Bitdefender Labs Sees Increased Malicious and Scam Activity Exploiting the War in Ukraine

Alina BÎZGĂ
March 04, 2022

As the war in Ukraine intensifies, researchers at **Bitdefender Labs are** picking up waves of fraudulent and malicious emails exploiting the humanitarian crisis and charitable spirit of recipients across the globe. What we've seen so far:

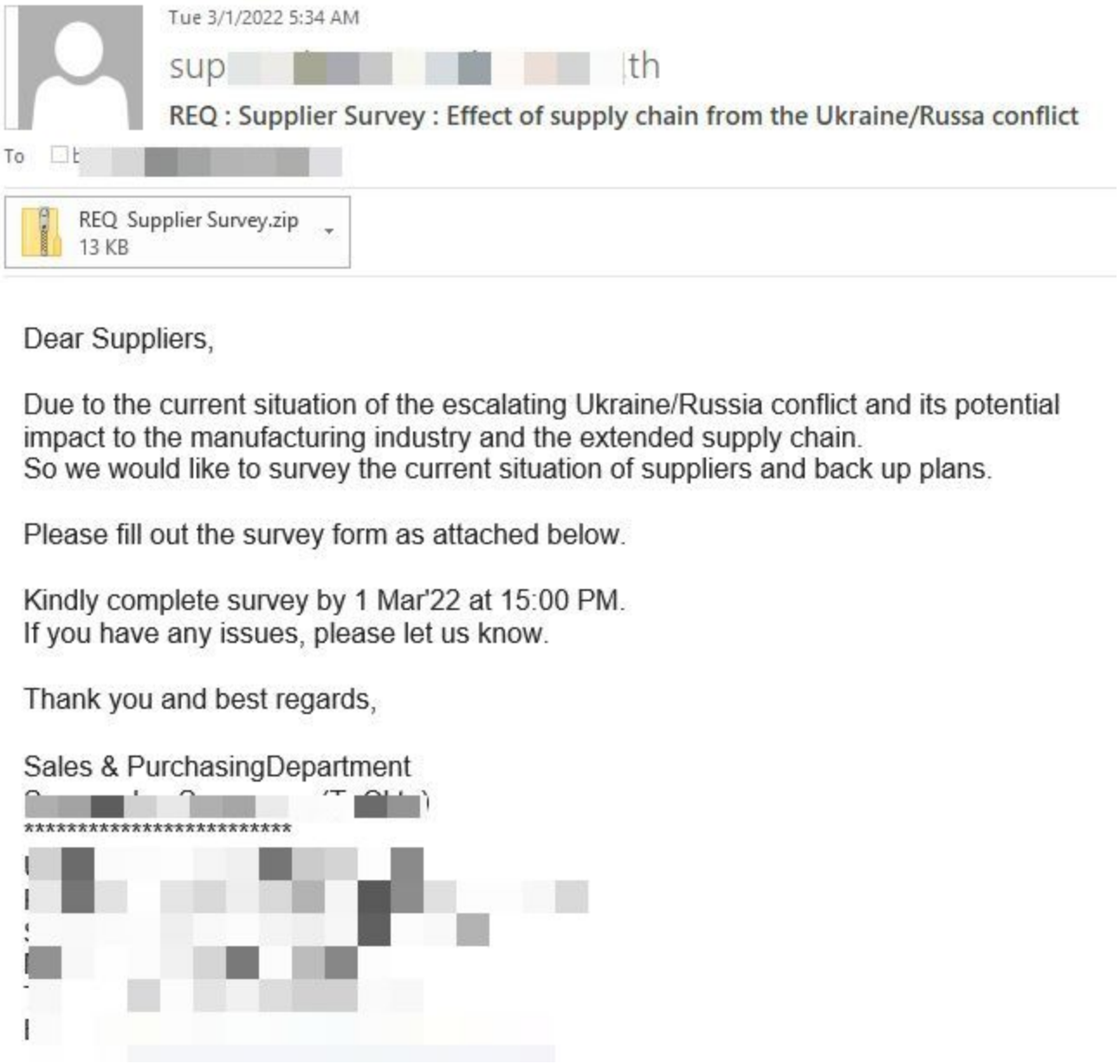
Malspam campaigns deliver Agent Tesla and Remcos RATs

Since March 1, Bitdefender Labs have been tracking two phishing campaigns attempting to infect recipients with two well-known remote access Trojans – Agent Tesla and Remcos.

