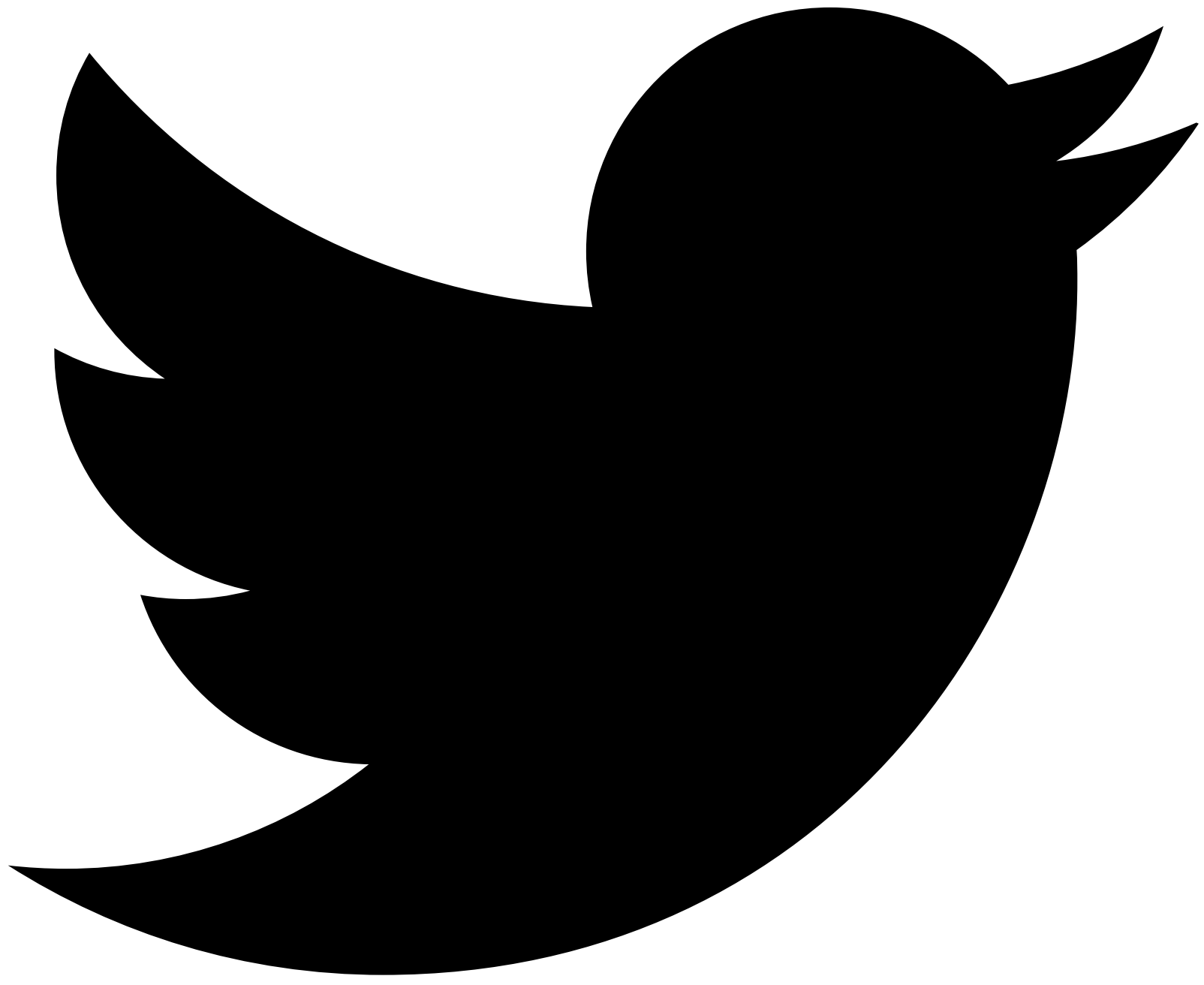
Cyber Attackers Leverage Russia-Ukraine Conflict in Multiple Spam Campaigns

access_timeMarch 25, 2022 person_outlineTrustwave SpiderLabs share



The Trustwave SpiderLabs email security team has been monitoring the ongoing Russia-Ukraine crisis to ensure that our clients are protected and aware of any imminent threats. This research blog captures some of the phishing email threats we have discovered.

