仮想通貨を要求する
セクストーションスパム

株式会社カスペルスキー　情報セキュリティラボ　大沼千亜希

JSAC 2019 Jan.18

#Who am I?

Chiaki Onuma

- 2008年から株式会社カスペルスキー勤務
- フィッシングサイト、偽ショッピングサイト、マルウェアを製品で検知できるように登録
- Kaspersky Daily（ブログ）執筆（たまに）
- CSIRTのお仕事もしています
- ねこがすき

#Agenda

1. 概要
2. 詳細
3. 被害額
4. 今後の展開

#Agenda

1. 概要
2. 詳細
3. 被害額
4. 今後の展開

Sex + Extortion

(性的な) + (ゆすり・恐喝)

はったりだけでぼろ儲け

スパムメール & Bitcoinアドレス

差出人 [redacted]@kaspersky.co.jp ☆

返信 | 全員に返信 | 転送 | その他

件名 **すぐにお読みください！**

2018/09/21 2:21

宛先 [redacted]@kaspersky.co.jp ☆

こんにちは！

あなたは私を知らないかもしれませんし、なぜあなたはこの電子メールを受け取っているのだろうと思っていますか？
この瞬間、私はあなたのアカウント([redacted]@kaspersky.co.jp)をハッキングし、そこからメールを送りました。私はあなたのデバイスに完全にアクセスできます！
実際に、私は大人のvids(ポルノ資料)のウェブサイトにマルウェアを置きました。あなたは何を知っていますか、あなたはこのウェブサイトを訪れて楽しんでいました。
あなたがビデオクリップを見ている間、インターネットブラウザはRDP(Remote Desktop)として動作するようになりました。
それは私にあなたのスクリーンとウェブカメラへのアクセスを提供するキーロガーを持っています。
その直後に、私のソフトウェアプログラムはあなたのメッセンジャー、ソーシャルネットワーク、そして電子メールから連絡先全体を集めました。

私は何をしましたか？
私は二重スクリーンビデオを作った。最初の部分はあなたが見ていたビデオを表示しています(あなたは良いと奇妙な味を持っている)、2番目の部分はあなたのウェブカメラの記録を示しています。
まさにあなたは何をすべきですか？

まあ、私は$ 570が私たちの小さな秘密の公正な価格だと信じています。あなたはBitcoinによる支払いを行います(これはわからない場合は、Googleの「ビットコインの購入方法」を検索してください)。
私のBTC住所: 18UytoFiFoJo9fqJA3T76oPvXHvmEvUMog
(それはcAsEに敏感なので、コピーして貼り付けてください)

注意:
お支払いを行うには2日以内です。
(この電子メールメッセージには特定のピクセルがあり、この瞬間にこの電子メールメッセージを読んだことがわかります)。

私がBitCoinを手に入れなければ、私は間違いなく、家族や同僚などあなたのすべての連絡先にビデオ録画を送ります。

しかし、私が支払いを受けると、すぐにビデオを破壊します。

これは非交渉可能なオファーですので、このメールメッセージに返信して私の個人的な時間を無駄にしないでください。

次回は注意してください！より良いウイルス対策ソフトウェアを使用してください！
さようなら！

あなたの（ポルノに関わる）姿を録画した

データを破棄してほしければ
Bitcoinを支払え

Sextorsionメールを受信した一般の人（日本人）の反応

From: [redacted]@yahoo.co.jp <[redacted]@yahoo.co.jp> on behalf of [redacted]
Sent: Friday, January 11, 2019 10:01 AM
To: [redacted]
Subject: [redacted]

Dear [redacted],

Akemashite Omedeyoh Gozaimasu.

Well, I receaved this mail.
What's this ?

Wa My tablet of my house infected when I saw the adult sight ?
Yse,I am a man.
But I am using the Kaspersky.

Daijoubu kashira ?

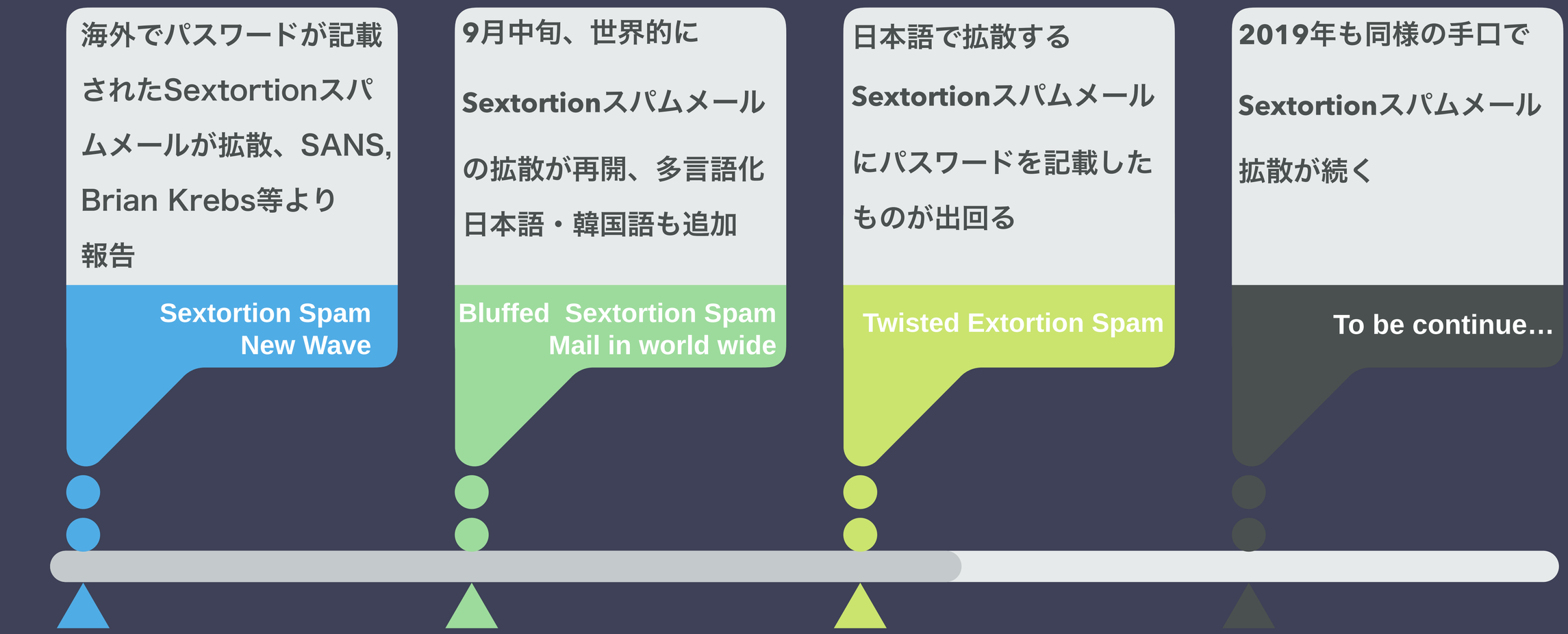
こんなメールが来たんだけど、これはなに？
僕のタブレットでアダルトサイトを見たから？
だって、男だからさ。
でも、僕はカスペルスキー使ってるよ。
大丈夫かな？

