Amazon: Charities, aid orgs in Ukraine attacked with malware

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** March 4, 2022 06:57 PM **1**

Charities and non-governmental organizations (NGOs) providing critical support in Ukraine are targeted in malware attacks aiming to disrupt their operations and relief efforts seeking to assist those affected by Russia's war.

Amazon has detected these attacks while working with the employees of NGOs, charities, and aid organizations, including UNICEF, UNHCR, World Food Program, Red Cross, Polska Akcja Humanitarna, and Save the Children.

"While we are seeing an increase in activity of malicious state actors, we are also seeing a higher operational tempo by other malicious actors.," Amazon said (https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine).

"We have seen several situations where malware has been specifically targeted at charities, NGOs, and other aid organizations in order to spread confusion and cause disruption.

"In these particularly egregious cases, malware has been targeted at disrupting medical supplies, food, and clothing relief."

Phishing attacks against European refugee helpers

Proofpoint researchers spotted a similar activity, observing spear-phishing attacks targeting European government personnel (https://www.bleepingcomputer.com/news/security/phishing-attacks-target-countries-aiding-ukrainian-refugees/) involved in logistics support for Ukrainian refugees.

Emails sent in the attacks delivered malicious macro attachments that would download a Lua-based malware dubbed SunSeed, used to deliver additional payloads onto compromised devices.

The campaign, tracked as Asylum Ambuscade, targeted only NATO entities using the compromised email account of a Ukrainian armed service member.

Based on the infection chain, it aligns and is likely related to July 2021 phishing attacks linked to the Ghostwriter (https://www.bleepingcomputer.com/tag/ghostwriter/) Belarusian threat group (also known as TA445 or UNC1151).

Facebook (https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/) and the Computer Emergency Response Team of Ukraine (CERT-UA) (https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/) also warned of Ghostwriter phishing campaigns against Ukrainian officials and military personnel.

Before Russia's invasion, the Ukrainian Security Service (SSU) said the country was being hit by a "massive wave of hybrid warfare (https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/)."

This deluge of attacks included DDoS attacks (https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-state-owned-banks-hit-by-ddos-attacks/) against Ukrainian government agencies and state banks, phishing (https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/) targeting the Ukrainian military, as well as multiple series of destructive malware attacks [1 (https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/), 2 (https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/)].