Whenever there is a global event, threat actors are sure to take advantage of the situation. As the war between Russia and Ukraine continues, cybercriminals are pumping out spam emails that use the crisis as a lure.

We have observed attackers sending various spam types ranging from crypto scams, malware emails, and phishing.

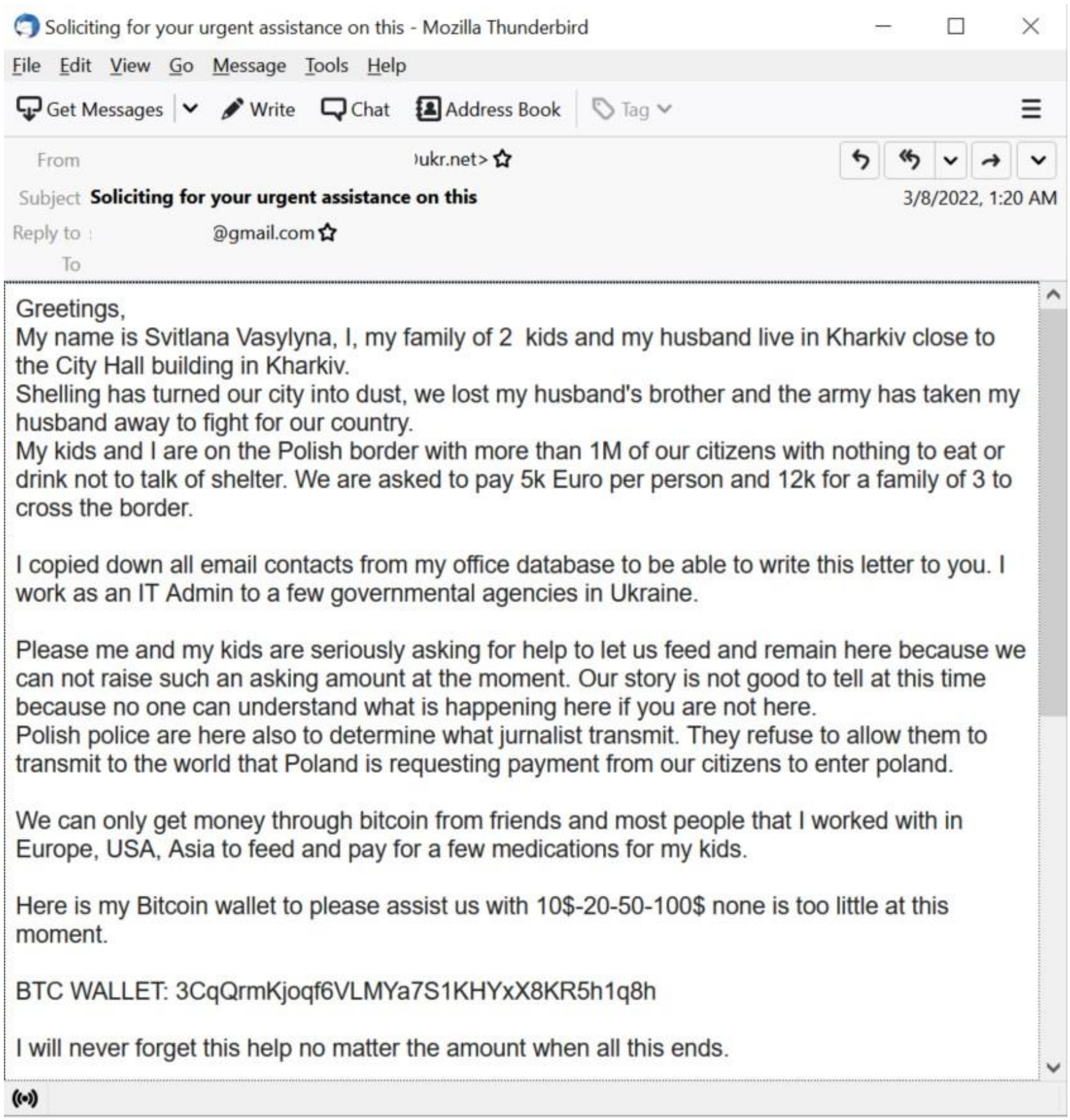
This activity is not unusual. Over the years, we have seen social engineering emails attempt to take advantage of world events such as the Olympics, the COVID-19 pandemic, natural disasters and more. So, it is not surprising that Trustwave SpiderLabs researchers are coming across phishing emails that use the Russian-Ukrainian war as a lure.

