Business Email Compromise (BEC): How does it attack your business and how can you prevent it?

Joint analysis : ITOCHU Corporation **July 1, 2020 Macnica Networks Corp.**

Analysts and authors:

Motohiko Sato
Senior Cyber Security Researcher, ITCCERT, Itochu Corporation
Associate Professor, National University of Chiba

Kenzo Masamoto
Head of Security Research Center, Macnica Networks Corp.

Takeshi Teshigawara
Security Analyst, Macnica Networks Corp.

Table of contents

1. Executive Summary

According to the Internet Crime Complaint Center (IC3) of the US Federal Bureau of Investigation (FBI), within a period of less than five years from October 2013 to May 2018 the number of reported cases of business e-mail compromise (BEC) was a little less than 80,000, and the total cost of damages came to approximately 12.5 billion USD (approximately 1.4 trillion yen). In Japan, there was a report at the end of 2017 about a major airline company that suffered damages of approximately 380 million yen[1], and in 2019 there were reports about a US subsidiary of a major news media outlet suffering damages of approximately 3.2 billion yen[2] and a European subsidiary of a major manufacturing company suffering damages of approximately 4 billion yen[3]. The cases of damage from BEC reported by the media in Japan are just the tip of the iceberg. If we include cases in which the amount of financial damage was comparatively small, the number of victims will actually be quite high.

Macnica Networks has analyzed not only BEC email received by group affiliates of the parent company (Macnica Fuji Electronics Holdings) from 2015 to 2019, but also BEC email received by trading partners purporting to be from Macnica Fuji Electronics Group, as well as BEC cases handled through the incident response service provided by Macnica Networks, and has exposed the methods used by attackers. Furthermore, with the cooperation of Itochu's ITCCERT[4], which has provided analysis results regarding the daily BEC attacks on the Itochu Group, as it continues to expand around the world, we have now been able to shed even more light on the methods and identities of attackers. ITCCERT began monitoring BEC attacks from 2014, and in 2017 ITCCERT also began observation of BEC email written in Japanese. It can be considered the most knowledgeable organization in Japan regarding BEC attacks. We explain the current state of BEC attacks observed by Itochu Group and Macnica Fuji Electronics Group in Chapter 2, using actual examples.

Before sending a BEC email, an attacker will first go through a stage of careful preparation. In many cases, because the attacker needs to first understand the details of a transaction before pulling a scam in the middle of the transaction, the attacker will try to break into email accounts through various methods. By eavesdropping on email exchanges through the compromised account, the attacker can drop into the exchange with effective timing to pull the scam. This sequence of events, in which the attacker first makes careful preparations, then sends a BEC e-mail to implement the scam, and finally gets the victim to transfer money to an account prepared by the attacker, is described in Chapter 3 as the "BEC kill chain".

There is no silver bullet for dealing with BEC. It is extremely important to implement not only countermeasures in the IT system, but also measures to prevent infiltration by means of the accounting department noticing anything suspicious. The countermeasures currently considered to be effective to some degree, from the aspect of the IT system and the perspective of the accounting department, are outlined in Chapter 4. Furthermore, the incident responses needed when encountering a BEC are outlined in Chapter 5.

This report contains useful information that organizations within Japan can use when formulating countermeasures to BEC attacks, and it is our hope that it will be helpful in damage reduction.

1 https://piyolog.hatenadiary.jp/entry/20171220/1513795615

2 https://www.nikkei.com/article/DGXMZO51583520Q9A031C1SHA000/

3 https://www.asahi.com/articles/ASM965H5HM96OIPE02Q.html

4 https://tech.nikkeibp.co.jp/it/atcl/column/16/080500167/081100004/

2. Current state of BEC

Macnica Networks began observing BEC e-mail in 2015, and has continued to carry out observation of BEC e-mail to this day. From these, we have selected a number of actual cases to explain the characteristics and methods of such attacks.

2.1 Pretending to be the CEO of a trading partner

The e-mail shown in Figure 1 is a BEC e-mail received by an affiliate company of Macnica Fuji Electronics Group in 2019. The sender is pretending to be the CEO of a US trading partner. Yet, the e-mail address of the sender has a domain name unrelated to the trading partner, which makes this fraud relatively easy to spot. However, because the e-mail purports to be an urgent request from the CEO of a trading partner, the thought of not wanting to be seen as rude by showing suspicion creates a situation in which it is hard to reject the request.

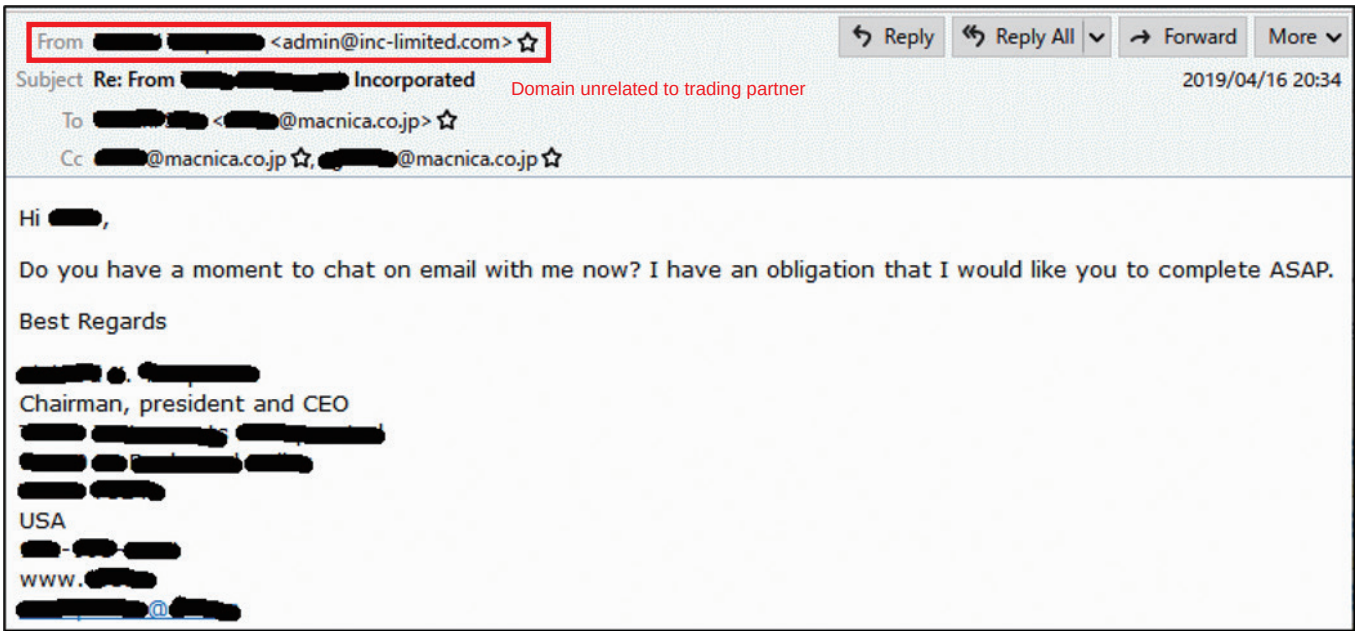


Figure 1: BEC e-mail purporting to be from a US trading partner

When a reply to this e-mail was sent for the purpose of investigation, the attacker sent back the reply shown in Figure 2. It claimed that the company was buying machinery from Dubai, but that the import tax would be too high for direct import to the US, and so requested that Macnica first import the machinery to Japan, then ship it to the US.

Figure 2: Request sent by attacker pretending to be a US trading partner

After that, the recipient continued to correspond with the attacker, while pretending to fall for the scam, and the attacker, now pretending to be a distributor in Dubai, sent transfer destination account details. Through the appropriate community, the recipient shared the account details with banks to help prevent any further crime from being committed.

2.2 BEC purporting to be internal e-mail from the company's own CEO

Figure 3 shows a BEC e-mail from 2019, purporting to be internal e-mail sent from Macnica Fuji Electronics Group's President and Co-CEO. Fraud in which the attacker pretends to be a company's CEO, even among BEC attacks, is referred to in particular as CEO fraud. In the e-mail below, addressed to a subsidiary in Brazil, the sender's domain is similar to Macnica's actual domain, macnica.com, with the sender instead using an r and an n together to make them look like an m: rnacnica.com. (Figure 4)

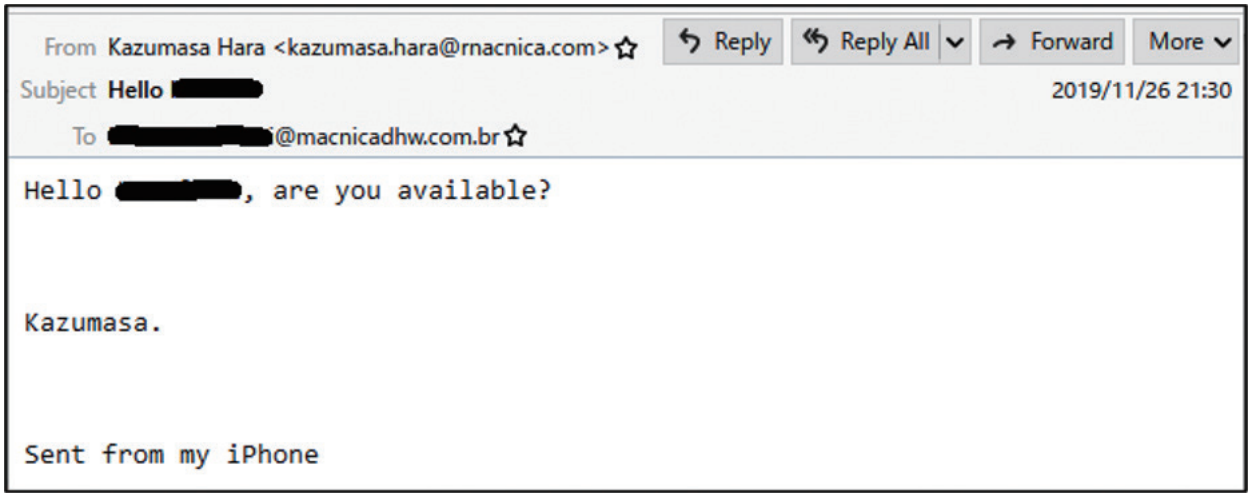


Figure 3: CEO fraud e-mail purporting to be from Macnica's President and Co-CEO

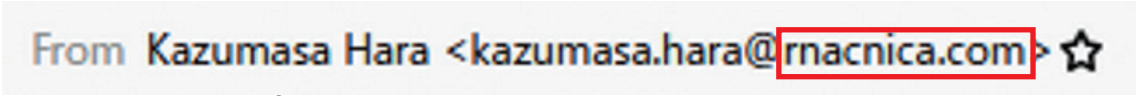


Figure 4: Similar domain used for the sender's e-mail address

The e-mail shown in Figure 5 is a CEO fraud e-mail purporting to be from Macnica's Representative Director and Chairman.

