

取引先のセキュリティ侵害から発生する ビジネスメール詐欺 (BEC) の実態

Jan 28, 2021

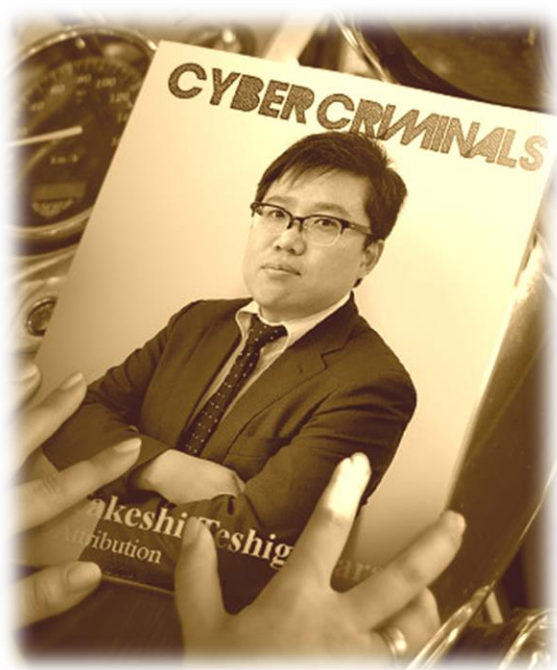
マクニカネットワークス株式会社

勅使河原 猛

政本 憲蔵

About Us

勅使河原猛
セキュリティサービス室
シニアアナリスト



共同分析：伊藤忠商事株式会社



政本憲蔵
セキュリティ研究センター
センター長

サンドボックス、EDR、ハニーポット、
メールセキュリティなどの対策技術に精通
海外のセキュリティ対策技術をリサーチ

Macnica-CIRT

ビジネスメール詐欺の実態と対策アプローチ

Search

標的型攻撃の実態と対策アプローチ

Search

研究センターブログ

Search

濱せっく

官公庁 非常勤職員

笹川平和財団

サイバーインテリジェンス研究会 研究員

濱せっく 運営委員

Macnica-CIRT

twitter.com/anemone_fish

- 事案 1（フリーメールサービスの悪用）

- 事案 2（man-in-the-email）

- 今まで対処した事案から学んだこと

- インシデント対応と対策

事案 1 （フリーメールサービスの悪用）

攻撃者から振込口座変更の依頼

From [REDACTED] - [REDACTED] <sales14@[REDACTED].com> ☆
Subject Payment detail of 7 Aug
Reply to [REDACTED] - [REDACTED] <sales.[REDACTED]@dr.com> ☆
To [REDACTED] <[REDACTED]@[REDACTED].co.jp> ☆

*****@dr.comは
mail.comで取得可能なフリーメールアドレスで、
BECでよく使われる。

BECでは様々な理由を付けて口座の変更を依頼
してくる。

「監査のために今までの口座が使えない」
「経済制裁されている国とのやり取りが発生し
口座が一時的に凍結されている」
「COVID-19による経済封鎖により銀行口座が
一時的に使えない」
「子会社の口座に振り込んで欲しい」
「追加料金（手数料や税金など）がかかること
が判明したから別口座に振り込んでほしい」

Dear [REDACTED],

Thank you once more for your kind email, Pls make this payment to this our bank account here below.
We are having some problem with the other bank account and can't be used for any form of payment or transaction for now.

Total Amount is: 16,374.000

BANK FOR THIS PAYMENT

BANK NAME : POSTAL SAVINGS BANK OF CHINA
ACCOUNT NAME : T[REDACTED] GROUP.
ACCOUNT NUMBER : 621[REDACTED]
SWIFT CODE: PSBCCNBJ
BANK ADDRESS : No.39-2 SHENG LI DONG LU ZHANGZHOU SHI,FUJIAN ,CHINA.

Will wait for your reply of this email with the bank copy.

Regards,
Sharon

On Mon, Aug 3, 2015 at 12:19 PM, [REDACTED] <[REDACTED]@[REDACTED].co.jp> wrote:
Hi [REDACTED]-san,

I will pay following invoice on 7 Aug.
Please see and check it.