Over the first several weeks of the conflict, we uncovered several attack schemes. Some emails intend to spread malware, while others gather personally identifiable information (PII). In all cases, the phishing attempts try to take advantage of the empathy the world has for the human suffering that is taking place in Ukraine.

Phishing in a Time of War

The invasion has caused a humanitarian disaster and displaced millions of Ukrainian citizens from their homes. In response, people from around the world responded by organizing aid and donations. Scammers, unfortunately, have taken note of this activity and, in an attempt to take advantage of these good-hearted people, are sending fraudulent emails asking for donations via cryptocurrency.

Scammers are playing with people's emotions and are using fake heart-wrenching cries for help in this example below:



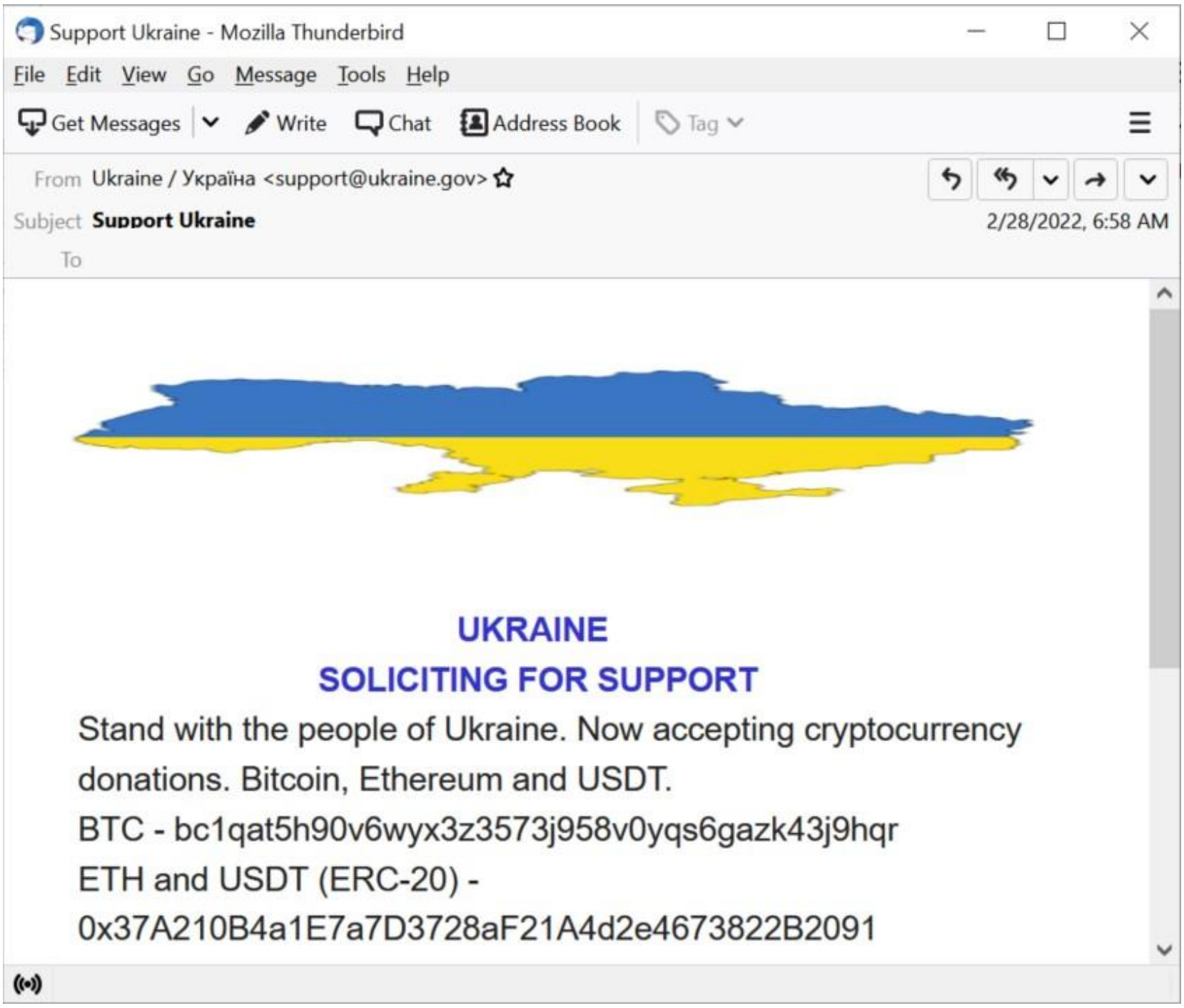
This message appears to be sent by a Ukrainian who has fled to Poland. The sender details the agonizing experience their family has suffered and falsely claims that Poland is charging refugees an entry fee to enter the country. The email also states that Bitcoin is their only means of acquiring financial assistance. One indicator that this email is fraudulent is that the sender address is from a free email service in Ukraine, but the reply-to field contains an entirely different email address. Upon closer inspection, we can see that the sender's IP came from the United States.