“高度なマルウェアを使わなくても
スパムメール送信だけで
攻撃者が収益を上げている”

#Agenda

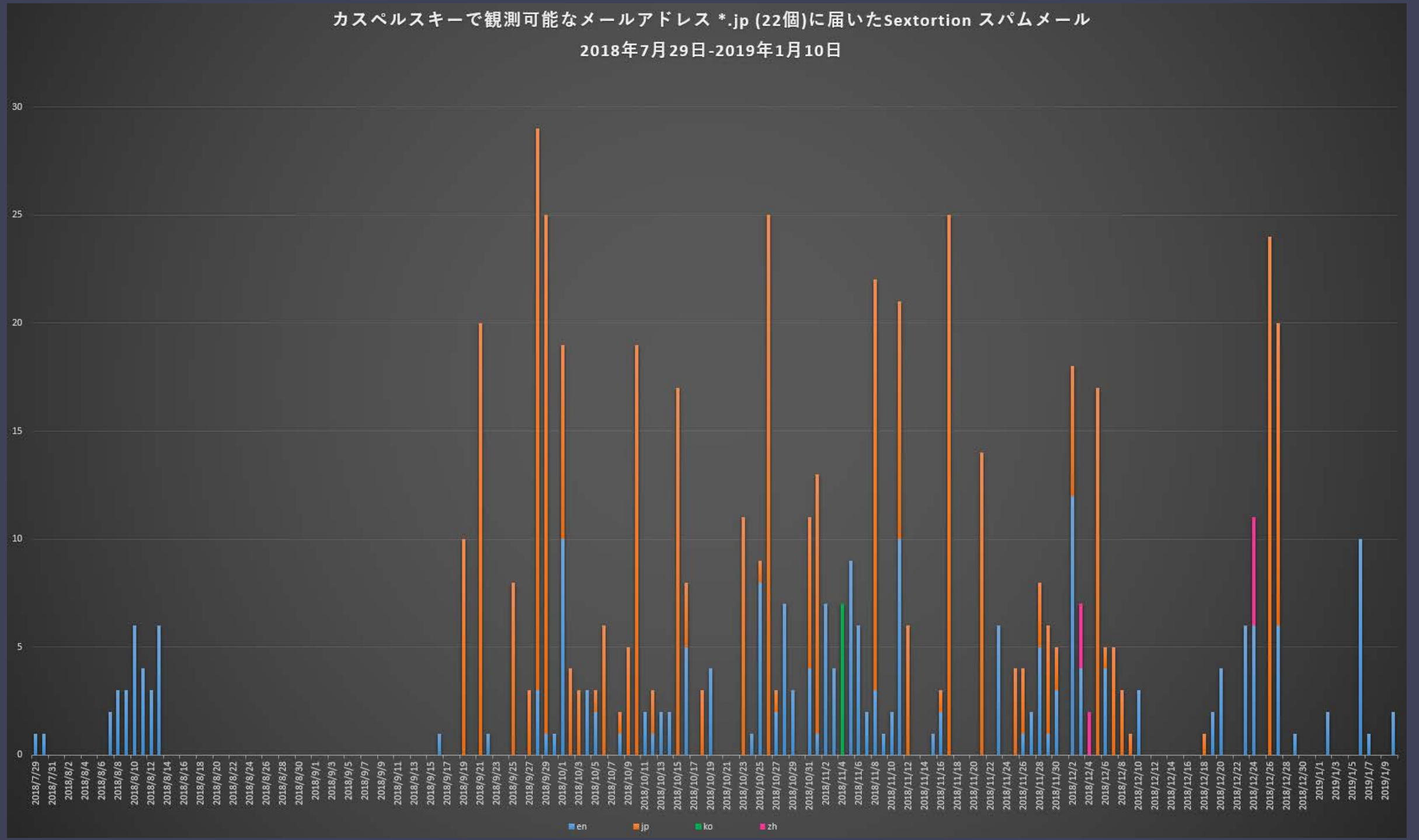
1. 概要
2. 詳細
3. 被害額
4. 今後の展開

#Time Line


海外でパスワードが記載されたSextortionスパムメールが拡散、SANS, Brian Krebs等より報告
Sextortion Spam New Wave
2018.7 - 8
9月中旬、世界的にSextortionスパムメールの拡散が再開、多言語化日本語・韓国語も追加
Bluffed Sextortion Spam Mail in world wide
2018.9
日本語で拡散するSextortionスパムメールにパスワードを記載したものが出回る
Twisted Extortion Spam
2018.10
2019年も同様の手口でSextortionスパムメール拡散が続く
To be continue…
2019.NOW

