Russia-Ukraine war exploited as lure for malware distribution

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

March 4, 2022 12:04 PM **0**

Threat actors are distributing malware using phishing themes related to the invasion of Ukraine, aiming to infect their targets with remote access trojans (RATs) such as Agent Tesla and Remcos.

of Ukraine.

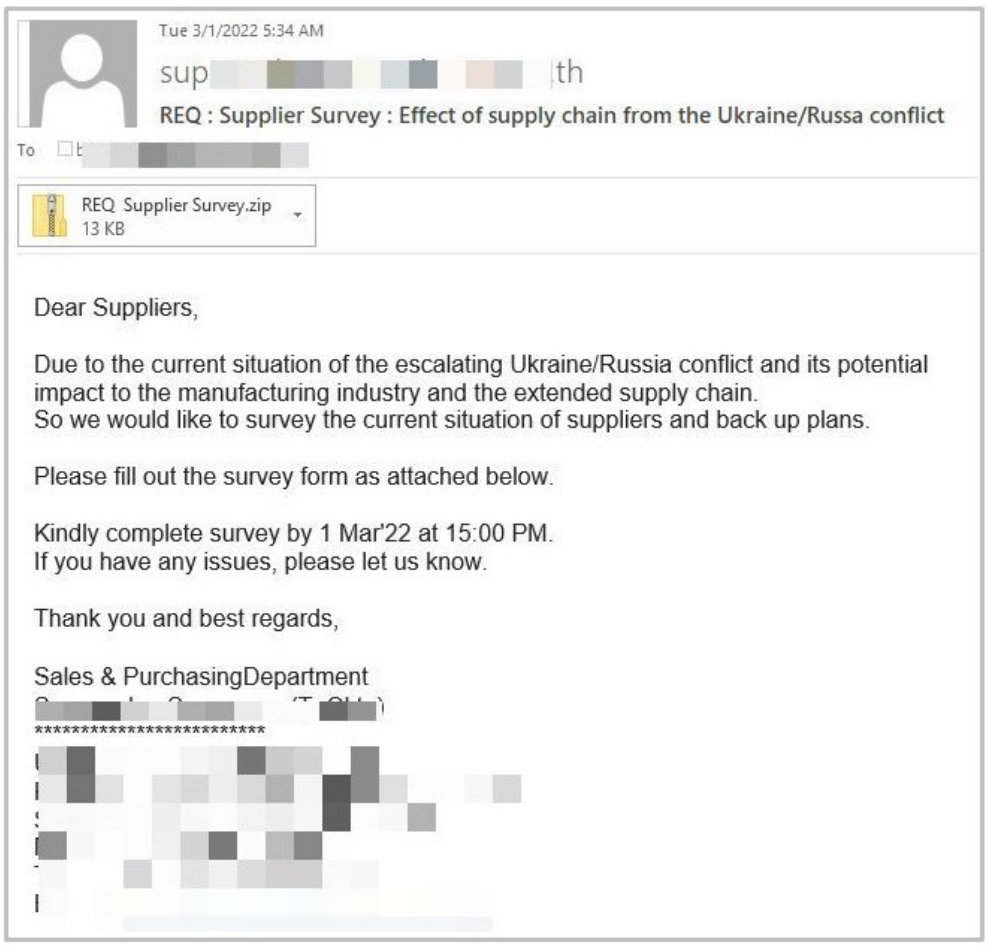
Using this theme, threat actors are sending malicious emails that install RATs on target systems to gain remote access, steal sensitive information, conduct network reconnaissance, disable security software, and generally prepare the ground for more potent payloads.

The report of the latest malicious operations comes from Bitdefender Labs, (https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine) whose researchers have been tracking two distinct phishing campaigns since March 01, 2022.

Targeting manufacturers

Ukraine is a manufacturing hub for various parts, and the current conflict has forced factories to close, inevitably creating supply chain problems (https://www.nytimes.com/2022/03/01/business/volkswagen-bmw-autos-germany-ukraine.html) and shortages.

The first campaign spotted by Bitdefender attempts to exploit these concerns by targeting manufacturers with a ZIP attachment that supposedly contains a survey that they are required to fill out to help their customers develop backup plans.