Another scam attempts to take advantage of the refugees fleeing the war zone. In this case, a social engineering scheme was designed to take advantage of the very real evacuations now taking place throughout Ukraine by passing along fake evacuation information in an attempt to obtain personal information.

Evacuation plan from: SBU (Urgent) -28.02.2022 original: 399029 Security Service of Ukraine Good afternoon, you need to get acquainted with the electronic evacuation plan from March 1, 2022, provide data on the number of staff, fill out the document on the form 198 \ 00-22 SBU-98. To ensure the confidentiality of transmitted data, the password is set to the attachment: 2267903645

One of the most common tactics threat actors use while conducting phishing campaigns is brand impersonation. Here an email is used to impersonate a trusted entity. By disguising the message as coming from a recognizable organization, attackers are more likely to trick the users into divulging information or transferring money to a fraudulent account.

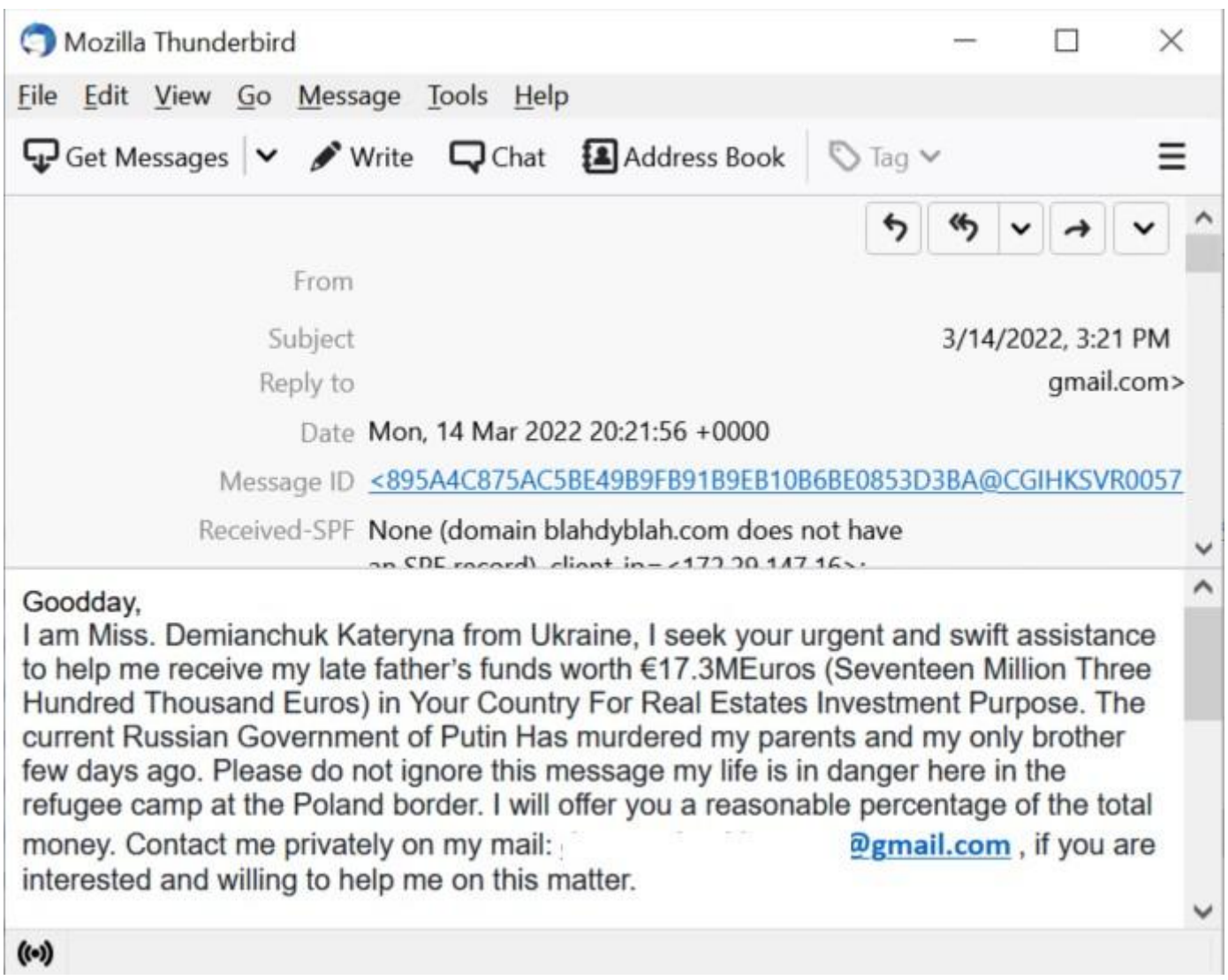
In the examples below, the message appears to be sent by the Ukrainian government.