Invoice #	Qty	Unit price	Amount US\$	[REDACTED] PO #
IV [REDACTED] 15	5	270.00	1,350.00	[REDACTED] 288643
IV [REDACTED] 06	2	476.00	952.00	[REDACTED] 303453
IV [REDACTED] 86	1	194.00	194.00	[REDACTED] 310092
IV [REDACTED] 61	7	69.00	483.00	[REDACTED] 303431

ヘッダに残る痕跡

Received: from H[REDACTED]14.apcprd06.prod.outlook.com ([REDACTED].246.29) by
Received: from S[REDACTED]006.apcprd06.prod.outlook.com ([REDACTED].58.46) by
Received: from AM1FF011FD022.protection.gbl (2a01:111:f400:7e00::139) by
Received: from nm27-vm2.bullet.mail.ne1.yahoo.com (98.138.91.215) by
Received: from [98.138.226.177] by nm27.bullet.mail.ne1.yahoo.com with NNFMP; 03 Aug 2015 23:10:09 -0000
Received: from [98.138.87.10] by tm12.bullet.mail.ne1.yahoo.com with NNFMP; 03 Aug 2015 23:10:09 -0000
Received: from [127.0.0.1] by omp1010.mail.ne1.yahoo.com with NNFMP; 03 Aug 2015 23:10:09 -0000
Received: by 98.138.105.213; Mon, 03 Aug 2015 23:10:08 +0000
Authentication-Results: spf=pass (sender IP is 98.138.91.215)
Received-SPF: Pass (protection.outlook.com: domain of yahoo.com designates
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1438643409; bh=+iwb9ZfMvtXk
X-Yahoo-Newman-Property: ymail-3
X-Yahoo-Newman-Id: 126189.95920.bm@omp1010.mail.ne1.yahoo.com
X-YMail-OSG: 6h000kkVM1mC1vhj4naMf2rBgISxhvY2dA_nUYZnWEibC3TI6LHJ9kvX3TLw9P4
Date: Mon, 3 Aug 2015 23:09:59 +0000
From: "[REDACTED] - [REDACTED]" <sales14@[REDACTED].com> ← 取引先のメールアドレス
Reply-To: [REDACTED] - [REDACTED] <sales.[REDACTED]@dr.com> ← フリーメールアドレス (@dr.com)
To: "[REDACTED]" <[REDACTED]@[REDACTED].co.jp>
Message-ID: <1676893878.7897.1438643399647.JavaMail.yahoo@mail.yahoo.com>
Subject: Payment detail of 7 Aug
MIME-Version: 1.0
Content-Length: 59329
Return-Path: hbol[REDACTED]@yahoo.com ← フリーメールアドレス (@yahoo.com)
X-MS-Exchange-Organization-Network-Message-Id: e5eb9a3d-3363-4e49-61b9-08d29c58ae54

2つのフリーメールアドレスは、どちらも攻撃者によって取得されたものと思われる。

Yahoo.comメールにおけるSend-onlyアドレスの設定

Send-only email address
Send emails from a different email address
0 of 10 used
[Add](#)

Disposable email address
Create an email address to sign up for third-party newsletters. Delete account to stop receiving.
0 of 500 used
[Add](#)

Add send-only email address
masamoto@macnica.net
[Next](#)

