SmugX: Unveiling a Chinese-Based APT Operation Targeting European Governmental Entities: Check Point Research Exposes a Shifting Trend

By matthewsu

Published: 2023-07-03 · Archived: 2026-04-05 17:31:12 UTC

Highlights:

- Check Point Research uncovers a targeted campaign carried out by a Chinese threat actor targeting foreign and domestic policies- focused government entities in Europe
- The campaign leverages HTML Smuggling, a technique in which attackers hide malicious payloads inside HTML documents
- The campaign, dubbed SmugX, overlaps with previously reported activity by Chinese APT actors RedDelta and Mustang Panda

Executive summary

In the last couple of months, Check Point Research (CPR) has been tracking the activity of a Chinese threat actor targeting foreign and domestic policy entities as well as embassies in Europe. Combined with other Chinese based group's activity previously reported by Check Point Research, this represents a larger trend within the Chinese ecosystem, pointing to a shift in target towards European entities, with a focus on their foreign policy. In this campaign, apart from the UK, most of the targeted countries are Eastern Europe countries like Czech Republic, Slovakia and Hungary, and as per our assessment, the goal of the campaign is to get ahold of sensitive information on the foreign policies of those countries.

The activity described in this report, utilizes HTML Smuggling to target foreign policy entities in Europe, focusing on Eastern Europe. HTML Smuggling is a technique in which attackers hide malicious payloads inside HTML documents.

This specific campaign has been active since at least December 2022, and is likely a direct continuation of a previously reported campaign attributed to RedDelta (and to the Mustang Panda group to some extent). The campaign uses new delivery methods to deploy (most notably – HTML Smuggling) a new variant of PlugX, an implant commonly associated with a wide variety of Chinese threat actors. Although the payload itself remains similar to the one found in older PlugX variants, its delivery methods result in low detection rates and 'successful' evasions, which until recently helped the campaign fly under the radar.
The way HTML Smuggling is utilized in the SmugX email campaign results in the download of either a JavaScript or a ZIP file. This leads to a long infection chain which results in PlugX infection of the victim.

Lures & Targets

The lure themes identified by our team are heavily focused on European domestic and foreign policies-governmental entities, and were used to target mostly governmental entities in Eastern and Central Europe. However, other western European countries were also referenced in the lures.


Smugx submissions origins

The majority of the documents contained diplomatic-related content. In more than one case, the content was directly related to China and human rights in China.

In addition, the names of the archived files themselves strongly suggest that the intended victims were diplomats and public servants in these government entities.
Here are a few examples of the names we identified:

- Draft Prague Process Action Plan_SOM_EN
- 2262_3_PrepCom_Proposal_next_meeting_26_April
- Comments FRANCE – EU-CELAC Summit – May 4
- 202305 Indicative Planning RELEX
- China jails two human rights lawyers for subversion


Smugx - Archived Files


Smugx - Archived Files

Conclusion

In this research, we analyzed a recent campaign which is highlighting the Chinese APT's shift to persistent targeting of European government entities. We identified multiple infection chains that employ the HTML Smuggling technique which leads to the deployment of the PlugX payload.

The campaign, dubbed 'SmugX', signifies a part of a larger trend we are seeing of Chinese threat actors shifting their focus to European entities, governmental ones in particular.

CPR will continue monitoring the trends and will further report accordingly.

Check Point Software Customers remain protected against the threat described in this research.

Check Point Threat Emulation and Harmony Endpoint provide comprehensive coverage of attack tactics, file-types, and operating systems and is protecting against the type of attacks and threats described in this report.

Check Point Threat Emulation:

- APT.Wins.MustangPanda.AP

Harmony End Point

- APT.Win.PlugX.O
- APT.Win.PlugX.Q
- APT.Win.PlugX.R