Campaign 1:

The first malspam campaign appears to be targeting organizations in the manufacturing industry via a .zip attachment 'REQ Supplier Survey'. The attackers ask recipients to fill out a survey concerning their backup plans in response to the war in Ukraine.

According to our threat researchers, the malicious payload is downloaded and deployed from a Discord link directly on the victim's machine. Interestingly though, interacting with the malicious file will also download a clean version of Chrome on the users' device – most likely an attempt at diverting users.


Tue 3/1/2022 5:34 AM

sup [redacted] th

REQ : Supplier Survey : Effect of supply chain from the Ukraine/Russa conflict

To [redacted]

REQ Supplier Survey.zip
13 KB

Dear Suppliers,

Due to the current situation of the escalating Ukraine/Russia conflict and its potential impact to the manufacturing industry and the extended supply chain.
So we would like to survey the current situation of suppliers and back up plans.

Please fill out the survey form as attached below.

Kindly complete survey by 1 Mar'22 at 15:00 PM.
If you have any issues, please let us know.

Thank you and best regards,

Sales & PurchasingDepartment

[redacted]

****

[redacted]

Agent Tesla is an infamous Malware-as-a-service (MaaS) RAT and data stealer that has been prevalent in numerous email-based cyberattacks during the health crisis. Perpetrators use Agent Tesla to exfiltrate sensitive information including credentials, keystrokes and clipboard data from their targets.

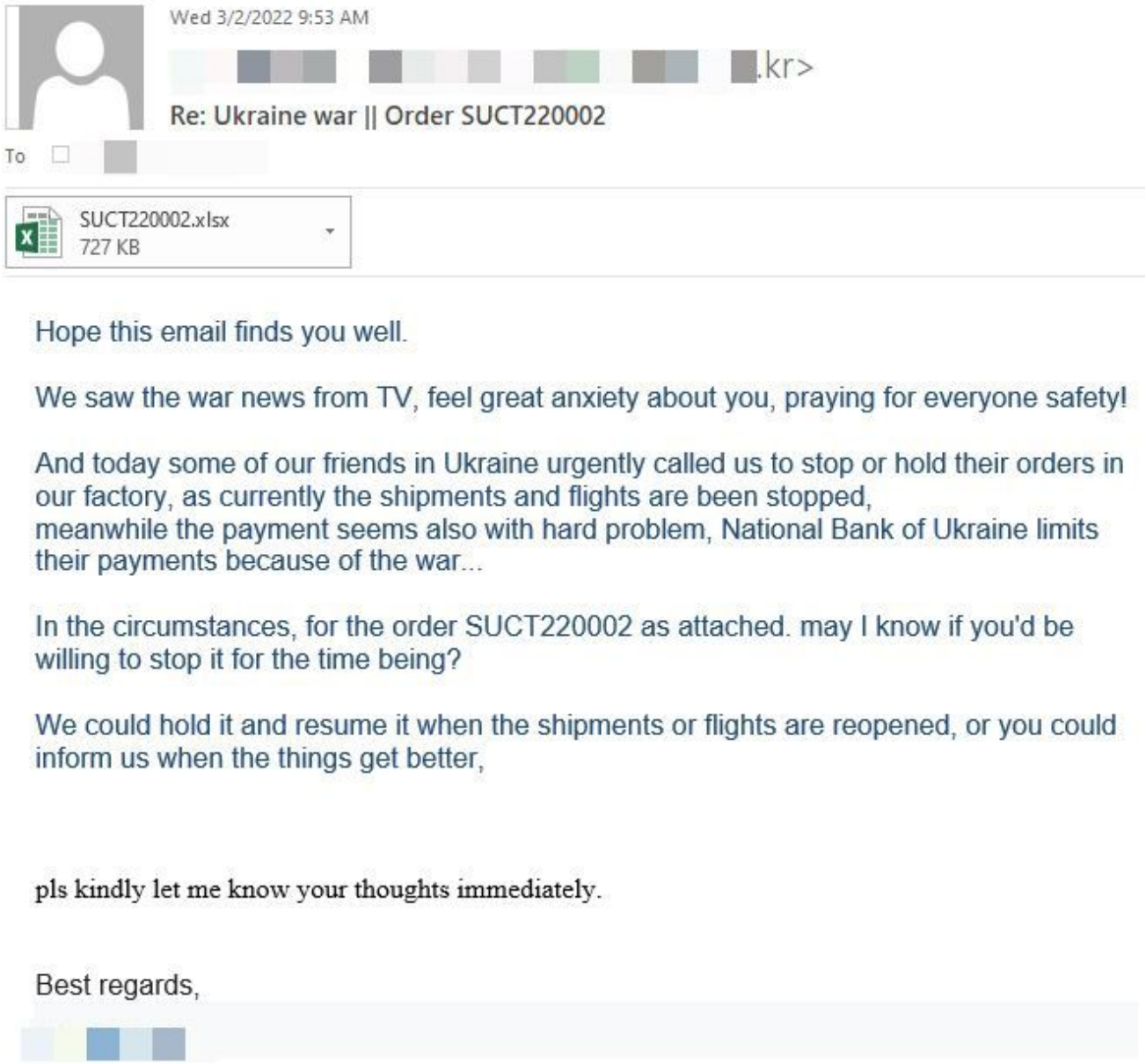
According to our analysis, the attacks seemingly originated from IP addresses in the Netherlands (86%) and Hungary (3%). The malicious emails have reached recipients worldwide including South Korea (23%), Germany (10%), the UK (10%), the US (8%), the Czech Republic (14%), Ireland (5%), Hungary (3%), Sweden (3%) and Australia (2%).