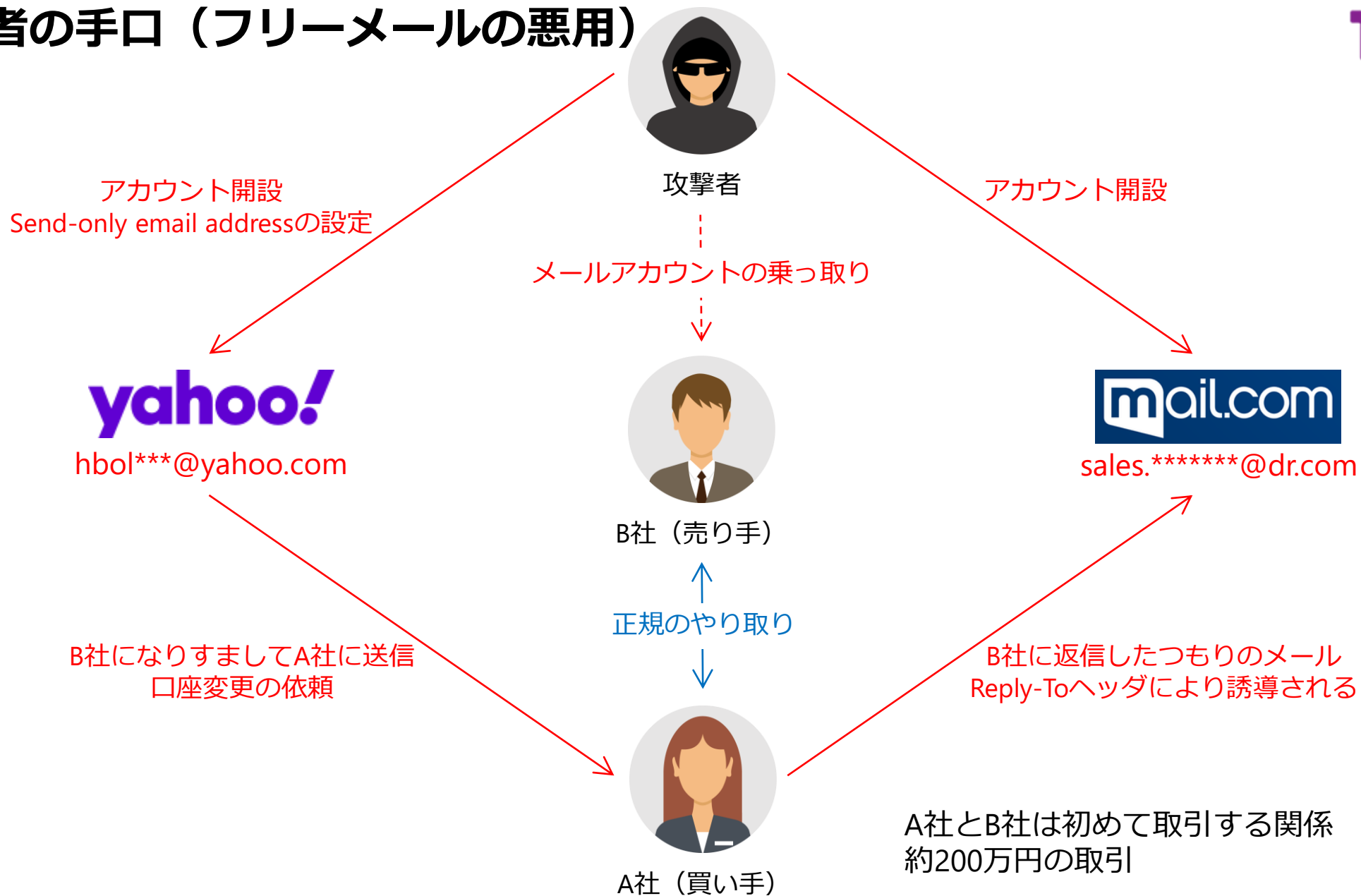
yahoo!
Hi [redacted].
You've added masamoto@macnica.net to your Yahoo account [redacted].
Please [click here](#) to verify this email address.
Have a great day!
Thanks,
Yahoo

Send-only email addressの設定から
Fromヘッダに指定するメールアドレスを追加後、
確認メールが送られるので、
メール内のリンク先へアクセスし
設定が有効化される。

Compose

From <masamoto@macnica.net>
To teshigawara-t@macnica.net
振込依頼
勅使河原さん
M&Aの案件で1億円が必要になりました。
至急、振り込み手続きをお願いしたいのですが、対応できますか?

攻撃者の手口（フリーメールの悪用）



他にも侵害されていた組織を確認

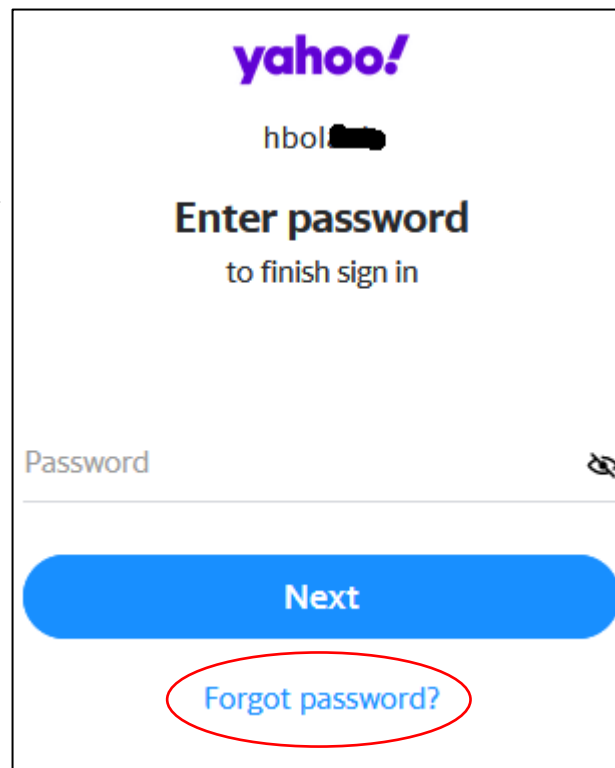
“Forgot password?”のリンクから、
犯人のメールアドレス(hbol***@yahoo.com)に
紐づいている他のメールアドレスを調査したところ、
B社の他にも、メールアカウントが侵害された企業を
確認。