#調査対象および調査期間

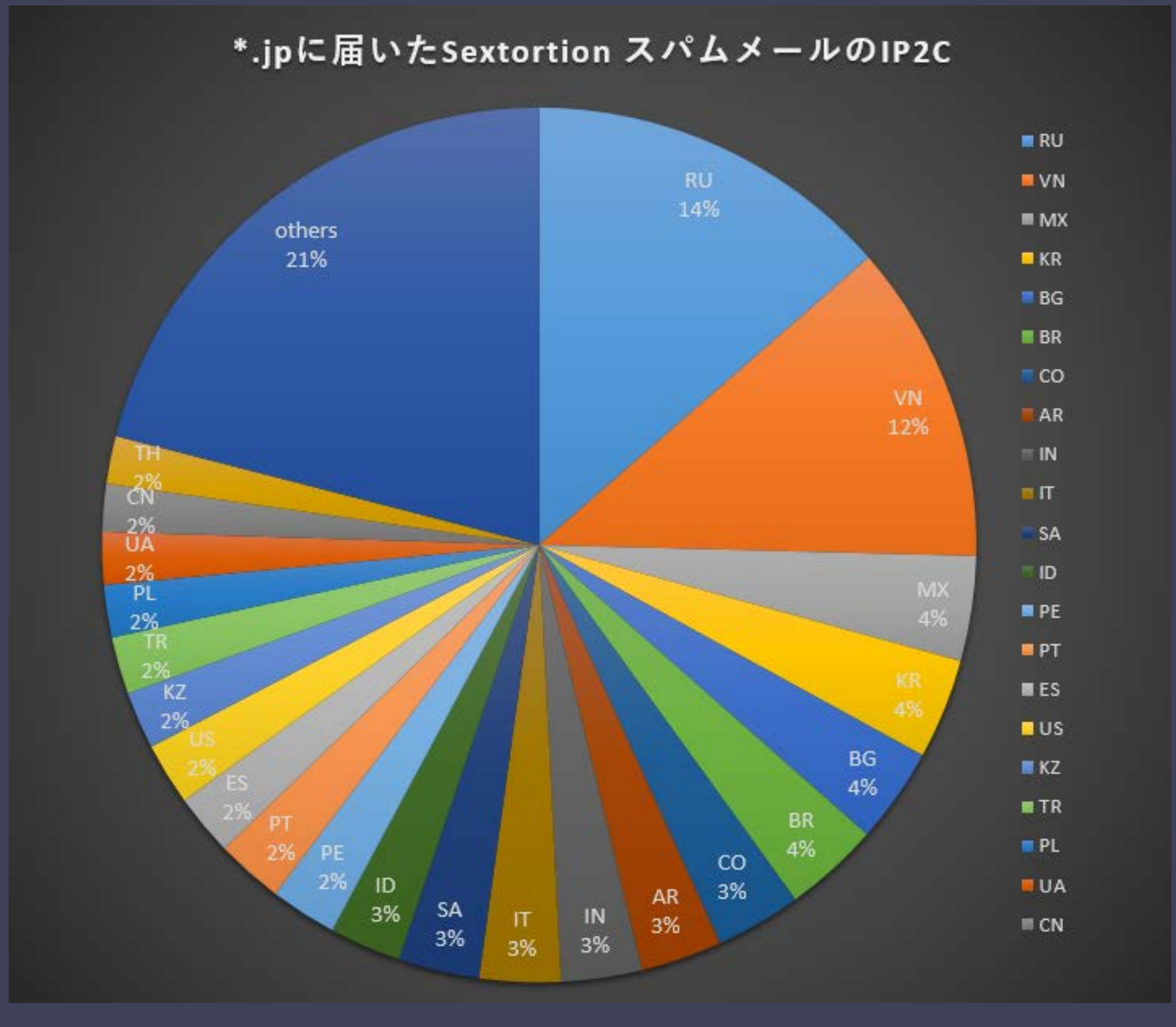
2018年7月 - 2019年1月10日
弊社で観測可能な *.jpアドレスで受信した
Sextortionスパムメール


カスペルスキーで観測可能なメールアドレス *.jp (22個)に届いたSextortion スパムメール
2018年7月29日-2019年1月10日
30
25
20
15
10
5
0
en
jp
ko
zh