Bitdefender customers are already protected against Agent Tesla attacks. The attached file *REQ Supplier Survey.zip*, detected as **Gen:NN.ZemsilCO.34232.cm0@aKLKBXo,** is detected and blocked by both our consumer and enterprise solutions.

Campaign 2:

Our researchers spotted a separate malspam campaign on March 2, where attackers impersonate a South Korean-based healthcare company that specializes in in-vitro diagnostics analyzers to deliver the Remcos RAT via an Excel attachment (SUCT220002.xlsx).

The message cites the ongoing conflict in Ukraine and asks recipients if they want to put one of their orders on hold until shipments and flights reopen. Cyber attackers mainly deploy Remcos RAT via malicious documents or archives to gain full control over their victims' systems. Once inside, they can capture keystrokes, screenshots, credentials, or other sensitive system information and exfiltrate it directly to their servers.



Eighty-nine percent of the malicious emails appear to originate from IP addresses in Germany and 19% from the US. The attackers' focus in on recipients in Ireland (32%), India (17%), the US (7%), the UK (4%), Germany (4%), Vietnam (4%), Russia (2%), South Africa (2%) and Australia (2%).

“Although the recent cyberattacks were not specifically aimed at Ukrainian infrastructure or civilian population, the global tension generated by the ongoing war will likely materialize in more targeted attacks that could deter emergency response services and humanitarian aid efforts in the country," said Alexandru Maximciuc, threat researcher at Bitdefender Labs.

"We've already seen mass DDoS attacks and wiper malware that hit financial institutions and organizations in Ukraine. Considering the extended economic sanctions imposed by western nations in response to the Russian invasion, digital aggressions aimed at disrupting critical infrastructures should not be dismissed in the current threat landscape.”

Bitdefender consumer and business solutions detect the malicious attachment *SUCT220002.xlsx* delivering the Remcos RAT as **Exploit.CVE-2017-11882.Gen**.

Charity crypto scams are intensifying

On Feb 25, Bitdefender Antispam Lab reported the first signs of scammers exploiting the Russian invasion of Ukraine and news of Ukrainian citizens fleeing the country. As expected, fraudsters continue to leverage the ongoing humanitarian crisis for their own financial gains.

Within hours after the invasion, the Ukrainian government announced it accepts BTC and ETH cryptocurrency donations, and the global community did not disappoint. According to the latest analysis of blockchain transactions, the ETH wallet received over 18,524 transactions totaling over $9.7 million, while the BTC wallet shows more than 9,300 transactions with a value of $9.4 million.

There’s no doubt about it; individuals, organizations, and governments are picking sides, and cybercriminals have to intensify their efforts to redirect any financial aid into their pockets.

“Major global events and crises are known to trigger malicious spam campaigns that exploit human emotion and people's desire to help,” said Adrian Miron, Antispam Research Manager at Bitdefender.

“So far, we've noticed that the attackers reacted very quickly to legitimate announcements of Ukraine and other organizations by mimicking the format of their messages. We expect the variety of phishing and malware campaigns, as well as the volume of messages sent daily, to increase steadily, and the attackers to adapt their persuasion methods accordingly.”

Bitdefender Labs is actively monitoring fraudulent donation emails luring recipients to donate money. Scammers are impersonating the Ukrainian government, international humanitarian agency **Act for Peace**, **UNICEF**, and other donation projects such as the **Ukraine Crisis Relief Fund** to deliver their pleas for financial assistance to help the Ukrainian army and millions of civilians and children caught in the military conflict.