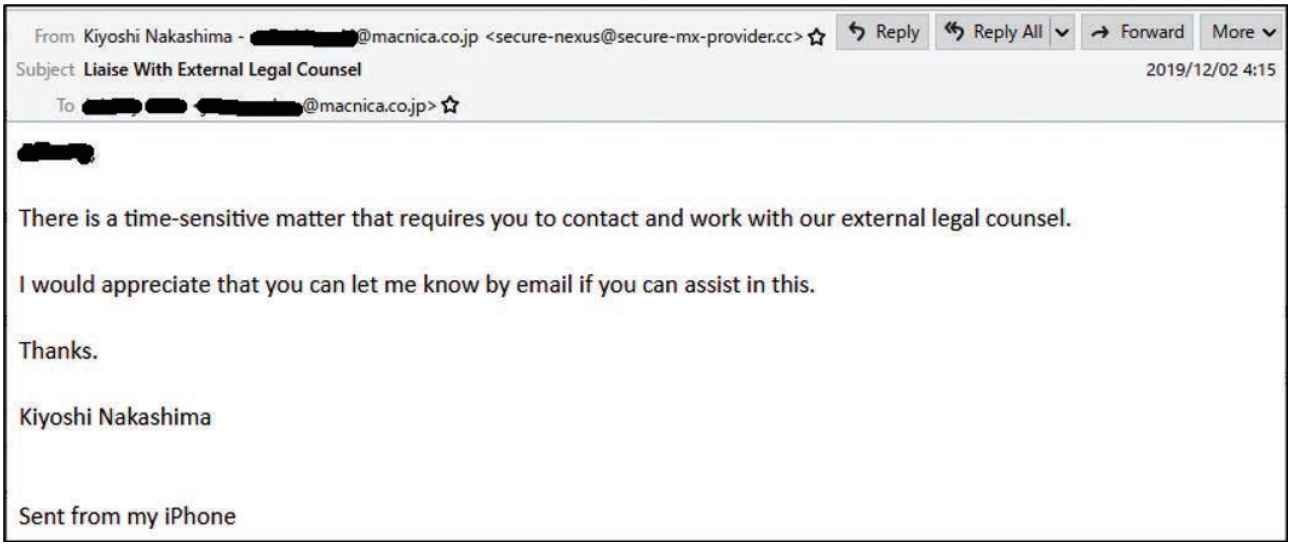


Figure 5: CEO fraud e-mail purporting to be from Macnica's Representative Director and Chairman

After this e-mail was ignored, the follow-up e-mail shown in Figure 6 was received a week later.

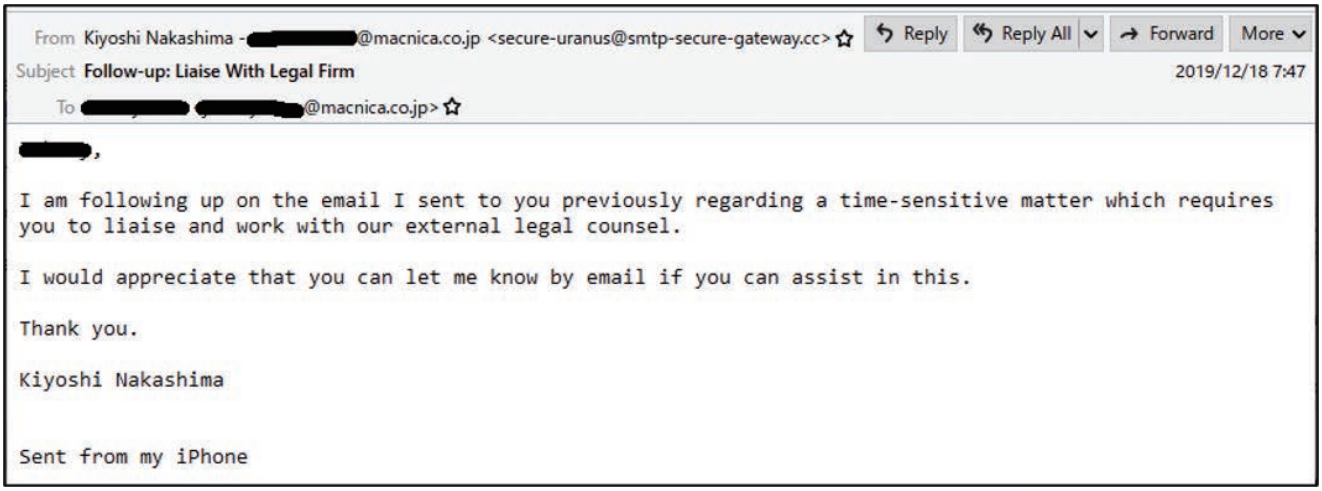


Figure 6: Follow-up e-mail sent by attacker pretending to be Macnica's Representative Director and Chairman

As it happens, if a reply is sent to this kind of CEO fraud e-mail, the attacker will then send an urgent request for prompt payment, along the lines of, "We have established a top-secret M&A deal and need to make an immediate payment."

2.3 Registration of similar domains

The e-mail shown in Figure 7 is a BEC e-mail received by a client in 2019, purporting to be from Netpoleon, an affiliate of Macnica Fuji Electronics Group. Immediately after this e-mail, the attacker sent bank account details. The attacker had acquired a domain very similar to the actual domain of Netpoleon and was using that to make a BEC attack on the client. Fortunately, the client realized there was something suspicious about the domain name, and the attack was thwarted.

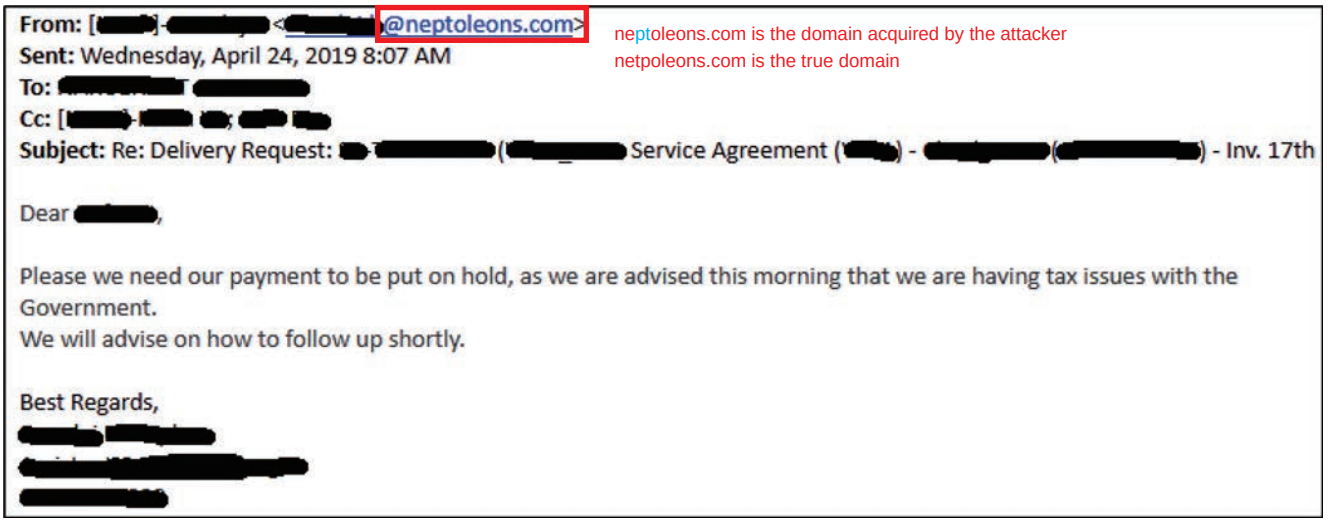


Figure 7: BEC e-mail sent to a client, purporting to be from Netpoleon

In May 2018, someone acquired the domain “macniica.com” (using two i’s), which is very similar to Macnica Fuji Electronics Group’s legitimate domain, macnica.com. This domain could not be confirmed to have been used in any actual BEC e-mail attack, but as shown in Figure 8, the Whois information on this domain revealed an e-mail address considered to belong to an attacker, and other domains tied to that e-mail address were able to be confirmed through Reverse Whois.

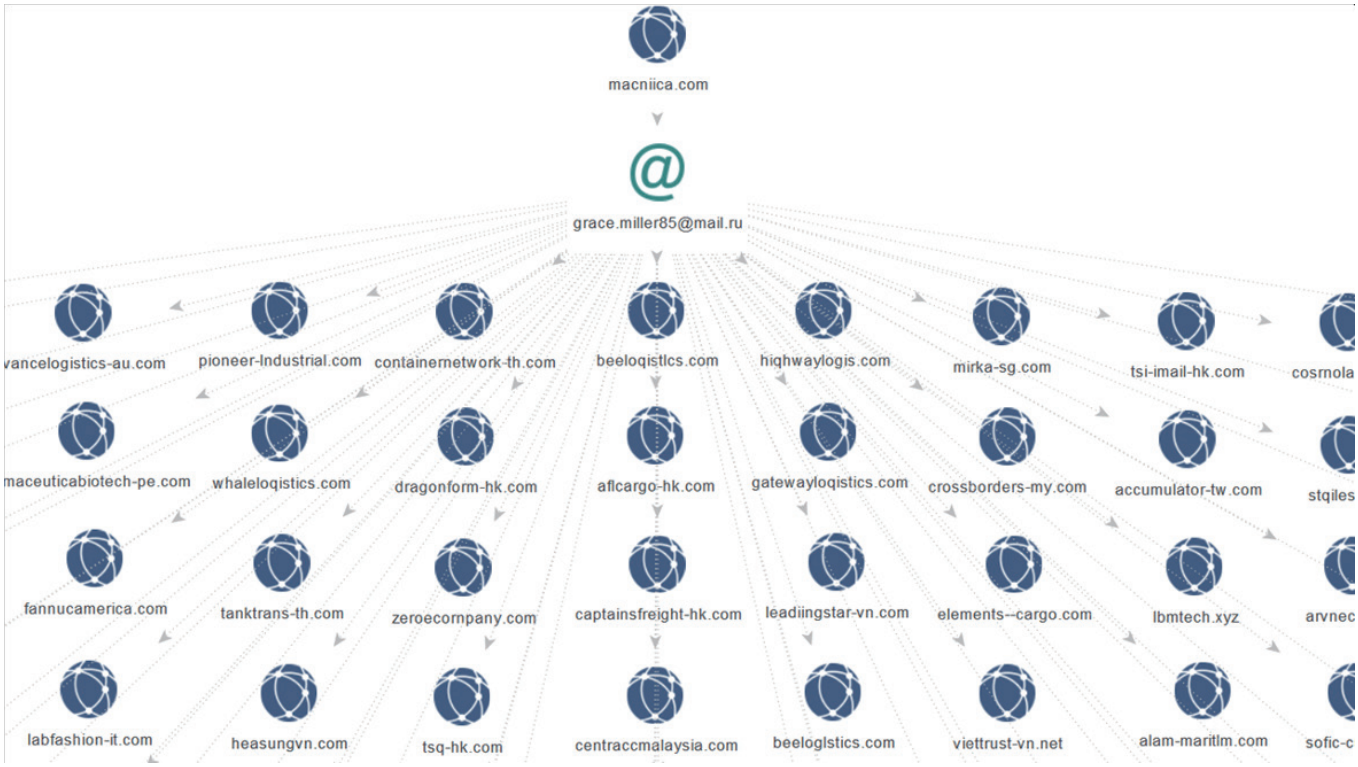


Figure 8: Other domains acquired by the attacker who acquired the domain “macniica.com”