業種：

プラント建設
航空機部品の卸売
射出成形製造
光学機器製造
輸送

企業所在国：

台湾
マレーシア
ベトナム
インドネシア
イタリア
米国



yahoo!

hbol***

Select an option
to sign in to your account

(7**) ***-**54
Msg & data rates apply

B社のメールアドレス

s****14@***.com

a**ar@***.com

d****ti@***air.com

i****he@***chemical.com

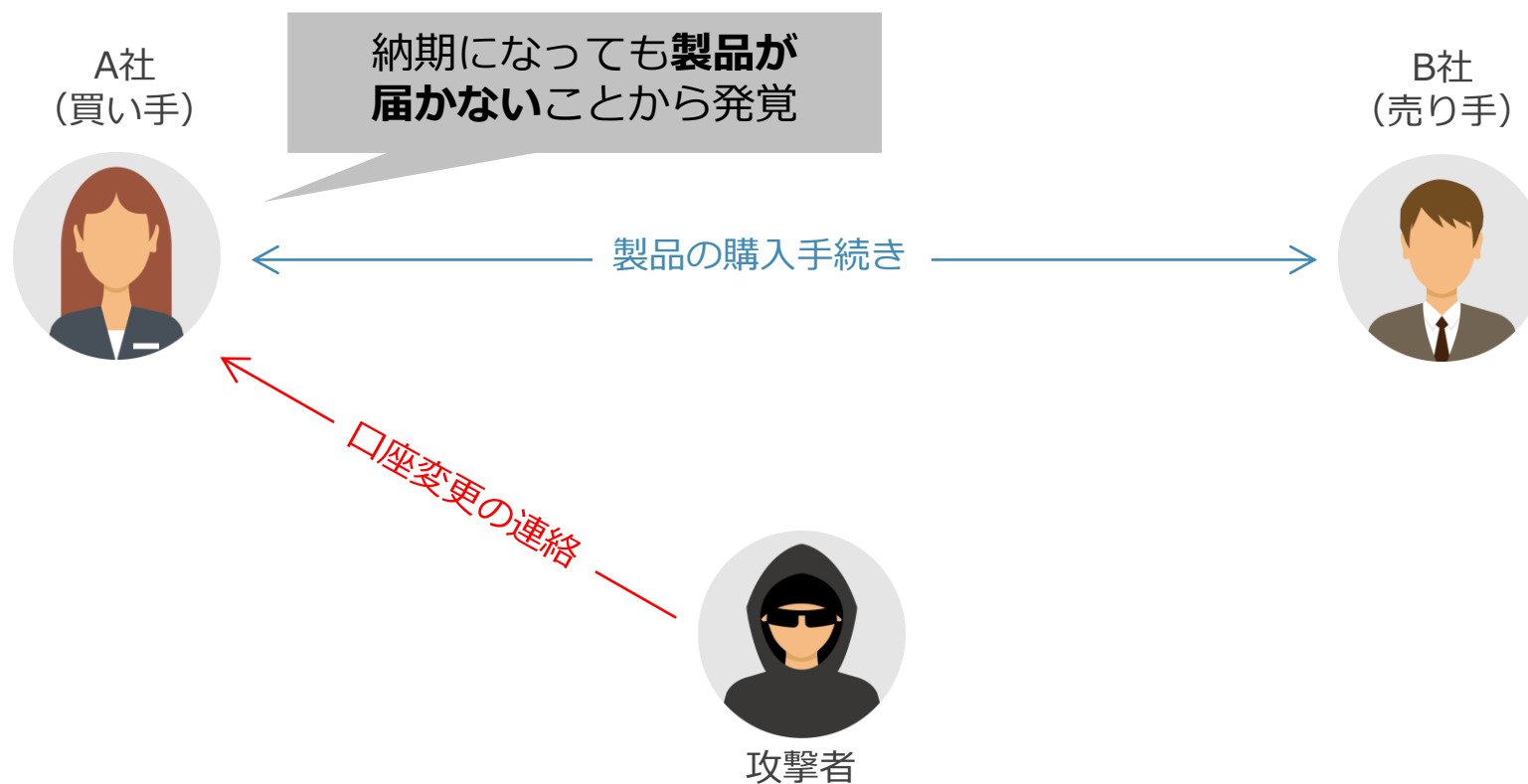
i**o@***a.com

i****he@***.vn

事案 2 (man-in-the-email)

