The day email encryption becomes commonplace is the day fraud emails die

The Internet Crime Report 2023 released by the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI) said, Business Email Compromise (BEC) caused $2.9 billion in losses to US companies in 2023, becoming the second most destructive Internet crime. Between October 2013 and December 2023, BEC attacks caused nearly $55.5 billion in losses to US and global organizations. So, FBI has made the following recommendations to reduce BEC attacks:

(1) Use multi-factor authentication (MFA) and multi-factor two-step verification to confirm requests to change payment account information.

(2) Use a unique password for each online service, and try to change your passwords regularly.

(3) Make sure the URL in the email is associated with the business/individual it claims to be from.

(4) Watch out for hyperlinks that may contain misspellings of real domain names.

(5) Never provide login credentials or personally identifiable information (PII) via email, even if the request appears legitimate.

(6) Verify the sender's email address, especially when using a mobile or handheld device, to ensure it matches the sender.

(7) Ensure that employee computer settings allow viewing of full email headers and other extended information.

(8) Monitor financial accounts regularly for unusual activity, such as missing deposits.

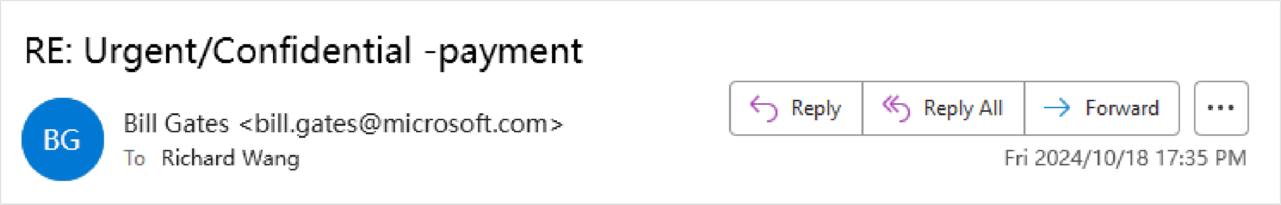
The UK National Cyber Security Centre (NCSC) has also designed an easy-to-understand PDF leaflet specifically for EBC attacks, explaining in detail what BEC attacks are and how to prevent them. Business email compromise (or BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information. The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain viruses disguised as harmless attachments, which are activated when opened. Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect. BEC is a threat to all organizations of all sizes and across all sectors, including non-profit organizations and government.

The author has written this article through case analysis of various emails sent to victims by BEC attacks to make it clear to everyone that only by popularizing the use of S/MIME email encryption technology can all BEC attacks be prevented. The suggestions of the FBI and NCSC can only play a certain role in helping but cannot completely solve the problem. Only by popularizing email encryption can BEC attacks be truly and effectively prevented, and email fraud be completely eliminated.

1. Email digital signatures can guarantee the trusted identity of the email sender and ensure that the recipient will not be deceived!

The first characteristic of a BEC attack is that an attacker impersonates a company executive to send an email to the financial staff to request payment or change the approved payee information. This is an attack launched by the attacker by exploiting a design vulnerability in emails, because the sender's email address can be written casually, and it can be written as the same email address as the company's CEO to send fraudulent emails. Although there are currently SPF, DKIM, DMARC and other sender identity verification standards, not all email systems and email clients support these standards, and even if they do, they cannot effectively block all attacks.