Phishing email used in the first campaign *(Bitdefender)*

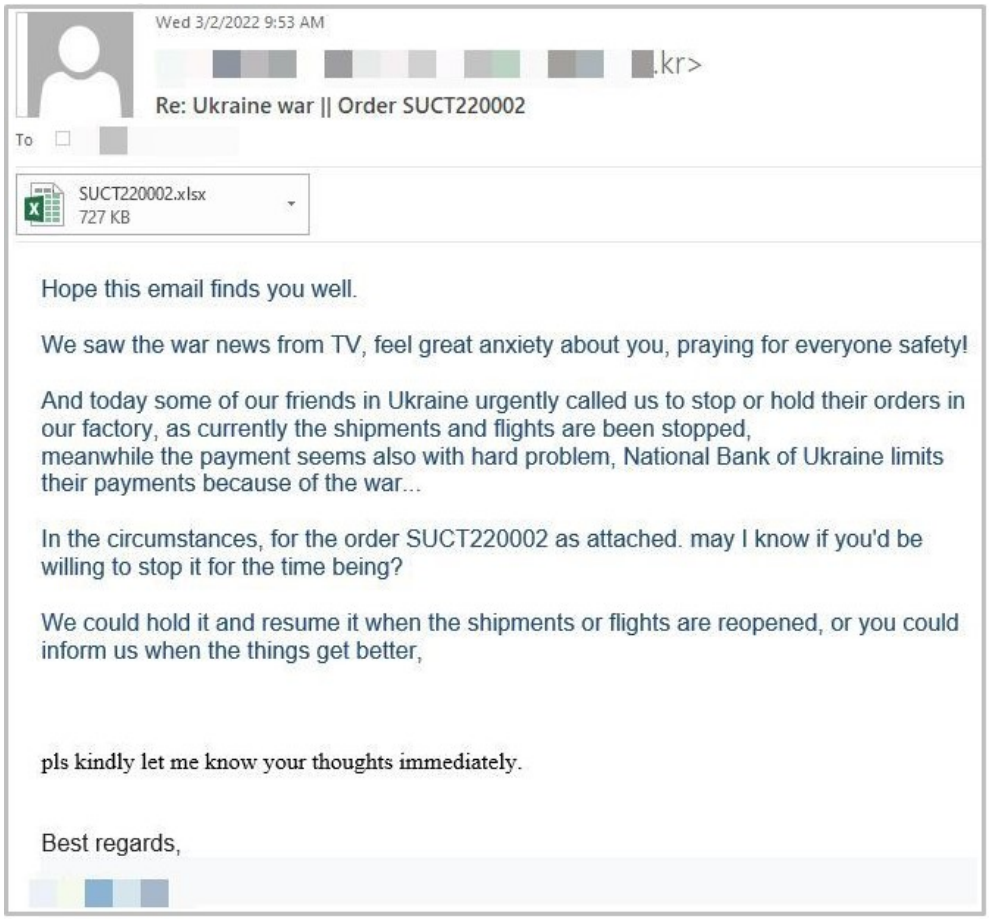
However, the ZIP archive contains the Agent Tesla RAT, which has been heavily used in various phishing campaigns (https://www.bleepingcomputer.com/news/security/phishing-campaign-uses-powerpoint-macros-to-drop-agent-tesla/) in the past.

Most (83%) of the phishing emails in this campaign originated from the Netherlands, while the targets are based in the Czech Republic (14%), South Korea (23%), Germany (10%), the UK (10%), and the US (8%).

Fake order holds

The second campaign involves the impersonation of a South Korean healthcare company that manufactures in-vitro diagnostic systems.

The message to targets claims that all orders have been put on hold due to flight and shipment restrictions from Ukraine.