調査のきっかけ

A社とB社は初めて取引を行う関係であり、前払いの取引であった
A社はB社が販売する製品を急ぎ購入するが必要があった



攻撃者から振込口座変更の依頼

From [redacted] <[redacted]@eon-i.com> ☆

Subject RE: Inventory of AT [redacted] 7-[redacted] Mi [redacted]

To [redacted]d@[redacted].co.jp ☆

Cc [redacted]-Customer-Service@[redacted].co.jp ☆, [redacted]@[redacted].co.jp ☆, [redacted] <[redacted]@nom-t.com> ☆, [redacted]@[redacted].co.jp ☆, [redacted]@[redacted].co.jp ☆

Dear [redacted],

Please refer to below information, here is the correct bank information

Sorry for the inconvenience caused.

●Needed information

Name of account holder: [redacted] CO.,LTD

Address of account holder: #1[redacted], [redacted] ([redacted]), Di [redacted], [redacted]gu, Seoul, Korea

Bank name: NORDEA BANK

Branch name: 1F, [redacted] TOWER [redacted], [redacted]

Branch address: Ha [redacted], [redacted] Stockholm

Account Number: SE [redacted] 4

SWIFT CODE: NDEASESS

IBAN: SE [redacted] 4

ABA No.: N/A

Please kindly register the above details into your system and do not use the previous details i send,
Your prompt response is highly appreciated

[www.\[redacted\].com](http://www.[redacted].com)

영업지원 / [redacted]

TEL [redacted]

REP +82 2 [redacted]

FAX +82 2 [redacted]

DIR +82 [redacted] 5[redacted]