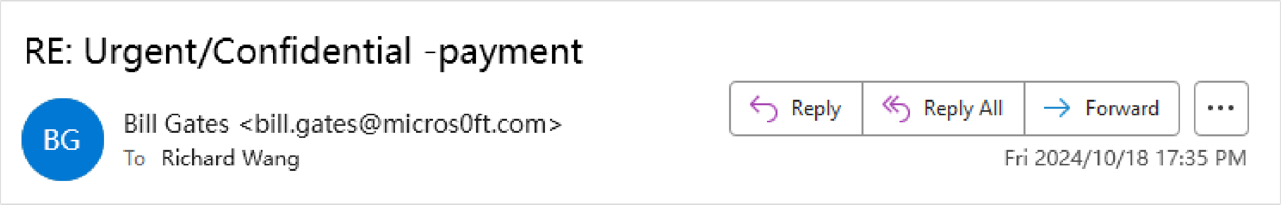
Even if the email server intercepts the emails from the fake email address after strictly verifying the sender's identity according to these standards, the attacker can still register a similar fake identity domain name to pass these strict verifications and successfully deliver the fraudulent email. As shown in Figure 1 below, the email sent by the real email address looks like a real email address (the figure is a simulation effect), and Figure 2 below is an email sent by an email address with a fake domain name that looks very similar to real domain (note the difference between 0 and o), and Figure 3 below is caused by the problem that the email client (such as Outlook) cannot fully display the long domain name and displays the email address that looks like a real email address, but actually hides the fake domain name behind it. It can be seen that most people cannot identify the authenticity of these seemingly real email addresses. This is why the NCSC requires to ensure that all important email requests are verified using other methods (such as SMS, phone, account login or confirmation by mail or in person).


RE: Urgent/Confidential -payment

Bill Gates <bill.gates@microsoft.com>
To Richard Wang

Fri 2024/10/18 17:35 PM

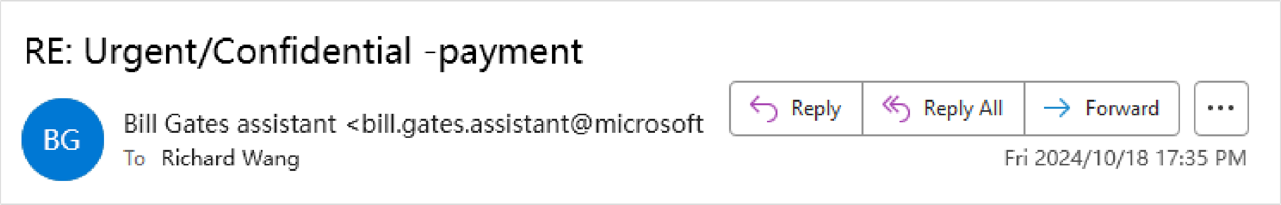
Figure 1 The fake email sender looks innocent