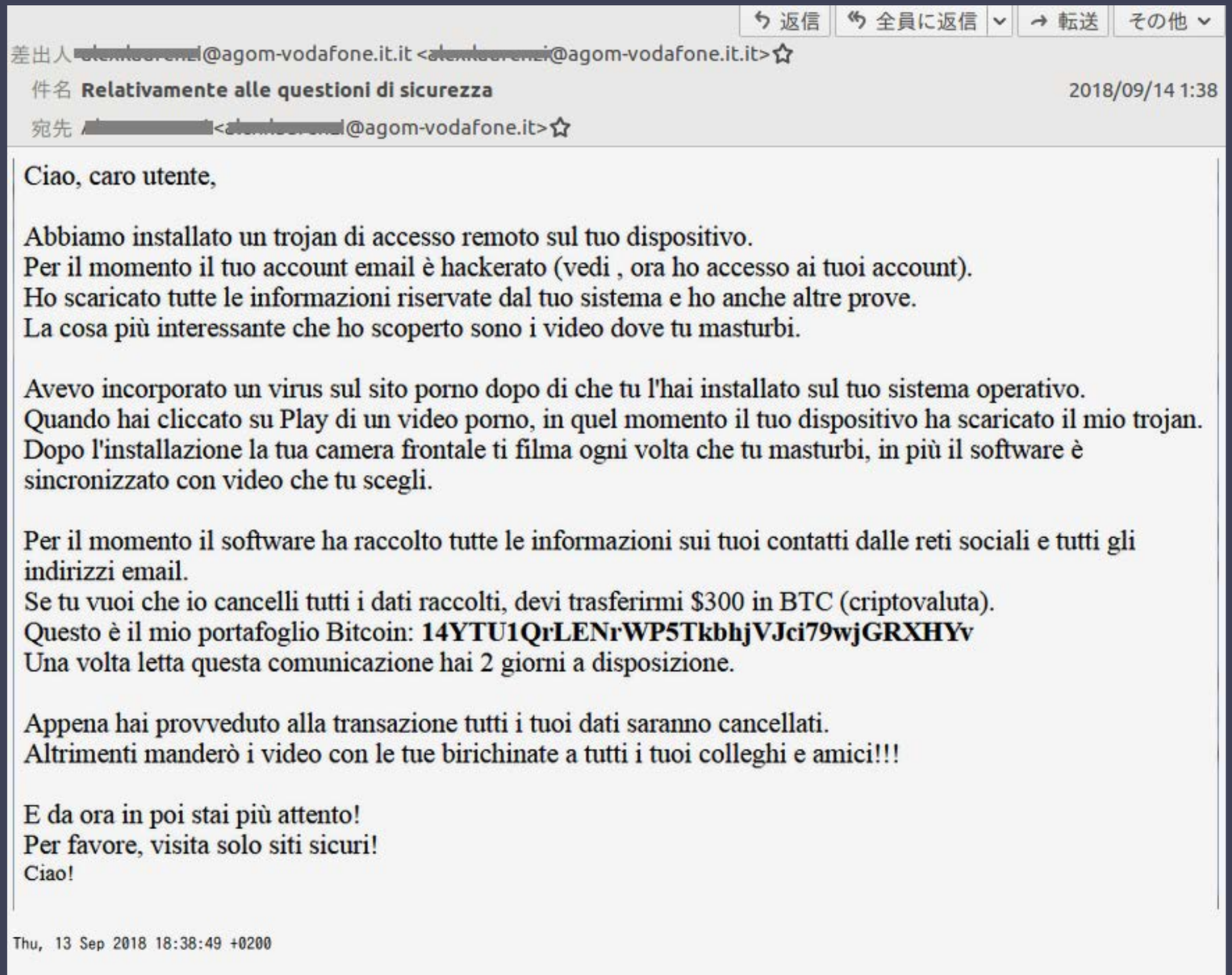
Mail Header IP and Country

ユニークなIPアドレス数

557



#スパムメールに利用された興味深いテクニック①



返信 | 全員に返信 | 転送 | その他

差出人 [redacted]@agom-vodafone.it.it <[redacted]@agom-vodafone.it.it>

件名 **Relativamente alle questioni di sicurezza** 2018/09/14 1:38

宛先 [redacted]<[redacted]@agom-vodafone.it>

Ciao, caro utente,

Abbiamo installato un trojan di accesso remoto sul tuo dispositivo.
Per il momento il tuo account email è hackerato (vedi , ora ho accesso ai tuoi account).
Ho scaricato tutte le informazioni riservate dal tuo sistema e ho anche altre prove.
La cosa più interessante che ho scoperto sono i video dove tu masturbi.

Avevo incorporato un virus sul sito porno dopo di che tu l'hai installato sul tuo sistema operativo.
Quando hai cliccato su Play di un video porno, in quel momento il tuo dispositivo ha scaricato il mio trojan.
Dopo l'installazione la tua camera frontale ti filma ogni volta che tu masturbi, in più il software è sincronizzato con video che tu scegli.

Per il momento il software ha raccolto tutte le informazioni sui tuoi contatti dalle reti sociali e tutti gli indirizzi email.
Se tu vuoi che io cancelli tutti i dati raccolti, devi trasferirmi $300 in BTC (criptovaluta).
Questo è il mio portafoglio Bitcoin: **14YTU1QrLENrWP5TkbhjVJci79wjGRXHYv**
Una volta letta questa comunicazione hai 2 giorni a disposizione.

Appena hai provveduto alla transazione tutti i tuoi dati saranno cancellati.
Altrimenti manderò i video con le tue birichinate a tutti i tuoi colleghi e amici!!!

E da ora in poi stai più attento!
Per favore, visita solo siti sicuri!
Ciao!

Thu, 13 Sep 2018 18:38:49 +0200

メール本文が画像

#スパムメールに利用された興味深いテクニック②

差出人 butcher <attacker@wrigleysoft.com>☆

返信

件名 **You are my victim.**

宛先 [redacted]@kaspersky.co.jp☆

Hi, my prey.

ダブルバイトのアルファベットが混ざっている

This is my last warning.

I write you since I buried a malware on the web page with porn which you have visited.
My tr o jan c a p tur e d a ll your p rivate d a ta and swit c h e d on y o ur c a m e r a which
solitary s e x. Just aft e r that the tr o jan s a v e d your c o nt a ct list.
I will e ras e the compromising video re c o rds and inf o rmati o n if y o u s e nd me 750 EU

This is address f o r p ayment : 1PXQQJ6vmLviMNX5tcYd1E5XFwT8DXW1wG

I giv e you 30 h o urs aft e r y o u o pen my mess a ge f o r making the p a ym e nt

#スパムメールに利用された興味深いテクニック③

送信元を宛先と同じメールアドレスに偽装

差出人 ksos@kaspersky.co.jp ☆

件名 **緊急対応!**

宛先 ksos@kaspersky.co.jp ☆

差出人も宛先もksos@kaspersky.co.jp

こんにちは!

おそらくあなたが推測したように、あなたのアカウントksos@kaspersky.co.jpは、私があなたからそれをあ

私は国際的なハッカーグループの一員です。
2018年7月23日から2018年9月17日まで、あなたが訪問した成人のウェブサイトを通じて、作成したウイ
これまでのところ、あなたのメッセージ、ソーシャルメディアアカウント、メッセンジャーにアクセスできます。

#スパムメールに利用された興味深いテクニック④

過去にリークしたメールアドレスと
パスワードを利用する

差出人 [redacted]@kaspersky.co.jp[redacted]@kaspersky.co.jp>

件名 **maby09**

宛先 maby09 <[redacted]@kaspersky.co.jp>

maby09

こんにちは!

あなたは私を知らないかもしれませんし、なぜあなたはこの電子メールを受け取っているのだろうと思っていますか?
この瞬間、私はあなたのアカウント([redacted]@kaspersky.co.jp)をハッキングし、そこからメールを送りました。私はあな

今私はあなたのアカウントにアクセスできます!
たとえば、[redacted]@kaspersky.co.jpのパスワードはmaby09です

実際に、私は大人のvids(ポルノ資料)のウェブサイトにマルウェアを置きました。あなたは何を知っていますか、あなたはこ

#日本のメールアドレスに送られてきた
韓国語・中国語のSextortionメール

差出人 [redacted]@kaspersky.co.jp
件名 긴급 통신!
宛先 [redacted]@kaspersky.co.

여보세요!