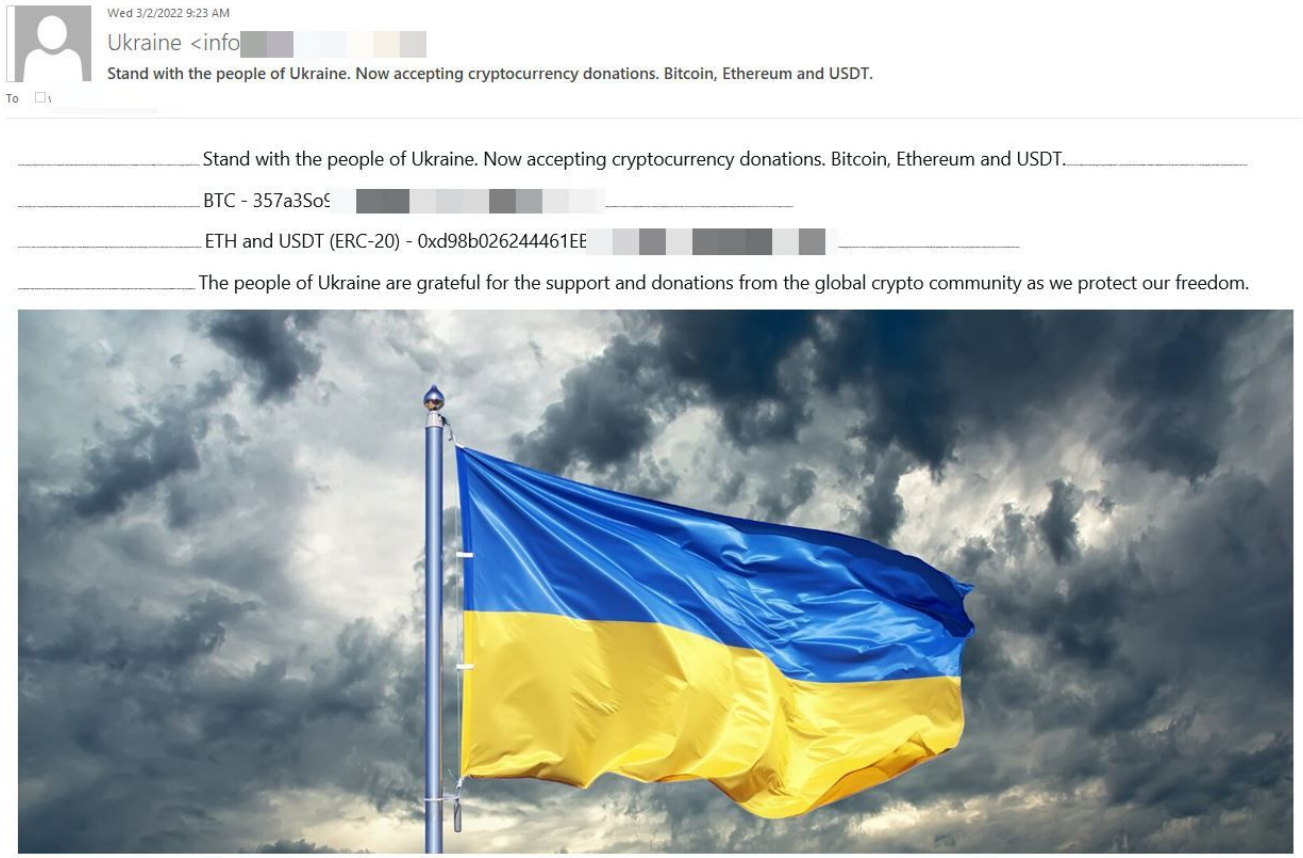
Subject lines are as follows:

- Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.
- HELP UKRAINE stop the war!
- Ukraine Humanitarian Donation
- Donate to Ukraine, Help save a life: Please read
- Urgent! Help Children in Ukraine
- Subject: Help Ukraine

The emails play on users' emotions citing the impact on communities in Ukraine and the growing number of refugees that are fleeing the country and in great need of supplies and housing.

Email-based charity scams peaked on March 2, according to Bitdefender Antispam Lab.