The sender appears to have a legitimate government email address, but a further examination of the email header shows that the email originated from Lithuania. Another red flag is the fact that the domain "Ukraine.gov" is not officially listed under the ownership of the Ukrainian government.

Investment Scam

Aside from the crypto scam, attackers are sending fraudulent messages regarding investment schemes. These spam messages are basically a spin-off of the classic "Nigerian Prince" scam and offer the victim the false promise of investment or inheritance to trick them into disclosing their bank information or remitting money directly to the scammers.



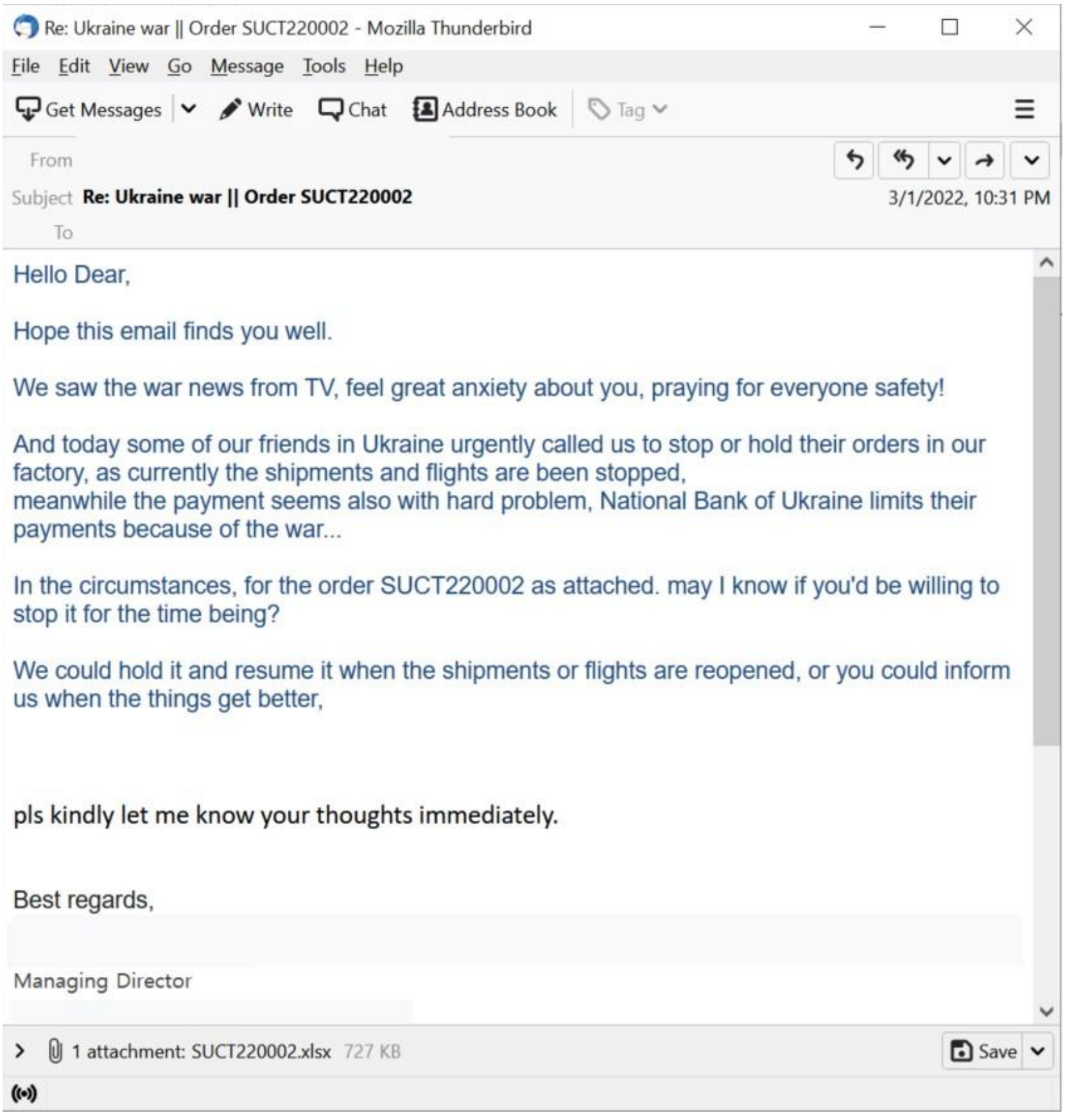
On the surface, this message appears to be sent by a Ukrainian who fled the country for safety. The person is asking for help to transfer a considerable amount of money to the recipient's country for investment purposes.