Looking carefully at these domains, we noticed that they are very similar to actual, legitimate domains. In some cases a q is used in place of a g, or an l is used instead of an i, or the combination of an r and an n (rn) is used to suggest an m. It is highly likely that these domains were acquired to carry out BEC attacks.

2.4 Abuse of freemail

The e-mail shown in Figure 9 is one of the cases handled by the incident response service provided by Macnica Networks, from 2015. This is a BEC e-mail sent to a business in Japan. The sender is pretending to be a foreign trading partner. The content is a typical BEC requesting a change of transfer destination.

Figure 9: BEC e-mail purporting to be from a foreign trading partner

Figure 10 is an enlargement of the forged sender's address (the From header) and the reply address (the Reply-To header), in which the sender's address is disguised as the correct domain held by the trading partner. The reply address is a freemail address (dr.com) prepared in advance by the attacker so that reply e-mail will be sent to the attacker.

Figure 10: Forged sender's address (From) and reply address (Reply-To)

The domain dr.com is one of approximately 200 domains that can be selected with the freemail service mail.com. Domains that can be selected with mail.com are often used for BEC e-mail, as in this case. Also, when the e-mail header was inspected, the real sender of this e-mail was discovered. As shown in Figure 11, numerous strings containing "yahoo" were discovered in the header, and because this is a characteristic header of Yahoo.com freemail, it was apparent that the e-mail had been sent from a Yahoo.com freemail account.

Figure 11: BEC e-mail header

The Return-Path header also revealed the freemail address thought to have been acquired by the attacker. In actual fact, with freemail services such as Yahoo and Gmail, the address of the sender can be changed to a different e-mail address.[5] In the case of Yahoo.com, for a sender to add a separate e-mail address, the sender must access a link from verification e-mail sent to the added e-mail address.[6] Which is to say, in this case, it was discovered that the attacker had already hijacked the trading partner's e-mail account and could view confirmation e-mail sent via Yahoo.com. In this way, many BEC attacks will involve the hijacking of one e-mail account or another. By hijacking an e-mail account, as in this case, an attacker can not only send e-mail with a forged sender's address, but also gain an understanding of transaction details by eavesdropping on e-mail exchanges, making it easy to pull off a scam. As seen in this case, BEC attackers frequently use freemail. They not only use freemail addresses as reply addresses, they also use freemail services as infrastructure for sending BEC e-mail.

In this case, unfortunately, the client who received the BEC e-mail transferred the money to the attacker's account. However, it was not the e-mail account of the Japanese company who made the transfer that was compromised, but the account of the foreign trading partner. For that reason, negotiations were held for an out-of-court settlement and damages were divided proportionally.

5 https://support.google.com/mail/answer/22370
https://www.yahoo-help.jp/app/answers/detail/p/622/a_id/47956/

6 https://help.smallbusiness.yahoo.net/s/article/SLN29479

The e-mail shown in Figure 12 is a BEC e-mail received by a client in 2018, purporting to be from an affiliate company of Macnica Fuji Electronics Group (macnica.com). As with the previous example, the domain of the reply e-mail address is a domain used with the mail.com freemail service (dr.com). (Figure 13)

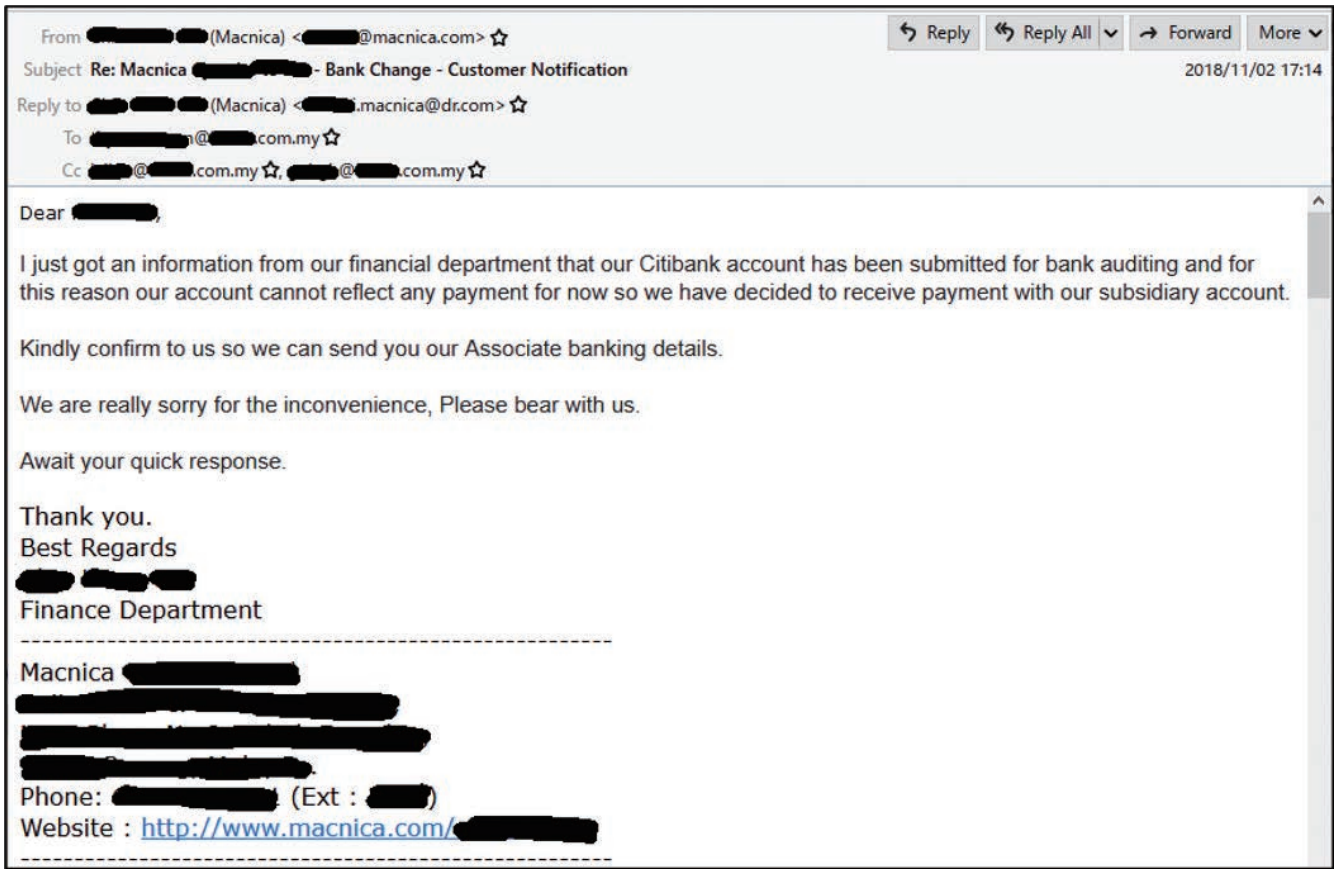


Figure 12: BEC e-mail purporting to be from “macnica.com”

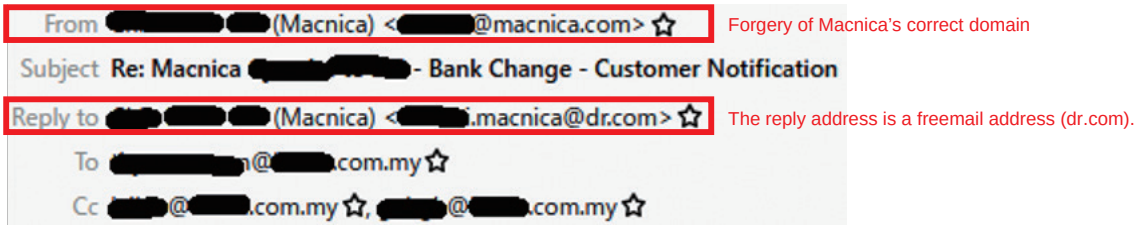


Figure 13: Forged sender’s address (From) and reply address (Reply-To)

2.5 BEC e-mail written in Japanese

The e-mail shown in Figure 14 is a CEO fraud e-mail purporting to be internal e-mail from Macnica's Representative Director and Chairman, received by the author (Masamoto) in 2019. The e-mail address of the sender is an unfamiliar domain (secure-server-smtp.cc), but the display name contains the e-mail address "macnica.co.jp", in an attempt to deceive the recipient. Moreover, because the destination e-mail address is just something the attacker has guessed from the author's name (Masamoto), and is different from the actual address held by the author (Figure 15), e-mail was not actually sent to the author's mailbox, but remained as trace files in the mail gateway.