RE: Urgent/Confidential -payment

Bill Gates <bill.gates@micros0ft.com>
To Richard Wang

Fri 2024/10/18 17:35 PM

Figure 2 Email address using fake domain name

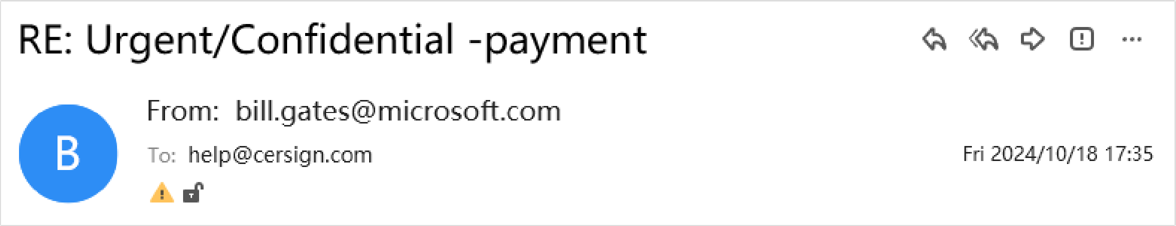

RE: Urgent/Confidential -payment

Bill Gates assistant <bill.gates.assistant@microsoft
To Richard Wang

Fri 2024/10/18 17:35 PM

Figure 3 Outlook cannot display the complete email address

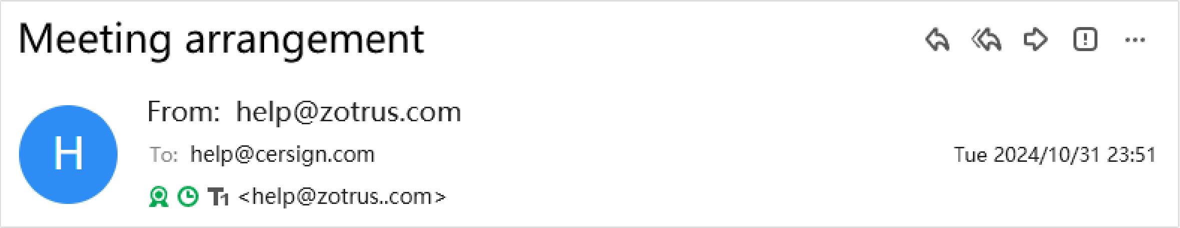
However, if you use ZT Browser to send and receive emails, ZT Browser do not display the sender’s name since the names set by the sender is not a trusted identity information, so only display the email address. All emails without digital signatures will display a warning exclamation icon and a black unlock padlock below the receiver email address line, it means this email has no digital signature and is not encrypted, to remind users whether the sender's identity is trusted, as shown in Figure 4 below. If there is a digital signature, the email address bound to the signer's email certificate and the identity information validated in the email certificate will be displayed. For senders who only validated the email address, the T1 trust level icon and the verified sender's email address will be displayed, as shown in Figure 5 below.


RE: Urgent/Confidential -payment

From: bill.gates@microsoft.com
To: help@cersign.com

Fri 2024/10/18 17:35

Figure 4 UI for emails without digital signature and encryption



Meeting arrangement

From: help@zotrus.com

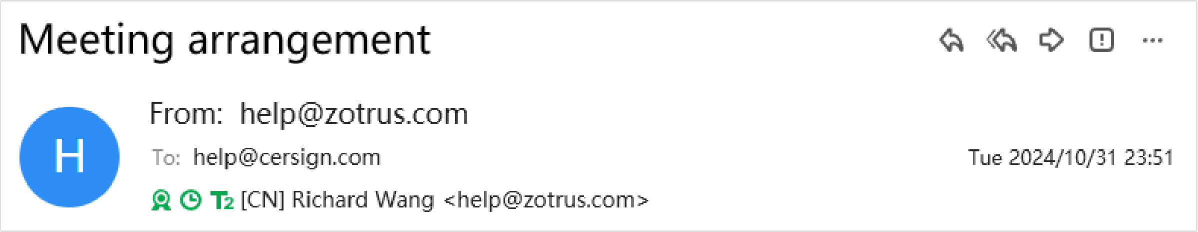
To: help@cersign.com

Tue 2024/10/31 23:51

T1 <help@zotrus..com>

Figure 5 UI for emails with digital signature (MV users)

For senders who have completed individual identity validation, the digitally signed email will display the T2 trust level icon, the sender's validated name and email address, as shown in Figure 6 below. For senders who have completed organizational identity validation, the digitally signed email will display the T3 trust level icon, sender email address and company name, but will not display the sender's name because the sender's individual identity has not been validated, as shown in Figure 7 below. For senders who have completed organizational identity validation and individual identity validation, the digitally signed email will display the T4 trust level, sender name, email address and organization name, as shown in Figure 8 below.



Meeting arrangement

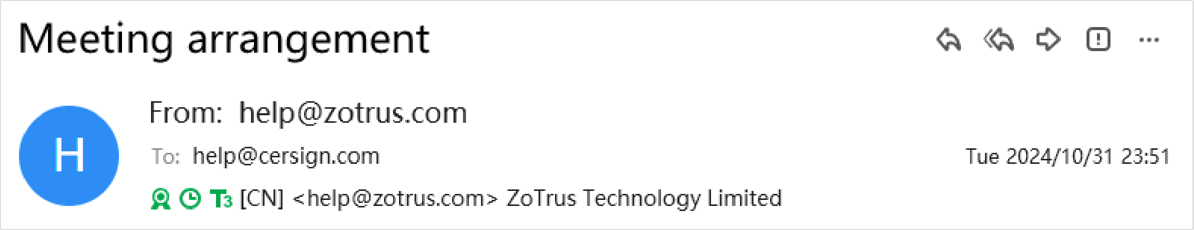
From: help@zotrus.com

To: help@cersign.com

Tue 2024/10/31 23:51

T2 [CN] Richard Wang <help@zotrus.com>

Figure 6 UI for emails with digital signature (IV users)