당신은 나를 알지 못할 수도
이 순간 나는 당신 계정 (
사실 성인 비디오 (포르노 소
는 것이 었습니다.
비디오 클립을 시청하는 동안 인터넷 브라우저가 RDP (원격 데스크톱)로 작동하기 시작했습니
그게 나에게 당신의 스크린과 웹캠에 대한 액세스를 제공하는 keylogger를 가지고있다.
그 직후, 내 소프트웨어 프로그램은 전자 메일뿐만 아니라 메신저, 소셜 네트워크에서 전체 대화

내가 뭘 한거지?
나는 이중 스크린 비디오를 만들었다. 첫 번째 부분은 시청 한 비디오 (좋고 이상한 맛)를 보여 주
줍니다.
정확히 무엇을해야합니까?

음, 888 달러는 우리의 작은 비밀에 대한 공정한 가격이라고 생각합니다. Bitcoin이 지불합니
인 구매 방법"검색).
내 BTC 주소 : 1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ
(민감한 cAsE이므로 복사하여 붙여 넣기하십시오)

노트 :
결제하려면 2 일이 소요됩니다.
(나는이 이메일 메시지에 특정 픽셀을 가지고 있으며,이 순간 당신은이 이메일 메시지를 읽었

BitCoins를받지 못하면 가족, 동료 등 모든 연락처에 비디오 녹음을 보내드립니다.

그러나 내가 돈을 받으면 즉시 비디오를 파괴 할 것입니다.

差出人 [redacted]@kaspersky.co.jp
件名 [redacted]@kaspersky.co.jp 被黑了！立即更改密码！

spersky.co.jp。

我首先攻击了这个路由器并将您的代码放在上面。
当您通过Internet输入时，我的木马安装在您设备的操作系统上。

之后，我完成了你的磁盘转储（我有你所有的地址簿，查看网站的历史记录，所有文件，电话号码和所有联系

一个月前，我想锁定你的设备并要求少量资金解锁。
但我查看了您经常访问的网站。你最喜欢的资源令我震惊。
我说的是成人网站。

我想说 - 你是个大变态者。你有一个令人眼花缭乱的幻想！

在那之后，我想到了一个想法。
我制作了你喜欢的成人网站的截图（你知道我的意思，是吗？）。
之后，我在浏览本网站时拍摄了你和你的娱乐照片（我使用了你设备的相机）。
结果很棒！不要犹豫！

我深信您不想向您的亲戚，朋友或同事展示这些照片。
我认为389美元对于我的沉默是少量的。
此外，我花了很多时间在你身上！

我在比特币接受钱。
我的BTC钱包：1P7bLeCJywaaDRQpT7iwb4qzUHa4CpRFyP

您不知道如何补充比特币钱包？

#Agenda

1. 概要
2. 詳細
3. 被害額
4. 今後の展開

*.jpアドレスでの受信メールに含まれる BTCアドレスへの支払い状況

BTCアドレスのユニーク数

124

BTC支払い総額

72.65316854 BTC

USD換算

265,877.21

JPY換算

28,908,700

864 tx

被害額：28,908,700円!?

