JOERG HABERMEIER - STOCK.ADOBE.C

NEWS

SunSeed malware hits those involved in Ukraine refugee relief

European governments involved in managing the logistics of hundreds of thousands of people fleeing Ukraine have been targeted by a suspected state-backed actor

Alex Scroxton, Security Editor

Published: **02 Mar 2022 10:21**

A newly identified phishing campaign, potentially linked to the government of Belarus and using a compromised email account belonging to the Ukrainian armed services, appears to be targeting European government personnel who are involved in managing the logistics of refugees attempting to cross into the European Union (EU) from Ukraine.

Between half a million and a million Ukrainians have already left the country in the face of the Russian invasion, with hundreds of thousands crossing into the EU states with which Ukraine shares a border –

Now, intelligence released by Proofpoint has revealed how relief efforts aimed at these refugees are being targeted by malicious actors with a Lua-based malware called SunSeed. Proofpoint said it was releasing this intel "in an effort to balance accuracy with responsibility to disclose actionable intelligence during a time of high-tempo conflict".

"This campaign represents an effort to target Nato entities with compromised Ukrainian military accounts during an active period of armed conflict between Russia, its proxies, and Ukraine," said Proofpoint's research team. "While the utilised techniques in this campaign are not ground-breaking individually, if deployed collectively, and during a high-tempo conflict, they possess the capability to be quite effective.

“As the conflict continues, researchers assess that similar attacks against governmental entities in Nato countries are likely. Additionally, the possibility of exploiting intelligence around refugee movements in Europe for disinformation purposes is a proven part of Russian and Belarussian state techniques. Being aware of this threat and disclosing it publicly are paramount for cultivating awareness among targeted entities.”

Proofpoint has tentatively linked the campaign to UNC1151 or Ghostwriter, which it tracks as TA445 – a Belarus-backed actor – which was earlier the subject of an alert by Ukraine’s Computer Emergency Response Team (CERT-UA).

This connection is still not fully confirmed, but Proofpoint said the timeline, use of compromised addresses and victimology align with the group’s modus operandi. Notably, there appear to be a number of links to a 2021 Ghostwriter campaign, dubbed Asylum Ambuscade, which unfolded around the migration crisis, during which the Belarussian government intentionally funnelled refugees to the Polish border. Both campaigns “may indicate” the weaponisation of both refugees and economic migrants through a hybrid of information warfare and targeted cyber attacks.

The phishing emails themselves include malicious macro attachments that leverage messaging around a 23 February emergency meeting of Nato’s Security Council, and a malicious attachment that attempts to download SunSeed. Targeted individuals are in a range of roles, but the campaign seems to preference those involved in transportation, financial and budget allocation, administration and population movement.

More information on the SunSeed malware, including indicators of compromise (IOCs) and Yara rules, can be obtained from Proofpoint.

Read more on Hackers and cybercrime prevention

Google: Former Conti ransomware members attacking Ukraine

By: Alexander Culafi

Russia-linked APTs targeted fleeing Ukrainian civilians

By: Alex Scroxton

Romance scammers exploit Ukraine war in cynical campaign

By: Alex Scroxton

Hundreds of thousands of Ukrainians take up free language app offer

By: Karl Flinders

SearchCIO

Experts highlight trust and safety practices for the metaverse

Creating a safe metaverse experience means bringing all stakeholders to the table, according to experts.

Business-led IT strategy casts shadow IT in more positive light

Traditional shadow IT is giving way to business-led technology deployments that have the IT department's approval. But CIOs must ...