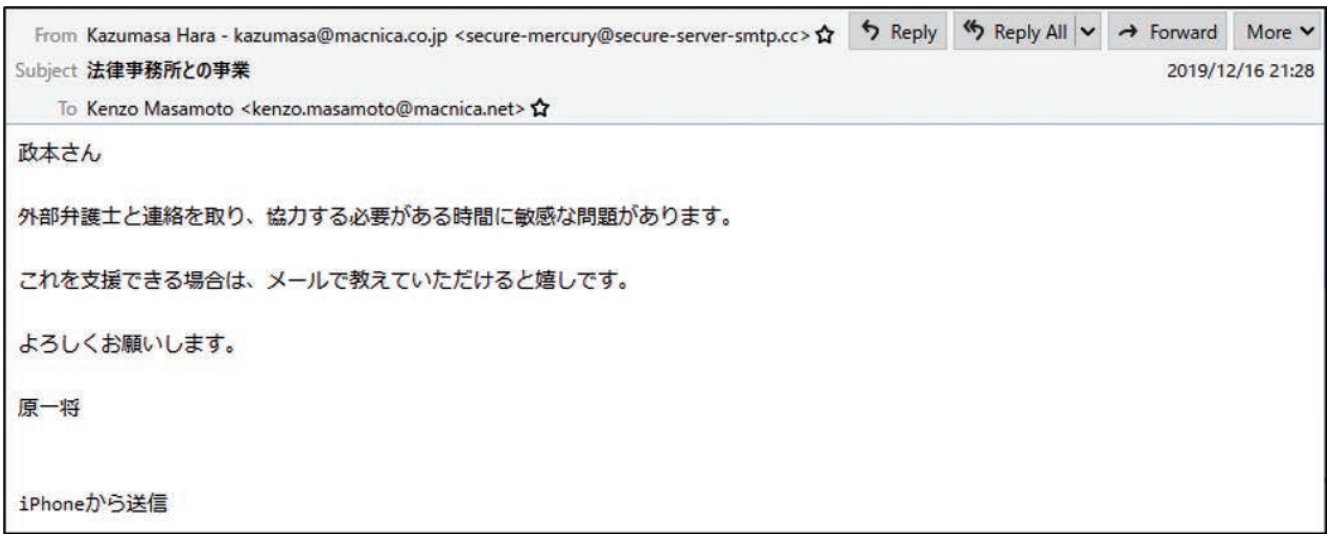


Figure 14: CEO Fraud impersonating Macnica CEO, received by the author (Masamoto)

Figure 15: Incorrect destination e-mail address

Figures 16 and 17 show BEC e-mail received by Itochu in the form of an interposition in the middle of a transaction. In either case, because the attacker is not fluent in Japanese, the wording is clearly not normal, and so to a native Japanese speaker it seems very odd. In such cases where the attacker attempts to use Japanese despite being unfamiliar with the language, they will use machine translation, resulting in unnatural wording, and so the recipient may become suspicious of and thereby recognize it is a scam.

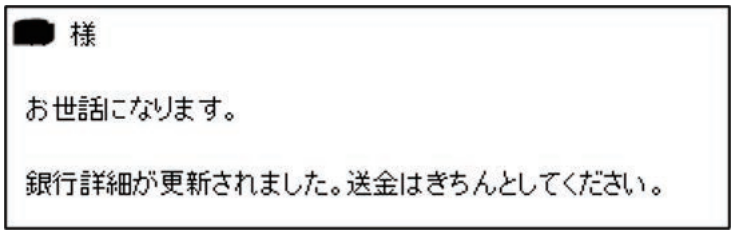


Figure 16: E-mail with unnatural Japanese received by Itochu (1)

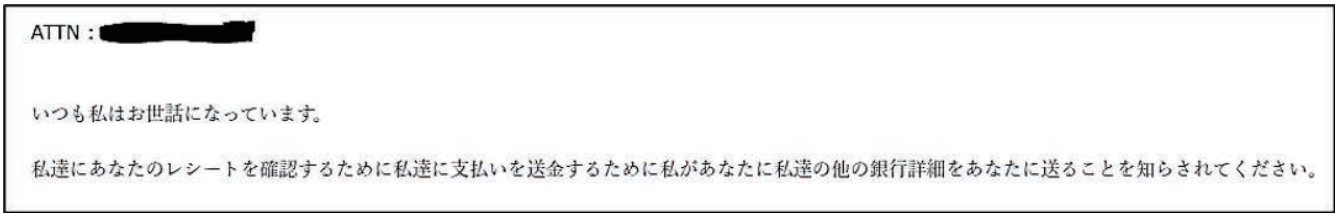


Figure 17: E-mail with unnatural Japanese received by Itochu (2)

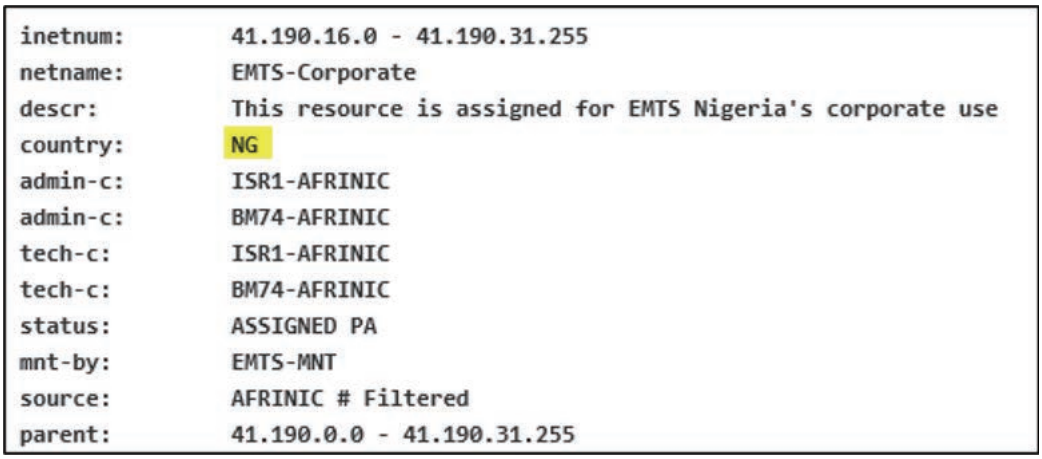
If, for example, there are members of a foreign trading partner who are capable of using Japanese, but it is not their native language, they may write e-mail with slightly unnatural Japanese. In such cases, it can be hard to judge whether the e-mail is genuine or not. In such circumstances, it becomes necessary to consider not just the writing, but also other elements to judge whether or not the e-mail could be a BEC

2.6 BEC e-mail using a hijacked e-mail account as it is

In performing analysis to determine whether or not an e-mail is a BEC, an example of a case that would be extremely difficult to determine is when a trading partner's e-mail account is hijacked and BEC e-mail is sent from that account. In analyses of whether e-mail is BEC e-mail, e-mail headers are often checked for abnormalities, but if an e-mail account has been hijacked, naturally there will be nothing suspicious discovered in the header. Obviously, this is because the fraudulent e-mail itself is delivered via the correct route. However, even in such a case, if the e-mail header is checked carefully, traces left by the attacker may still be discovered. Figure 18 shows the header of an e-mail sent to Itochu from a hijacked e-mail account, requesting a change of bank account.

Figure 18: Header of a BEC e-mail sent to Itochu from a hijacked e-mail account

At a glance, both the sender address and reply address seem to have the correct message ID and there does not appear to be anything abnormal. The sender's company is located in France, and when compared to the header of previous e-mail sent from the same company, there seems to be no abnormality. Both the date and time zone (UTC+2) shown in the header match the time zone for France. However, when the e-mail header is checked carefully, just one abnormality can be seen. That abnormality is the addition of the header "X-Originating-IP." Investigation of the information on the designated IP address reveals that it is a Nigerian IP address, as shown in Figure 19. A French company would not have a Nigerian IP address as its original IP address. For this reason, it was inferred that the trading partner's e-mail account had been hijacked and the attacker had made a connection from Nigeria to send fraudulent e-mail.



```
inetnum:        41.190.16.0 - 41.190.31.255
netname:        EMTS-Corporate
descr:          This resource is assigned for EMTS Nigeria's corporate use
country:        NG
admin-c:        ISR1-AFRINIC
admin-c:        BM74-AFRINIC
tech-c:         ISR1-AFRINIC
tech-c:         BM74-AFRINIC
status:         ASSIGNED PA
mnt-by:         EMTS-MNT
source:         AFRINIC # Filtered
parent:         41.190.0.0 - 41.190.31.255
```

Figure 19: IP address details left in the header

2.7 Forged e-mail signature

There are, no doubt, organizations that take the countermeasure of checking with the trading partner via a phone call before transferring money; however, some attackers will turn this countermeasure to their advantage and include a phone number in the e-mail signature that will connect to the attacker. When the recipient calls the number, the call will go to an acting secretary service that will give a message like, “The person in charge is currently unavailable and will call you back later.” Afterward, the attacker will call the recipient of the scam mail and reassure them that the bank account number given in the e-mail is correct. It pays to not trust phone numbers given in e-mail signatures.

2.8 Contact made using LinkedIn

With LinkedIn–the SNS service for businesses–because users register the organizations they belong to, attackers can easily search for details about an organization they want to target and make contact with its members. In the US, business acquaintances are often connected to each other via LinkedIn and it has become established as a business tool. For this reason, attackers are also aware of its usefulness, and seem to be exploring ways to exploit it.

Figure 20 shows a case of a fraudulent connection request encountered by the author (Sato), in which the sender, using a false name, pretended to be the manager of a nonexistent office. Also, in the case shown in Figure 21, the attacker created a false account masquerading as the CEO of Itochu to make a connection request. Of course, in this case the attacker's lack of skill exposed their fraud. The attacker misspelled the chairman's name, used a photograph of the CFO, and even gave their location as Nigeria. It is quite a poorly made fake account. Even so, it is important to be aware that attackers can gather information and establish contact in such a way.

LinkedIn is focusing efforts on countermeasures against fake accounts, and in both these cases, when the authors issued claims on the site against these unauthorized accounts, the accounts were immediately deleted. Of course, there are cases in which attackers may misappropriate the name of your organization in order to target other organizations, and so we consider it effective to perform regular searches and monitoring in LinkedIn to check whether fraudulent accounts have been created using your organization's name.