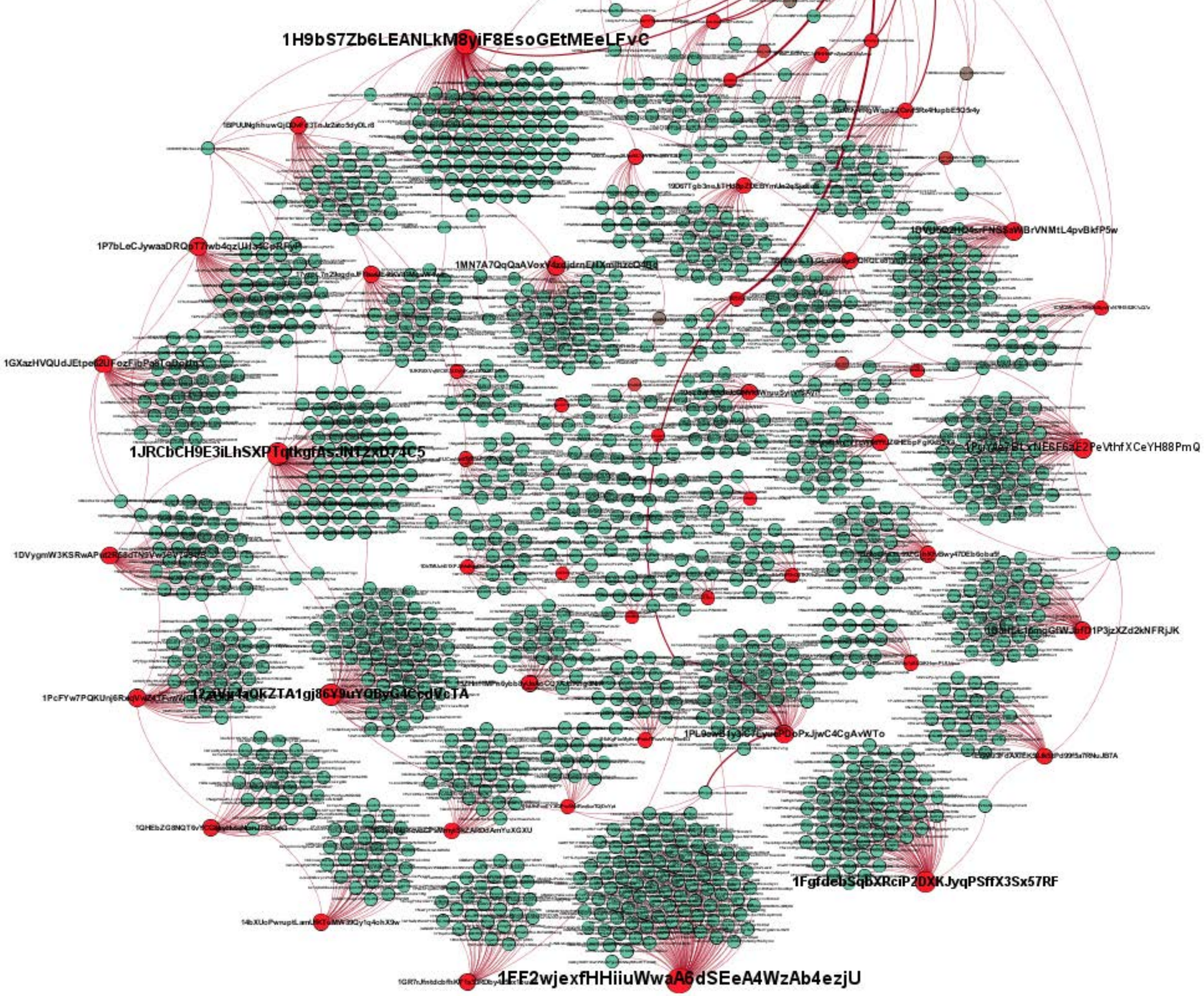
①被害者が
メールに記載された
アドレスに
Bitcoinを支払う

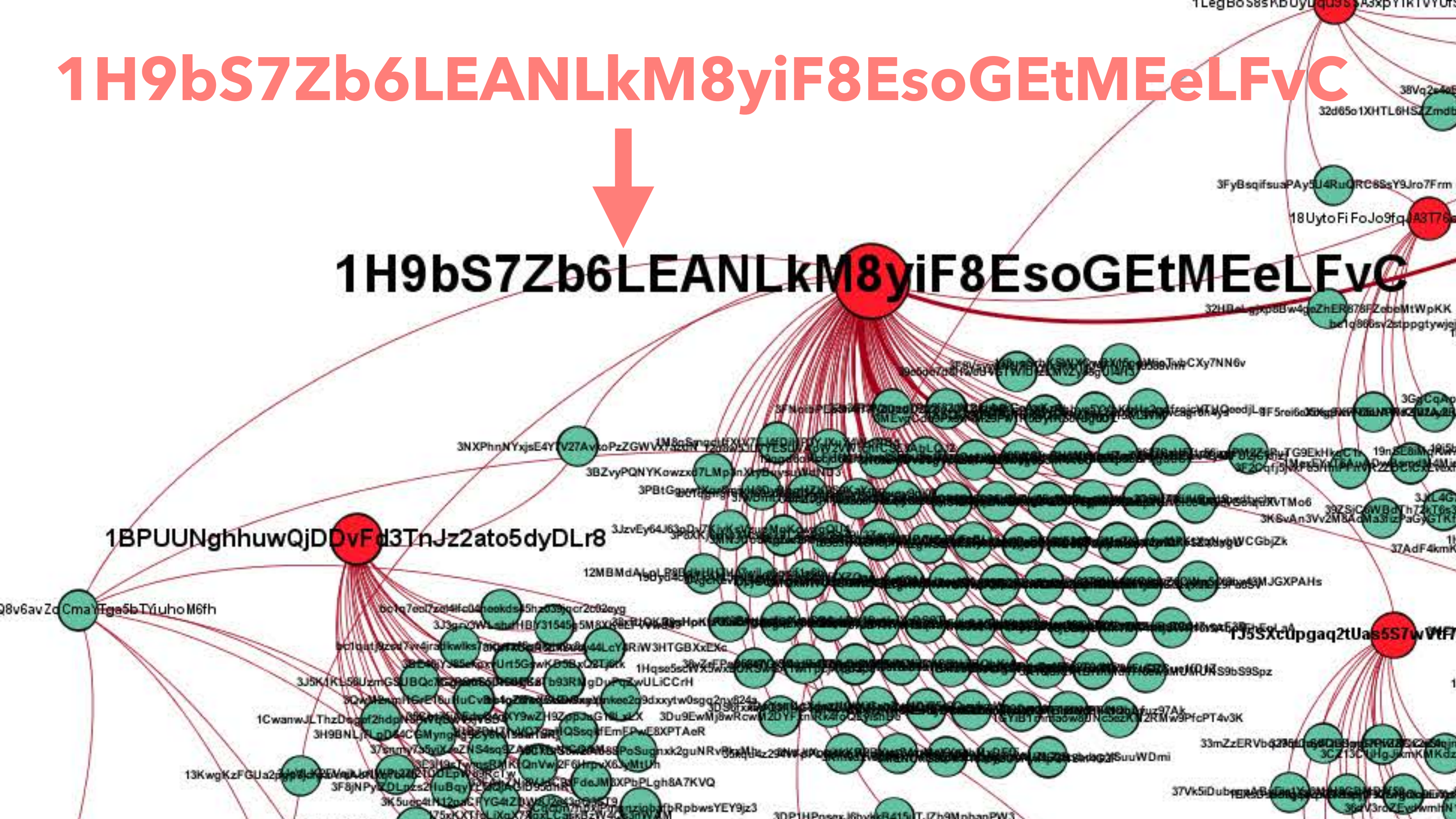
②攻撃者がBitcoinを
別のアドレスへ移動する

③攻撃者がBitcoinを
別のアドレスへ移動する

1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.073637|2018-12-05 10:03:47
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.057337|2018-12-04 10:37:03
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.027236|2018-12-02 08:52:29
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.16687009|2018-11-30 03:30:26
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.095493|2018-11-29 20:57:53
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.0701244|2018-11-29 18:57:48
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.13600641|2018-11-20 23:19:44
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.126|2018-11-20 08:16:54
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.14787665|2018-11-20 02:01:37
xdtyclm|1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.08608392|2018-11-19 19:34:49
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.15403392|2018-11-19 19:20:37
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.14118096|2018-11-19 18:46:14
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.14033172|2018-11-19 18:01:20
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.13903687|2018-11-19 17:55:47
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.00640252|2018-11-19 17:52:03
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.14256167|2018-11-19 16:01:42
qv9dj09|1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|0.0098|2018-11-19 15:39:22

被害者のBTCアドレスからスパムに書かれたBTCアドレスへのトランザクション




1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC
1BPUUNghhuwQjDDvFd3TnJz2ato5dyDLr8