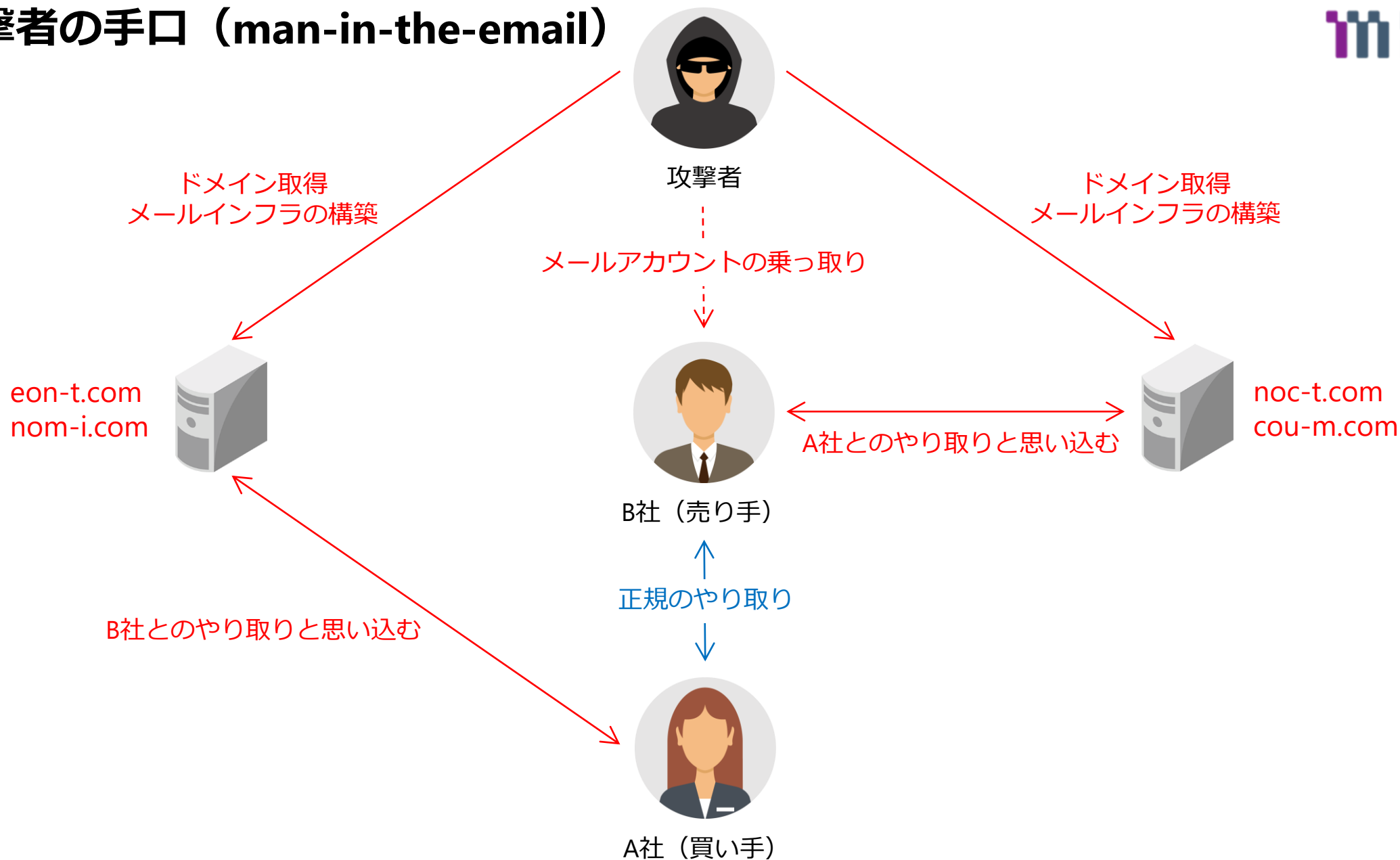
e.M [redacted]@[redacted].com

Confidentiality Note ▲

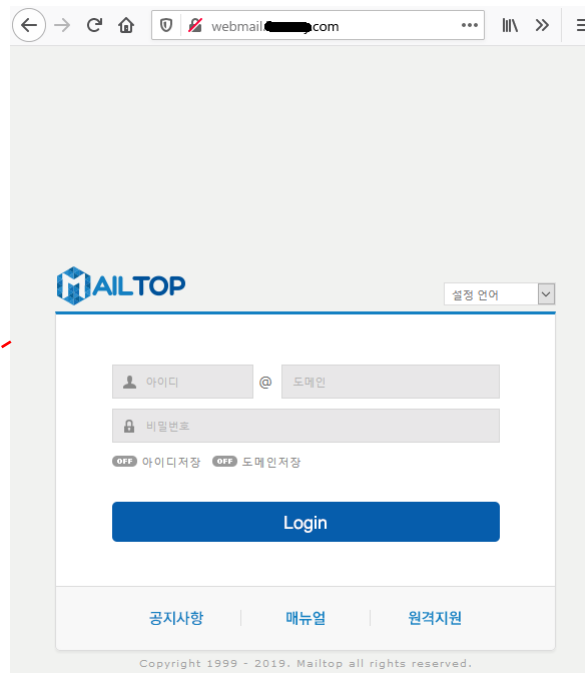
본 메시지에 포함되어 전송 된 정보는 기밀로 취급되며 의도 된 수신자의 사용만을위한 것이고 [redacted] 또는 협력 업체의 재산입니다. 귀하가 의도 된 수신자가 아닌 경우, 이 정보를 무단으로 복사, 배포 또는 사용은 법으로 금지되어 있음을 유의하십시오. 이 메시지를 실수로받은 경우 즉시 메시지를 보낸 사람에게 반송하고 시스템에서 이 메시지를 삭제하여 주십시오.

正規の口座通知から約4時間後に、
攻撃者から口座変更の依頼がA社に届いた

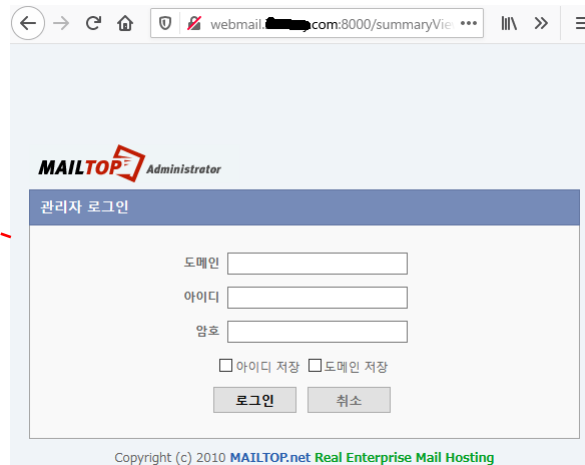
攻撃者の手口 (man-in-the-email)