Phishing email used in the second campaign *(Bitdefender)*

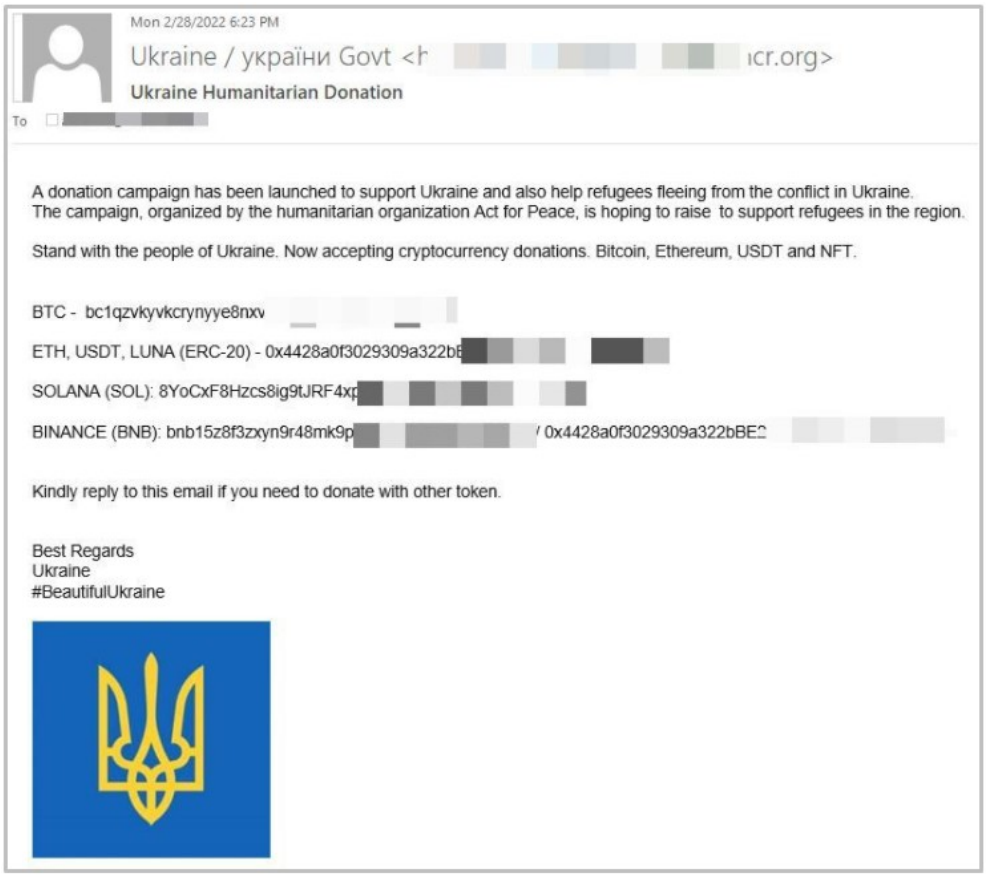
The attached Excel document supposedly contains more details about the order, but in reality, it's a macro-laced file that exploits the always popular four-years-old Microsoft Office Equation Editor bug (https://www.bleepingcomputer.com/news/security/office-equation-editor-security-bug-runs-malicious-code-without-user-interaction/) tracked as CVE-2017-11882 vulnerability to deliver the Remcos RAT on the system.

89% of these emails originate from German IP addresses, while the recipients are based in Ireland (32%), India (17%), and the US (7%).

Crypto-donation scams on the rise

Bitdefender also reports seeing an explosion in the number of scammers (https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/) who attempt to convince users they are legitimate charities collecting donations to support Ukraine.

These scams have intensified, with malicious actors impersonating the Ukrainian government, the Act for Peace, UNICEF, and the Ukraine Crisis Relief Fund.



Crypto-donations scam email *(Bitdefender)*

Some example subject lines used by the scammers are:

- 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

Stay safe

In general, but especially during periods of turbulence and uncertainty, avoid clicking on links or downloading attachments arriving at your inbox via unsolicited communications.

If you want to donate to Ukraine, consider donating directly to the Save Life (https://savelife.in.ua/en/donate/) organization or the Ukrainian Red Cross (https://redcross.org.ua/en/donate/). Also, the official Ukraine government has published the following cryptocurrency addresses to use for donations.

For protection against phishing emails and other online threats, the Romanian National Cyber Security Directorate (DNSC) and Bitdefender offer free protection (https://www.bitdefender.com/ukraine/) for citizens and companies alike and extend the trial period of 'Total Security' to 90 days (https://www.bitdefender.com/media/html/consumer/new/get-your-90-day-trial-opt/index.html?cid=soc%7Cc%7cblog%7C90DaysTrial).