One particular campaign, using the subject line "Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT" originating from IP addresses in China has reached tens of thousands of inboxes on March 2nd. Twenty-five percent of the scam emails were directed to users in the UK, 14% in the US, 10% in South Korea, 8% in Japan, 7% in Germany, 4% in Romania, and 2% each in Greece, Finland and Italy.



Additional crypto charity scam samples can be seen below:

Tue 3/1/2022 6:18 PM

HELP UKRAINE <[redacted].ua>

HELP UKRAINE stop the war!

To [redacted]

Army of Ukraine need your support ! Please help us defend our freedom and independence!
Thank you for everyone !
The National Bank of Ukraine has decided to open a special fundraising account to support the Armed Forces of Ukraine.
Here is original source : https://bank.gov.ua/en/news/all/natsionalniy-bank-vidkriv-spetsrahunok-dlya-zboru-koshtiv-na-potrebi-armiyi
PLEASE, DO NOT IGNORE THIS MESSAGE !

Stand with the people of Ukraine.
Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - bc1qv729ckc4[redacted]

ETH and USDT (ERC-20) - 0x0dcf682C[redacted]

We very sorry for a such spam ! But people of Ukraine need your support !
Thank you for everyone !
Here is original source : https://bank.gov.ua/en/news/all/natsionalniy-bank-vidkriv-spetsrahunok-dlya-zboru-koshtiv-na-potrebi-armiyi
Please, do not blacklist this domain !

Mon 2/28/2022 6:23 PM

Ukraine / україни Govt <h[redacted]icr.org>

Ukraine Humanitarian Donation

To [redacted]

A donation campaign has been launched to support Ukraine and also help refugees fleeing from the conflict in Ukraine.
The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT.

BTC - bc1qzvkyvkcrynyye8nxv[redacted]

ETH, USDT, LUNA (ERC-20) - 0x4428a0f3029309a322bE[redacted]

SOLANA (SOL): 8YoCxF8Hzcs8ig9tJRF4xp[redacted]

BINANCE (BNB): bnb15z8f3zxyn9r48mk9p[redacted] / 0x4428a0f3029309a322bBE2[redacted]

Kindly reply to this email if you need to donate with other token.

Best Regards
Ukraine
#BeautifulUkraine

Tue 3/1/2022 3:10 PM

Ukraine Crisis Relief Fund < org>

Donate to Ukraine, Help save a life: Please read

To

Hello ,

We are urging you to please donate to Ukrainians as many people have fled their homes to seek refuge. Help us provide a safe solution for Ukrainian families who have already suffered too much, Shelter, water for those who need it the most in this time of crisis.

You can give any amount, since the banks are not working, kindly save a life, and donate to us through our UCRF (Ukraine Crisis Relief Fund) wallet.

Bitcoin Wallet: 18FSzjrRAQC7

We sincerely appreciate your help.

Thank You,

Ukraine Crisis Relief Fund

Tue 3/1/2022 10:43 AM

UNICEF <.org>

Urgent ! Help Children in Ukraine

To Recipients

5tgd-300x200.jpg 13 KB | 12sdx-min-768x415.jpg 47 KB | 56f-300x200.jpg 13 KB

Hello

In times of crisis, we turn to others for help or step up to assist.

Millions of civilians are caught in the middle of an escalating military conflict and humanitarian crisis, and casualties are rising.

Your donation to this fund will support Ukrainians in need, with a focus on the most vulnerable, including children.

We receive this through BTC OR ETH since all banks are closed.

All Supporters (5265)