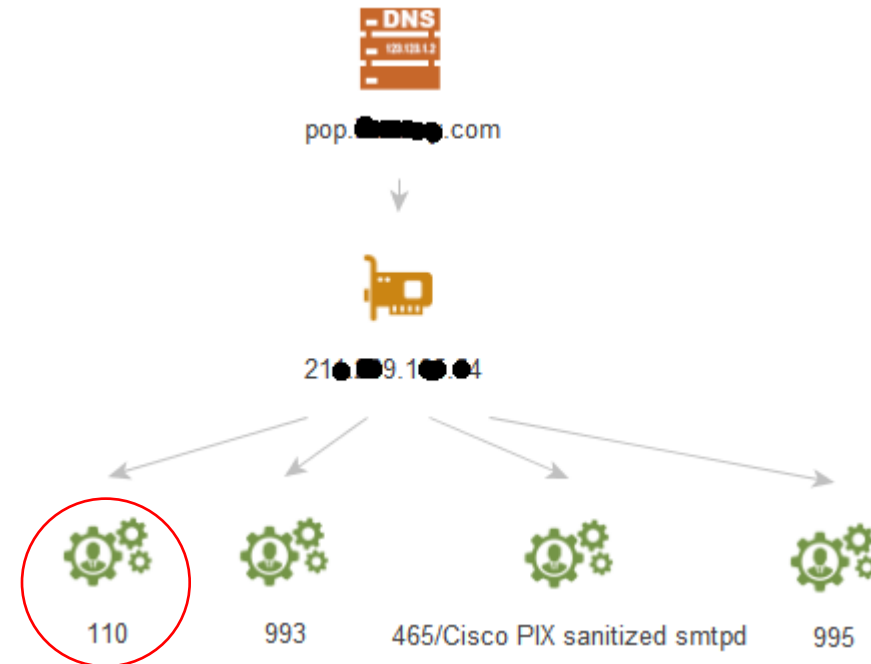
B社（取引先）のセキュリティ成熟度（OSINTによる調査）



Webメール・ログイン画面（社員用）



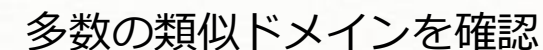
Webメール・ログイン画面（管理者用）



レガシーなプロトコルの使用

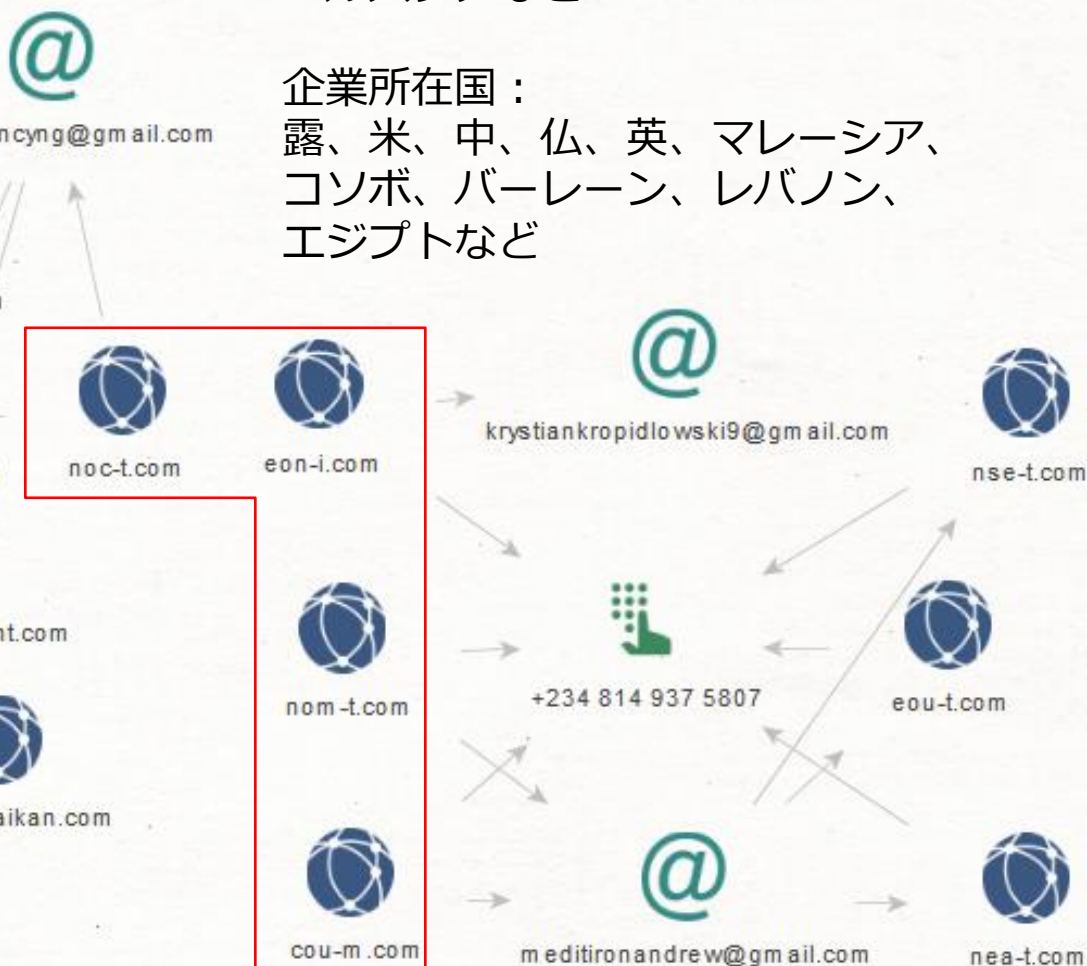
その他、脆弱性を抱えてそうなERPのサーバなどが
見つかり、セキュリティ対策の成熟度が低い
ことが伺える。