Meeting arrangement

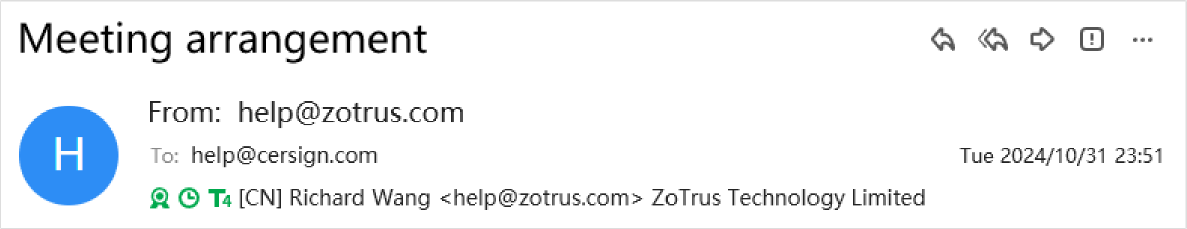
From: help@zotrus.com

To: help@cersign.com

Tue 2024/10/31 23:51

T3 [CN] <help@zotrus.com> ZoTrus Technology Limited

Figure 7 UI for emails with digital signature (OV users)



Meeting arrangement

From: help@zotrus.com

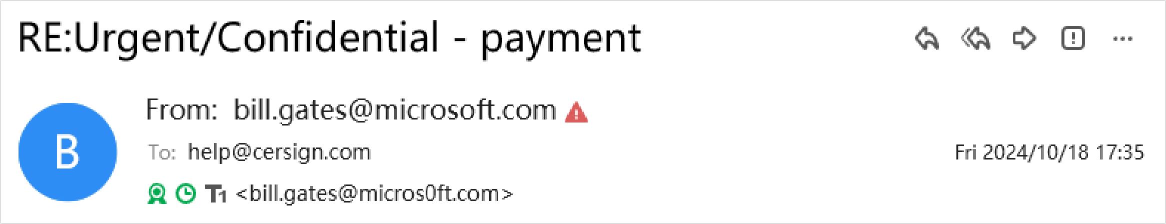
To: help@cersign.com

Tue 2024/10/31 23:51

T4 [CN] Richard Wang <help@zotrus.com> ZoTrus Technology Limited

Figure 8 UI for emails with digital signature (OV users)

Since all CAs must validate the user's control over the email address before issuing an email certificate, a fake email address cannot apply for an email certificate bound to the real email address that it has no control over. Therefore, even if the impostor can write the sender's email address as a real email address, ZT Browser will display the email address bound in its email certificate, and add a warning icon after the sender's claimed email address to remind the user that the claimed email address is inconsistent with the email address bound to the email certificate, as shown in Figure 9 below.



RE:Urgent/Confidential - payment

From: bill.gates@microsoft.com ⚠

To: help@cersign.com

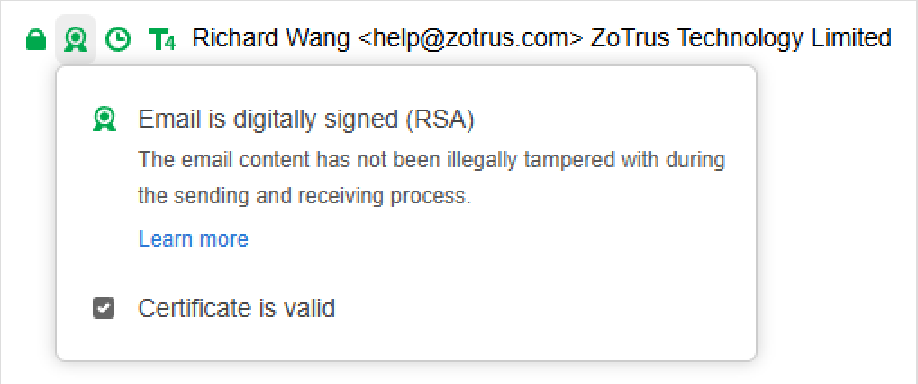
Fri 2024/10/18 17:35

<bill.gates@micros0ft.com>

Figure 9 UI for emails that email address claimed is inconsistent with the email in the certificate

