Fighting Business Email Compromise with Kaspersky Security for Microsoft Office 365

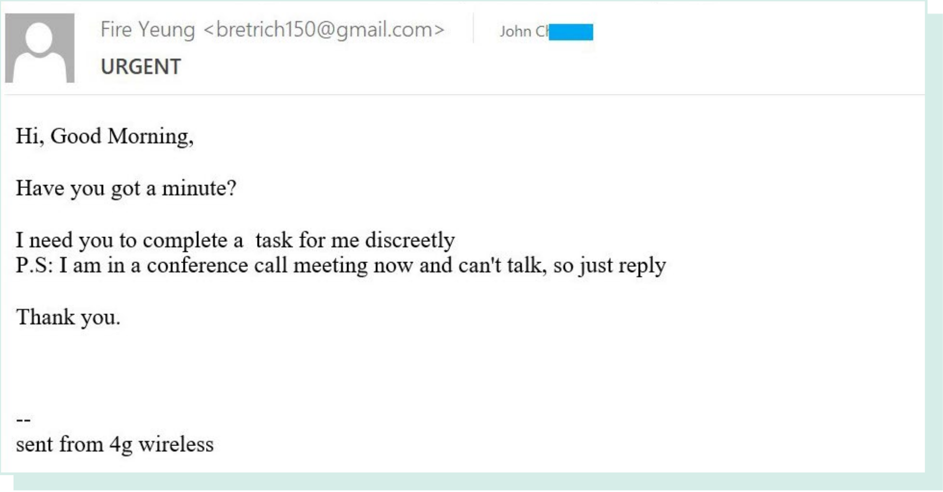
kaspersky

What is BEC?

Business Email Compromise (BEC) is a form of phishing where scammers attempt to convince their victim to transfer money to the attackers' accounts by posing as some sort of authorized representative. Important sensitive data can be obtained in this way, in addition to conducting simple financial fraud, and the goal may be to cause reputational damage to the organization under attack.

Organizations around the world are falling victim to this type of financial fraud. In 2019, as a result of a BEC attack, St. Ambrose Catholic Parish in Brunswick (USA, Ohio) lost $1.75 million from church funds. And at the end of 2019/start of 2020, the government of Puerto Rico lost approximately $5 million as a result of a series of such email phishing attacks.

In a BEC attack, the attacker relies on the victim not being too attentive, and uses a domain or sender name in the 'From' field extremely similar to one the victim would be familiar with.



Fire Yeung <bretrich150@gmail.com> John C[redacted]

URGENT

Hi, Good Morning,

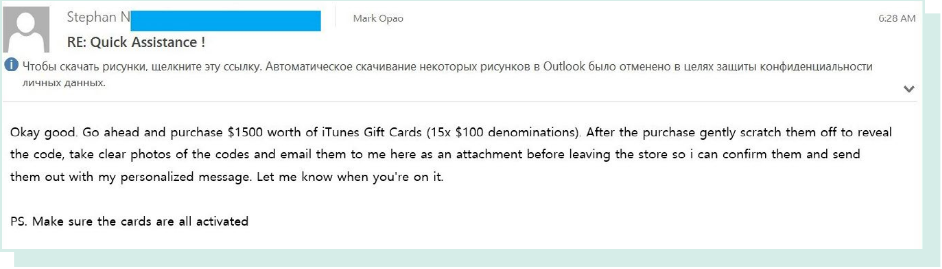
Have you got a minute?

I need you to complete a task for me discreetly
P.S: I am in a conference call meeting now and can't talk, so just reply

Thank you.

--
sent from 4g wireless

Building comprehensive security in the contemporary threat landscape is impossible without effective Endpoint Detection and Response (EDR), offering security managers a real-time view of any threat, no matter how complex. EDR provides such essential capabilities as deep visibility and the ability to reveal the true scope and root cause of threats, as well as instant automatic response across all endpoints. A vendor on your short list must demonstrate these EDR capabilities as well as ways to increase security efficiency with automation, simple controls and deployment.



Stephan N[redacted] Mark Opao 6:28 AM

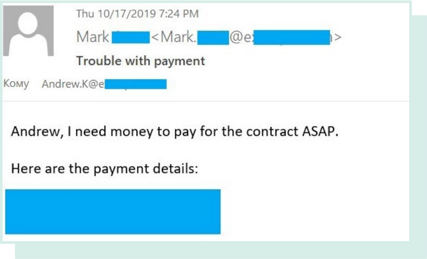
RE: Quick Assistance !

Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

Okay good. Go ahead and purchase $1500 worth of iTunes Gift Cards (15x $100 denominations). After the purchase gently scratch them off to reveal the code, take clear photos of the codes and email them to me here as an attachment before leaving the store so i can confirm them and send them out with my personalized message. Let me know when you're on it.

PS. Make sure the cards are all activated

This type of threat is called Internal BEC: an attack that occurs from one or more of the organization's internal addresses.