被害者から1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvCへBTC支払い

被害者から集めたBTCをさらに別のアドレスへ移動

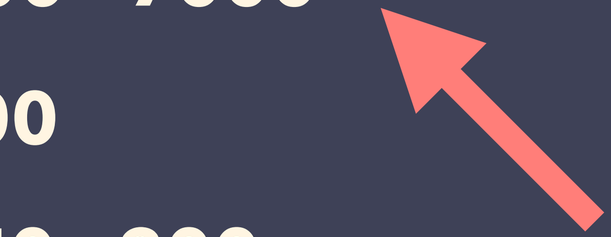
```
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|3KkiQBXBLxyEUtMCEnrtcnbR6Phw4RTfRT|0.13216322|2019-01-06 19:29:26
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|36J9BpnKedfben5YzPssgX1wbhgcJAf5XA|0.8121734|2018-12-06 22:34:51
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|31om3g8agy8ivVCnYe5rco4hTJS4BNkL2F|0.99057008|2018-12-03 22:57:50
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|38opW9yESqvFmQZ1dqR7erJndLtLAuVqs3|2.13254327|2018-11-27 21:56:37
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|38ezWFTTFJbyAD1oHXzydfVAxsXUwZYukg|2.14648522|2018-11-22 22:04:03
1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvC|38b3k1qkYDQDxX7FTZ14UtioemUmvH6Wfv|3.4666468|2018-11-19 20:35:47
```

1H9bS7Zb6LEANLkM8yiF8EsoGEtMEeLFvCから

別のアドレスへ

ゆすりの相場感 (収集したコレクションより)

- 英語　　＄100 - 7000
- ドイツ語　　$300
- フランス語　$250 - 300
- イタリア語　＄300
- 日本語　　＄483 - 1000
- 韓国語　　＄800 - 900
- 中国語　　$300 - 400



英語だけ要求金額の幅が広い
世界中で英語を理解する人は多いので、
そんなに注意深く対象を選んでいない？

#Agenda

1. 概要
2. 詳細
3. 被害額
4. 今後の展開

#攻撃の拡大①

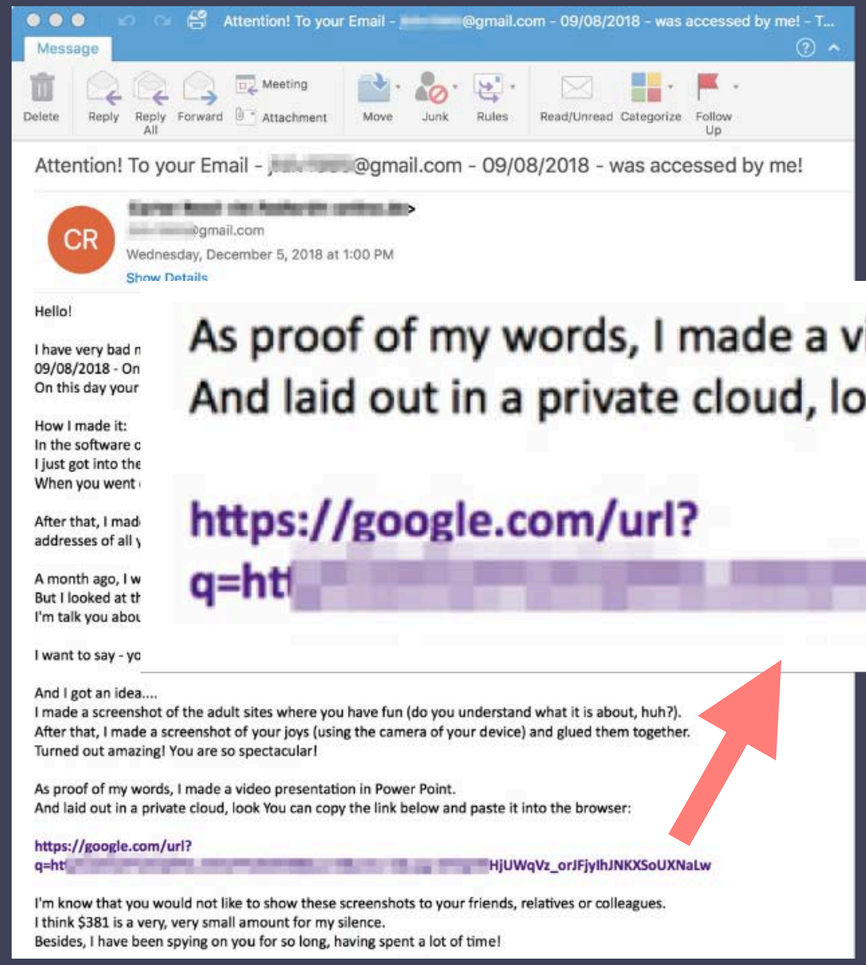
Sextortionだけでなく、BTCを要求する脅しメール全般

https://www.bleepingcomputer.com/news/security/new-extortion-email-threatens-to-send-a-hitman-unless-you-pay-4k/

#攻撃の拡大②

Sextortion + Malware

Sextortion + Malware



As proof of my words, I made a video presentation in Power Point.
And laid out in a private cloud, look You can copy the link below and paste it into the browser:

https://google.com/url?
q=ht[redacted]HjUWqVz_orJFjyIhJNKXSoUXNaLw

ダウンローダー → マルウェア

https://www.proofpoint.com/us/threat-insight/post/sextortion-side-ransomware

#より高度な
ソーシャルエンジニアリング

世界中でリークしたデータが大量にあるため、
悪意ある集団が個人情報を悪用して攻撃する

攻撃の拡大を早期に検知するには？

#ご提案＆検証

スパムメールに書かれた
Abused BTCアドレスを
スパム判定に取り入れては？

BTCアドレスを検知要素とする理由

スパムメールに記載されている時点で、
攻撃者に関連していると判断できる

お金を支払う部分なので、攻撃者が細工をやり難い
（ユーザーがコピペしやすいように、
正しいアドレスを書かなくてはいけない）

```
rule sextortion_btc {

strings:
$a0 = "121MLg3x41nA7opsyg2zkpT4HyDti1nF2K" ascii
$a1 = "127NFGEYLGpB3WqacaRMGdv1z9YATR2BjV" ascii
$a2 = "127fnd1eojhha6ym6uXhhYkphvgY3AMTcU" ascii
$a3 = "12DA8mpQCnTB1cEHLPFU7ckP44zN5Xmgu3" ascii
$a4 = "12K5pURDxA3wNmuaqU1zACuXJaxEtSwzqp" ascii
$a5 = "12LVkk5MjQLYzjnxkkWX1dEx8wc16AN1Xu" ascii
$a6 = "12S8JjArWwuPCKxBxXgHWpbynAjfbDexUZ" ascii
$a7 = "12VoGgYXU899dUk4zW9JRTouFy7kve1kJR" ascii
$a8 = "12quE25n9WuqUeNqCbJH7YNE1xFdABYyiU" ascii
$a9 = "12ziVv4aQkZTA1gj86Y9uYQByG4CcdVcTA" ascii
$a10 = "136WC35NBV5r9eF7Cch2bHeYexLPYbVinu" ascii
$a11 = "138poQvftVpDZ2Rx9C3VNaMa7ni2xM5iC6" ascii
$a12 = "13Uw4tqt31ar8RauE8AEtdTxYe52wD9Y3Z" ascii
```