This is the power of digital signature. Users will not be deceived after seeing these different trust level icons, related warning information and displayed validated identity information, the fake identity fraud will no longer succeed. This is the charm of S/MIME technology, other solutions that do not care about the identity validation of email senders and only focus on email encryption cannot achieve this effect in preventing identity fraud. Advanced email encryption solutions must focus on sender identity validation and encryption at the same time to ensure email security.

Users can also click on each icon to view the specific meaning, as shown in Figure 10 below, click on the digital signature icon, it displays “Email is digitally signed (RSA)”, and the signature algorithm is displayed in parentheses. And clearly tell the user that the email content has not been illegally tampered with during the sending and receiving process, which is the core function of digital signature. If the content of the email is tampered with, the digital signature is invalid, ZT Browser will display a warning icon and display "There are problems with the digital signature. Please do not trust the email content!", as shown in Figure 11 below, it is believed that anyone who sees such a warning will not execute the instructions in the email requesting the transfer. As shown in Figure 12 below, Outlook will also have a warning for tampered emails.



Richard Wang <help@zotrus.com> ZoTrus Technology Limited

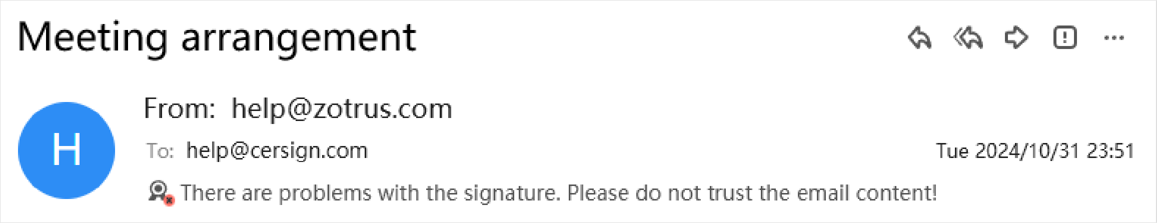
Email is digitally signed (RSA)

The email content has not been illegally tampered with during the sending and receiving process.

Learn more

☑ Certificate is valid

Figure 10 Click on the signature icon to view the details



Meeting arrangement

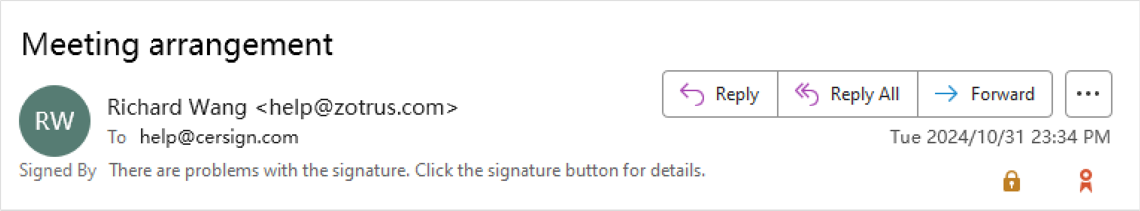
From: help@zotrus.com

To: help@cersign.com

Tue 2024/10/31 23:51

There are problems with the signature. Please do not trust the email content!

Figure 11 UI warning for emails that email content is tampered with



Meeting arrangement

Richard Wang <help@zotrus.com>

To help@cersign.com

Reply | Reply All | Forward | ···

Tue 2024/10/31 23:34 PM

Signed By There are problems with the signature. Click the signature button for details.