httpsへリダイレクトされないWebメール



メディア、家畜飼料、法律事務所、ヘルスケアなど

露、米、中、仏、英、マレーシア、
コソボ、バーレーン、レバノン、
エジプトなど



困難な帰属（分析から得られたタイムゾーン情報）

WHOIS情報

Name:	agbasoga ogbondu
Street:	No. 46, Level 1, Sector 6, 12th Main, HSR Layout lagos Nigeria
City:	lagos
State:	lagos
Postal Code:	110001
Country:	NG
Phone:	+234.8149375807
Email:	neditironandrew@gmail.com

UTC + 0100 (ナイジェリア)

UTC + 0530 (インド)

メールヘッダ

```
Content-Type: multipart/alternative;  
boundary="=_b240d05bc28a6763f1d09ccdf30dfbc2"  
Date: Fri, 11 Sep 2020 07:19:32 +0200  
From: [REDACTED] <[REDACTED]@eon-i.com>  
To: [REDACTED]@[REDACTED].co.jp  
Cc: [REDACTED]-S[REDACTED]-Customer-Service@[REDACTED].co.jp,  
[REDACTED]@[REDACTED].co.jp,
```

UTC + 0200

PDFファイル（偽の請求書）のメタデータ

```
Modify Date      : 2020:09:16 03:17:47-04:00  
Create Date      : 2020:09:16 03:17:47-04:00  
Metadata Date    : 2020:09:16 03:17:47-04:00
```

UTC - 0400

今まで対処した事案から学んだこと

- 取引先のセキュリティ対策レベルが低いと、メール内容が盗み見され、詐欺に遭う。（自分たちのセキュリティ対策レベルが低いと、メール内容が盗み見され、取引先に多大な迷惑がかかる。）
- 初めて取引する相手とのやり取りが狙われやすい。
- 英語で書かれた詐欺メールが圧倒的に多いが、日本語の事案も散見される。
- SPF Passすることも多く、Secure Email Gateway (SEG)で検知することは困難。
- IT部門の観点だけで対策するだけでは不十分で、会計部門の観点でも対策が必要。

インシデント対応と対策

CSIRT

■ 調査と分析

- 一連のメールの証跡保全
- メールアカウントの侵害の有無の調査
 - 外部ドメインへの不審なメール転送設定
 - 不審なメール振り分けルール
 - 不正ログオンの分析
- マルウェア感染の有無の調査
- 上記被害が確認された場合、パスワード変更など攻撃者の足掛りを削除するなどの対処
- 攻撃者ドメインのテイクダウン
- 攻撃者ドメインのセキュリティコミュニティへの共有

会計部門・法務部門

■ 送金の取り戻し

- 送金の取り戻すために金融機関・現地捜査機関へ連絡

■ 取引先との交渉と按分

- 自組織が被害者の場合、確認できた事実をもとに、取引先と被害額を按分することが可能
- 逆の場合、被害額の按分を求められる場合もあります。



BECのインシデント対応は、複数のステークホルダーと連携して動く必要がある



攻撃ステップ	対策
メールアカウントへ不正ログイン （メールアカウントの乗っ取り）	- 多要素認証 - レガシープロトコル（IMAP/POP）の停止 - ブルートフォース・パスワードスプレー攻撃対策 - フィッシング対策 - 継続的なセキュリティ意識トレーニング（eラーニングなど）
メールボックスの偵察	- メール転送ルールの監視や制限 - 不審なログインの監視
詐欺メールの送付	取引先を装った攻撃者に騙されないために： - メール受信ポリシーの強化 - 継続的なセキュリティ意識トレーニング 攻撃者が自組織を装って取引先に被害を与えないために： - DMARC設定 - 自組織の類似ドメインの検索 - 口座変更伝達にポリシーの明文化
送金の説得	- 口座登録や変更時に、口座が正規なものであることを確認

ご清聴ありがとうございました。



共同分析：伊藤忠商事株式会社

ビジネスメール詐欺の実態と対策アプローチ

Search