～中略～

```
$a275 = "1fkogKaEf86Tc3XcpSEGG3cGStFgfr8b3" ascii
$a276 = "1h4yQ2BecSkY83tHwchm4domwVfodz3Jn" ascii
$a277 = "3FyPJBaymuwZWqEQScRTpzsVBKzxeRkvx5" ascii
$a278 = "3Jy5Ag9WYya7XD7aVwmRnpcrkehqnFhp5G" ascii

condition:
 filesize < 100000 and
 (any of ($a*))

}
```

収集したSextortion

スパムメールから

BTCアドレスを収集

↓

BTCアドレスの文字列で

パターンマッチングできる

YARAルールを作る

```
[                                    ]$ yara wallet_2.yar eml_converted_all
sextortion_btc eml_converted_all/163.eml
sextortion_btc eml_converted_all/162.eml
sextortion_btc eml_converted_all/161.eml
sextortion_btc eml_converted_all/135.eml
sextortion_btc eml_converted_all/134.eml
sextortion_btc eml_converted_all/133.eml
sextortion_btc eml_converted_all/132.eml
sextortion_btc eml_converted_all/988.eml
sextortion_btc eml_converted_all/990.eml
sextortion_btc eml_converted_all/131.eml
sextortion_btc eml_converted_all/142.eml
sextortion_btc eml_converted_all/139.eml
sextortion_btc eml_converted_all/152.eml
sextortion_btc eml_converted_all/136.eml
sextortion_btc eml_converted_all/138.eml
sextortion_btc eml_converted_all/137.eml
```

70%以上
検知

VirusTotal Intelligence Retro Scan

Rulesets | Notifications | Scan file | Retrohunt

Job status	Running
Progress	
Rules	/* Paste your rules here. Malware Hunting-specific features won't work. Use pure YARA rules only. */ rule sextortion_btc { strings: $a0 = "121MLg...
Creation time	Jan. 17, 2019, 7:19 a.m.
ETA	Calculating...
Scanned data	376.7 TB
Scanning speed	Calculating...
Matches	2228 Download hashes

2300 +

HASH検知!!

Abort

Blog | Twitter | Contact us | ToS | Privacy policy

差出人 [redacted]@[redacted].go.jp☆, [redacted]@[redacted].go.jp☆, [redacted]@[redacted].go.jp☆, [redacted]@[redacted].go.jp☆

返信 | 全員に返信 | 転送 | その他

件名 **あなたのパスワードが侵害されました**

2018/12/07 20:07

宛先 newuser <[redacted]@[redacted].go.jp>☆, [redacted]@[redacted].go.jp☆ [redacted]@[redacted].go.jp☆, [redacted]@[redacted].go.jp☆

こんにちは！

私は数ヶ月前にあなたの電子メールとデバイスをクラックしたハッカーです。
あなたが訪問したサイトの1つにパスワードを入力君た。それを傍受しました。

宛先がxxx@xxx.go.jp

これは、ハッキングの瞬間に , , , からのあなたのパスワードです: [redacted]

もちろん、それを変更したり、すでに変更したりすることができます。
しかし、それは問題ではありません、私のマルウェアは毎回それを更新しました。

私に連絡したり、私を見つけようとしないでください。それは不可能です。私はあなたのアカウントからメールをあなたに送ったので、

あなたの電子メールを介して、私はあなたのオペレーションシステムに悪質なコードをアップロードしました。
私は友人、同僚、親戚とのあなたの連絡先のすべてを保存し、インターネットリソースへの訪問の完全な履歴を保存しました。
また、あなたのデバイスにトロイの木馬をインストールしました。

あなたは私の唯一の犠牲者ではない、私は通常、デバイスをブロックし、身代金を求める。
しかし、私は頻繁に訪れる親密なコンテンツのサイトにショックを受けました。

私はあなたの幻想にショックを受けている！ 私はこれのようなものを見たことがない！

だから、あなたがサイトで楽しむとき（あなたは私が何を意味するか知っています！）
あなたのカメラのプログラムを使用してスクリーンショットを作成しました。
その後、私はそれらを現在閲覧されているサイトのコンテンツに結合しました。

これらの写真を連絡先に送信すると素晴らしいことがあります。
しかし、あなたがそれを望んでいないと確信しています。

したがって、私は沈黙のためにあなたからの支払いを期待しています。
私は$555が良い価格だと思います！

Bitcoin経由で支払う。
私のBTCウォレット: 1LnpqtSP4xqXJUPg29PzGng6qAhkW7zmZQ

あなたがこれを行う方法を知らない場合 - Googleに「BTCウォレットに送金する方法」を入力します。難しくない。

検証結果：Abused BTCアドレスを検知の要素として利用するのは有効

- セクストーションだけでなく、スパムメール拡散の初期に利用されているBTCアドレスを検知することで、その後の被害を防げる可能性がある

- シンプルなアプローチであるものの、既存のスパム判定手法と合わせて利用することで、検知精度を上げることができる

- BTCアドレスを利用することで、新しい検体を入手できることがわかった

→脅威ハンティングに利用できる！

- スパムメール送信というごくシンプルな手段で
  攻撃者は収益を上げている

- Sextortionに限らず、
  脅してBitCoinをゆするスパムメールは続く

→早期に組織間が情報共有することで、
被害の低減やより良い調査ができる

Thank you!

conuma@kaspersky.co.jp
Kaspersky Lab Japan
www.kaspersky.com
Slide https://github.com/sanographix/azusa-keynote