE FEDERAL DE LA POL,
 Address: Golsanplatz 1A/CH-3003 Bern

Citazione in tribunale
 Per la sezione IX su indagini giudiziarie

A vostra attenzione,
 Alla richiesta della Signora **Carla Berio De Bolle** Commissaria generale della polizia federale, eletta alla mansione di **Direttore di ERODPOA**, legata a protezione dei minori vi rivolgiamo questa convocazione. La convocazione mediante un ufficiale della polizia giudiziaria è prevista dall'articolo 399-b) del codice della procedura penale. Tale convocazione vale dinanzi al Tribunale ed è decisa dal procuratore della Repubblica.

In applicazione della disposizione dell'articolo 528 del codice penale articolo 1), **Chiamate**, allo scopo di fare commercio o distribuzione ovvero di esporli pubblicamente, fabbrica, introduce nel territorio dello Stato, acquista, detiene, espone, ovvero mette in circolazione scritti, disegni, immagini od altri oggetti occesi di qualsiasi specie e soggetto alla sanzione amministrativa pecuniaria da euro 10.000 a euro 50.000(1).

All'articolo 510 del codice penale dispone: 1) **Chiamate**, fuori dei casi preveduti dall'articolo 509 del codice penale, atti di libidine su persona o in presenza di persona minore degli anni 16, è punita con reclusione da sei mesi a tre anni.

Ci invogliamo al vostro incontro dei profili giudiziari poco dopo aver ricevuto alcune informazioni tramite al server infiltrazione per:

- Pedopornografia
- Pedofilia
- Falsificazione
- Sfilata
- Traffico

Avete commesso **infiltrazione dopo esser stati visionati su Internet (foto di annunci), visualizzazione di video a carattere pornografico, delle foto, video di nudi di minori sono Stati registrati attraverso il nostro server** con internet e costituisce delle prove delle vostre infrazioni.

Vi rivolgiamo questa e-mail siete pregati di rispondere tramite e-mail attivando la vostra giustificazione affinché sia messa in esame e verificata al fine di valutare le sanzioni questo in un tempo limite di 72 ore. Superato questo tempo limite saremo obbligati di trasmettere il nostro rapporto a signora **Francesca NANNI**, procuratrice generale di Milano e specialista di cyber criminalità a mettere un mandato d'arresto sui vostri confronti, vi mandiamo una Raccomandata con avviso di ricevimento mediante il posto di carabinieri più vicino al luogo di abitazione e sarete pubblicati al registro nazionale dei delinquenti sessuali. In tale situazione il vostro caso sarà trasferito alle associazioni di lotta contro la pedofilia ed al media per pubblicazione di persone denunciate al nudo.

NB: In mancanza del rispetto della procedura e della scadenza della lettera di convocazione sarete mandati tramite Corriere postale.
 Coordinamento:
 Lamberto GIANNINI
 DIRETTORE GENERALE INTERPOL
 Ufficio di Polizia
 POLIZIA CRIMINALE
 Comodo provinciale carabinieri Cremona (Italia) via Dante GARBIZARIA



BUNDESPOLIZEI

Code Einheit	Num Pr	Jahr	Num Ordner	Gerechtigkeit
04351	01542	2022		

VORUNTERSUCHUNG ANWÄRTSPROZESS
 AKTE NR. 245640GN81 MIT EINER ANKLAGE

Num Block 1/1
 Blatt 1/1

VORLADUNG VOR GERICHT

Ich bin Frau **Dagmar Busch** Generaldirektorin der nationalen Polizei. Ich kontaktieren Sie kurz nach einer Cyber-Infiltration (Erfahrung, insbesondere in Bezug auf Kinderpornografie, Pornografie, Cyber-Pornografie), um Ihnen mitzuteilen, dass Sie Gegenstand mehrerer aktueller Strafverfahren sind:

- CYBERPORNOGRAFIE
- PORNOGRAFISCHE SEITE
- KINDERPORNOGRAFIE

Sie werden gebeten, sich per E-Mail zu melden und uns Ihre Belege zu schreiben, damit wir sie untersuchen und überprüfen können, um die Sanktionen zu bewerten; dies muss innerhalb von 48 Stunden geschehen. Nach Ablauf dieser Frist müssen wir unseren Bericht an die stellvertretende Staatsanwältin für Cyberkriminalität am Landgericht Hamburg weiterleiten, damit diese einen Haftbefehl gegen Sie ausstellt, bis an die Ihrem Wohnort nächstgelegene Gendarmerie weiterleitet, damit Sie verhaftet und als Sexualstraftäter registriert werden können. Warten auf Ihren Nachweis zur Eröffnung des PV (Protokoll).

GENERALDIREKTION: brigade.protection14@gmx.fr
 jetzt sind Sie gewarnt

Frau Dagmar Busch,
 BUNDESPOLIZEIDIREKTORIN
 GENERALDIREKTION INTERPOL
 Anschrift: Golsanplatz 1A/CH-3003 Bern



Bogus extortion emails in different languages, here in French, Italian and German

The emails make drastic accusations against the recipients in the name of randomly composed prosecution authorities. The aim is to get the recipients to reply to the email address mentioned in the letter. If someone contacts the fraudsters, they promise to drop the alleged "accusations" against payment of a high four-digit sum of money. However, this is not the end of the story for people who do pay the amount requested. In these cases, the fraudsters keep coming back with new demands for money until the victim finally realises the fraud and stops paying. The resulting loss can be very considerable.

Since the email addresses used by the fraudsters are crucial for communicating with the victims and sending such messages en masse, the NCSC reports the email addresses used by the attackers to the corresponding email providers. Currently, these are mostly student email accounts at various universities. In some cases, the NCSC's rapid intervention stopped further emails from being sent, thus averting potential loss.

- Do not allow yourself to be put under pressure and do not react to such threats.
- Ignore such messages and mark them as spam.

Current statistics

Last week's reports by category:

Current figures

Last modification 22.02.2022