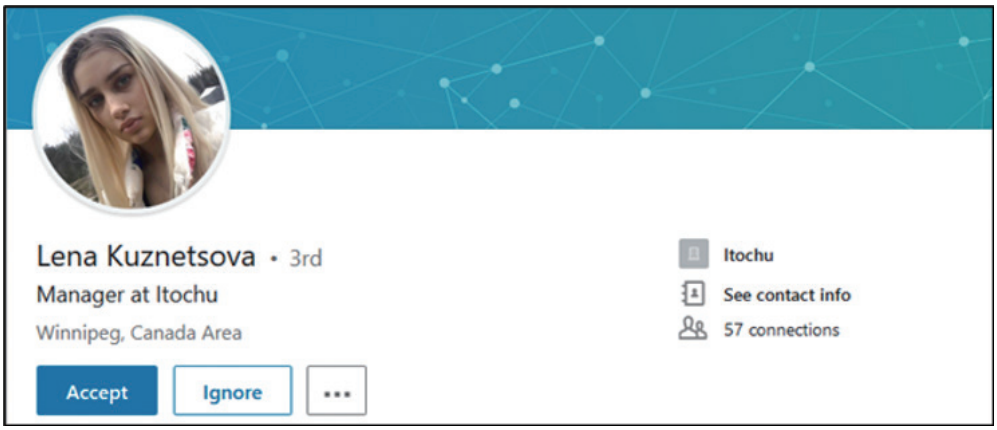


Figure 20: A LinkedIn account masquerading as a work colleague's account

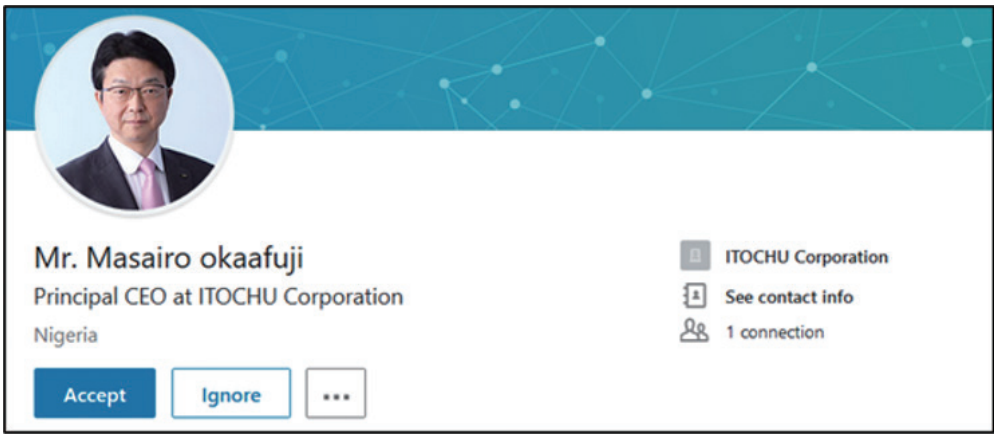


Figure 21: A LinkedIn account masquerading as an executive's account

2.9 Identity of attackers

As previously described in 2.6, in some cases it is possible to infer the source of the attack from the e-mail header or other elements. In addition to the X-Originating-IP header, time zone information about the source is sometimes included in the Date header. Moreover, if the attacker has sent a fake invoice (PDF), they may have left their time zone information in the meta data of the PDF file. In the past, there have been news reports of members of Nigerian-based criminal organizations being arrested by the FBI and other authorities, and in Japan, also, there have been similar arrests made over suspected BEC activities, including arrests of Nigerian suspects and Japanese suspects believed to have been acting under the direction of Nigerian criminal organizations operating in the background. [7] Since the age of letters and faxes to the current age of widespread internet use, it seems that Nigeria has been one of the central locations for various types of fraud, from romance scams to BEC.[8]

7 https://www.sankei.com/affairs/news/181003/afr1810030018-n1.html
https://www.asahi.com/articles/DA3S13954689.html

8 https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/

3. Sequence of events from targeting to getting money transferred (BEC Kill Chain)

It is important to not forget that there is a stage of careful preparation before an attacker sends a BEC scam e-mail. The series of actions that an attacker follows, from targeting to persuading the target to transfer money, can be divided into 5 phases in a model known as the "BEC kill chain." (Figure 22)

Figure 22: BEC Kill Chain – The series of phases from targeting to getting money transferred

3.1 Targeting via OSINT

In order to gain information on potential target organizations, such as their industry type, mission statement, management, and names of people in charge of finances, it seems that attackers often utilize organizations' Websites and SNS accounts, or services commonly used for acquiring sales leads, such as those listed below. Searching for target information from such public information sources is called OSINT (Open Source Intelligence).

Services for acquiring sales leads
Intelius - https://www.intelius.com/
leadiQ - https://leadiq.com/
lead411 - https://www.lead411.com/
Prospect.io - https://prospect.io/
SalesRipe - https://www.salesripe.com/

At the same time, attackers will utilize various OSINT tools or any leaked information they can get hold of to collect e-mail addresses that they could use as fake sender identity for scam e-mail.

3.2 Unauthorized login to e-mail accounts

To effectively carry out a scam, an attacker must gain an understanding of the conditions of a transaction in advance. In many cases, the attacker will steal the authentication information of a targeted e-mail account, illegally log in to the account, and look through the e-mail. By looking into details such as the transaction amount and scheduled time of transfer, the attacker can then carry out the scam (making a request for transfer to a designated bank account) with perfect timing. The methods used for stealing authentication information are phishing, password spraying, and malware. We will explain the details of each.

Firstly, in regard to phishing, with the recent trend of e-mail systems migrating to cloud services, we now see many cases of phishing attacks going after Microsoft Office 365 authentication information in particular. In fact, Macnica Fuji Electronics Group has also received phishing e-mail like the one shown in Figure 23 pretending to be a notification from OneDrive, one of Microsoft's Office 365 services.

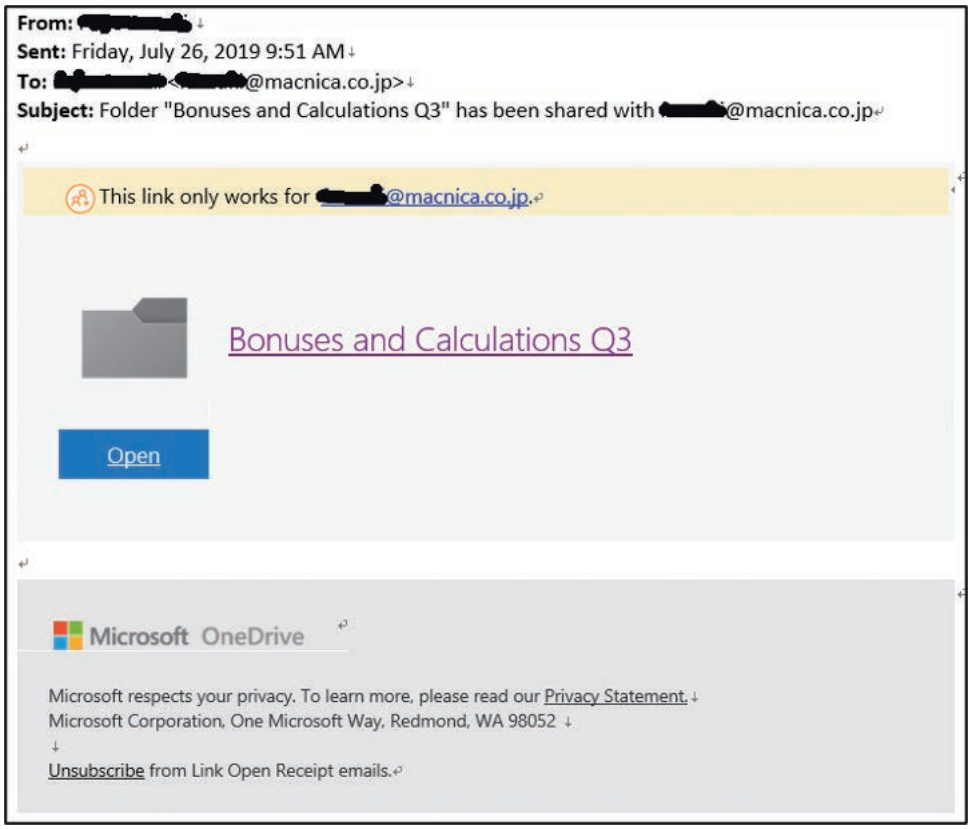


Figure 23: Phishing e-mail attempting to steal Office 365 authentication information

If the target accesses the link in the e-mail, they are directed to a phishing site mimicking the Office 365 login screen, as shown in Figure 24. This screen prompts the target to enter their password, but if the target actually does so, the password will be stolen by the attacker.

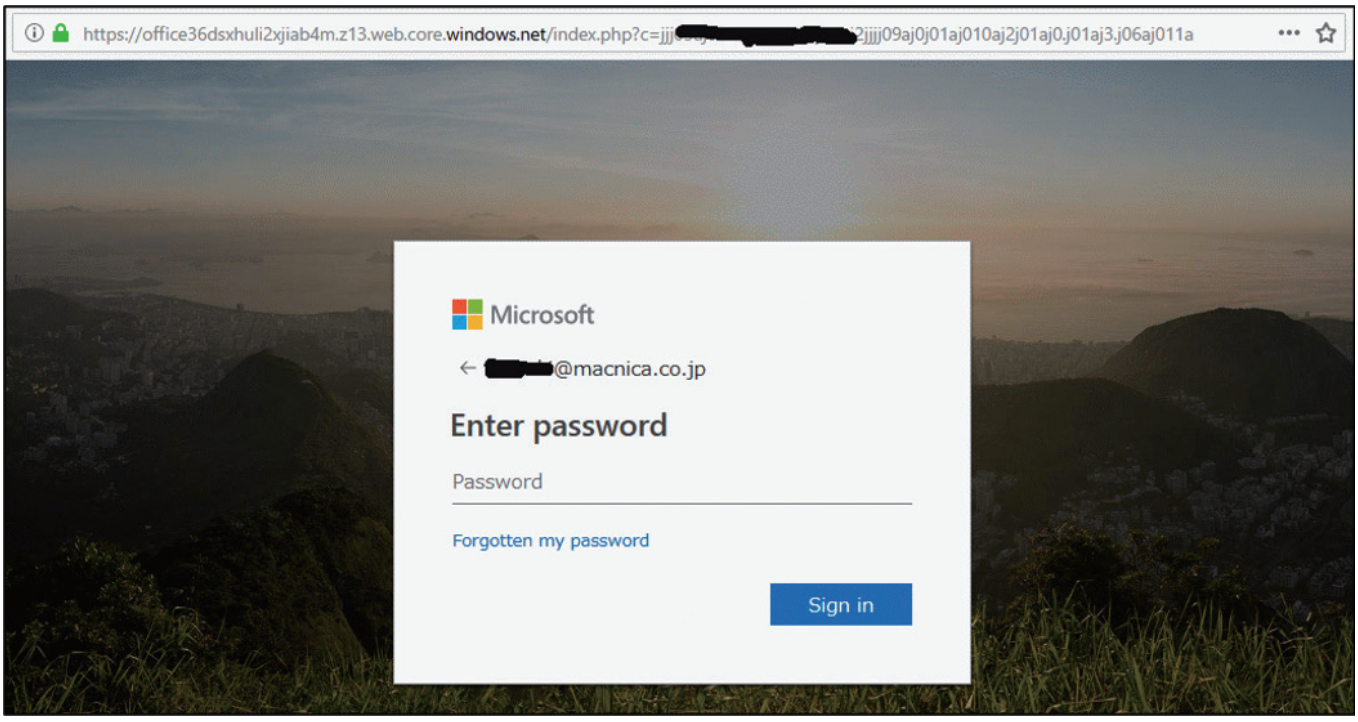


Figure 24: Phishing site mimicking the login screen of Office 365

Because the fake login screen shown in Figure 24 is hosted by the Microsoft Azure service, the domain is one owned by Microsoft (windows.net), and so the presence of the green padlock symbol indicating SSL/TLS connection, as shown in Figure 25, makes it relatively hard to recognize that this is a phishing site.