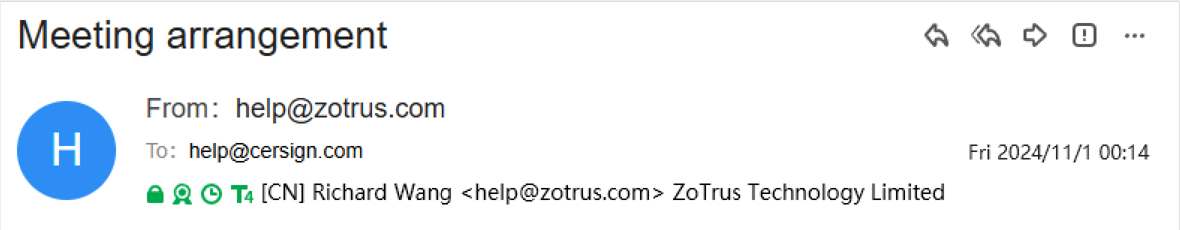
Figure 12 Outlook UI for emails that email content is tampered with

2. **Email encryption can ensure that the content of the email will not be illegally tampered with or stolen, which also ensures that the recipient will not be deceived!**

The second characteristic of BEC attacks is more aggressive. They do not impersonate the sender to send fraudulent emails. The emails are indeed sent by real senders, such as the company's CEO. However, since the emails do not use encryption technology, they are illegally tampered with by attackers during transmission. The CEO's email content requesting a transfer to Company A is changed to a transfer to Company B. Even highly vigilant financial personnel cannot prevent this kind of attack.

However, if the email is encrypted, the attacker will not be able to tamper with the content of the email at all, and the BEC attack will not be carried out, and there will be no loss of up to $55.5 billion, which is the importance of email encryption. Email with digital signature is not enough, because the attacker may also tamper with the email with digital signature, and the recipient may ignore the warning message of the email client, because the email may lose packets during transmission, resulting in incomplete email content and displayed as "There are problems with the signature".

This is why every email sent by ZT browser is encrypted by default, in order to ensure that the email will not be illegally tampered with during transmission, and the email content will not be illegally stolen during the storage, only every email is encrypted to ensure that the recipient will not be deceived by EBC attacks, as shown in Figure 13 below, the encryption icon will be displayed in the email encryption status bar.



Meeting arrangement

H

From: help@zotrus.com

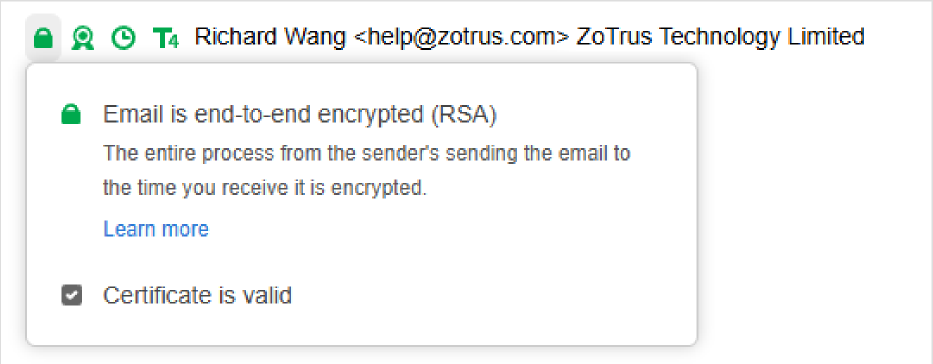
To: help@cersign.com

Fri 2024/11/1 00:14

T4 [CN] Richard Wang <help@zotrus.com> ZoTrus Technology Limited

Figure 13 UI for encrypted and signed emails, with timestamp and T4 icon

Users can also click on the encryption icon, which displays "Email is end-to-end encrypted (RSA)", the encryption algorithm will be displayed after parentheses, and it also displays "The entire process from the sender’s sending the email to the time you receive it is encrypted", which can make the user believe that the email content is authentic and cannot be tampered with, as shown in Figure 14 below, the user can also click "Certificate is valid" to view the details of the email encrypting certificate.