The email contains several tells that it is fake, besides the story itself.

The email address in the "from" field belongs to a company that is not based in Ukraine. The email also contains a separate email address, which is entirely different from the sender's address and instead belongs to a free mail service. This particular red flag is a common scammer tactic. The scammer spoofs the sender's address because people are more likely to engage with the content of the email if the sender appears to be legitimate. The attacker also created a false sense of urgency as the sender claims to be in danger.

Malware Attachments in Spam Emails

Along with scam emails, malware-related spam is also being sent out to users. A common pretext being used in these messages is the cancellation or postponement of business transactions due to the shutdown of many Ukrainian establishments.



The email shown above uses an order shipment suspension to bait the user into opening the attachment. The attached Excel file supposedly contains the details of the transaction that they want to suspend.

The malicious Excel file exploits a vulnerability in Microsoft Office Equation editor called CVE-2017-11882. It downloads an executable from http://136[.]144[.]41[.]109/HRE[.]exe. Finally, this executable file downloads the final payload, which is Remcos. Remcos is a remote access Trojan (RAT) that can give an attacker full control over its target's system.

IOC

SUCT220002.xlsx

4907309437e12932d437f8c3ae03fbfde7d4e196b6f1dc7f2d98e3a388ce585c

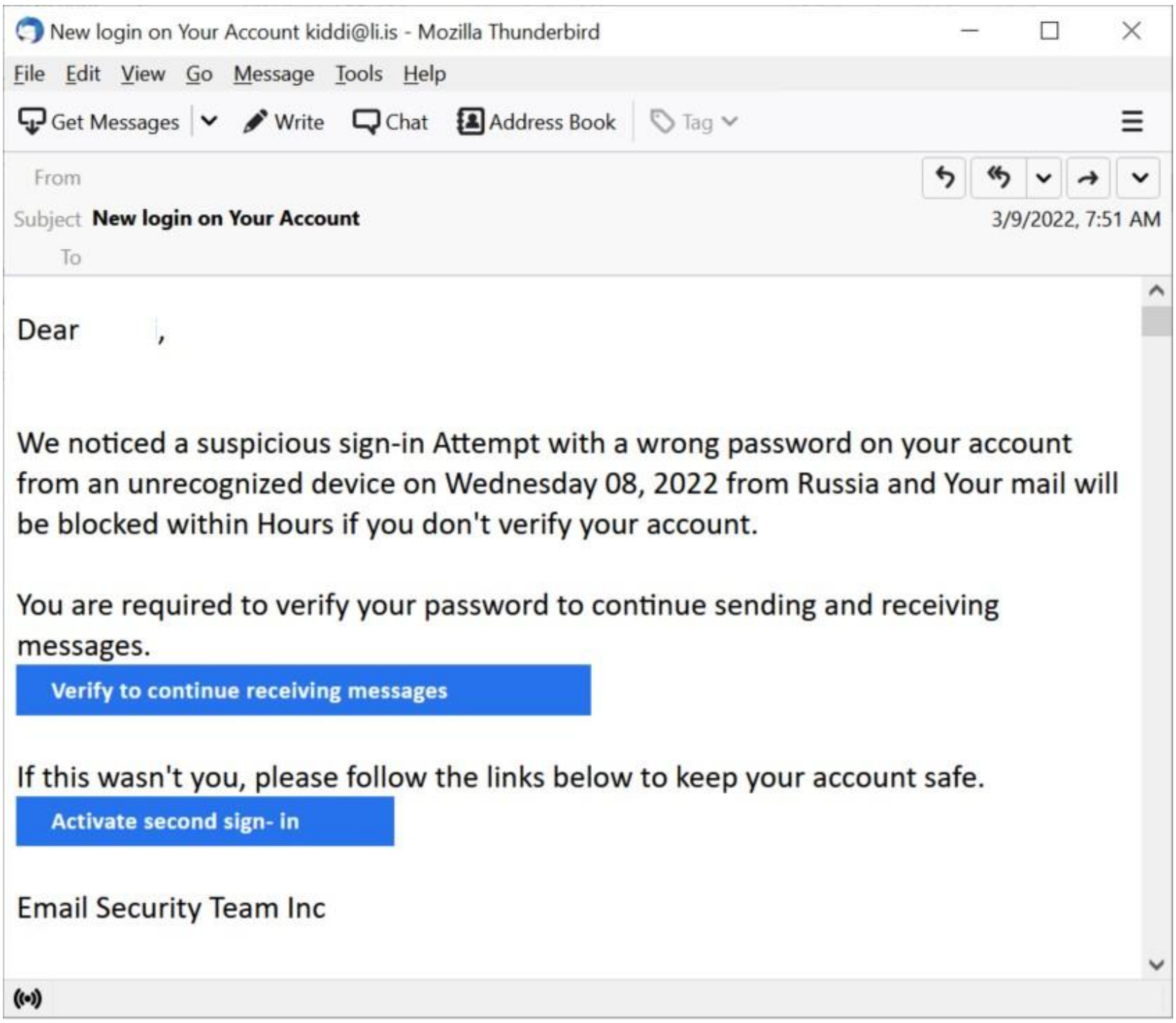
http://136[.]144[.]41[.]109/HRE[.]exe

faef8505886bc30e045f0eb3f1422528cdab1fedc8e02c601605b41bd205d348

0a9babd846b1edf99e75f3c9de492c6341f9ca9a8e91851ad323bf8f325f9799

Log-In Attempt Phishing Emails

