Chinese phishing actors consistently targeting EU diplomats

By

Bill Toulas

- March 9, 2022
- 02:02 AM
- 0

The China-aligned group tracked as TA416 (aka Mustang Panda) has been consistently targeting European diplomats since August 2020, with the most recent activity involving refreshed lures to coincide with the Russian invasion of Ukraine.

According to a new report by Proofpoint, TA416 spearheads cyber-espionage operations against the EU, consistently focusing on this long-term role without reaping opportunistic gains.

By keeping their tools and tactics essentially unchanged since 2020 and only refreshing their phishing themes and peripheral components, TA416 has made attribution simple for the analysts.

PLAY Top Articles Video Settings Full Screen About Connatix V155205


Read More


Read More


Read More Read More

Read More

Read More New Phishing

toolkit lets anyone create fake Chromebrowser windows 1/1 Skip Ad Continue watching after the ad Loading PodsVisit Advertiser websiteGO TO PAGE

Timeline of activity

Starting in August 2020, the phishing actors impersonated EU-based organizations to target governments in the continent.

United Nations A/74/976–S/2020/773

General Assembly
Security Council

Distr.: General
XX August XXXX

Original: English

Advance Unedited Version

General Assembly
Seventy-Fifth session
Agenda item 64
Peacebuilding and sustaining peace

Security Council

2020 Report of the Secretary-General on Peacebuilding and Sustaining Peace

I. Introduction

1. The third review of the United Nations peacebuilding architecture, requested by landmark twin resolutions on peacebuilding and sustaining peace, General Assembly resolution 70/262 and Security Council resolution 2282 (2016), and launched in October 2019, takes place when there is greater consensus than ever that the human and financial costs of responding to crisis rather than investing in prevention are unsustainably high. As we mark the 75th anniversary of the United Nations, we are reminded of the Charter's aspirations to "save succeeding generations from the scourge of war." The Charter highlights the critical relationship between peace and security, development, human rights and international cooperation. Member States reaffirmed these interlinkages in adopting the 2030 Agenda for Sustainable Development as the framework for collective efforts to build peaceful, just, prosperous and inclusive societies. The COVID-19 pandemic and its consequences have brought the necessity of this into more acute focus.

2. The 2016 resolutions affirmed the primary responsibility of national Governments and authorities in identifying and driving priorities, strategies and activities for sustaining peace, at all stages of conflict, and emphasized that inclusivity was key to advancing national peacebuilding objectives. Inclusive and sustainable development, anchored in the protection and promotion of human rights, gender equality, and the goal of leaving no one behind, is the best defense against conflict. Since assuming office, I have reiterated that we must place the prevention of crisis and human suffering at the heart of our work. This is how, together, we address root causes of vulnerability, and provide pathways to sustainable development and peace.