Figure 25: URL of the phishing site hosted on Microsoft Azure Storage

Figure 26 shows a phishing site mimicking the login screen of Outlook Web Access (OWA).

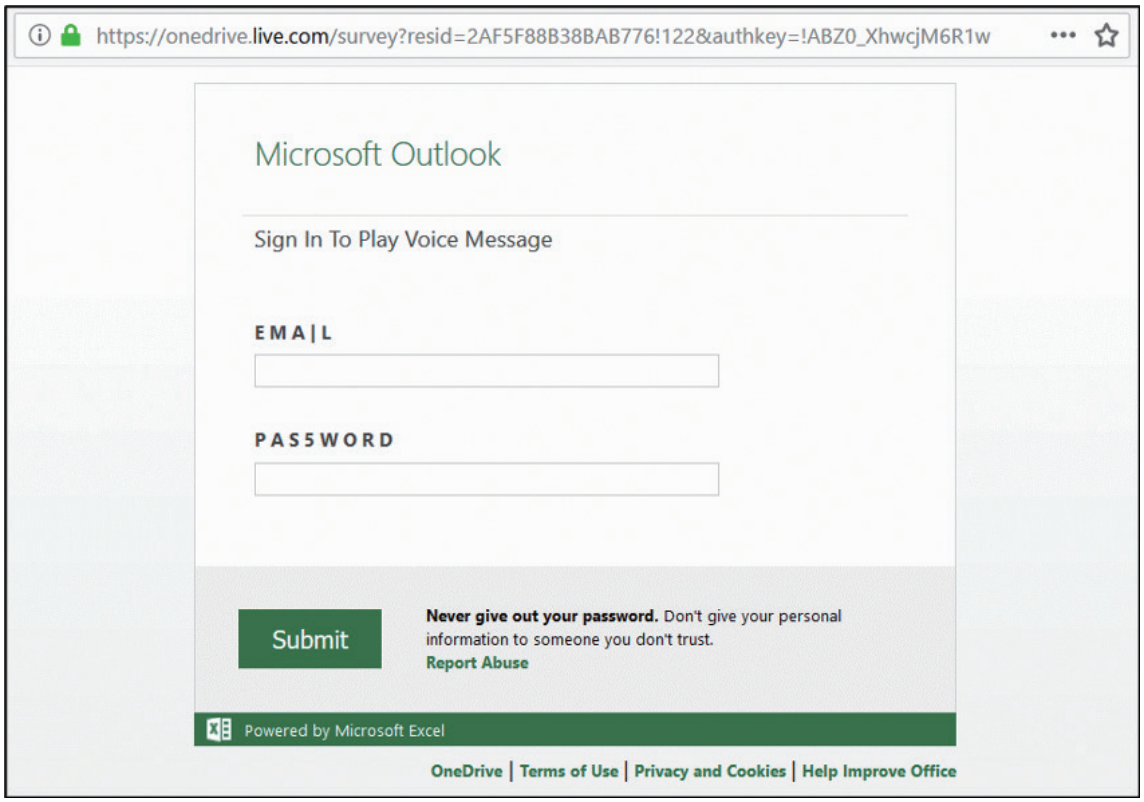


Figure 26: Phishing site mimicking the login screen of Outlook Web Access (OWA)

A close look at the fake login screen reveals that what should be the prompts "**EMAIL**" and "**PASSWORD**" actually have the suspicious misspellings of "**EMA|L**" and "**PAS5WORD**", which is likely done to avoid detection. Also, the bottom of the page contains the description "Powered by Microsoft Excel," indicating that this form was made with the Excel survey function, which is also suspicious. And yet, as shown in Figure 27, because the domain is one owned by Microsoft (live.com), as with the case shown in Figure 24, the presence of the green padlock symbol makes it seem like a legitimate site at first glance.

Figure 27: URL of a phishing site hosted on Microsoft OneDrive

In either case, this kind of phishing attack is the most commonly used method of stealing e-mail account authentication information.

The next most commonly used method is a password spraying attack on an e-mail system. Brute-force attacks, which involve trying out all possible combinations of IDs and passwords, can be ineffective because an account may become locked if numerous login failures occur with the same ID. For that reason, password spraying attacks do not involve successive login attempts using the same ID, but rather the testing of a single password with multiple IDs, avoiding account locking by spreading out the intervals between login attempts with any given ID. It has been reported that password spraying attacks on Office 365 IMAP and POP have caused a lot of damage.[9] Because two-factor authentication cannot be implemented with legacy authentication protocols like POP or IMAP, they become targets of password spraying. We strongly recommend disabling such legacy authentication.

The last method we will discuss is the theft of authentication information using malware. The use of InfoStealer type malware (LokiBot, Agent Tesla, etc.), RATs (Adwind RAT, NetWire, NanoCore, DarkComet, etc.), and Keylogger (Ardamax, etc.) in the preparatory stage of BECs has been reported by multiple security vendors.[10] Several of these types of malware have actually been discovered in BEC cases dealt with through the incident response service that Macnica Networks provides.

3.3 Mailbox reconnaissance

If an attacker is able to make an unauthorized login to an e-mail account, the attacker will look through the content of e-mail exchanges in order to gain an understanding of transaction conditions. The attacker may set the forwarding rules to forward e-mail to the attacker's own e-mail address. By setting the forwarding rules, the attacker no longer needs to make an unauthorized login every time they check the target's e-mail. This means they can reduce the amount of effort they need to go through, as well as their risk of being detected. By looking through the content of e-mail exchanges, an attacker can gain an understanding of the details of a transaction, the amount of money, the timing of the transfer, etc.

3.4 Delivery of scam e-mail

Now, at last, we come to the phase where the attacker sends scam e-mail. Because the attacker has carried out careful preparation and reconnaissance in the previous phase, they are able to carry out the scam with perfect timing. The attacker will give a plausible excuse, such as, "We are unable to use our regular bank account due to auditing, so please transfer the money to a different account," and will urge the recipient to transfer money to an account prepared in advance by the attacker. The infrastructure used to send scam e-mail can be categorized into three types: freemail addresses, similar domains (e.g., rnacnica.com or ltochu), and hijacked e-mail addresses. In some cases, when attackers send fraudulent e-mail from hijacked e-mail addresses, in order to reduce the risk of being discovered, they will set the e-mail sorting rules so that all e-mail received from trading partners will automatically be sorted into the trash or another folder that is not normally checked. Also, to increase their credibility, they may send a fake invoice that closely resembles a genuine invoice, including details of the account to which payment is to be transferred.

3.5 Persuasion of remittance

Even if the attacker asks for a transfer to be made to a different account than the usual one, if the account name is different from the trading partner's company name, the target may be reluctant to transfer the money. In such cases, the attacker will give some sort of plausible excuse, such as, "The account is in the name of a subsidiary, so there is no need for concern," and will try to convince the target to transfer the money quickly.

9 https://www.helpnetsecurity.com/2019/03/20/imap-based-password-spraying/

10 https://threatpost.com/nigerian-bec-scammers-growing-smarter-more-dangerous/131854/
https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf

4. Approach to countermeasures

When BEC countermeasures are discussed, people tend to think only of IT-based countermeasures, but this perception is incorrect. With the understanding that there is no silver bullet for dealing with BEC, it is important to approach countermeasures with collective strength, including the perspectives not only of the IT department, but also management and the accounting department.

4.1 Recognizing BECs as a management issue

Managers need to have the following kind of understanding.

- A BEC attack could result in the loss of several billion yen.
- If an attacker masquerades as your organization to launch a BEC attack on your trading partner, your trading partner will suffer damages.
- It is necessary for various players, such as the accounting department, the IT department, and the legal department, to deal with issues comprehensively.

4.2 Strengthening of checks within the accounting department

While it is also important to implement countermeasures in the IT system, the most important thing is for the accounting department to notice any abnormalities. As a basic stance, it is important to recognize that messages such as the following are all suspicious.

- Messages claiming, “Our account has changed.”
- Messages urging, “Please transfer the money to a different account, as we are unable to use our regular bank account due to auditing.”
- Messages claiming, “Our account has been temporarily frozen due to interactions with countries under economic sanctions.”
- Messages claiming, “We are temporarily unable to use our bank account because of an economic blockade due to COVID-19.”
- Messages urging, “We want you to transfer the money to the account of our subsidiary.”
- Messages claiming, “We have discovered that there would be additional fees (processing fees, taxes, etc.), so please transfer the money to a different account.”
- Messages instructing monetary transfer purporting to be from an executive of a trading partner or your own organization
- Messages instructing monetary transfer that are worded unnaturally (either in Japanese or English)
- Messages regarding cross-border monetary transfer (with some exceptions)
- Cases in which the name of the account given for the transfer is an individual’s name or the name of a different company

Irregular changes of bank accounts used for transactions can occur due to trading partner M&A, etc. For such cases, it is also important to create in advance a list of items that the accounting department (in charge of transfers) needs to check when it receives notification of account changes or new account registrations from operating departments. For example, it is advisable to create a list containing confirmation items like the following.

- Was the account information confirmed to be correct via a telephone call?
- Was the number called for confirmation obtained from a business card or other reliable source, and not a number included in the e-mail ● signature? Or, was the telephone number checked against the numbers provided in the organization’s official website?
- Were there no suspicious elements in the explanation for the change of account?
- Does the account name match the company name of the trading partner? (Caution: In some scams, the account name may actually match the company name.)