Amidst the news of cyberattacks conducted by groups backing Russia, threat actors are pushing out phishing emails disguised as a sign-in attempt notification.



In this sample, the sender, who claims to be from the victim's email security team, says there was a sign-in attempt originating from Russia. The victim is required to verify their account and activate two-step verification. First, the attackers mimic the victim's company domain and forges the sender's address making it appears like a legitimate notification email.

The embedded URL belongs to a web hosting platform and leads to a fake login site, also known as a Chameleon phishing page, that can mimic the logo of the company domain of the victim's email address. It even has a countdown timer to heighten the sense of urgency of the victim and make them divulge their credentials.

The Very Real Threat of Phishing Attacks

Once an employee clicks on a link in a phishing email, malicious activities can occur that could affect an organization — malware, ransomware, credential theft and more.

For example, Trustwave has spotted attackers distributing malware, including AgentTesla, through phishing campaigns focused on Ukraine. AgentTesla has several features. A threat actor can use it as a keylogger, a downloader, a password-stealer, and a screen-capturing malware. These abilities give it the power to record various data, including login credentials, or download and execute malware.

Trustwave MailMarshal Secure Email Gateway can block these types of phishing and scam emails.

The Trustwave SpiderLabs Email Security Team Continues to Stay Vigilant

Certainly, these Ukrainian-related malicious mails won't be the last that we'll see. Cybercriminals will always piggyback on the current global crisis to make their profits. As always, we strongly advise users to never open emails, access links or click on attachments from unknown or unsolicited sources.