T4 Richard Wang <help@zotrus.com> ZoTrus Technology Limited

Email is end-to-end encrypted (RSA)

The entire process from the sender's sending the email to the time you receive it is encrypted.

Learn more

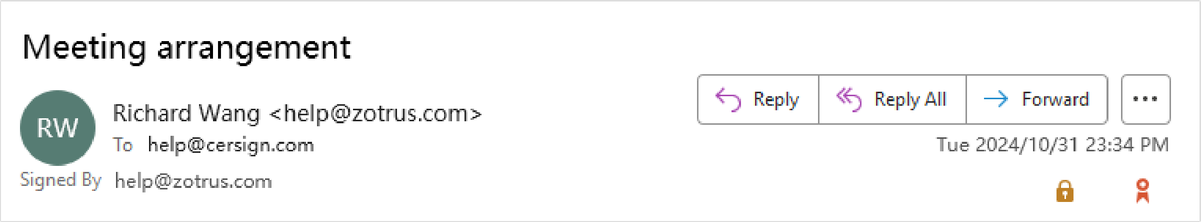
☑ Certificate is valid

Figure 14 Click on the encryption icon to view the details

3. **Email timestamping ensure that the email sending time is trusted, and completely solves the problem of email sending time fraud.**

There is another situation of BEC attack that the author exclusively discovered, that is, the email sending time fraud, which is the same problem as the sender’s email address can be set at will, and the email sending time can also be set at will, which gives the fraud that needs to prove the time of sending the email has the opportunity to exploit the loophole, this kind of fraud email is very hidden, and ordinary users cannot find this problem at all, because at present, all email clients directly display the email sending time claimed in the email header.

As shown in Figure 13 below, use Outlook to view this email, and the email time you see is 23:34 on October 31. However, if you use ZT Browser to view this email, as shown in Figure 14 below, the email time you see is 0:14 on November 1, which is the timestamp time that is automatically attached when the user uses ZT Browser to send emails, and this is the real email sending time. It can be seen that the sender's computer time is 40 minutes behind the standard time.