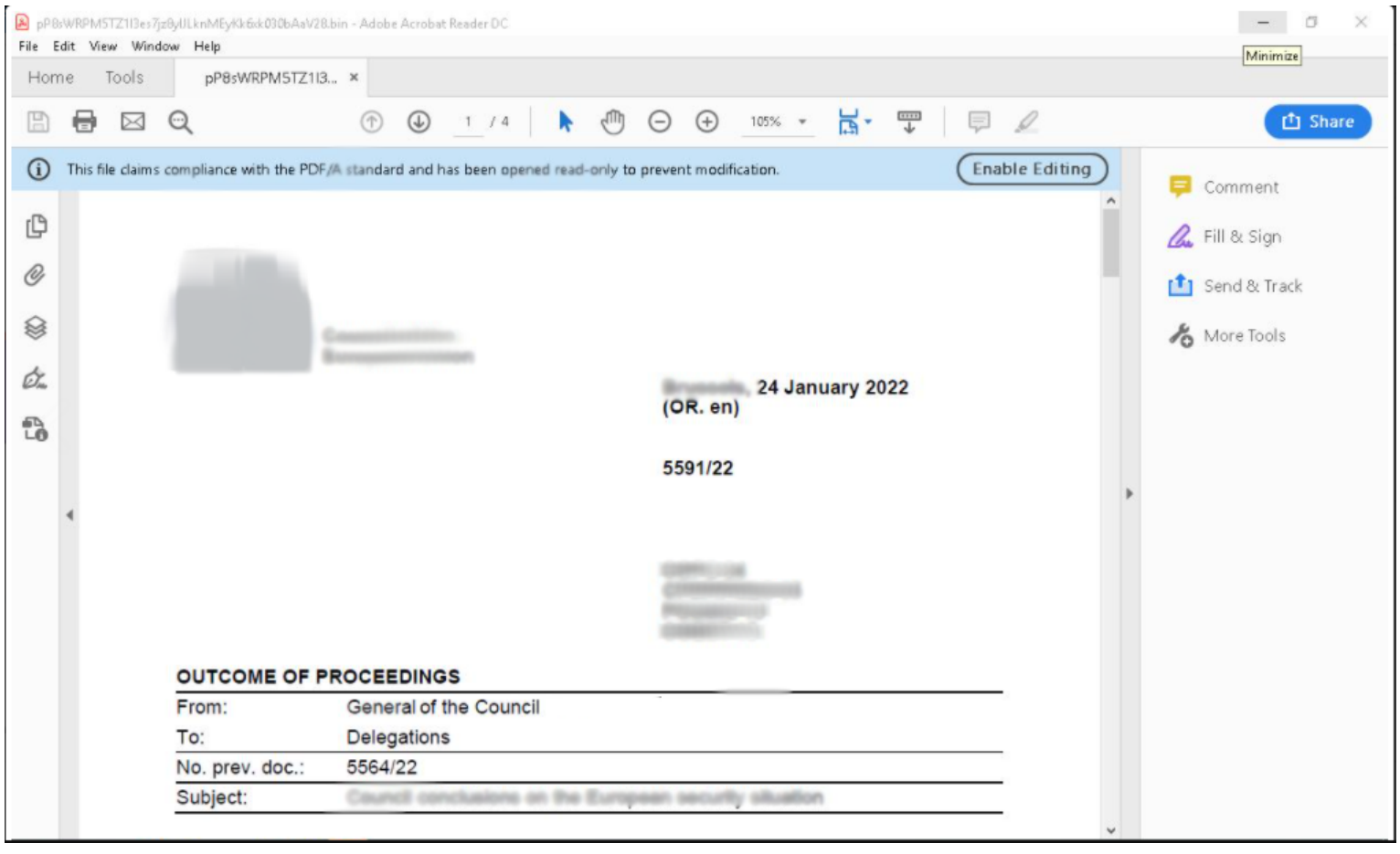
3. The world's population continues to face increased poverty, inequality, exclusion as well as threats to peace and security. By the end of 2019, 79.5 million persons had been forcibly displaced, double the level of 20 years ago. A record 19 million children were internally displaced due to

Email impersonating a UN agent (Proofpoint)

The malicious emails used a DropBox URL to deliver a variant of the PlugX malware, which was previously deployed in attacks against Australian organizations.

In November 2021, TA416 added hidden image trackers on emails to validate message openings and follow a more targeted approach in their campaign.

On January 17, 2022, Proofpoint noticed new delivery attempts involving ZIP files that were custom-named to match the target's interests.



January 2022 phishing email (Proofpoint)

A change in tactic also occurred at this point, as the ZIP files weren't fetched from a cloud hosting service but instead leveraged a dropper malware executable.

The four components downloaded this way were the PlugX malware, its loader, the DLL search order hijacker (process loader), and a PDF decoy file.

Finally, on February 28, 2022, the Chinese threat actors were spotted using a compromised diplomat's address to target other top-ranking officials of NATO countries with lures involving the Russian invasion of Ukraine.

The most recent phishing lure linked to TA416 (Proofpoint)

The compromised person worked in refugee and migrant services, an area that was recently targeted by Belarusian hackers as well.

Superficial changes

While the tactics, malware drop, installation, and loading methods remain constant across campaigns, Mustang Panda puts some effort into regularly changing the components used.

"The group uses different legitimate PE files to initiate side-loading, as well as a variety of PlugX DLL loaders including the PotPlayer and DocCon versions," elaborates the Proofpoint report.

"TA416 also uses different variants of the final PlugX payload in which the communication routines are observed to be different when closely analyzed."

However, too many elements form a common ground between 2020, 2021, and 2022 campaigns, as reflected in the following table.

Common TA416 tactics throughout the years (Proofpoint)

As Proofpoint's report underlines in conclusion, these superficial variations will continue unabated, especially now that a fresh set of indicators of compromise has been published, so vigilance and good email security practices are advised to all potential targets.

- China

- Mustang Panda
- Phishing
- ta416

- Facebook
- Twitter
- LinkedIn

- Email
-

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.