Save Children
$436,792
Donated of 500,000 goal

BITCOIN ID = 3Q437aYNYuT

ETH ID = 0xa666e53BdF65b1

Looking forward to receive your abundant help

Thank you for your understanding

Regards

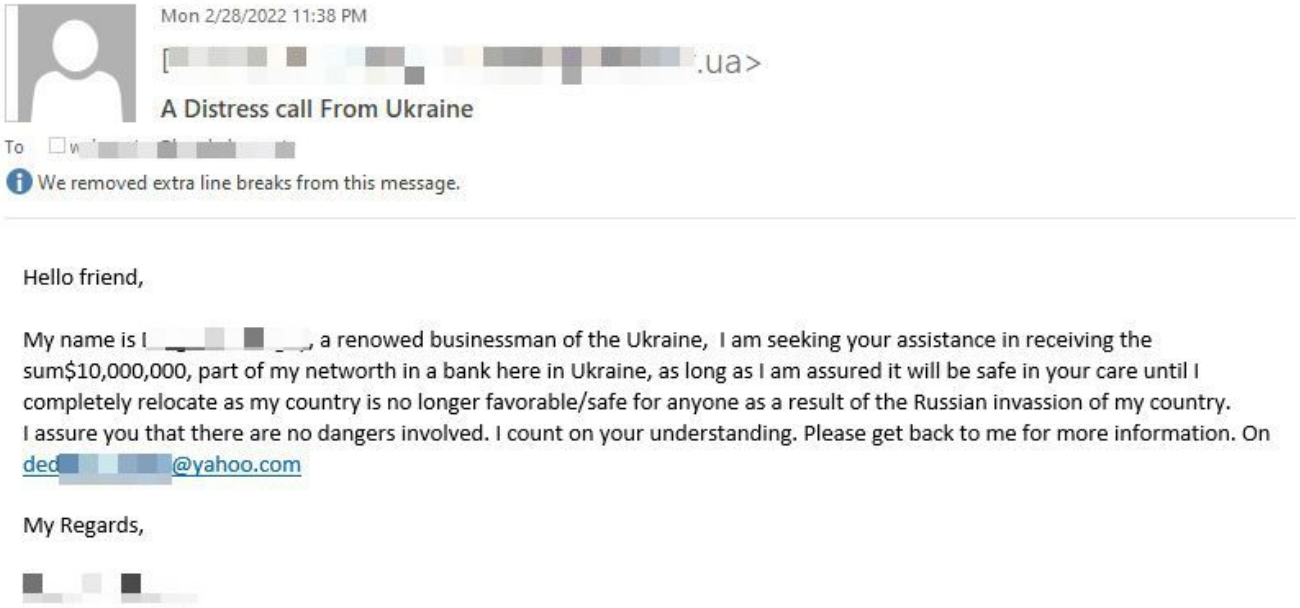
Nigerian Prince-style email schemes

Bitdefender spam filters have also noticed a Ukraine variation of the Nigerian Prince scam. The email, allegedly sent by a renowned businessman from Ukraine seeks your assistance to transfer $10 million until he is able to relocate somewhere safe.

Fraudsters behind this particular scam are sending emails from IP addresses in Botswana (83%), Germany (10%) and France 5%. Their main audience are users in Germany (42%), Turkey (16%), the US (16%), Ireland (8%) and Poland (3%).

Unfortunately, users who respond to this email will get in touch with the scammer who will ask for personal information to help transfer the money out of the country. Although the email does not promise recipients any financial awards for their help, the con artist will likely specify remuneration for helping him finalize the transfer. Most often the scammer will ask

recipients to pay administration fees, often associated with moving large sums. Upon deceiving the victim, the scammer will either disappear with the money or, worse, drain their bank account in the process.



Sample 7

Bitdefender's focus on cybersafety

The fact that cybercriminals and scammers are using the crisis in Ukraine to steal users' money and spread malicious payloads comes as no surprise to cybersecurity experts. Although the war in Ukraine may be thousands of miles away from many of us, people's suffering triggers a strong emotional response to users worldwide who wish to lend a hand to refugees fleeing the war-struck European country.

We urge all internet users to be extra vigilant during these troubled times and practice good cyber hygiene to ensure that their hard-earned money does not end up in the wrong hands:

- Never click on links or attachments in emails or messages that ask you to donate urgently
- Donate exclusively via official and trusted charities, non-profit organizations and fundraisers
- Check your financial accounts regularly for any suspicious activity or unauthorized charges
- Set up unique passwords for all online accounts

For more tips, please check our dedicated cybersecurity guide in armed conflict zones.

In response to the military crisis and increased cybercriminal activity, Bitdefender & the Romanian National Cyber Security Directorate (DNSC) are offering **free cybersecurity protection** for any Ukrainian citizen, company or institution, as long as necessary.

Additionally, users across the globe can also boost their cyber resilience and fend off online scams and e-threats with our extended Bitdefender Total Security trial, free of charge for 90-days. With **Bitdefender Total Security**, you get the best anti-malware protection against e-threats across all major operating systems. The real-time protection feature included in our security software offers continuous protection against all e-threats, including viruses, worms, Trojans, ransomware, zero-day exploits, rootkits, and spyware to keep you and your data safe.

Note: This article is based on technical information provided courtesy of Bitdefender Labs

Stay Safe!

TAGS

industry news threats ukraine

AUTHOR

Alina BÎZGĂ

Alina is a history buff passionate about cybersecurity and anything sci-fi, advocating Bitdefender technologies and solutions. She spends most of her time between her two feline friends and traveling.

View all posts