Thu 10/17/2019 7:24 PM

Mark [redacted] <Mark.[redacted]@e[redacted]>

Trouble with payment

Кому Andrew.K@e[redacted]

Andrew, I need money to pay for the contract ASAP.

Here are the payment details:

[redacted]

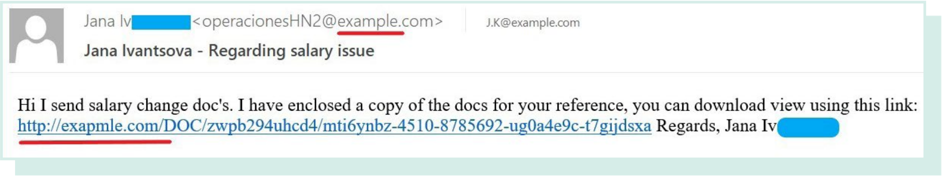
Why are Internal BEC attacks so dangerous?

Unlike ordinary BEC attacks, which rely on the recipient's inattention or lack of email authentication checks, Internal BEC attacks are indistinguishable from any normal message from a company employee in terms of their 'technical' details.

Because the attacker's address is genuine, and the request to transfer money or provide information is framed as something pressing and urgent, an unsuspecting recipient is likely to fall for the scam and fulfil the attacker's demands.

Scammers can also use fake (phishing) sites in Internal BEC attacks, using an address which may differ from that of the attacked organization by just one or two letters - easily overlooked. For example, a scammer might replace a lowercase L('l') with a capital i ('I'), which is completely indistinguishable to the naked eye. Such a phishing site may contain a payment form, or a survey used to obtain confidential information, for example.

In these cases, the attacker doesn't need to conduct a long correspondence with the victim to persuade them to transfer the required amount to their bank account, or to provide sensitive information - they simply insert a link to the fake website in their message.



Jana Iv[redacted] <operacionesHN2@example.com> J.K@example.com

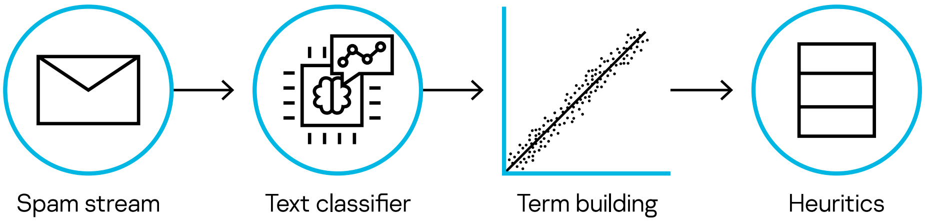
Jana Ivantsova - Regarding salary issue

Hi I send salary change doc's. I have enclosed a copy of the docs for your reference, you can download view using this link: http://exapmle.com/DOC/zwpb294uhcd4/mti6ynbz-4510-8785692-ug0a4e9c-t7gijdsxa Regards, Jana Iv[redacted]

Protection against Internal BEC threats in Kaspersky Security for Office 365

Kaspersky researchers are constantly working to improve the protection of email traffic from the most complex threats, including Internal BEC. The main focus is on email content, given that the technical headers of a malicious Internal BEC email will be the same as those of a genuine email from that colleague or department.

Millions of spam messages enter our email traps from around the world every day. To isolate messages from this stream, and subsequently the text that contains signs of fraud, we use a complete ensemble of machine learning classifiers.



In order to learn how to work with the text, we use a language model that is based on AWD-LSTM architecture (Average-Stochastic Gradient Descent (SGD) Weight-Dropped LSTM), which is a recurrent neural network. This model is trained using a very large number of texts obtained from open sources in a specific language. After the model has been trained, we can begin to reuse it for text classification (transfer learning). The classifier, in turn, is trained using a very small amount of data. To explain how this works, let's draw an analogy with human learning. Having read a lot of books in English and gradually learnt the language, we are then shown the phrase "Roses are red" and have to choose the corresponding phrase from the examples below:

- "Violets are blue"
- "Work is over"
- "Green Card"

As we understand that the original phrase is talking about both flowers and color, we choose the first option. Our model learns to draw conclusions in exactly the same way, but working with examples of fraudulent phrases.

After the emails have been filtered by content, we analyze the text and extract the most relevant fraudulent phrases. The logit model is responsible for this process (Logistic regression with L1 regularization). Training takes place using n-grams from texts obtained as a result of primary filtering of the messages. Validation is carried out on the same data. Thanks to combining the two algorithms, we automatically extract malicious text from the streams and create terms for detecting suspicious messages.

We create heuristics that detect and stop Internal BEC attacks by combining and considering a combination of these terms, and analyzing in an email those domains that are similar to the sender's own.

However, we should never omit to be vigilant, despite of the continuous improvement in protection systems against Internal BEC. As with any BEC threat, users need to respond very carefully to messages that contain a request for a financial transfer or the disclosure of confidential data. If you receive a message from a colleague asking you to transfer a certain amount of money, or share data from an internal report, the best advice might be to implement your own 'two factor authentication' — call your colleague, write to them in a messenger or speak in person to clarify the details.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.