Also, in some cases the attacker will try to make a change of bank account not just for an individual transaction, but for all transactions. In such cases, the attacker understands that they will likely be asked to provide a signed letter as part of the procedure. Although it is effective to require a letter as evidence in the verification procedures, since the attacker also understands this and will have prepared such a letter, it is important to remember to compare the letter with the previous application letter, to see whether the format, signature, and other aspects match those of the original.

4.3 Dissemination to trading partners

To prepare for the possibility that any BEC attack against your organization will also be made against your trading partners, it is necessary to share the following things with trading partners.

- Notify them that your organization will never request a change of bank accounts used for transfers via an e-mail message.
- Tell them in advance the number they should call to consult with your organization about anything unusual.

While your trading partners should be responsible for any damages they may suffer due to their own unpreparedness, in some cases it could lead to problems affecting business, such as organizational weaknesses causing financial problems or disputes over who is to blame causing poor relations. To eliminate the possibility of a BEC within a trading partner, so as to avoid falling into such a situation, it is necessary for both parties to properly align their awareness regarding BECs in advance.
Moreover, because some organizations may be outsourcing their accounting work, and BEC attackers have been known to also pull scams on such outsourcing companies, it is necessary to share awareness of BEC risks with outsourcing companies in the same manner as with trading partners.

4.4 Multi-factor authentication

As explained in the discussion of the BEC kill chain, attackers will attempt unauthorized login to e-mail accounts in order to look through e-mail. Multi-factor authentication is an extremely effective method for reducing the risk of unauthorized login, even a little. Also, because multi-factor authentication cannot be mandated with legacy authentication protocols like POP or IMAP, we strongly recommend disabling these protocols. In particular, even if you are using a cloud service like Office 365 or G-Suite, we recommend that you check whether legacy authentication is enabled.

4.5 Warnings about receiving messages from freemail addresses

Attackers often exploit freemail services such as Gmail and Yahoo Mail, and have also shown a tendency to use e-mail addresses registered with the freemail service mail.com, shown in Figure 28, likely in the expectation that recipients will be unfamiliar with it.

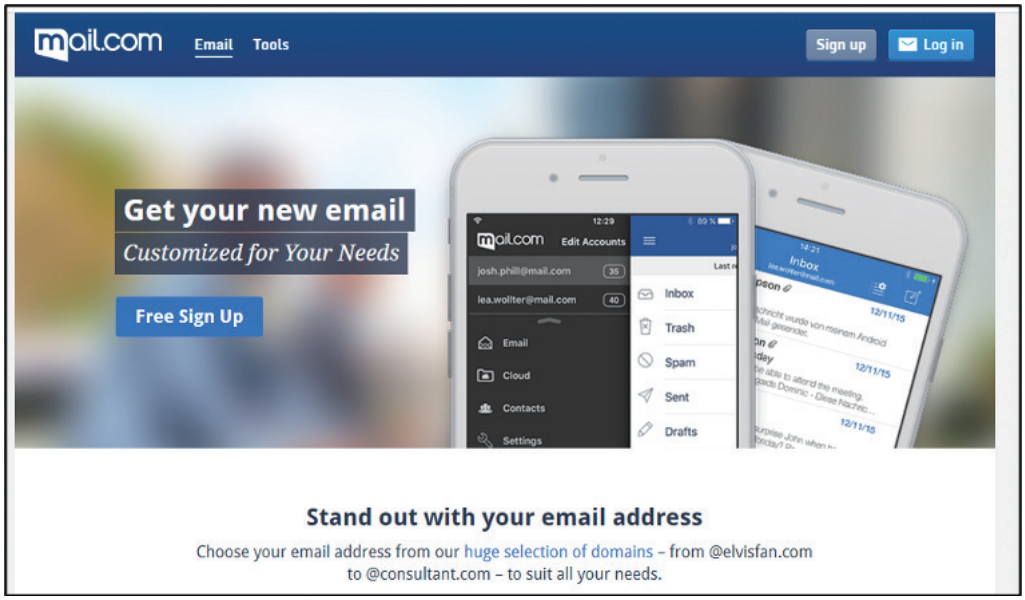


Figure 28: The mail.com freemail service

For this reason, setting up a spam filter or other such tool, and applying a subject marker that clearly identifies e-mail received from freemail addresses, with a focus on identifying domains held by mail.com, has the effect of encouraging a certain degree of caution among recipients. If an attacker appropriates e-mail from an exchange and proceeds to send e-mail under the same subject, a specific character string will appear in the subject line to identify that the delivery is from a freemail service, as shown in Figure 29, which will distinguish the scam e-mail from the subject line of past exchanges and increase the likelihood of the recipient recognizing an abnormality.

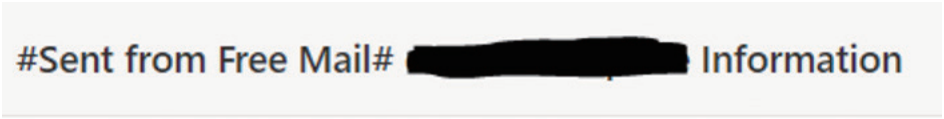


Figure 29: Example of a marker in the e-mail subject line to indicate that it has been sent from a freemail address

Because there are a great many small and medium-sized enterprises in Southeast Asia that use freemail for their business, restricting the reception of deliveries from freemail addresses would create difficulties in business operations. For that reason, unilaterally applying a subject marker to identify all e-mail deliveries from freemail accounts is an effective measure. It is also possible to implement a plugin to the mailer so that it will respond to specified domains and notify users if they receive any e-mail from a freemail account. (Figure 30)

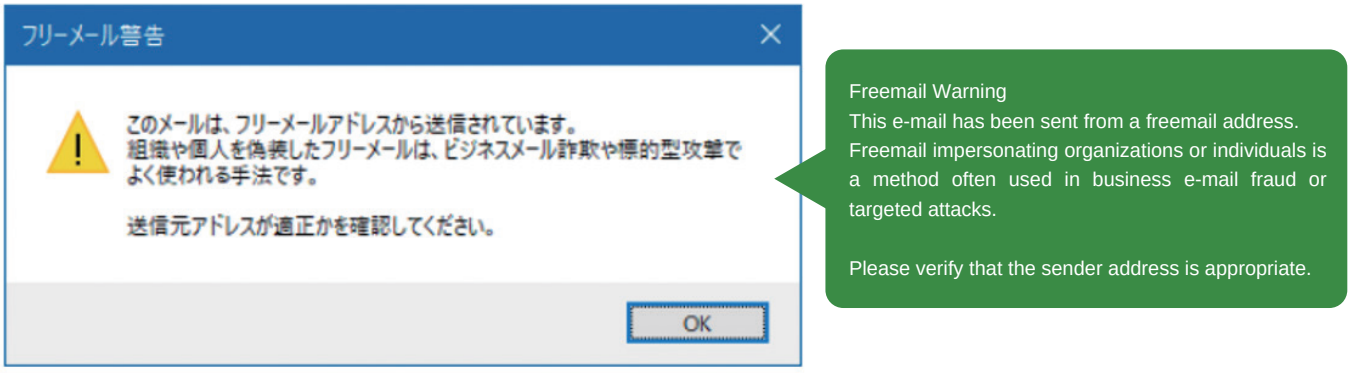


Figure 30: Dialog warning of e-mail sent from a freemail account

4.6 Warnings about deliveries to freemail addresses

As with receiving freemail messages, it is also effective to have warnings when a reply is being made to a freemail address. Although, unlike e-mail reception, it is hard to perform verification of outgoing e-mail through a spam filter or similar tool, it is possible to do so through implementation of a plugin to the mailer. (Figure 31)

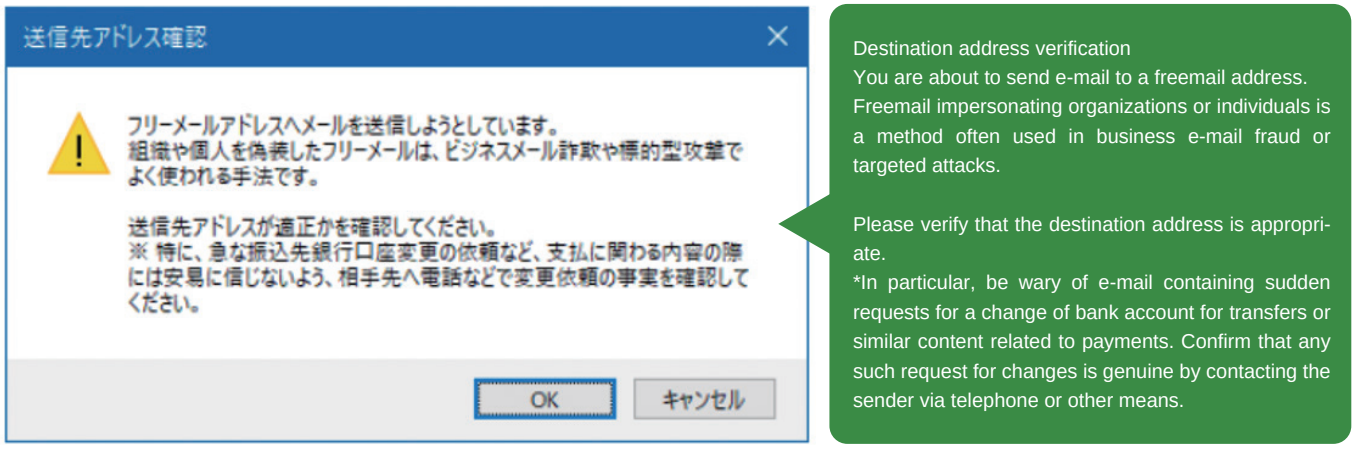


Figure 31: Dialog warning that e-mail is being sent to a freemail account

This kind of control is effective even if the attacker falsifies the sender address and sets the reply destination (Reply-To) as a freemail address.