Meeting arrangement

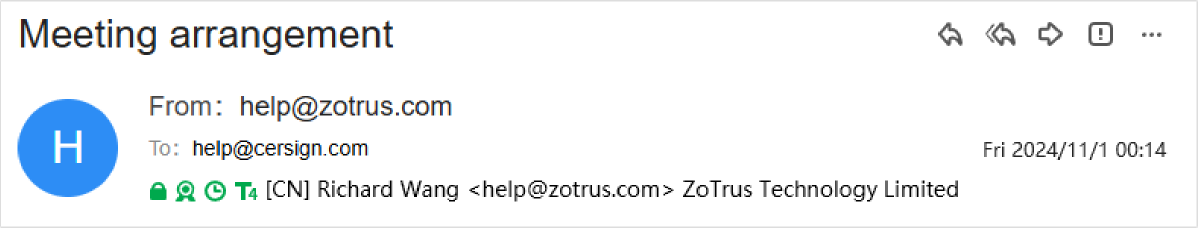
Richard Wang <help@zotrus.com>

To help@cersign.com

Signed By help@zotrus.com

Tue 2024/10/31 23:34 PM

Figure 13 The email sending time displayed in Outlook is not a trusted time



Meeting arrangement

From: help@zotrus.com

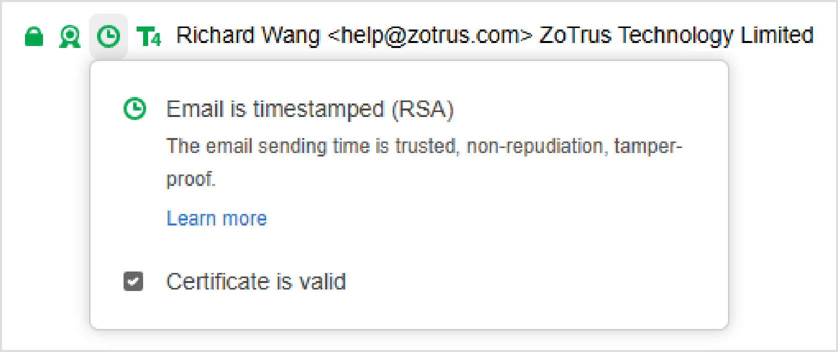
To: help@cersign.com

Fri 2024/11/1 00:14

[CN] Richard Wang <help@zotrus.com> ZoTrus Technology Limited

Figure 14 The email sending time is a trusted time from ZT Browser timestamp

As can be seen from this demonstration case, if October 31 is the deadline for sending emails for a certain event, then only ZT Browser can correctly identify that the user's email sending time has passed the deadline, and all other email clients will only read the untrusted time in the email header and will think that the email sender sends the email time is in accordance with the requirements. This is the power of the email timestamping service provided by ZT Browser for free, which makes the email sending time trusted, non-repudiation and undeniable, because the timestamped digital signature can prove the real email sending time. Users can click the timestamp icon to view the details, as shown in Figure 17 below.



T4 Richard Wang <help@zotrus.com> ZoTrus Technology Limited

Email is timestamped (RSA)

The email sending time is trusted, non-repudiation, tamper-proof.

Learn more

Certificate is valid

Figure 17 Click on the timestamp icon to view the details

The email timestamping service provided by ZT Browser can effectively eliminate email sending time fraud, ensure that the sending time of each email is trusted time, and this function can be used in various application scenarios that need to prove the email sending time, which completely solves the original design defects of email sending time, so that fraudsters cannot exploit loopholes and implement email sending time fraud.

4. The day email encryption becomes commonplace is the day fraud emails die

The author believes that everyone has fully experienced the power and charm of email digital signatures, encryption and timestamps by reading the above content. Why has such a good technology not been popularized and applied to effectively prevent BEC attacks? Because it is very difficult to implement email digital signatures and encryption. Not only does it cost money to apply for email certificates, but it also costs time and effort to configure and use them. At present, only ZoTrus Technology in the world has realized the automation of email digital signature and encryption. Users only need to download and install ZT Browser, set up their email account to enable ZoTrus Email Encryption Automation Service, then they can send encrypted emails completely without feeling like sending plaintext emails. And this email encryption service is completely free, which is very conducive to popularizing email encryption applications.

Perhaps someone will question the motivation of ZoTrus Technology. Why is such a good service provided for free? Are there other motives? As the founder of the company, the author must also make this question clear here. As the author said in the blog post **"Email encryption still has a long way to go with a heavy load"**, the use of cryptographic technology to achieve email encryption has been my constant pursuit for 20 years. No matter how many setbacks encountered in the process, the author always firmly believes that this technical direction can completely solve the problem of email security, and only this solution can truly and completely solve the century problem of email fraud. Therefore, as long as there is an opportunity, the author will never forget the original intention and continue to explore solutions to the email encryption problem.

The author firmly believes that the current email encryption automation solution based on ZT Browser can completely solve the problems encountered in the past, and can finally realize the author's dream of popularizing email encryption. As for the profit model, everyone has seen that ZoTrus Technology provides paid services while providing free services. The free service only validates the user's mailbox control, but does not validate the user's identity, so it is impossible to display the sender's identity. The recipient can only judge whether it is trusted based on the sender's email address. The free service can only guarantee that the sender's email address is authentic, that the email content has not been tampered with, and that the email content will not be illegally stolen. In order to allow the recipient to handle your email with confidence, you are welcome to purchase a paid service that can clearly and prominently display the authentic and trusted sender's full name and/or organization name to the recipient, enhance online trust, and promote more online transactions.

The author welcomes everyone to use ZoTrus email encryption service for free, and also welcomes everyone to purchase paid services, so that we can contribute to the popularization of email encryption and work together to completely eliminate email fraud, so that the ancient email can be revitalized and continue to benefit mankind better.

Richard Wang

November 14, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 80 articles in English (more than 103K words) and 191 articles in Chinese (more than 547K characters in total).