4.7 Warning of when sender address and reply address do not match

There are a great many cases where an attacker will disguise the sender information (From header) to look like the proper sender information, while making the reply destination (Reply-To) the attacker's own e-mail address. For this reason, a warning function that alerts the user when the sender information and reply address do not match is useful for recognizing abnormalities. (Figure 32)

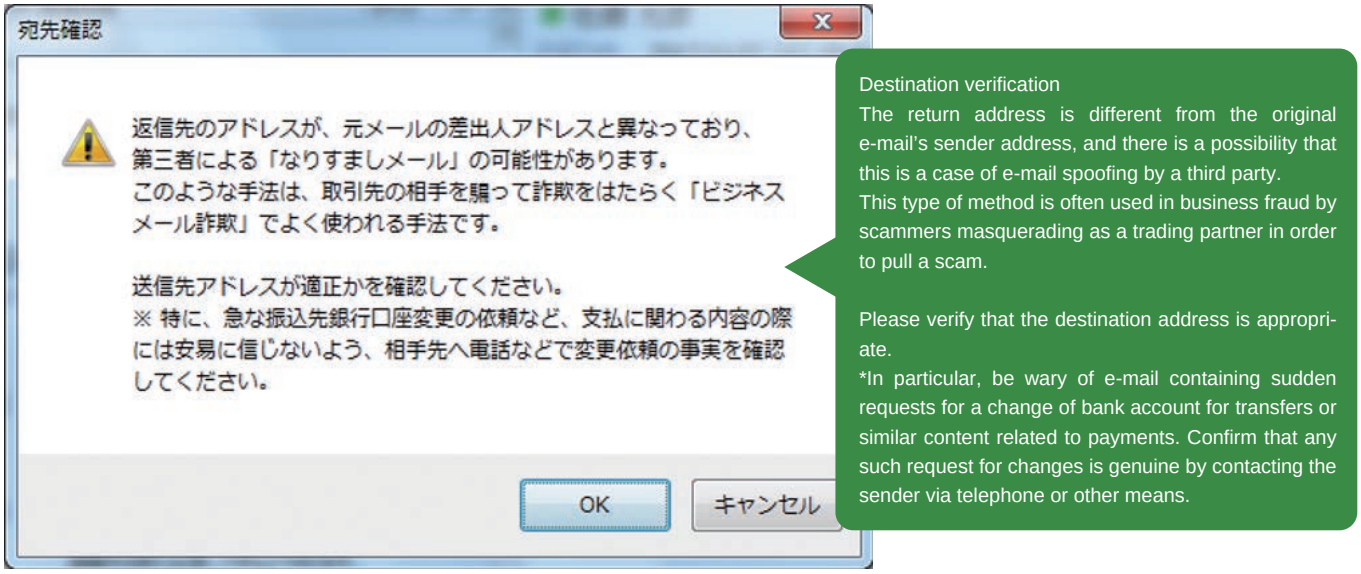


Figure 32: Dialog warning that the sender's address (From) and reply address (Reply-To) do not match (Japanese)

4.8 Detection of e-mail received from an unreliable TLD

Freenom is a service that allows people to acquire domains with specific TLDs (.tk .ml .ga .cf .gq) free of charge, but because these are exploited for cybercrimes more often than other TLDs, they should, as a rule, be set as targets for detection or blocking. (Figure 33)

Figure 33: Freenom domain service

However, the TLDs that can be used with freenom also represent the names of various countries, such as .ml for Mali and .ga for Gabon, and in some cases the governments of those countries do in fact use those TLDs for their official domains. Because of this, it is necessary to implement complete restriction against freenom itself, after first verifying the extent of its utilization within your own organization.

4.9 Detection of e-mail received from an address with a TLD before the @ symbol

In some cases, an attacker may use an address with a TLD before the @ symbol to try and make it seem a little less unusual. E-mail addresses like those in the examples below are seldom used in actual business and often used by attackers, so they should be flagged as potentially dangerous e-mail and copies should be checked by system administrators.

Services for acquiring sales leads	lead411 - https://www.lead411.com/
Intelius - https://www.intelius.com/	Prospect.io - https://prospect.io/
leadiQ - https://leadiq.com/	SalesRipe - https://www.salesripe.com/

Through the monitoring of this type of address and abnormal e-mail sent through freemail or unreliable TLDs, as previously described, Itochu was able to discover two BEC e-mails in 2019 and thereby prevent the attacks. There are numerous such e-mails monitored every day, almost none of which are legitimate business-related e-mail. (Any legitimate e-mail that is encountered can be accommodated by use of a white list.) Considering the potential damage of a BEC, this can be considered an effective, low-cost solution.

4.10 Searching for similar domains

It is sometimes possible to discover BECs by checking whether there are any domain names registered that are similar to that of your own organization. Domains with different TLDs or possible mistypings of domain names can be searched for using free services such as those provided by the sites indicated below (Figure 34). However, these services do not perform searches that take into consideration the replacement of characters with visually similar characters, such as rnacnica.com or ltochu.

Services that can be used to search for similar domains:
https://dnslytics.com/domain-typos
https://dnpedia.com/tlds/search.php
https://dnstwister.report/

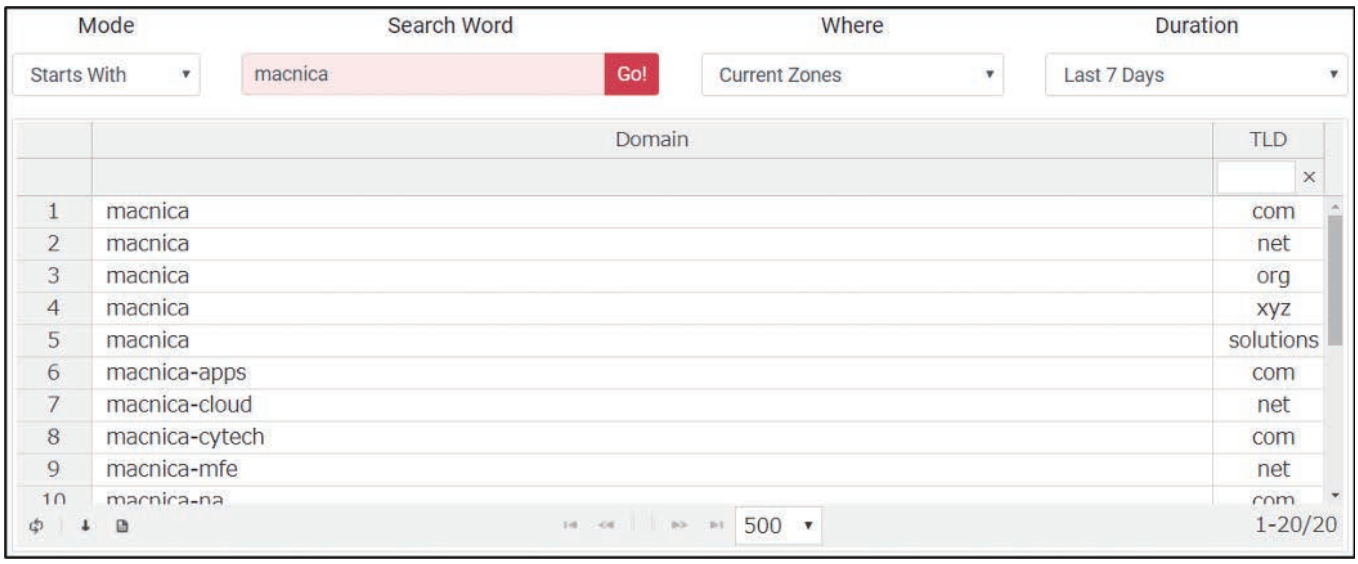


Figure 34: A service used to search for similar domains

4.11 DMARC

By implementing DMARC, you can get an understanding of the destinations and extent of e-mail that imitates your own organization's domain. This makes it possible to prevent any actual damages from occurring within trading partners due to BEC attacks masquerading as your own organization. However, this is only effective if an attacker uses a fake domain using the exact same domain as that of your organization, and DMARC does not work for detecting similar domains, (e.g., rnacnica.com or ltochu). Also, for DMARC to be effective, it needs to be implemented in both organizations (at both the sender's end and the recipient's end), and the fact that its level of use within Japan is currently extremely low is an issue.

5. Incident responses

If a BEC attack is encountered, regardless of whether it is successful or not, various actions must be taken. Here, we describe several items that would actually require a response.

5.1 Contacting banks or law enforcement agencies (for recovery of transferred money)

If a transfer has been made to an attackers account, above all, it is necessary to take steps to recover the transferred money as soon as possible. Communication and cooperation with local investigating authorities and financial institutions should be carried out in collaboration with your own organization's legal department. It goes without saying that the sooner such actions are taken, the better.

5.2 Checking that e-mail accounts have not been compromised

As shown in the section about the BEC Kill Chain, to gain an understanding of transaction details, it is a common tactic for an attacker to steal e-mail account authentication information in advance. In the case of a scam being carried out with a great deal of understanding about transaction details, it is highly likely that the e-mail account of either your own organization or your trading partner has been compromised. Specifically, you can confirm whether an e-mail account has been compromised by an attacker by checking the following points.

Confirmation items:
Check that there are no suspicious forwarding rules.
Check that there are no e-mail sorting rules applied.
Check the log for any unauthorized login.

5.3 Checking that there is no malware infection

As previously described in 3.2, malware such as InfoStealer, RAT, and Keylogger are sometimes used to steal e-mail account authentication information, so it is advisable to check whether PCs have been infected with such malware. Takes such measures as updating antivirus definition files and performing a full scan, or using a specialized tool to search for any traces of malware intrusion.

5.4 Changing of passwords

All passwords related to e-mail accounts that may have had unauthorized login or passwords of accounts that have been used on any PC suspected to be infected with malware should be changed.

5.5 Takedown of domains acquired by attackers

In cases where domains similar to that of your own organization have been acquired, if they are not taken care of then the attackers will continue to masquerade as your organization to make BEC attacks on your trading partners To prevent that, consult the domain registrar's abuse contact and request a takedown of the domain in question. You can verify the domain registrar and abuse contact (e-mail address) from Whois information. As the domain registrar will often require reasonable evidence, it is recommended to submit a screenshot of the BEC e-mail, or similar evidence. Depending on the domain registrar, in some cases the response may be slow or may not seem to be sufficiently aggressive, but it is important to be persistent and keep up negotiations until the problem domains are taken down.

5.6 Negotiations and division of damages with trading partners

As previously described in 2.4, if your organization incurs any actual damages (i.e., the transfer of money to an attacker) due to a BEC masquerading as a trading partner, it is possible that a security problem has occurred at the trading partner's end (e.g., compromised e-mail accounts). If both parties can recognize this, it may be possible in some cases to negotiate a proportional division of the damages (the amount lost in the transfer). Conversely, if a trading partner incurs any actual damages due to a BEC masquerading as your own organization, it is possible that a security problem has occurred at your organization's end, and in some cases it may be necessary to divide damages proportionally.

Macnica Networks Corp.
Macnica Bldg. No. 2
1-5-5 Shin-Yokohama, Kohoku-ku, Yokohama, Kanagawa Prefecture
222-8562 Japan
TEL: 045-476-2010
https://www.macnica.net